NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61513

Première édition
First edition
2001-03

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

**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

.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

© 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 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

CONTENTS

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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 liasing 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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- 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
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

- 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
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

Spécification des exigences relatives aux FSE d'I&C importants pour la sûreté
à partir de la revue de conception de la sûreté de la centrale nucléaire
5.1 et 5.2

5.1 Elaboration des exigences relatives à l'I&C à partir de la conception de la sûreté de la centrale	5.2 Prescriptions relatives à la documentation
5.1.1 Exigences de fonctionnalité, de performance et d'indépendance 5.1.2 Exigences de catégorisation 5.1.3 Contraintes de la centrale	Spécification des exigences générales relatives aux FSE d'I&C importants pour la sûreté

Conception de l'architecture globale d'I&C, établissement des plans
et affectation des fonctions d'I&C aux systèmes d'I&C
5.3 à 5.5

5.3 Prescriptions relatives aux objectifs	5.4 Prescriptions relatives aux plans globaux	5.5 Prescriptions relatives à la documentation
5.3.1 Conception de l'architecture de l'I&C 5.3.2 Affectation des fonctions 5.3.3 Analyses requises	5.4.1 Programme G. d'AQ 5.4.2 Plan G. de sécurité 5.4.3 Plan d'intégration et de mise en service globales 5.4.4 Plan G. d'exploitation 5.4.5 Plan G. de maintenance	5.5.1 Conception de l'architecture 5.5.2 Affectation des fonctions

6 Réalisation des systèmes d'I&C, établissement des plans

6.1 Prescriptions relatives aux objectifs des phases du cycle de vie du système	6.2 Prescriptions relatives aux plans pour le système	6.3 Prescriptions relatives à la documentation
6.1.1 Exigences 6.1.2 Spécification 6.1.3 Conception détaillée 6.1.4 Intégration 6.1.5 Validation 6.1.6 Installation 6.1.7 Modifications	6.2.1 Plan d'AQ S. 6.2.2 Plan de sécurité S. 6.2.3 Plan d'intégration S. 6.2.4 Plan de validation S. 6.2.5 Plan d'installation S, 6.2.6 Plan d'exploitation S. 6.2.7 Plan de maintenance S.	6.3.1 Exigences 6.3.2 Spécification 6.3.3 Conception 6.3.4 Intégration 6.3.5 Validation 6.3.6 Modifications

6.4 Qualification

6.4.1, 6.4.2, 6.4.3 Prescriptions relatives à la qualification des systèmes	6.4.4 Prescriptions relatives aux documents de qualification

6.5 Résumé des principales prescriptions spécifiques

7 Intégration et mise en service globales

7.1 Prescriptions relatives aux objectifs	7.2 Prescriptions relatives à la documentation

8 Exploitation et maintenance globales

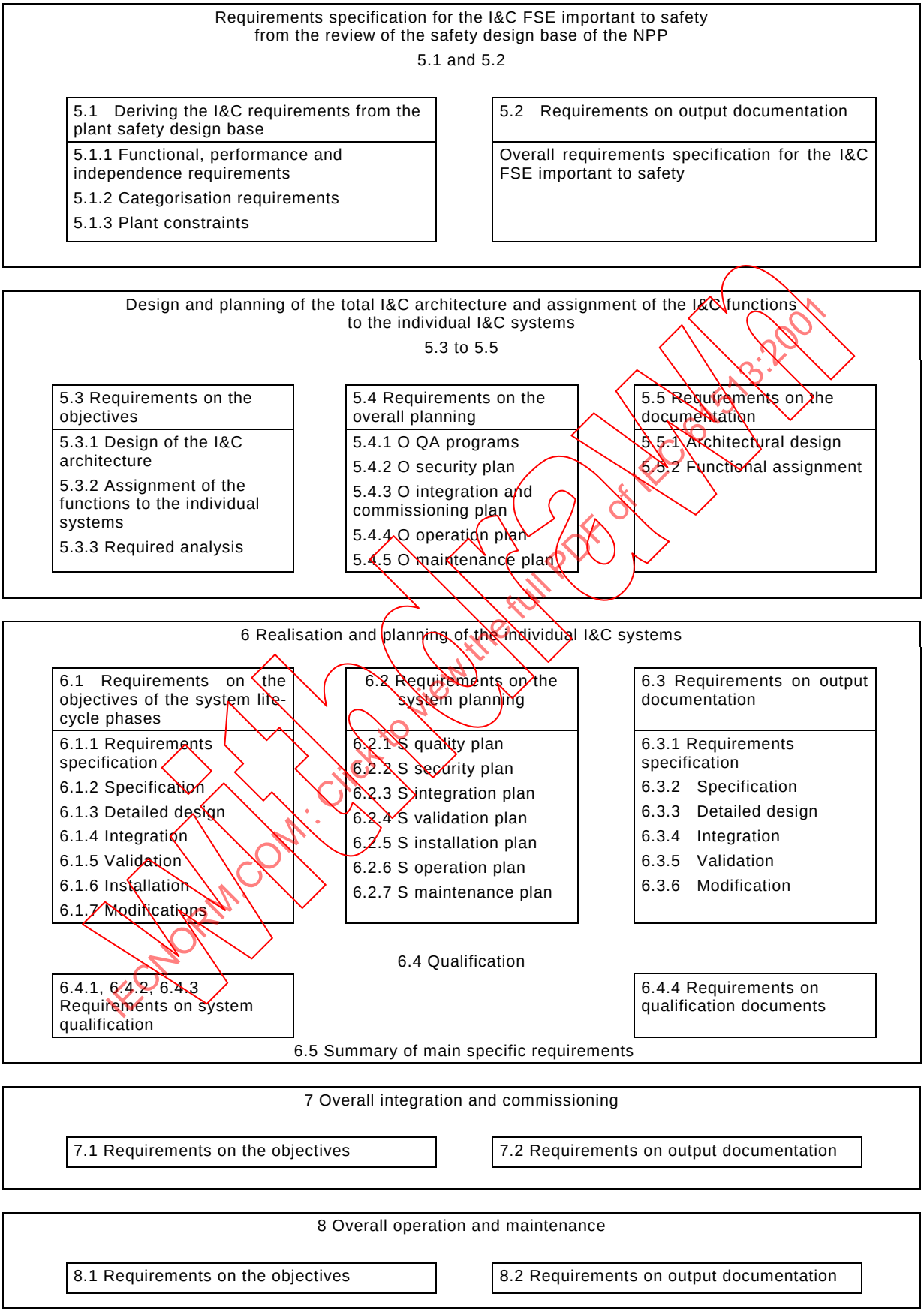
8.1 Prescriptions relatives aux objectifs	8.2 Prescriptions relatives à la documentation

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

IEC 188/01

Figure 1 – Cadre général de la présente norme

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn



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

IEC 188/01

Figure 1 – Overall framework of this standard

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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*

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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*

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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 Sûrete 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*

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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*

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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».

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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”.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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'AIEA 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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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».

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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”.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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 fonctionnalité 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:

a) 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;

b) structures, systèmes et composants qui empêchent les incidents opérationnels hypothétiques d'engendrer des situations accidentelles;

c) 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».

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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”.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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 utilisé 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».

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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”.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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».

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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".

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

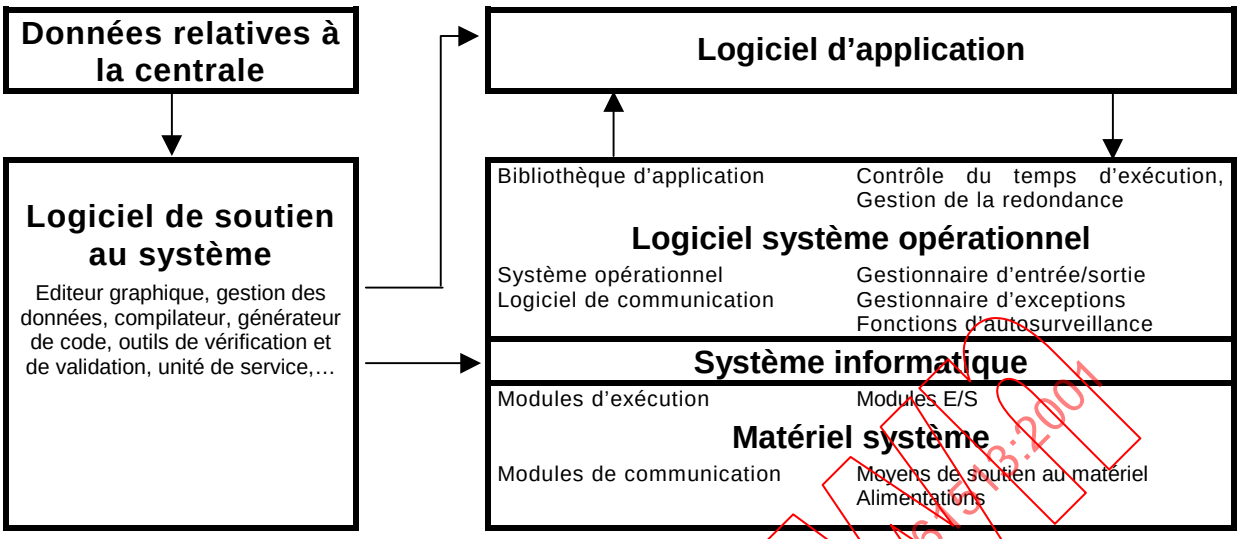


Figure 2 – Relations types entre logiciel et matériel d'un système informatique

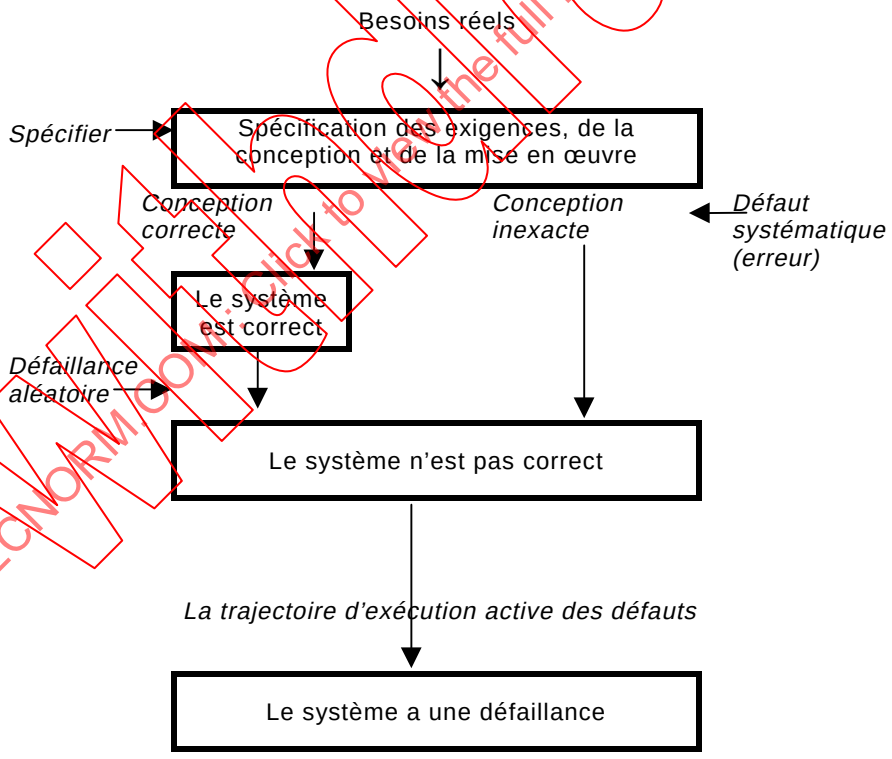


Figure 3 – Relations entre défaillance, défaillance aléatoire et défaut systématique

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

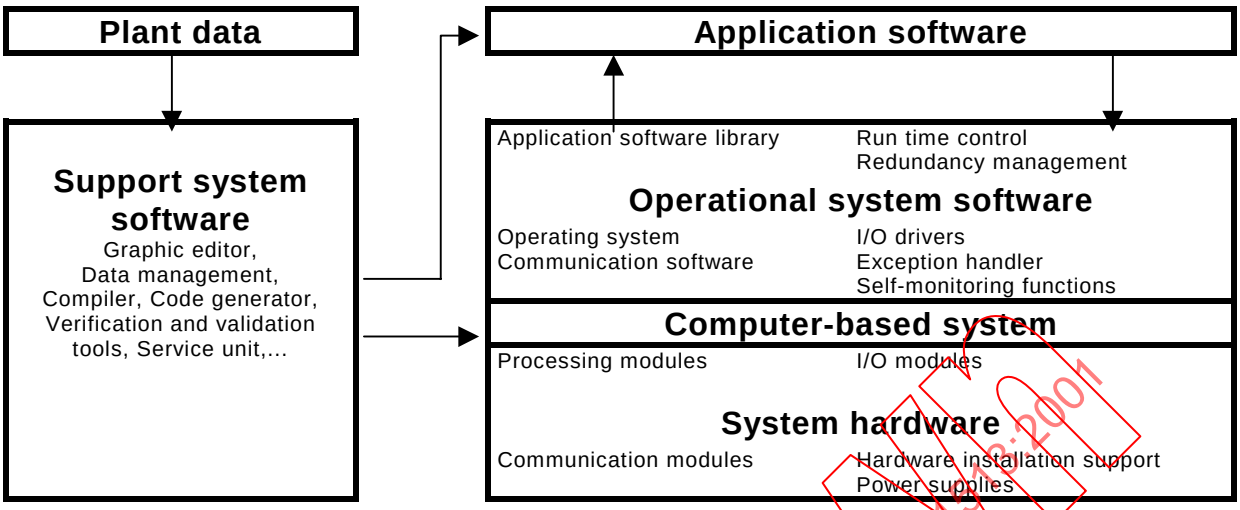


Figure 2 – Typical relations of hardware and software in a computer-based system

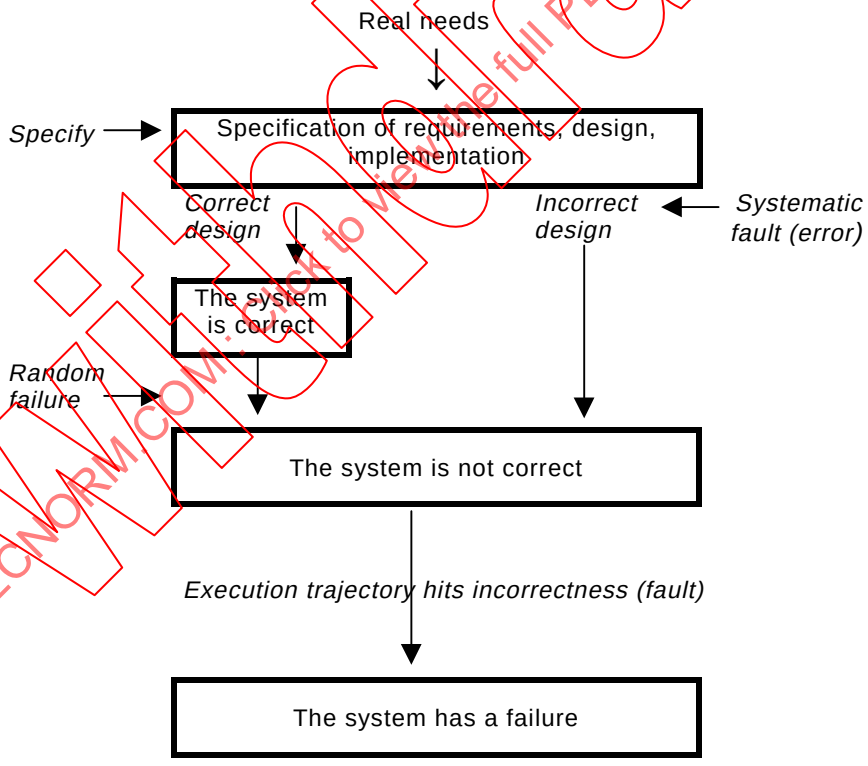


Figure 3 – Relations between system failure, random failure and systematic fault

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

4 Symboles et abréviations

DCC	Défaillance de cause commune
COTS	Composants sur étagère du commerce
EUC	Equipement 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	Evénement 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);

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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);

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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).

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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 *Elaboration des exigences relatives à l'I&C à partir de la conception de la sûreté de la centrale*				
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'aménage-ment 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 *Conception de l'architecture globale de l'I&C et affectation des fonctions d'I&C*				
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)

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

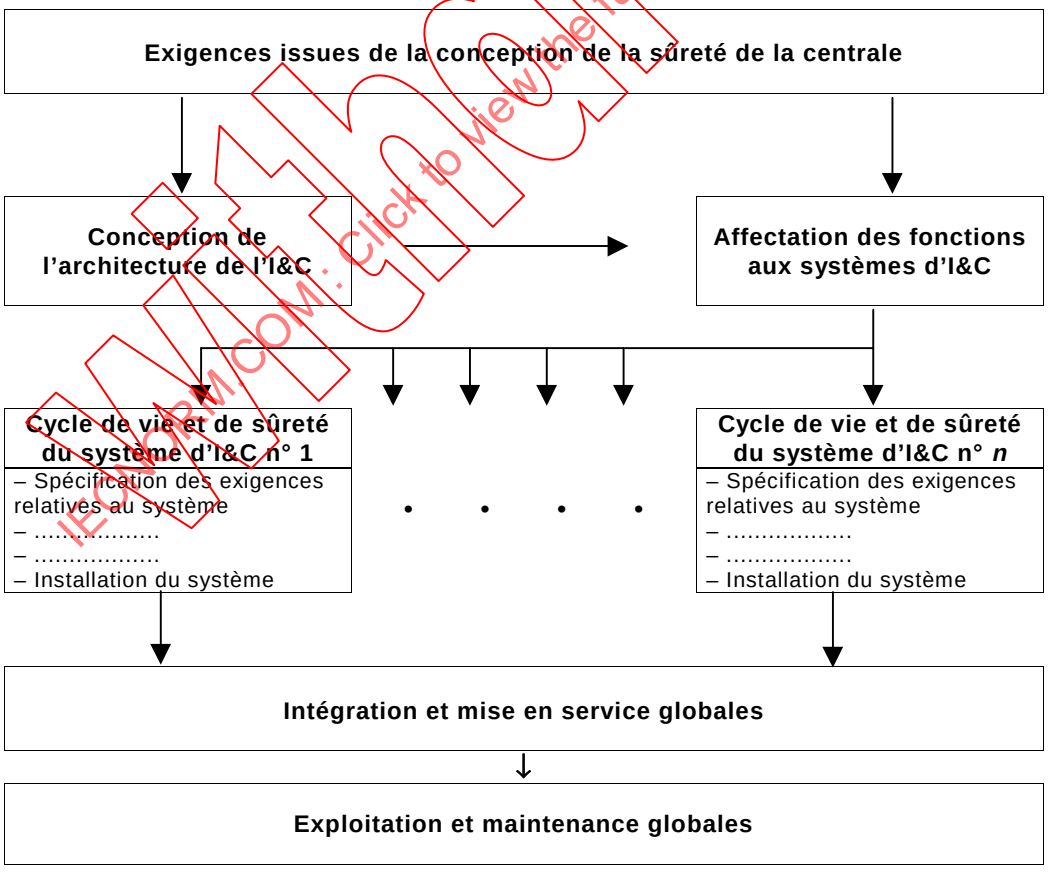
Clause or subclause	Inputs	Objectives of the activity	Scope	Outputs
5	Requirements placed upon the overall safety life cycle and its relationship to the systems' life cycles			
5.1 *Deriving the I&C requirements from the plant safety design base*				
5.1.1 Review of the functional, performance and independence 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)

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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 fonction-nement	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.				

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

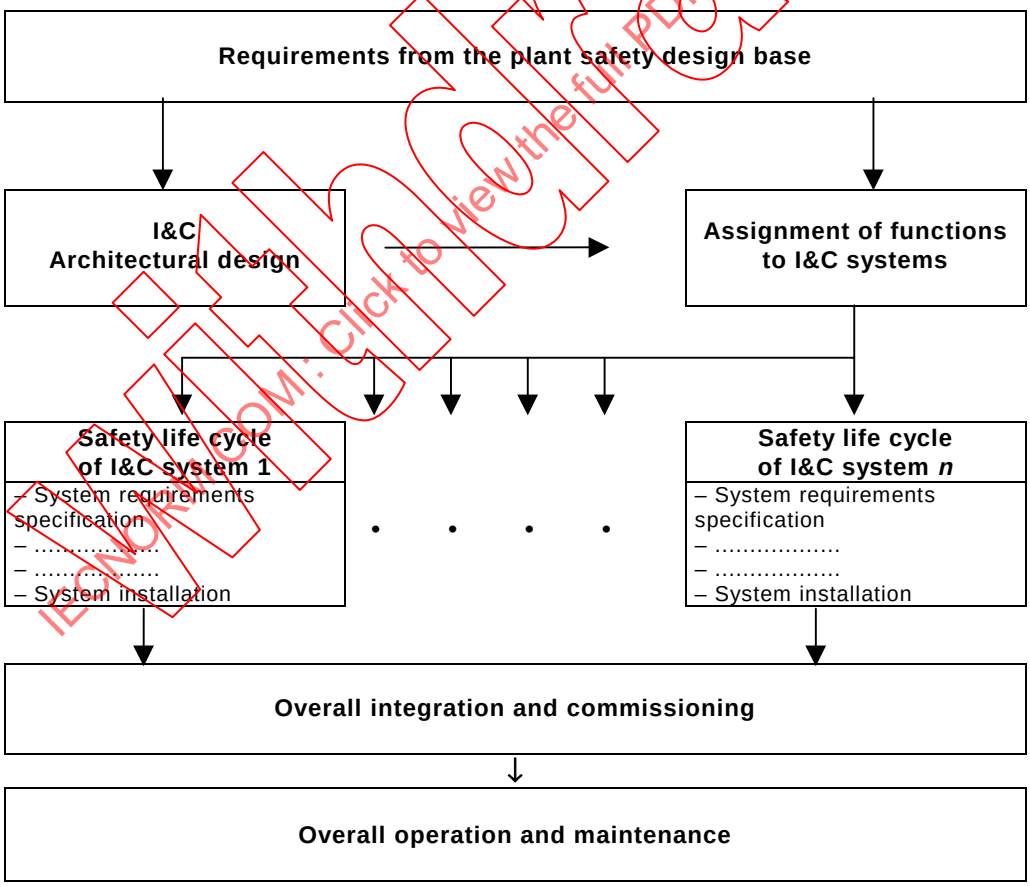


IEC 191/01

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

Table 1 *(continued)*

Clause or subclause	Inputs	Objectives of the activity	Scope	Outputs
5.4 Overall planning	Output of 5.3	To develop plans for QA, security, integration, commissioning, operation and maintenance of systems	I&C systems working co-operatively	Plans for the designated activities
6 System safety life cycle	Output of 5.5	To specify and create I&C systems conforming to the I&C architecture specification (see clause 6)	Individual I&C systems	Outputs are described in table 3
7 Overall integration and commissioning	Output of 5.4.3 and 6.2.5	To test and commission the interconnected systems of the I&C architecture	I&C systems of the I&C architecture	Fully integrated and commissioned systems Report of the overall commissioning (see 7.2)
8 Overall operation and maintenance	Output of 5.4.4, 5.4.5 and 7.1	To operate maintain and repair the systems in order that the safety is maintained	I&C systems of the I&C architecture	Continuing achievement of functions. Records of operation and maintenance (see 8.2)
NOTE For a comparison of this definition of phases with that of IEC 61508-1, see annex D.				



IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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

5.1 Elaboration des exigences relatives à l'I&C à partir de la conception de la sûreté de la centrale

L'objectif des prescriptions du présent article est d'identifier les exigences devant être prises en compte lors de la spécification des FSE d'I&C, et les contraintes d'architecture de l'I&C, à partir de la conception de la sûreté de la centrale et de son environnement.

Les documents AIEA 50-C-D Rév. 1 et AIEA 50-SG-D11 définissent un certain nombre de «principes de sûreté» qui forment une «approche intégrée et globale de la sûreté» garantissant la sûreté d'une centrale nucléaire. Ces principes seront utilisés dans la conception, en tenant compte de tous les «événements initiateurs hypothétiques» (EIH) pertinents et de toutes les barrières physiques successives, afin de maintenir l'exposition aux rayonnements des employés, du public et de l'environnement dans certaines limites (voir articles A.1, A.2 et A.3). Dans cette approche, la conception de la centrale spécifie le niveau de qualité requis pour les fonctions et systèmes de la centrale nécessaires pour le maintien de celle-ci dans un état opérationnel normal, pour garantir une réponse correcte à tous les EIH et pour faciliter la gestion à long terme de la centrale après un accident.

5.1.1 Revue des exigences de fonctionnalité, de performance et d'indépendance

Les exigences de fonctionnalité, de performance et d'indépendance relatives aux fonctions d'I&C importantes pour la sûreté ainsi que les principes d'exploitation de la centrale sont définis dans la conception de la sûreté de la centrale. Cette conception est un élément fondamental de la conception globale de l'I&C. Les exigences relatives aux interactions homme – machine prennent en compte les principes d'exploitation et des considérations ergonomiques, afin de minimiser les défaillances dues aux facteurs humains.

Les éléments suivants doivent figurer dans la conception de la centrale:

- les principes de défense en profondeur de la centrale (voir article A.3) et les groupes de sûreté prévus pour faire face aux séquences d'EIH et remplir les objectifs de sûreté (voir article A.2);

  NOTE 1 Si la fiabilité d'une fonction doit être d'un niveau très élevé, la spécification des exigences relatives à la centrale et l'I&C stipule différentes lignes de défense pour le même EIH, par exemple au moins deux critères de déclenchement indépendants et fonctionnellement différents et, si nécessaire, un second système mécanique redondant, indépendant et fonctionnellement différent, pour le contrôle des accidents.

  NOTE 2 Les échelons de défense en profondeur peuvent contenir les fonctions importantes pour la sûreté ainsi que d'autres fonctions. Les exigences de la présente norme ne concernent que les fonctions importantes pour la sûreté.

- les exigences de fonctionnalité et de performance relatives aux fonctions de la centrale importantes pour la sûreté et nécessaires pour répondre aux exigences de sûreté globale (voir article A.3);

  NOTE 3 Lorsqu'une validation fonctionnelle est requise (voir 6.1.3.1), la conception de la centrale fournit les conditions initiales, les limites admissibles et le taux admissible de variation des variables de la centrale devant être contrôlées par les systèmes d'I&C importants pour la sûreté.

- le rôle des automatismes et les actions requises de l'opérateur pour gérer les incidents opérationnels hypothétiques et les situations accidentelles (voir article A.3);
- une analyse des tâches conformément à 3.2 de la CEI 60964 définissant les fonctions qu'il convient d'affecter à l'opérateur et celles qu'il convient d'affecter aux machines;
- les variables à afficher pour l'opérateur en cas d'actions manuelles;
- les principes de priorité entre actions automatiques et manuelles, en tenant compte des catégories des fonctions et du lieu d'émission des actions manuelles.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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

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

IAEA 50-C-D Rev 1 and IAEA 50-SG-D11 define a number of individual “safety principles” that together make up an “integrated overall safety approach” ensuring the safety of a NPP. These principles will be used in the design by considering all relevant “Postulated Initiating Events” (PIEs) and successive physical barriers to keep radiation exposure to workers, public, and environment within limits (see clauses A.1, A.2 and A.3). Following this approach, the plant design base specifies an appropriate quality level for the plant functions and systems necessary to maintain the plant in a normal operating state, to ensure the correct response to all PIEs, and to facilitate the long-term management of the plant following an accident.

5.1.1 Review of the functional, performance and independence requirements

The functional, performance and independence requirements for the I&C functions important to safety and the principles of operation of the plant are defined in the plant safety design base which is an inherent element of the overall I&C design project. The requirements concerning human-machine interactions consider the principles of operation together with ergonomic considerations in order to minimise failures due to human factors.

The following inputs shall be provided in the plant safety design base:

- the defence in-depth concept of the plant (see clause A.3), and the groups of functions provided to address PIEs sequences in order to fulfil the safety objectives (see clause A.2);

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

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

- the functional and performance requirements of the functions of the plant important to safety needed to meet the general safety requirements (see clause A.3);

  NOTE 3 Where functional validation is required (see 6.1.3.1), the design base provides the initial conditions, allowable limits and allowable rate of change of the plant variables to be controlled by the I&C systems important to safety.

- the role of automation and prescribed operator actions in the management of anticipated operational occurrences and accident conditions (see clause A.3);
- a task analysis in accordance with 3.2 of IEC 60964 defining which functions should be assigned to operators and which functions should be assigned to machines;
- the variables to be displayed for the operator to use in taking manual actions;
- the priority principles between automatic and manually initiated actions, taking into account functional categories, operator rooms or locations.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

5.1.2 Revue des exigences de catégorisation

5.1.2.1 Hypothèses de la présente norme concernant la catégorisation des fonctions et la classification des systèmes

Les fonctions, systèmes et équipements de la centrale sont classés selon leur degré d'importance pour la sûreté (voir article B.1). La présente norme fait la distinction entre la catégorisation des fonctions d'I&C et la classification des systèmes d'I&C. La justification de cette double classification et les relations avec celles de l'AIEA et de la CEI 61226 sont données à l'annexe B.

NOTE Les termes «catégorisation» et «classification» sont parfois confondus. Dans un but de clarté, dans la présente norme le terme «catégorisation» est réservé aux fonctions et «classification» aux systèmes.

Une fonction d'I&C est affectée à une catégorie selon son degré d'importance pour la sûreté. Les catégories sont définies par un ensemble de prescriptions relatives à la spécification, la conception, l'intégration, la vérification et la validation de la fonction d'I&C, ainsi que par des prescriptions sur la classe minimale requise pour les systèmes et équipements associés nécessaires à la réalisation des fonctions. Des prescriptions cohérentes s'appliquent à l'ensemble des éléments nécessaires à la réalisation de la fonction, indépendamment de sa répartition dans un réseau de systèmes d'I&C interconnectés (voir article A1 de l'AIEA 50-SG-D1).

Un système ou équipement d'I&C est affecté à une classe selon son degré d'importance pour la sûreté. Les classes sont définies par un ensemble d'exigences sur les propriétés et la qualification du système. La satisfaction à ces exigences rend le système classé apte à supporter une ou plusieurs fonctions d'I&C jusqu'à une certaine catégorie. Les exigences concernent les fonctions d'application, les fonctions de service et les fonctions du logiciel système.

Le processus de catégorisation des fonctions d'I&C fait partie de la conception de la sûreté de la centrale et sort du cadre de la présente norme (voir article B.2). La présente norme suppose que la conception de la sûreté de la centrale a réparti les fonctions d'I&C importantes pour la sûreté en trois catégories, A, B ou C et que les principales exigences de conception pour les systèmes et équipements associés à ces catégories sont conformes à celles de l'article 8 de la CEI 61226. De plus, les exigences relatives à la catégorie A sont conformes à celles requises par l'AIEA pour les systèmes de sûreté.

NOTE Les références normatives de catégorisation peuvent varier selon les pays. Pour cette raison, une catégorisation unique des fonctions d'I&C ne peut être attendue lors de l'application de la présente norme, qui s'adresse aussi bien aux nouvelles centrales qu'à celles déjà existantes. Dans ces cas, une analyse spécifique de la catégorisation des fonctions d'I&C rencontrées est nécessaire afin de parvenir à une correspondance entre les catégories des fonctions d'I&C et les exigences relatives aux systèmes et composants associés.

La classification des systèmes d'I&C est définie par l'organisation en charge du projet de l'I&C pendant la phase de conception de l'architecture d'I&C, avant l'affectation des fonctions d'I&C aux systèmes (voir 5.3.1 et 5.3.2).

5.1.2.2 Exigences

a) La catégorisation des fonctions d'I&C doit être indiquée dans la conception de la sûreté de la centrale et doit servir de référence pour la spécification des exigences relatives aux FSE d'I&C (voir 5.2).

b) L'organisation en charge du projet d'I&C doit effectuer une revue de la catégorisation des fonctions d'I&C et vérifier qu'elle est exhaustive et réalisable. En cas de non-faisabilité (par exemple affectation de la catégorie maximale à une fonction trop complexe), des itérations des fonctions de la centrale et des fonctions d'I&C doivent être effectuées jusqu'à l'atteinte d'une solution réalisable.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

5.1.2 Review of the categorisation requirements

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

Functions, systems, and equipment in the NPPs are classified according to their importance to safety (see clause B.1). This standard distinguishes between categorisation of I&C functions and classification of I&C systems. The rationale for this double gradation scheme and the relations with the IAEA and IEC 61226 classification concepts are explained in annex B.

NOTE The terms "categorisation" and "classification" are used sometimes as synonym. For the purpose of clarity in this standard, the term "categorisation" is reserved for the functions and the term "classification" for the systems.

The categorisation process places each I&C function into a category according to its importance to safety. These categories are characterised by sets of requirements on the specification, design, implementation, verification, and validation of the I&C function, as well as by requirement on the minimal required class for the associated systems and equipment necessary for the implementation of the functions. Consistent requirements apply to the whole chain of items which are necessary to implement this function regardless of how it is distributed in a number of interconnected I&C systems (see clause A1 of IAEA 50-SG-D1).

The classification process places I&C systems and equipment into classes according to their importance to safety. These classes are characterised by sets of requirements on the properties of the system and its qualification. Fulfilment of these requirements makes the classified system suitable to implement one or more I&C functions up to a defined category. The requirements address the application functions, the service functions, and the system software functions of the system as appropriate.

The categorisation process of the I&C functions is part of the plant safety design base and is outside the scope of this standard (see clause B.2). This standard assumes that the plant safety design base has assigned the individual I&C functions important to safety into one of three categories A, B or C and that the main design requirements for the systems and equipment associated with these categories are consistent with those of clause 8 of IEC 61226. Furthermore, the requirements for category A are consistent with the requirements for safety systems of the IAEA.

NOTE The normative references for categorisation may vary between countries. For this reason, a unique input categorisation of I&C functions cannot be expected when applying this standard, which addresses both new and pre-existing plants. In such cases, a specific analysis of the input categorisation is needed to provide the correspondence between categories of I&C functions and requirements for the associated systems and equipment.

The classification of the I&C systems is defined by the I&C project organisation in the design phase of the I&C architecture before the functional assignment of the I&C functions to the systems (see 5.3.1 and 5.3.2).

5.1.2.2 Requirements

a) The categorisation of the I&C functions shall be provided in the plant safety design base and shall constitute a reference input to the overall I&C FSE requirements specification (see 5.2).

b) The I&C project organisation shall review the categorisation and verify it for completeness and feasibility. In the case of non-feasibility (for example, assignment of the highest category to too complex a function), iterations of the plant and I&C functions review shall be performed until a feasible solution is achieved.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

5.1.3 Revue des contraintes de la centrale

La conception de l'architecture de l'I&C (voir 5.3) est soumise à des contraintes imposées par la nature de la centrale.

a) L'organisation en charge du projet d'I&C doit identifier les contraintes imposées aux équipements d'I&C par l'aménagement de la centrale, les interfaces avec les équipements de la centrale et les événements externes à l'I&C, en particulier

- les limites entre les systèmes et équipements d'I&C d'une part et les systèmes de la centrale d'autre part, y compris les interfaces avec les systèmes de mise en marche électriques/mécaniques et les alimentations électriques;
- les plages d'évolution des régimes transitoires et permanents des paramètres environnementaux, dans les situations normales, anormales et accidentelles de fonctionnement des systèmes d'I&C;
- les plages d'évolution des régimes transitoires et permanents des alimentations de puissance et de commande, dans les situations normales, anormales et accidentelles de fonctionnement des systèmes d'I&C;
- les contraintes générales sur l'installation et le cheminement des câbles;
- les contraintes spécifiques sur l'installation et le cheminement des câbles pour les points de convergence, tels que la salle de commande et les salles de regroupement de câbles;
- les contraintes sur la mise à la terre et sur la distribution de l'alimentation électrique;
- les événements dangereux internes et externes à prendre en considération en fonction des hypothèses prises au niveau de la centrale. Ceux-ci incluent les incendies, les inondations, le gel, la foudre, la surtension ou l'interférence électromagnétique, les tremblements de terre, les explosions ou les effets chimiques.

b) L'organisation en charge du projet d'I&C doit identifier les contraintes relatives aux équipements d'I&C issues des principes d'exploitation, c'est-à-dire les contraintes

- de sécurité;
- d'exploitation et de maintenance (voir 2.6 de CEI 60964);
- de maintien en conditions opérationnelles des systèmes d'I&C.

5.2 Documentation

Les documents produits par l'activité décrite en 5.1 sont les exigences globales de chaque FSE d'I&C important pour la sûreté.

NOTE 1 Les exigences globales couvrent la fonction d'I&C dans sa totalité, c'est-à-dire depuis les entrées (capteurs, opérateurs et autres équipements) jusqu'aux sorties (dirigées vers les actionneurs, opérateurs ou autres équipements). Une répartition plus fine de ces exigences permettra de spécifier les exigences relatives aux sous-fonctions associées aux systèmes individuels d'I&C. Cela dépendra de l'architecture de l'I&C choisie (voir 5.3) et de la manière dont les fonctions sont réparties sur les équipements (instrumentation, automates et actionneurs).

a) Une spécification des exigences globales doit être établie pour chaque FSE d'I&C. Elle doit contenir

1) une spécification des exigences de fonctionnalité définissant la manière dont la fonction transforme les informations d'entrée en informations de sortie afin d'exploiter et de surveiller la centrale;
2) une spécification des exigences de performance définissant le domaine de valeur, la précision et la performance dynamique de la fonction;

NOTE 2 Cela comprend les exigences relatives au comportement temporel qui peuvent avoir été omises dans le passé pour les systèmes traditionnels câblés.

3) la spécification de la catégorie de la fonction.

NOTE 3 La catégorie de la fonction définit implicitement la classification minimale des systèmes d'I&C réalisant la fonction (voir tableau 2).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

5.1.3 Review of plant constraints

The I&C architectural design (see 5.3) is subject to constraints imposed from the plant context.

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

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

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

- security;
- operation and maintenance (see 2.6 of IEC 60964);
- "in-service maintenance" of the I&C systems.

5.2 Output documentation

The output documents of the activity described in 5.1 are the overall requirements specifications for the individual I&C FSE important to safety.

NOTE 1 The overall requirements specifications encompass the whole of the I&C function from its inputs (sensors, operators, other equipment) to its outputs (directed to actuators, operators or other equipment). Further splitting of these requirements specifications will provide the requirements specifications of the subfunctions at the level of the individual I&C systems. This will depend upon the selected I&C architecture (see 5.3) and how the functions are implemented through distributed equipment (instrumentation, processing and actuators).

a) An overall requirements specification shall be established for each I&C FSE. It shall include

1) a functionality requirements specification defining the way the function transforms input information to output information in order to operate or monitor the plant;

2) a performance requirements specification defining the range, accuracy, and dynamic performance of the function;

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

3) specification of the category of the function.

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

b) La spécification des exigences globales doit définir toutes les contraintes relatives à l'affectation des fonctions aux systèmes d'I&C. Cela inclut

   1) les associations de fonctions à surveiller pour commander les mesures de protection;

   2) les associations de fonctions assurant la défense en profondeur;

   3) l'association de fonctions qui constituent un groupe de sûreté.

c) Les spécifications des exigences globales relatives à tous les FSE d'I&C doivent être vérifiées afin de permettre l'affectation des fonctions aux systèmes et l'élaboration des spécifications de ces systèmes (voir 6.1).

5.3 Conception de l'architecture globale de l'I&C et affectation des fonctions d'I&C

Le présent paragraphe décrit la manière dont

- les contraintes de 5.1.3 et les exigences de 5.2 s'appliquent à la conception de l'architecture d'ensemble des systèmes d'I&C importants pour la sûreté (en abrégé architecture de l'I&C);
- les fonctions d'I&C sont affectées aux systèmes individuels d'I&C.

5.3.1 Conception de l'architecture de l'I&C

La conception de l'architecture de l'I&C fournit une description de haut niveau des systèmes d'I&C de la centrale nucléaire (voir article B.4), de la communication entre ces systèmes et des outils nécessaires pour assurer une interface convenable entre ces systèmes.

5.3.1.1 Prescriptions générales

a) La conception de l'architecture de l'I&C doit englober la totalité de l'I&C nécessaire à l'intégration des fonctions d'I&C importantes pour la sûreté spécifiées en 5.2.

b) La conception de l'architecture de l'I&C doit décomposer la totalité de l'I&C en systèmes et composants suffisants pour garantir le respect des exigences relatives

   - à l'indépendance des fonctions des différentes lignes de défense;
   - à la séparation appropriée des systèmes de classes différentes;
   - au respect des contraintes sur la séparation physique et l'isolation électrique résultant des contraintes de l'environnement et de l'implantation dans la centrale, de l'analyse des risques et de la maintenance pendant l'exploitation (voir 5.1.3).

c) La conception de l'architecture de l'I&C doit garantir que le critère de défaillance unique est vérifié pour les fonctions de catégorie A, dans toutes les configurations possibles des systèmes et de la centrale (voir 7.5 de l'AIEA 50-SG-D3).

d) Chaque système d'I&C doit être classé en fonction de sa capacité à réaliser des fonctions d'I&C jusqu'à une certaine catégorie.

Tableau 2 – Corrélation entre les classes des systèmes d'I&C et les catégories des FSE d'I&C

Catégories de fonctions d'I&C importantes pour la sûreté			Classes correspondantes des systèmes d'I&C importants pour la sûreté
A	(B)	(C)	1
	B	(C)	2
		C	3
NOTE Les fonctions d'I&C de catégorie A peuvent être supportées par des systèmes de classe 1 uniquement, les fonctions de catégorie B par des systèmes de classe 1 et 2, et les fonctions de catégorie C par des systèmes de classe 1, 2 et 3.			

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

b) The overall requirements specification shall define any dependency between functions which generate constraints on the assignment of functions to the I&C systems. This includes

   1) the combinations of functions to be monitored to control protective actions;

   2) the combination of functions ensuring defence in depth;

   3) the combination of functions which constitute a safety group.

c) The overall requirements specifications of all the I&C FSEs shall be verified to ensure that functions and constraints are defined for the purpose of assignment of functions to systems and the production of the specification of those systems (see 6.1).

5.3 Design of the total I&C architecture and assignment of the I&C functions

This subclause describes how the

- constraints from 5.1.3 and requirements from 5.2 apply to the design of the total architecture of the I&C systems important to safety (short "I&C architecture");
- I&C functions are assigned to the individual I&C systems.

5.3.1 Design of the I&C architecture

The design of the I&C architecture provides a top-level definition of the I&C systems of the NPP (see clause B.4), of the communication between these systems, and of the tools necessary to ensure a consistent interface between these systems.

5.3.1.1 General requirements

a) The design of the I&C architecture shall encompass the entire I&C necessary to implement the I&C functions important to safety specified in 5.2.

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

   - independence of the functions in different lines of defence;
   - adequate separation of the systems of different classes;
   - fulfilment of the constraints on the physical separation and electrical isolation arising from the environmental and layout constraints, hazard analysis, and maintenance during operation (see 5.1.3).

c) The design of the I&C architecture shall provide sufficient systems and sub-systems so that the single failure criterion is met for category A functions, for all permitted configurations of the systems and the plant (see 7.5 of IAEA 50-SG-D3).

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

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

Categories of I&C functions important to safety			Corresponding classes of I&C systems important to safety
A	(B)	(C)	1
	B	(C)	2
		C	3
NOTE I&C functions of category A may be implemented in class 1 systems only, I&C functions of category B may be implemented in class 1 and 2 systems, I&C functions of category C may be implemented in class 1, 2, and 3 systems.			

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

e) Les interfaces avec la centrale et les interconnexions entre les systèmes d'I&C doivent être définies dans le cadre de la conception de l'architecture afin d'identifier

- le partage de signaux (de mesure) par différentes fonctions importantes pour la sûreté;
- le vote entre des signaux de commande provenant de différents systèmes, et les priorités entre ces signaux;
- les chemins communs et les équipements communs aux signaux de commande automatiques ou manuels agissant dans différentes lignes de défense.

f) La description des systèmes, équipements et de leurs interconnexions dans la conception de l'architecture de l'I&C doit être suffisamment détaillée pour permettre l'analyse de sûreté de l'I&C.

5.3.1.2 Interfaces homme–machine

a) La conception de l'architecture de l'I&C doit structurer les systèmes d'IHM des diverses zones de commande et de surveillance de la centrale, en particulier la salle de commande principale, les salles de commande annexes, le panneau d'arrêt à distance (voir CEI 60965), les panneaux de commande locale et le centre de crise, avec le degré de redondance nécessaire pour être en accord avec les contraintes d'exploitation et de maintenance de la centrale (voir 5.1.3).

b) La conception de l'architecture de l'I&C doit répondre aux principes d'exploitation de la centrale définis dans la conception de la centrale (voir 5.1.1), en particulier

- les principes de priorité entre les signaux automatiques et les signaux de commande manuels;
- les principes de priorité entre les différents systèmes d'IHM pendant l'exploitation normale, accidentelle et post-accidentelle;
- les principes de priorité entre les systèmes d'IHM normaux et de secours;
- les principes relatifs aux conditions de basculement entre les moyens d'IHM normaux et de secours.

c) La conception de l'architecture doit définir la manière dont les défauts ou défaillances détectées par les outils de diagnostic des systèmes sont signalés à l'opérateur de la centrale. La forme de la présentation doit être telle que l'opérateur puisse:

- immédiatement reconnaître la signalisation d'une défaillance et la distinguer des autres signalisations opérationnelles;
- décider de l'opportunité de réagir manuellement afin de restaurer l'état sûr de la centrale;
- désigner les systèmes concernés au personnel d'entretien concerné.

d) Il doit être démontré que la conception de l'architecture de l'I&C s'accorde avec les principales décisions concernant la technologie des systèmes d'IHM (notamment informatisée ou traditionnelle). Il convient que des systèmes plus complexes soient utilisés pour la présentation des informations aux opérateurs de la centrale si cela permet de réduire la contribution des facteurs humains aux défaillances à la demande et si ces effets peuvent être réduits par une amélioration des informations. Il convient que le potentiel de DCC d'un système d'information de technologie informatique soit vu en fonction du potentiel de défaillances dû aux facteurs humains.

e) La conception de l'architecture de l'I&C doit

- affecter les fonctions à un contrôle automatique ou humain, en accord avec l'analyse des tâches établie lors de la conception de la centrale (voir 5.1.1);
- déterminer les capacités de traitement des systèmes d'I&C requises par le traitement des informations et nécessaires à l'accomplissement des tâches requises par les interactions avec l'opérateur (voir 3.2.2 de la CEI 60964);

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

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

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

5.3.1.2 Human machine interfaces

a) The design of the I&C architecture shall structure the HMI systems of the different plant control and monitoring areas including the main control room, supplementary control rooms, remote shutdown panel (see IEC 60965), local control panels and emergency control centre, with the degree of redundancy necessary to accommodate the constraints from the plant operation and maintenance (see 5.1.3).

b) The design of the I&C architecture shall comply with the principles for plant operation established in the plant design base (see 5.1.1) including

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

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

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

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

e) The design of the I&C architecture shall

- assign the functions to human control or to automatic control in accordance with the plant design base task analysis (see 5.1.1);
- determine I&C system processing capability necessary to process the information and capability to complete the tasks defined for operator interaction (see 3.2.2 of IEC 60964);

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

- assurer que les informations et le temps dont dispose l'opérateur pour une action manuelle s'accordent avec les exigences de conception de la centrale (voir 5.1.1).

f) Les techniques relatives aux facteurs humains basées sur la CEI 60964 et la CEI 60965 doivent être utilisées pour garantir l'efficacité des IHM dans la conception de la salle de commande principale et des autres zones de commande de la centrale.

g) Pour l'analyse des tâches de l'opérateur et l'optimisation des exigences relatives aux IHM, les tâches importantes et non importantes pour la sûreté doivent être prises en compte.

5.3.1.3 Communication de données

Les communications de données entre les systèmes constituant l'architecture de l'I&C incluent toutes les liaisons prévues pour transmettre un ou plusieurs signaux ou messages via un ou plusieurs chemins et utilisant différentes techniques de multiplexage.

a) Les communications doivent être capables de satisfaire aux spécifications des exigences globales de performance (voir 5.2) dans toutes les conditions d'exploitation de la centrale.

b) L'architecture et la technologie des communications doivent assurer que les exigences relatives à l'indépendance entre les systèmes sont remplies. En plus de la séparation physique et de l'isolation électrique, il convient que la conception contienne des dispositions pour garantir que des problèmes de communication ne perturbent pas les modules de traitement.

c) Les communications doivent contenir des dispositions pour vérifier le fonctionnement des composants de communication et l'intégrité des données transmises.

d) Il convient qu'une redondance des communications soit prévue afin de pallier aux défaillances.

e) Les communications doivent être conçues de telle manière que le fonctionnement et la communication de données par des fonctions appartenant à la plus haute catégorie de sûreté ne soient pas perturbées par la communication de données avec des fonctions de classes inférieures. Par exemple, les essais en fonctionnement ne doivent pas perturber la fonction de la catégorie la plus élevée.

5.3.1.4 Outils

a) La conception de l'architecture de l'I&C doit contenir la définition des outils, généralement informatiques (voir 4.2 de la CEI 60880-2), à utiliser pour assurer la compatibilité des données échangées entre les systèmes d'I&C travaillant ensemble et pour assurer la compatibilité des données avec la base de données de la centrale.

NOTE Les outils spécifiques aux systèmes individuels sont définis pendant la phase de spécification du système (voir 6.1.2.1).

b) Il convient que des outils soient utilisés dans toutes les phases du cycle de vie et de sûreté global lorsqu'ils permettent l'amélioration de l'assurance qualité et de la fiabilité des fonctions importantes pour la sûreté, notamment

- pour aider à la conception des interfaces entre les systèmes d'I&C;
- pour aider à l'intégration et à la mise en service globales des fonctions réparties.

5.3.1.5 Défense contre les DCC

L'un des objectifs de l'architecture de l'I&C est de prévoir des mesures contre l'apparition d'une DCC au sein de systèmes d'I&C réalisant différentes lignes de défense contre le même EIH (voir 5.1.1). Ces mesures incluent

- des dispositions de conception pour tolérer les événements dangereux de la centrale. Les événements dangereux internes et externes (voir 5.1.3) qui ne sont pas isolés dans une partie restreinte de l'architecture de l'I&C peuvent conduire à une DCC;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- ensure that information and time available to the operator for manual control action is consistent with the requirements of the plant design base (see 5.1.1).

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

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

5.3.1.3 Data communication

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

a) Communication links shall be capable of meeting the overall performance requirements specifications (see 5.2) under all plant demand conditions.

b) Communication links architecture and technology shall ensure that the independence requirements between systems are met. In addition to physical separation and electrical isolation, the design should include provisions to ensure that problems with communication links do not impair processing modules.

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

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

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

5.3.1.4 Tools

a) The I&C architectural design shall include the definition of the tools, usually computer based (see 4.2 of IEC 60880-2), that are to be used to assure consistency of data exchanged between I&C systems working co-operatively and to ensure consistency of data with the plant data base.

NOTE Tools specific to the individual systems are defined in the system specification phase (see 6.1.2.1).

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

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

5.3.1.5 Defence against CCF

A design goal for the I&C architecture is to provide measures against the occurrence of a CCF within I&C systems implementing different lines of defence against the same PIE (see 5.1.1). These measures include

- design provisions to tolerate plant hazardous events. Internal and external hazards (see 5.1.3) which are not confined to a restricted part of the I&C architecture may lead to CCF;

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

- des dispositions de conception contre les défaillances provoquées par des modifications de l'utilisation de la centrale. La charge de certains composants matériels tels que les amplificateurs de puissance et les relais, ou la charge de certains composants logiciels tels que ceux relatifs à l'acquisition des informations d'entrée, à la communication de données et au changement de mode opérationnel peut dépendre d'événements se produisant dans la centrale;
- des dispositions de conception pour minimiser, dans l'architecture d'I&C et dans l'IHM, l'utilisation de ressources communes par différentes lignes de défense. De telles ressources communes pourraient par exemple être un signal de mesure unique ou un traitement en commun de différentes actions de commande;
- des dispositions pour minimiser le risque dû à des défauts systématiques. Avec tout système d'I&C, il existe un risque d'erreurs de conception ou de réalisation. Par conséquent, la possibilité qu'un défaut logiciel provoque une défaillance ne peut être exclue de l'analyse des défauts d'un système. Lorsque le même module logiciel est utilisé dans des conditions similaires dans différents systèmes informatiques, il existe un risque de DCC dû à des défauts logiciels;
- l'utilisation de moyens diversifiés. La diversité offre plusieurs manières différentes de détecter et de répondre à un événement significatif afin d'accroître la défense contre les DCC. Elle inclut la diversité humaine, la diversité des signaux (utilisation de paramètres différents pour initier une action protectrice), la diversité fonctionnelle, la diversité de conception et d'essais, la diversité logicielle et la diversité d'équipements;
- des décisions stratégiques appropriées pour limiter la complexité. L'emploi d'ordinateurs permet d'utiliser des algorithmes et des processus plus complexes que pour des systèmes non informatiques. Pour les exigences plus complexes, la possibilité d'erreurs et d'omissions dans la spécification des exigences et d'erreurs dans la conception et la réalisation est intrinsèquement plus importante que pour les exigences plus simples.

5.3.1.5.1 Tolérance aux événements dangereux internes et externes pouvant engendrer une DCC

Des mesures doivent être prises afin d'assurer que les groupes de sûreté peuvent exécuter les fonctions de catégorie A qu'il est nécessaire de maintenir en réponse aux événements dangereux internes et externes. Ces mesures incluent

- la séparation, c'est-à-dire par exemple la localisation des parties redondantes d'un système dans des salles différentes;
- l'indépendance, par exemple des systèmes de chauffage, ventilation et climatisation (CVC) et des alimentations électriques des voies de communication et des systèmes;
- la prévention, par exemple contre les incendies, la contamination chimique et les vibrations;
- la conception, avec par exemple des équipements conformes aux normes appropriées de la CEI relatives aux interférences électromagnétiques;
- la qualification environnementale, par exemple sismique (voir 6.4).

5.3.1.5.2 Défense contre les DCC dues à une modification de l'utilisation de la centrale

a) Les composants des systèmes de CC assurant des fonctions de catégorie A et dont la charge dépend de la demande doivent être identifiés. Il convient que les modes et séquences de défaillance possibles (y compris leurs effets sur les composants dont la charge ne dépend pas de l'utilisation de la centrale) soient évalués en fonction des causes et effets possibles des DCC.

b) Il convient que le risque de DCC pour des systèmes de classe 1 soit minimisé en prévoyant des systèmes d'I&C et de soutien fonctionnant de la même manière avant, pendant ou après une modification de l'utilisation de la centrale, c'est-à-dire dont le fonctionnement est conçu pour être indépendant du profil d'utilisation.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- design provisions against failures that might be triggered by changes in plant demand. The loading of some hardware components, e.g. power amplifiers and relays, or the loading of software components, e.g. those handling input acquisition, data communication, and switching of operational modes, may be dependent on events occurring in the plant;
- design provisions to minimise the use of common resources in the I&C architecture and HMI of different lines of defence. Such common resources might include use of a unique measurement signal or common processing between different control actions;
- provisions to minimise risk due to systematic faults. With any I&C system, there is a risk of design errors or implementation faults being present. So the possibility of a software fault causing a failure cannot be excluded from any system fault analysis. When the same software modules are used in similar conditions in different CB systems, there is a risk of CCF due to such software faults;
- use of diverse features. Diversity provides several different ways of detecting and responding to a significant event in order to increase defence against CCF. Types of diversity include human diversity, signal diversity (use of different sensed parameters to initiate protective action), functional diversity, design and test diversity, software diversity, and equipment diversity;
- appropriate strategic decisions to limit complexity. The use of computers enables more complex algorithms and processes to be used than is possible with hardware. With the more complex requirements, the possibility of errors and omissions in the requirements specification and errors in the design and implementation is inherently greater than for simple requirements.

5.3.1.5.1 Tolerance to internal and external hazards which can lead to a CCF

Measures shall be taken to ensure that the safety groups can still perform the category A functions that are required to be maintained in response to internal and external hazards. These measures include

- separation, e.g. locating redundant parts of a system in different rooms;
- independence, e.g. of heating, ventilation and air conditioning (HVAC) systems, and of the power sources for the channels and systems;
- prevention e.g. of fire, chemical contamination, and vibration;
- design, e.g. of the equipment to comply with the appropriate IEC electromagnetic interference standards;
- environmental qualification, e.g. against seismic event (see 6.4).

5.3.1.5.2 Defence against CCF due to a change of plant demand

a) The components of the I&C systems performing category A functions whose loading is demand dependent shall be identified. The possible failure modes and the failure sequences (inclusive of their effects on the components whose loading is independent of demand) should be assessed with regard to possible sources and effects of CCF.

b) The risk of CCFs in class 1 systems should be minimised by providing I&C systems and support systems that operate in the same way before, during, or after a change in plant demand, i.e. operation designed to be independent of the demand profile.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

5.3.1.5.3 Défense par la conception de l'architecture de l'I&C et de l'IHM

a) Il convient que des systèmes ou sous-systèmes indépendants soient prévus pour les différentes lignes de défense d'un même EIH (voir la note 1 de 5.1.1). Si des ressources communes sont utilisées, elles doivent être conformes à l'objectif de fiabilité du groupe de sûreté.

b) Il convient que des moyens indépendants soient affectés à la surveillance et au fonctionnement des systèmes et fonctions de la centrale importants pour la sûreté, afin que suffisamment d'informations demeurent disponibles pour l'exploitation sûre de la centrale suite à une défaillance, par exemple d'une liaison de données multiplexée ou d'un ordinateur.

c) Lorsque des actions de commande manuelles sont utilisées comme secours à des commandes automatiques concernant des fonctions de catégorie A ou B, il convient que les possibilités de DCC entre ces actions soient minimisées.

d) Lorsqu'une fonction de catégorie A peut provoquer l'activation d'un système de sauvegarde et qu'une autre fonction de catégorie A fonctionnant dans des circonstances différentes peut provoquer une activation contraire, une analyse doit être effectuée afin de déterminer l'action à mener en cas de défaillance des systèmes d'I&C.

5.3.1.5.4 Défense contre les DCC provenant de défauts systématiques

a) L'application de plans de développement et de fabrication de haute qualité pour les différents systèmes d'I&C d'un groupe de sûreté devrait limiter la présence de défauts et rendre une DCC improbable. La présente norme contient des dispositions qui doivent être utilisées pour adapter la qualité des systèmes d'I&C à leurs classes respectives.

b) Il convient que les défaillances systématiques soient détectées par des autosurveillances (gestion des exceptions, chiens de garde, contrôle de plausibilité), que la détection d'une défaillance mette le(s) système(s) affecté(s) dans un état prédéfini, de préférence sûr, et que les défaillances soient signalées à l'opérateur.

c) Si la fiabilité requise pour la mise en position sûre d'une fonction de sûreté est supérieure à celle prédite par l'évaluation du système, alors la conception doit être modifiée.

NOTE 1 Le degré de défense requis contre les défaillances dépend de la catégorie des fonctions à exécuter.

NOTE 2 Le présent paragraphe a pour objet de donner une vue d'ensemble. Le détail des exigences relatives aux défenses contre les DCC provenant d'erreurs de logiciels concernant des fonctions de catégorie A figure en 4.1 de la CEI 60880-2.

5.3.1.5.5 Défense par l'utilisation de moyens diversifiés

a) Il convient que la conception de l'architecture de l'I&C utilise le principe de la diversité lorsqu'une fiabilité élevée est requise pour un groupe de sûreté, notamment lorsqu'il existe des incertitudes sur l'évaluation de la conception.

b) Il convient que la diversité fonctionnelle et la diversité des signaux soient envisagées. Ce sont des méthodes particulièrement efficaces pour réduire le risque de DCC dues aux erreurs dans la spécification des exigences ou dans la spécification et la réalisation du logiciel d'application.

c) La diversité des équipements peut être efficace contre les DCC des composants matériels ou contre les défauts logiciels du système. Il convient notamment de la prendre en compte pour les systèmes complexes dont l'expérience opérationnelle est réduite.

d) Il convient que des procédures ou méthodes de vérification et de validation diversifiées (par exemple moyens d'essai sur site diversifiés, contrôle par rapport à un simulateur, etc.) soient utilisées. Celles-ci contribuent à éviter les DCC sans accroître la complexité du système, comme cela peut être le cas avec d'autres techniques de diversification.

e) Si la diversité est utilisée pour aider à la défense contre les DCC, la conception doit contenir une analyse de l'efficacité des techniques employées pour minimiser les DCC potentielles. Il est recommandé que les avantages et désavantages soient justifiés et documentés (voir 5.3.3).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

5.3.1.5.3 Defence by design provisions in the I&C architecture and HMI

a) Independent systems or subsystems should be provided for different lines of defence for the same PIE (see note 1 of 5.1.1). If common resources are used, these shall be consistent with the required reliability target of the safety group.

b) Independent means should be provided for the monitoring and operation of the plant functions and systems important to safety so that sufficient information remains available for safe plant operation following a failure, for example of a multiplexed data link or computer.

c) When manual control actions are used as back-up to automatic actions for category A or B functions, the potential of CCF within these actions should be minimised.

d) When one category A function can cause an actuation of an engineering safety system and another category A function applicable in different circumstances can cause an opposite actuation, an analysis shall be performed to determine the action required under failure conditions of the I&C systems.

5.3.1.5.4 Defence against CCF due to systematic faults

a) High-quality planning in development and manufacturing for the different I&C systems of the safety group should avoid undetected faults such as to make CCFs risks within these systems unlikely. This standard contains provisions which shall be used to tailor the quality of the I&C systems of different classes.

b) Systematic failures should be detected by means of self-supervision (exception handler, watchdog, plausibility checks) and detected failures should set the affected system(s) in a predefined, preferably fail-safe state; and the failure announced to the operator.

c) If the required reliability for a fail-safe actuation of a safety function is higher than the reliability predicted from the evaluation of the fail-safe behaviour of the system, then the design shall be modified.

NOTE 1 The required degree of defence against failures depends on the category of the functions to be performed.

NOTE 2 This subclause is intended to give an overview. Detailed requirements for defences against CCFs due to software faults for category A functions are given in 4.1 of IEC 60880-2.

5.3.1.5.5 Defence by use of diverse features

a) The I&C architectural design should use the principle of diversity where high reliability is required for a safety group notably when there are uncertainties in the evaluation of the design.

b) Functional diversity and signal diversity should be considered. These are particularly effective methods to reduce risk of CCF due to errors in the requirements specifications or in the specification and implementation of application software.

c) Equipment diversity may be effective against CCF of hardware components and may provide defence against system software faults. In particular, it should be considered for complex systems where there is limited operational experience.

d) Diverse verification and validation procedures or methods (for example diverse field test facilities, back-to-back testing with a simulator, etc.) should be used. These contribute to the avoidance of CCFs, without increasing the system complexity, as may be the case with use of other diverse features.

e) If diversity is used to support defence against CCF, the design shall include an analysis of the effectiveness of diverse features claimed to minimise the potential for CCF. The benefits and drawbacks should be justified and documented (see 5.3.3).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

5.3.1.5.6 Décisions stratégiques pour limiter la complexité

Afin de réduire le risque de DCC dans des systèmes complexes, le processus de conception de l'architecture de l'I&C doit inclure une analyse stratégique démontrant que le degré d'utilisation des ordinateurs (voir note) par rapport à des systèmes câblés, ainsi que le degré d'intervention humaine sont acceptables pour la sûreté.

NOTE Cela peut dépendre de l'expérience nationale, de l'attitude de la réglementation et de la confiance accordée à l'informatique.

5.3.2 Affectation des fonctions

Le processus d'affectation des fonctions attribue les exigences globales relatives aux FSE des I&C importants pour la sûreté établies en 5.2 aux systèmes individuels de l'architecture I&C. Il peut décomposer, si nécessaire, une fonction en plusieurs sous-fonctions réparties sur plusieurs systèmes. Toutes les fonctions ou sous-fonctions sont appelées fonctions d'application des systèmes d'I&C (voir 6.1.1.1).

a) Les exigences de fonctionnalité et de performance relatives aux fonctions d'application doivent être compatibles avec celles relatives aux FSE d'I&C. Si une fonction est répartie sur plusieurs systèmes d'I&C, ces systèmes interconnectés doivent être disposés de manière que les exigences globales qui font l'objet de 5.2 soient respectées.

b) Les exigences de fonctionnalité et de performance relatives aux fonctions d'application doivent inclure les fonctions auxiliaires de validation, de verrouillage et de surveillance qui ont été identifiées lors de la conception de l'architecture de l'I&C, par exemple état et mode de fonctionnement des systèmes interconnectés, validation des signaux en provenance d'autres systèmes.

c) L'affectation des fonctions d'application aux systèmes doit être conforme aux principes définis dans le tableau 2 sur la classe des systèmes et la catégorie des fonctions.

d) Les fonctions de catégorie A doivent être attribuées à des systèmes satisfaisant au critère de défaillance unique.

e) L'affectation à des systèmes des fonctions de catégorie A d'un même groupe de sûreté doit prendre en compte les mesures de défense contre les DCC prescrites en 5.3.1.5. Des exemples d'affectation de fonctions de catégories différentes sont donnés à la figure C.1.

f) L'affectation des fonctions d'application aux systèmes doit viser à minimiser la complexité des systèmes de classe 1.

   NOTE Cela est en particulier valable pour les nouvelles centrales. En cas de remplacement de systèmes câblés par des systèmes informatiques, les exigences pour les fonctions d'application du système câblé sont normalement reportées au système informatique.

g) La fiabilité requise de chaque fonction d'application doit s'accorder avec les limites, DCC comprises, reconnues comme réalisables.

5.3.3 Analyses requises

Des analyses sont requises pour vérifier l'architecture de l'I&C et l'affectation des fonctions aux systèmes d'I&C. De telles analyses représentent une démarche itérative qui doit être effectuée avec le processus de conception (voir article 6).

5.3.3.1 Estimation de la fiabilité et des défenses contre les DCC

a) Il convient qu'une évaluation de la fiabilité des fonctions de catégorie A d'un groupe de sûreté soit réalisée. Elle devrait prendre en compte les dépendances dues à des services communs, tels que la fourniture d'énergies électrique et pneumatique, et les moyens de ventilation.

b) Cette évaluation peut être initialement basée sur la fiabilité estimée atteignable pour les fonctions des différents systèmes. Il convient qu'elle soit vérifiée à la fin du processus de conception, en se basant sur l'estimation de la fiabilité des systèmes (voir 6.1.3.1.2).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

5.3.1.5.6 Strategic decisions to limit complexity

In order to minimise potential CCF from complex systems, the design process of the I&C architecture shall include an analysis to demonstrate that the extent to which computers are used (see note) versus hard-wired systems, and the degree of human action is acceptable for safety.

NOTE This may depend on national experience, regulatory attitude and confidence in computer technology.

5.3.2 Functional assignment

The functional assignment process assigns the overall requirements of the I&C FSE important to safety, established in 5.2, to the individual systems of the I&C architecture. Where necessary, single functions may be decomposed into a number of subfunctions distributed over a number of systems. All the functions or subfunctions are called the application functions of the I&C systems (see 6.1.1.1).

a) The functional and performance requirements specification of the application functions shall address the overall requirements of the I&C FSE. If a function is distributed over more than one I&C system, these interconnected systems shall be arranged in such a way that the overall requirements defined in 5.2 are met.

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

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

d) Category A functions shall be assigned to systems which comply with the single failure criterion.

e) The assignment of category A functions of the same safety group to systems shall take into account the measures for defence against CCF stated in 5.3.1.5. Examples of assignment of functions of different categories are given in figure C.1.

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

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

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

5.3.3 Required analysis

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

5.3.3.1 Assessment of reliability and defences against CCF

a) An evaluation of the reliability of a safety group category A functions should be performed. The evaluation should include dependencies on common services, such as electrical and pneumatic power supplies and heating ventilation facilities.

b) This may be based initially on the estimated reliability achievable for the functions of the different systems and should be verified following completion of the design process based on the reliability assessment of the individual systems (see 6.1.3.1.2).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

c) Une évaluation de l'efficacité des mesures utilisées pour réduire la sensibilité aux DCC des groupes de sûreté contenant des fonctions de catégorie A doit être effectuée.

d) La documentation de conception des systèmes (voir 6.3.3) doit être analysée afin d'identifier les composants matériels ou logiciels, communs ou identiques, impliqués dans différentes fonctions d'un groupe de sûreté contenant des fonctions de catégorie A. Si des éléments communs ou identiques sont détectés dans différentes lignes de défense, une justification doit prouver un faible potentiel de DCC.

e) Il n'existe aucune méthode unanimement reconnue pour procéder à une estimation quantitative du potentiel de DCC, et les méthodes utilisées sont essentiellement qualitatives (voir annexe C). Il convient que les méthodes à utiliser, par exemple la méthode du facteur β pour le matériel, soient définies au début de la conception.

NOTE 1 L'objectif de cette recommandation est d'éviter des changements tardifs dans la planification et la conception d'un système en réponse à des modifications d'exigences, des DCC potentielles pouvant résulter d'erreurs lors de la réponse à ces modifications.

NOTE 2 Le niveau de détail de l'analyse des DCC peut dépendre de la catégorie des fonctions impliquées dans les systèmes et sera justifié.

NOTE 3 Les exigences relatives à l'analyse des DCC logicielles sont données en 4.1.3 de la CEI 60880-2.

NOTE 4 L'évaluation du potentiel de DCC peut être améliorée pour les systèmes d'I&C ayant une structure modulaire telle que les composants et l'intégration du système puissent être évalués en termes qualitatifs par des vérifications et, dans la mesure du possible, en termes quantitatifs.

5.3.3.2 Estimation des facteurs humains

Il convient que la vérification de la conception de l'architecture contienne une analyse des exigences relatives aux facteurs humains afin de permettre l'optimisation de la conception des systèmes d'IHM.

5.4 Planification globale

Le présent paragraphe impose des prescriptions sur le développement des plans globaux afin d'assurer que les exigences relatives aux fonctions d'I&C importantes pour la sûreté réparties sur les système d'I&C seront respectées et maintenues pendant la durée de vie des systèmes.

Les prescriptions du présent article coordonnent et complètent les plans établis en 6.2 pour les systèmes individuels d'I&C.

NOTE Les prescriptions suivantes sur les plans n'empêchent pas d'organiser ceux-ci avec un nombre de documents différents.

Les plans globaux doivent être établis avant que les activités concernées ne soient mises en œuvre.

5.4.1 Programme global d'assurance qualité

La présente norme suppose qu'un programme d'assurance qualité en accord avec les exigences de l'AIEA 50-C-QA (Rév. 1) existe en tant que partie intégrante du projet de centrale nucléaire, et qu'il prévoit le contrôle des activités qui le constituent.

a) Des programmes d'assurance qualité doivent être établis et mis en œuvre pour chaque activité ayant trait au cycle de vie et de sûreté de l'I&C (voir article 2 de l'AIEA 50-C-QA (Rév.1)).

b) Les programmes d'assurance qualité doivent englober toutes les activités nécessaires pour atteindre la qualité ainsi que les activités vérifiant que la qualité demandée a bien été atteinte (voir l'article 102 de l'AIEA 50-C-QA (Rév. 1)).

c) Les activités de vérification doivent être définies dans les plans de vérification. Ceux-ci traitent des moyens, processus et informations de sortie des phases du cycle de vie et de sûreté de l'I&C et définissent

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

c) An evaluation of the effectiveness of measures used to reduce the sensitivity of the safety groups to CCF including category A functions shall be performed.

d) The design documentation of the systems (see 6.3.3) shall be analysed to identify common or identical hardware or software components supporting different functions of a safety group including category A functions. If common or identical items are found in different lines of defence, a justification shall be provided to show that there is a low CCF potential.

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

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

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

NOTE 3 Requirements for the analysis of CCF due to software are given in 4.1.3 of IEC 60880-2.

NOTE 4 The evaluation of CCF potential may be improved when the I&C systems have a modular structure such that the components and the system integration can be evaluated in qualitative terms by verification steps and additionally, as far as possible, in quantitative terms.

5.3.3.2 Human factors assessment

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

5.4 Overall planning

This subclause places requirements upon the development of the overall plans to ensure that the requirements of the I&C functions important to safety distributed over the I&C systems will be achieved and maintained throughout the life of the systems.

The requirements of this clause co-ordinate and complement the plans established in 6.2 for the individual I&C systems.

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

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

5.4.1 Overall quality assurance programs

This standard assumes that a quality assurance program consistent with the requirements of IAEA 50-C-QA (Rev. 1) exists as an integral part of the NPP project and that it provides control of the constituent activities.

a) Quality assurance programmes shall be established and implemented for each activity related to the I&C safety life cycle (see clause 2 of IAEA 50-C-QA (Rev. 1)).

b) The quality assurance programs shall include all activities that are necessary to achieve quality and the activities which verify that the required quality has been achieved (see clause 102 of IAEA 50-C-QA (Rev. 1)).

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

- les procédures et les outils des activités de vérification;
- les enregistrements à faire et à vérifier;
- les aspects relatifs à la sûreté à vérifier;
- les procédures de résolution des défaillances et incompatibilités;
- les critères permettant de déclarer la fin de chaque phase;
- les rapports finals à établir, montrant la conformité des résultats de la phase aux exigences en entrée et la résolution des anomalies.

d) Les programmes d'assurance qualité doivent être prévus et inclus dans le programme général d'assurance qualité du projet de centrale nucléaire, et leurs activités doivent être incluses dans le calendrier général des activités du projet de centrale nucléaire.

5.4.2 Plan global de sécurité

Des mesures de sécurité sont requises pour protéger les informations traitées dans les systèmes importants pour la sûreté contre les modifications non autorisées (intégrité), les blocages d'accès (disponibilité) et la divulgation non autorisée (confidentialité).

NOTE 1 Pour les systèmes d'I&C dans les centrales nucléaires, les exigences relatives à l'intégrité et à la disponibilité ont priorité sur celles relatives à la confidentialité.

Les logiciels (codes ainsi que paramètres et données) peuvent être particulièrement vulnérables pendant la conception et la maintenance. Les menaces qui nécessitent d'être prises en compte sont en particulier les modifications malintentionnées provoquant un comportement erroné des logiciels, soit d'une manière générale, soit déclenché par des contraintes de temps ou de données.

NOTE 2 Les menaces résultant de modifications non intentionnelles sont traitées dans la spécification des exigences relatives aux systèmes (voir 6.1.1.4).

Le plan global de sécurité spécifie les procédures et les mesures techniques à prendre pour protéger l'architecture des systèmes d'I&C contre les attaques intentionnelles et intelligentes pouvant compromettre des fonctions importantes pour la sûreté.

a) Les exigences de sécurité relatives aux fonctions et systèmes importants pour la sûreté doivent être identifiées dans le plan de sécurité des systèmes (voir 6.2.2).

b) Le risque résultant d'un accès ou modification non autorisés doit être géré de manière systématique pendant toutes les phases du cycle de vie et de sûreté d'un système, depuis la conception jusqu'au démantèlement.

c) Les mesures de sécurité dans un système doivent être telles qu'elles n'ont pas d'influence importante sur sa fiabilité ou sa disponibilité.

d) La rigueur des exigences de sécurité pour un système particulier avec ses composants associés est déterminée par les fonctions que ce système accomplit. Les systèmes informatiques supportant des fonctions de catégorie A ont des exigences de sécurité plus strictes que celles qui seraient acceptables pour ceux supportant des fonctions de catégorie B ou C.

e) Afin de maintenir en permanence la sécurité des systèmes à un niveau élevé, une politique de sécurité spécifique au site doit être établie. Elles doit contenir des procédures relatives à l'interface entre la sécurité administrative et technique, l'accès aux systèmes, la sécurité de la gestion des données, la sécurité des modifications et de la maintenance, l'audit et les rapports sur l'état de la sécurité et sur la formation à la sécurité.

f) Les systèmes supportant des fonctions importantes pour la sûreté doivent être physiquement protégés contre les accès non autorisés. Le contrôle des accès doit inclure une identification et une authentification rigoureuses du personnel pour des systèmes supportant des fonctions de catégorie A ainsi qu'une identification fiable du personnel des systèmes supportant des fonctions de catégorie B et C (voir 7.12 de l'AIEA 50-SG-D3).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

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

5.4.2 Overall security plan

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

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

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

NOTE 2 Threats arising from unintended modifications are addressed in the system requirements specification (see 6.1.1.4).

The overall security plan specifies the procedural and technical measures to be taken to protect the architecture of I&C systems from deliberate and intelligent attacks that may jeopardise functions important to safety.

a) The security requirements of functions and systems important to safety shall be identified in the system security plan (see 6.2.2).

b) The risk arising from unauthorised access and modification shall be managed in a systematic manner during all phases of the life cycle from inception to disposal.

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

d) The rigour of security requirements for a particular system and associated equipment is determined by the functions performed by the system. CB systems that perform category A functions have higher security requirements than those that would be acceptable for CB systems carrying out category B or C functions.

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

f) Systems performing functions important to safety shall be physically protected against unauthorised access. Access control shall include strong identification and authentication of personnel for systems carrying category A functions and reliable identification of personnel for systems carrying category B and C functions (see 7.12 of IAEA 50-SG-D3).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

g) L'accès à distance depuis l'extérieur de la centrale aux systèmes supportant des fonctions de catégorie A ne doit pas être possible. Si l'accès à distance depuis l'intérieur de la centrale est prévu, il doit être analysé et il doit être démontré qu'il n'engendre pas de risque supplémentaire d'accès non autorisé aux systèmes ni ne représente une source supplémentaire de défaillances.

h) Il convient que l'accès aux systèmes soit enregistré en indiquant la personne, le type d'accès, l'heure et les actions effectuées.

i) Les registres de sécurité doivent être rigoureusement inspectés à intervalles de temps définis pour les systèmes exécutant des fonctions de catégorie A. Il convient qu'il soient vérifiés périodiquement pour les systèmes exécutant des fonctions de catégorie B et C.

5.4.3 Plans d'intégration et de mise en service globales

L'intégration globale regroupe toutes les mesures techniques et administratives réalisées sur site permettant aux système d'I&C installés sur site d'être interconnectés, testés, étalonnés et préparés pour une utilisation opérationnelle.

La mise en service globale regroupe toutes les mesures techniques et administratives réalisées sur site nécessaires pour garantir que les systèmes installés et la centrale sont aptes au service, avant leur mise en exploitation (voir 4.4 de l'AIEA 75-INSAG-3).

NOTE La mise en service globale de l'I&C fait partie de la mise en service de la centrale nucléaire (voir 3.11).

L'intégration et la mise en service globales complètent la validation et l'installation de chacun des systèmes (voir 6.1.5 et 6.1.6).

a) Après l'intégration des systèmes d'I&C sur site, la conformité des fonctions d'I&C importantes pour la sûreté à leurs exigences de fonctionnalité et de performance doit être établie pour tous les modes d'exploitation spécifiés de la centrale.

b) L'étendue des activités d'intégration et de mise en service à réaliser au niveau de la centrale peut être réduite lorsque des essais d'intégration ont déjà été effectués en usine ou sur site, ou si la centrale nucléaire n'est pas une première réalisation. Ces réductions doivent être justifiées et documentées.

5.4.3.1 Plan d'intégration globale

Un plan d'intégration globale des systèmes d'I&C doit être établi dans le cadre du programme d'assurance qualité. En complément des prescriptions génériques de 5.4.1 sur l'assurance qualité et la vérification, les prescriptions techniques suivantes s'appliquent:

a) Les systèmes interconnectés doivent être testés pour confirmer que

- toutes les interfaces des systèmes interconnectés fonctionnent correctement;
- la détection des défaillances, leurs actions correctives et l'affichage des données associées sont conformes aux exigences des fonctions d'I&C.

b) Le test d'immunité des systèmes interconnectés aux interférences électromagnétiques doit être effectué conformément aux prescriptions de la CEI 61000-4-1 à la CEI 61000-4-6.

c) La mise à la terre de tous les équipements et des blindages de câbles doit être vérifiée.

d) La réponse des systèmes à la perte des alimentations électriques externes doit être testée afin de vérifier le comportement et la disponibilité des systèmes en cas de coupure et de restauration des alimentations électriques.

e) La conformité des conditions environnementales par rapport à leurs spécifications doit être vérifiée sur le lieu d'utilisation des systèmes d'I&C.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

g) Features for remote (external to the plant) access to systems implementing category A functions shall not be implemented. If remote access features internal to the plant are provided, they shall be analysed and it shall be demonstrated that they do not introduce additional risk of either unauthorised system access or additional sources of potential failures of the systems.

h) Access to systems should be logged recording the personnel, the type of access, the time, and the actions carried out.

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

5.4.3 Overall integration and commissioning plans

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

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

NOTE Overall commissioning of the I&C is part of the commissioning of the NPP (see 3.11).

The overall integration and commissioning processes complete the validation and installation of the individual systems (see 6.1.5 and 6.1.6).

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

b) The extent of the integration and commissioning activities to be performed on the overall level may be reduced when integrated tests have already been carried out in the factory or on site, or the NPP is not a first-off plant. These reductions of the overall verification and validation shall be justified and documented.

5.4.3.1 Overall Integration plan

An overall integration plan for I&C systems shall be developed within the framework of the quality assurance program. In addition to the generic requirements of 5.4.1 on quality assurance and verification, the following requirements apply:

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

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

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

f) Les signaux logiques et analogiques échangés entre les systèmes doivent être testés pour montrer que des valeurs et états corrects sont fournis aux différentes fonctions importantes pour la sûreté. Lorsque des fonctions d'affichage, d'alarme, d'enregistrement et de calcul sont exécutées dans un système non important pour la sûreté, il convient que ces tests soient effectués conjointement avec ce système, à moins qu'une méthode plus simple démontre l'exactitude des données qui lui sont transmises.

g) Les fonctions de commande logique et de commande en boucle fermée doivent être testées, depuis les entrées jusqu'aux sorties et en tenant compte des interfaces avec l'opérateur et les actionneurs.

h) Les tests doivent confirmer que des informations exactes sont fournies à chaque système en cas de défaillance d'équipements redondants, de moyens de communication, de capteurs ou d'actionneurs. Ces tests devraient confirmer la conformité des temps de réponse et le bon fonctionnement des commandes de commutation.

i) Les commandes multiplexées doivent être testées pour garantir la bonne transmission des données ainsi qu'un temps de réponse acceptable, depuis l'émission de la commande jusqu'à la réception de l'indication correcte de l'état de l'actionneur. Il convient que les tests soient effectués en simulant des conditions opérationnelles normales, accidentelles, critiques, et en simulant des défaillances matérielles.

5.4.3.2 Plan de mise en service globale

Un plan de mise en service globale complétant la validation des FSE d'I&C doit être établi dans le cadre du programme de mise en service des systèmes de la centrale (voir 4.4.200 de l'AIEA 75-INSAG-3). Les prescriptions suivantes s'appliquent.

a) Les points de réglage, seuils, paramètres et valeurs d'étalonnage doivent être vérifiés et ajustés pendant la mise en service des systèmes de la centrale pour confirmer que les fonctionnalités et les performances des systèmes satisfont à leurs exigences globales.

b) Les procédures d'exploitation des systèmes d'I&C doivent être vérifiées et mises à jour pendant la mise en service de la centrale.

5.4.4 Plan global d'exploitation

Le plan global d'exploitation traite du fonctionnement des systèmes d'I&C interconnectés. Ce plan global d'exploitation est un complément des plans d'exploitation des systèmes individuels d'I&C (voir 6.2.6).

Un plan global d'exploitation doit être établi dans le cadre du programme d'assurance qualité. En complément des prescriptions génériques de 5.4.1 sur l'assurance qualité et la vérification, les prescriptions suivantes s'appliquent.

a) Le plan doit décrire

- les moyens permettant le démarrage, l'initialisation et le maintien dans un état opérationnel des systèmes interconnectés;
- les moyens permettant de vérifier la capacité des systèmes à réaliser les fonctions importantes pour la sûreté;
- les actions de routine, par exemple les tests périodiques, qui doivent être effectuées pendant le fonctionnement de la centrale afin de maintenir la fiabilité requise des fonctions importantes pour la sûreté.

b) Le plan doit spécifier les conditions sous lesquelles la modification des paramètres ou commandes des systèmes peut être effectuée ainsi que les effets de ces modifications sur le fonctionnement des systèmes et sur l'exploitation et la sûreté de la centrale. Il doit également indiquer les modifications qu'il est possible d'apporter:

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

g) Closed-loop control functions and logic control functions shall be tested, from inputs to outputs including actuators and operator interfaces.

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

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

5.4.3.2 Overall commissioning plan

An overall plan to complete the validation of the I&C FSE shall be developed within the framework of the commissioning programme of the plant systems (see 4.4.200 of IAEA 75-INSAG-3). The following requirements apply.

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

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

5.4.4 Overall operation plan

Overall operation planning addresses the operation of the interconnected I&C systems. The overall operation plan complements the operation plans for the individual I&C systems (see 6.2.6).

An overall operation plan shall be developed within the framework of the quality assurance program. In addition to the generic requirements of 5.4.1 on quality assurance and verification, the following requirements apply.

a) The plan shall describe

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- sous contrôle administratif;
- sous contrôle administratif et après approbation du concepteur et réalisation de tests et vérifications appropriés.

NOTE Le processus de mise en œuvre de modifications et les autorités autorisant ces modifications peuvent dépendre de l'exploitant et des réglementations nationales.

c) Le plan doit identifier tous les modes de fonctionnement des systèmes interconnectés et spécifier la façon dont les systèmes doivent être exploités dans chaque mode. En particulier

- les mesures à prendre et les contraintes d'exploitation des systèmes et de la centrale, en cas de défaillance des systèmes ou d'événement dangereux externe aux systèmes;
- les contraintes d'exploitation des systèmes et de la centrale pendant les essais périodiques, la maintenance et/ou la mise en place de modifications;
- lorsque ces contraintes peuvent être levées, les procédures permettant de revenir à un fonctionnement normal, et confirmer que le fonctionnement normal est bien rétabli.

5.4.5 Plan global de maintenance

Le plan global de maintenance traite de la maintenance au niveau des systèmes interconnectés de l'architecture de l'I&C. Il complète et coordonne les plans de maintenance des systèmes individuels (voir 6.2.7).

Un plan global de maintenance doit être établi dans le cadre du programme d'assurance qualité. En complément des prescriptions génériques de 5.4.1 sur l'assurance qualité et la vérification, les prescriptions suivantes s'appliquent.

a) Des contraintes doivent être imposées aux activités de maintenance des systèmes individuels d'I&C afin d'assurer que tout effet sur la sûreté de la centrale est acceptable. En particulier, lorsque cela est exigé (voir 6.1.1.2.5), les systèmes doivent continuer à satisfaire au critère de défaillance unique pendant la maintenance. Le plan doit identifier les équipements pouvant être retirés du service, les conséquences de ces retraits et les moyens pour remettre en état ces équipements et pour vérifier une remise en service correcte.

b) Une approche systématique d'essai et de remplacement doit être mise en œuvre afin de rendre les DCC improbables dans les parties de l'architecture de l'I&C soumises à des changements d'environnement en cas d'accident. Il convient que l'approche garantisse que les parties du système soumises aux rayonnements, et pouvant de ce fait subir un vieillissement rapide ou des modifications de leurs propriétés physiques (câbles, capteurs), ou dont la charge est modifiée en réponse à une sollicitation (par exemple commutation des amplificateurs de puissance, relais), ne peuvent provoquer de défaillances non détectées.

NOTE Les intervalles de remplacement peuvent être déterminés par un vieillissement accéléré.

c) Les activités de maintenance nécessitant l'ajustement de données de configuration ou d'étalonnage doivent être réglementées par des procédures documentées assurant que:

- les ajustements sont dans les limites définies (ces limites peuvent être imposées par la conception des systèmes ou par la conception de la centrale, auquel cas il n'est pas nécessaire d'imposer de restrictions formelles au personnel de maintenance);
- lorsque les ajustements sont effectués pendant le fonctionnement d'un système, les prescriptions de 5.4.4 ci-dessus s'appliquent;
- un registre de tous les ajustements est tenu à jour.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

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

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

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

5.4.5 Overall maintenance plan

The overall maintenance plan addresses maintenance at the level of the interconnected I&C systems. It complements and co-ordinates the maintenance plans of the individual I&C systems (see 6.2.7).

An overall maintenance plan shall be developed in the framework of the quality assurance program. In addition to the generic requirements of 5.4.1 on quality assurance and verification, the following requirements apply.

a) Constraints shall be placed on maintenance activities of the individual I&C systems to ensure that any effect on the plant safety is acceptable. In particular, where required (see 6.1.1.2.5), the systems shall continue to meet the single-failure criterion during maintenance. The plan shall identify what equipment may be removed from service, the consequences of withdrawal, and the means for returning and verifying its correct return to service.

b) A systematic approach to test and replacement shall be implemented to make CCFs unlikely within those parts of the I&C architecture which are subjected to changed environmental conditions in the event of an accident. The approach should ensure that those parts of the system subject to radiation, and thereby to possible rapid ageing, or changes in physical properties (cables, sensors), or whose loading is changed in response to a challenge (for example, switching of power amplifiers, relays) cannot result in undetected failures.

NOTE Replacement intervals may be determined by accelerated ageing.

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

- maintenance adjustments are within defined limits (such limits may be imposed by the system design and plant design base in which case no formal restrictions need to be placed upon the maintenance staff);
- where such adjustments are performed while a system is in use, the requirements of 5.4.4 above apply;
- a record of all maintenance adjustments is preserved.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

5.5 Documentation

La documentation de l'architecture d'I&C et de l'affectation des fonctions fournit les informations nécessaires à la spécification des exigences relatives aux systèmes individuels de l'architecture de l'I&C (voir 6.1.1).

5.5.1 Documentation de la conception de l'architecture

a) La documentation doit définir, pour les systèmes d'I&C individuels
   - les contraintes de conception provenant de la centrale (voir 5.1.3);
   - les contraintes de conception provenant de l'architecture d'I&C (voir 5.3.1);
   - les limites physiques et fonctionnelles des systèmes.

b) Il convient que les outils utilisés soient documentés afin de préciser:
   - comment une activité donnée du cycle de vie et de sûreté d'un système est facilitée par ces outils;
   - comment chaque outil doit être utilisé;
   - comment les résultats obtenus avec chacun de ces outils doivent être vérifiés.

NOTE Les exigences relatives aux méthodes et outils logiciels pour les systèmes de classe 1 figurent en 4.2 et 4.3 de la CEI 60880-2.

5.5.2 Documentation de l'affectation des fonctions

a) La documentation doit définir les exigences de fonctionnalité, performance et fiabilité relatives aux fonctions d'application (voir 5.3.2) affectées à chaque système. Les exigences peuvent être représentées sous forme de texte, schéma mécanique, matrices, schéma logique, etc., pourvu que les fonctions soient clairement explicitées.

b) Il convient que les exigences relatives aux fonctions d'application d'un système informatique ne dépendent pas des solutions envisagées pour la réalisation, par exemple calculateurs, relais.

c) Il convient que des méthodes et outils soient utilisés pour créer des documents d'exigences qui soient facilement compréhensibles par les auteurs des exigences et par les opérateurs de la centrale.

6 Cycle de vie et de sûreté du système

L'architecture de l'I&C identifie les systèmes d'I&C supportant les fonctions importantes pour la sûreté (voir 5.3.1). Le présent article développe les objectifs et prescriptions relatifs à des systèmes informatiques.

NOTE La plupart de ces prescriptions peuvent aussi s'appliquer aux systèmes d'I&C conventionnels.

Afin de s'assurer que toutes les exigences ayant trait à la sûreté et devant être respectées par le système sont bien prises en compte, mises en œuvre et maintenues, une approche systématique est nécessaire. A cet effet, les activités liées au développement, à la réalisation et à l'exploitation des systèmes sont introduites dans un cycle de vie et de sûreté du système. Ce cycle de vie et de sûreté fait référence, à son tour, aux activités du cycle de vie et de sûreté global de l'I&C (voir article 5 et figure 4).

Les phases du cycle de vie et de sûreté type d'un système informatique incluent

- la spécification des exigences du système;
- la spécification du système;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

5.5 Output documentation

The output documentation of the I&C architectural design and functional assignment process, provide the necessary inputs for the requirements specification of the individual systems of the I&C architecture (see 6.1.1).

5.5.1 Architectural design documentation

a) The output documentation shall define for the individual I&C systems
   - the design constraints derived from the plant context (see 5.1.3);
   - the design constraints from the architectural design (see 5.3.1);
   - the physical and functional boundaries between systems.

b) The engineering tools used should be documented to address:
   - how a design activity of the system life cycle is supported by such tools;
   - how each tool is to be used;
   - how the output of each tool is to be verified.

NOTE Requirements on software engineering methods and tools for class 1 systems are given in 4.2 and 4.3 of IEC 60880-2.

5.5.2 Functional assignment documentation

a) The output documentation shall define the functional, performance and reliability requirements of the application functions (see 5.3.2) assigned to each system. The requirements may be documented in text, flow diagrams, matrices, logic diagrams, etc., providing the functions are clearly conveyed.

b) The requirements specifications of the application functions of a CB system should not depend on properties of the technology intended for the implementation, i.e. computers, relays.

c) Software and system engineering methods and tools should be used to create requirement documents which can be easily understood by the authors of the system requirements specification and by the plant operators.

6 System safety life cycle

The I&C architectural design defines the individual I&C systems which implement the functions important to safety (see 5.3.1). This clause sets out the objectives and requirements for such individual I&C systems. The requirements of this clause address CB systems.

NOTE Most of these requirements may also be applied to conventional I&C systems.

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

The phases of the typical system safety life cycle include

- the system requirements specification;
- the system specification;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- la conception détaillée et la réalisation du système;
- l'intégration du système;
- la validation du système;
- l'installation du système;
- les modifications apportées à la conception du système (le cas échéant).

La qualification du système est prise en compte séparément car elle peut être réalisée en partie indépendamment du cycle de développement du système. Cette approche correspond à la pratique actuelle qui consiste à utiliser de plus en plus des composants préexistants.

La figure 5 présente un cycle de vie et de sûreté du système et indique les liens avec les cycles de vie du logiciel et du matériel prescrits dans la CEI 60880 et la CEI 60987.

Le tableau 3 présente une vue d'ensemble des objectifs, entrées et sorties des différentes activités pendant le cycle de vie et de sûreté du système et fait référence aux paragraphes correspondants.

Le présent article inclut

- des prescriptions qui s'appliquent à tous les systèmes importants pour la sûreté;
- des prescriptions qui s'appliquent, en complément des précédentes, à des classes de systèmes et catégories de fonctions particulières. Les prescriptions spécifiques sont résumées au tableau 4.

Le cycle de vie et de sûreté du système est un processus itératif; une phase peut débuter avant l'achèvement de la précédente, mais ne peut se terminer que si les phases précédentes sont achevées et si ses sorties sont en accord avec les entrées fournies par ces phases précédentes.

NOTE Cette prescription diffère de celles de 6.1 de la CEI 60880. Pour les logiciels, il est souhaitable, sans que ce soit une nécessité, de terminer chaque phase d'un développement avant de commencer la suivante, à condition que les exigences susmentionnées aient été prises en compte.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

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

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

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

This clause includes

- requirements to be applied equally for all systems important to safety;
- requirements to be applied, in addition to the previous ones, to specific classes of systems or categories of functions. The specific requirements are summarised in table 4.

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

NOTE This requirement differs from that stated in 6.1 of IEC 60880. For software, it is desirable, but not considered necessary, to complete each phase of a development before starting the next phase providing the requirements defined above have been addressed.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

Tableau 3 – Vue d'ensemble du cycle de vie et de sûreté du système

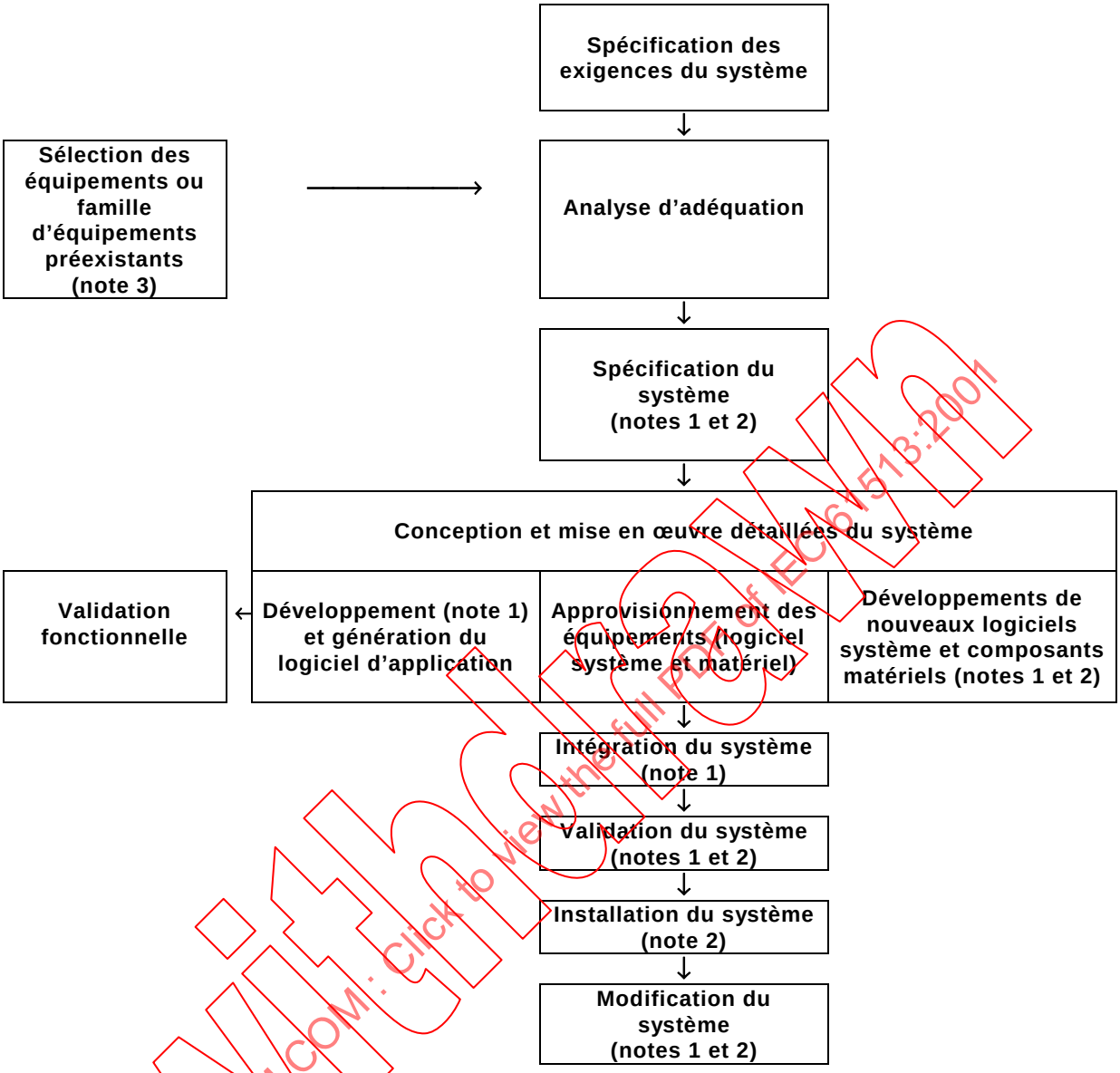
Article ou paragraphe	Entrées	Objectifs de l'activité	Sorties
6	Prescriptions relatives au cycle de vie et de sûreté du système et relation de ce cycle avec le cycle de vie et de sûreté global		
6.1.1 Exigences sur le système	Sorties de 5.5, 5.4 Sorties de 6.2.1, 6.2.2	Spécifier les exigences sur le système pour: – les fonctions – les contraintes de conception – les limites et interfaces avec les autres systèmes et outils – les interfaces avec les opérateurs – les conditions environnementales	Spécification des exigences du système Spécification des exigences des fonctions d'application
6.1.2 Spécification du système	Sorties de 6.1.1 Documentation des composants candidats préexistants Sorties de 6.2.1, 6.2.2	Evaluer et déterminer la faisabilité de l'intégration des composants candidats préexistants dans la conception du système Concevoir l'architecture du système de façon à satisfaire aux exigences sur le système Affecter les fonctions d'application aux sous-systèmes	Spécification du système (6.3.2) incluant: – l'identification des équipements choisis et les analyses de faisabilité – l'architecture du système – la spécification du logiciel
6.1.3 Conception détaillée et réalisation du système	Sortie de 6.1.2 Sortie de 5.1.1 Sorties de 6.2.1, 6.2.2	Elargir et améliorer la conception de l'architecture Développer le matériel et le logiciel (système ou d'application) Valider les exigences relatives aux fonctions d'application	Documentation détaillée de la conception détaillée du système (6.3.3) Validation fonctionnelle et estimation de la fiabilité (6.1.3.1) Composants et sous-systèmes matériels et logiciels
6.1.4 Intégration du système	Sorties de 6.1.3 Sorties de 6.2.1, 6.2.2, 6.2.3	Intégrer les composants matériels et logiciels qui forment ensemble le système	Rapport d'intégration Système intégré
6.1.5 Validation du système	Sorties de 6.1.2, 6.1.4 Sorties de 6.2.1, 6.2.2, 6.2.4	Valider le système par rapport à sa spécification	Rapport de validation du système
6.1.6 Installation du système	Sorties de 6.1.5 Sorties de 6.2.1, 6.2.2, 6.2.5	Installer et tester le système sur site	Rapport d'installation Système installé et testé sur site
6.1.7 Modifications du système	Demande de modification (si besoin) Sorties de 6.2.1, 6.2.2, 6.2.7	Apporter les corrections, améliorations ou adaptations au système	Rapports sur les modifications Système modifié
6.2 Planification du système	Sorties de 5.4, 6.1	Développer les plans de validation, d'installation, d'exploitation, de maintenance, de sécurité	Plans du système
6.4 Qualification du système	Sorties de 6.2.1, 6.2.2	Développer le plan de qualification	Documentation concernant la qualification
NOTE Pour une comparaison de cette définition des phases avec celle de la CEI 61508-2, voir annexe D.			

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

Table 3 – Overview of the system safety life cycle

Clause or subclause	Inputs	Objectives of the activity	Outputs
6	Requirements on the system life cycle and its relation with the overall safety life cycle		
6.1.1 System requirements specification	Outputs of 5.5; 5.4 Outputs of 6.2.1, 6.2.2	To develop the system requirements specification for – the functions – the design constraints – the boundaries and interfaces with other systems and tools – the interfaces with persons – the environmental conditions	System requirements specification Application functions requirements specification
6.1.2 System specification	Outputs of 6.1.1 Documen-tation of candidate pre-existing equipment Outputs of 6.2.1, 6.2.2	To evaluate and assess the suitability of candidate pre-existing equipment to be integrated in the system design To develop the design of the system architecture in order to implement the system requirements specification To assign the application functions to subsystems	System specification documentation (see 6.3.2) including: – identification of selected equipment and suitability analysis – system architecture – software specification
6.1.3 System detailed design and implementation	Output of 6.1.2 Output of 5.1.1 Outputs of 6.2.1, 6.2.2	To expand and refine the architectural design To develop the hardware and (system or application) software To validate the application functions requirements	System detailed design documentation (see 6.3.3) Functional validation and reliability assessment (see 6.1.3.1) The hardware and software subsystems and components
6.1.4 System integration	Output of 6.1.3 Outputs of 6.2.1, 6.2.2, 6.2.3	Assembly of the individual hardware and software components that make up the system	Integration report The integrated system
6.1.5 System validation	Outputs of 6.1.2 and 6.1.4 Outputs of 6.2.1, 6.2.2, 6.2.4	Validation of the system specification	System validation report
6.1.6 System installation	Outputs of 6.1.5 Outputs of 6.2.1, 6.2.2, 6.2.5	Installation and testing of the system	Installation report The system installed and tested on site
6.1.7 System design modifications	Modification request (if any) Outputs of 6.2.1, 6.2.2, 6.2.7	To make corrections, enhancements or adaptations to the system	Modification reports The system modified
6.2 System planning	Outputs of 5.4, 6.1	To develop the validation plan, installation plan, operation and maintenance plan, security plan	System plans
6.4 System qualification	Outputs of 6.2.1, 6.2.2	To develop the qualification plan	Qualification documentation
NOTE For a comparison of this definition of phases with that of IEC 61508-2, see annex D.			

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001



IEC 192/01

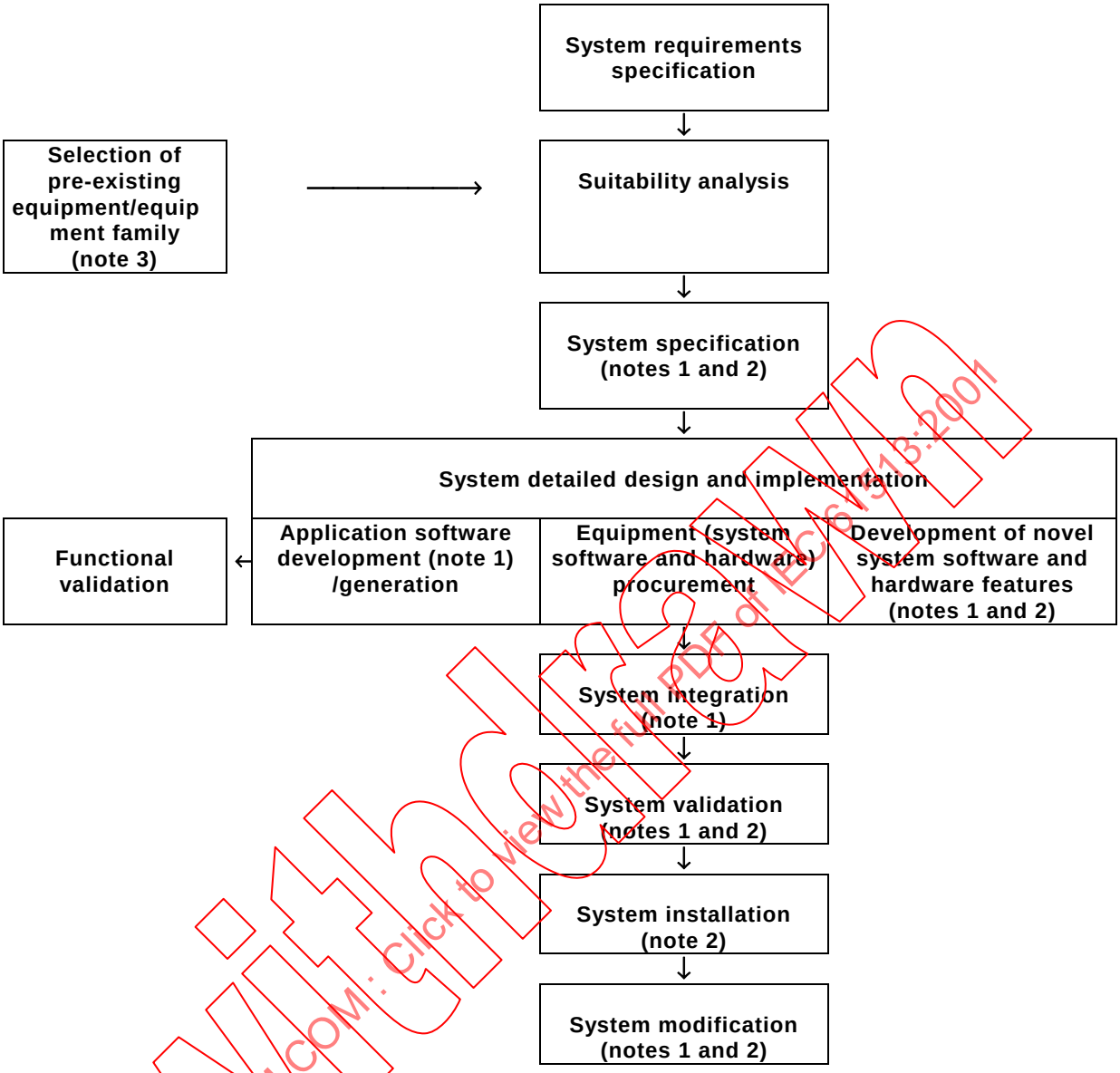
NOTE 1 Pour les systèmes de classe 1, les prescriptions relatives au logiciel et à cette activité sont définies dans la CEI 60880.

NOTE 2 Pour les systèmes de classe 1, les prescriptions relatives au matériel et à cette activité sont définies dans la CEI 60987.

NOTE 3 Pour les systèmes de classe 1, les prescriptions relatives aux logiciels prédéveloppés sont définies dans la CEI 60880-2.

Figure 5 – Cycle de vie et de sûreté du système

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn



NOTE 1 For class 1 systems, software requirements on this activity are defined in IEC 60880.

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

NOTE 3 For class 1 systems, requirements for predeveloped software are defined in IEC 60880-2.

Figure 5 – System safety life cycle

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

6.1 Prescriptions

Le présent article définit les prescriptions pour le cycle de vie et de sûreté du système.

Ces prescriptions couvrent également

- les fonctions spécifiques affectées au système par le processus d'affectation des fonctions;
- les caractéristiques génériques qui, selon la classification du système, rendent celui-ci apte à réaliser les fonctions importantes pour la sûreté des catégories spécifiées.

NOTE L'article 8 de la CEI 61226 spécifie les prescriptions relatives aux FSE d'I&C et les prescriptions spécifiques aux différentes catégories de FSE d'I&C. Ces prescriptions sont prises en compte de manière appropriée dans la présente norme lors du développement des prescriptions relatives aux systèmes et fonctions.

6.1.1 Spécification des exigences du système

L'objectif de cette phase est de fournir une description de haut niveau des exigences relatives au système, indépendamment du choix d'une solution technique particulière.

La documentation de l'architecture de l'I&C et de l'affectation des fonctions (voir 5.5) fait partie des entrées de la spécification des exigences du système.

La documentation de sortie de cette phase est le document de référence permettant à ceux qui définissent le problème et ceux qui apporteront une solution technique de communiquer.

La spécification des exigences du système doit indiquer

- les fonctions du système;
- les contraintes sur la conception du système;
- les limites du système et les interfaces avec les autres systèmes;
- les interfaces avec les utilisateurs du système;
- les conditions d'environnement du système;
- la qualification requise.

6.1.1.1 Fonctions

Les exigences à prendre en compte sont celles relatives aux fonctions d'application et celles relatives aux fonctions de service du système. Ce qui suit s'applique:

6.1.1.1.1 Fonctions d'application

Les exigences relatives aux fonctions d'application importantes pour la sûreté sont régies par le processus d'affectation des fonctions (voir 5.5.2).

a) Les exigences relatives à chaque fonction d'application doivent établir

   1) la fonctionnalité, y compris les domaines de variation des entrées/sorties et des points de réglage. Pour les fonctions d'arrêt d'urgence, les exigences définissent les marges entre les points de réglage et les valeurs admissibles (c'est-à-dire celles incluant toutes les incertitudes dues aux erreurs d'étalonnage ou aux dérives de l'instrumentation);

   2) les performances, y compris la précision et les temps de réponse. Si nécessaire, les exigences de performance sont définies pour différentes conditions d'exploitation de la centrale et différents EIH.

   NOTE La CEI 61069-2 [6] peut être utile pour l'identification et la définition des critères de performance.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.1 Requirements

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

These requirements encompass features related to the

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

NOTE Clause 8 of IEC 61226 gives basic requirements for I&C FSE and requirements specific to the different categories of I&C FSE. These requirements are appropriately taken into account in this standard when developing the requirements for systems or functions respectively.

6.1.1 System requirements specification

The objective of this phase is to provide a high-level description of the system requirements, independent of the decision to adopt any specific technical solution.

The output documentation describing the I&C architecture and functional assignment (see 5.5) is one of the inputs to the system requirements specification.

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

The system requirements specification shall indicate

- the functions of the system;
- the constraints on the design of the system;
- the boundaries and interfaces with other systems;
- the interfaces with the users;
- the environmental conditions of the system;
- the qualification required.

6.1.1.1 Functions

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

6.1.1.1.1 Application functions

The requirements specifications of the application functions important to safety are defined by the functional assignment process (see 5.5.2).

a) The requirements specification of each application function shall establish

   1) the functionality, including input/output ranges and setpoints. For trip functions, the specification defines the margins between setpoints and allowable values (i.e. those including all uncertainties due to calibration errors or instrument drifts);

   2) the performance, including accuracy and response times. Where appropriate, performance requirements are defined for different initial plant conditions and PIEs.

   NOTE IEC 61069-2 [6] may be useful in the identification and definition of the performance criteria.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

b) La spécification des exigences relatives à chaque fonction d'application doivent indiquer sa catégorie ainsi que l'existence éventuelle de contraintes d'indépendance vis à vis d'autres fonctions du même groupe de sûreté. Ces exigences définissent implicitement et qualitativement la fiabilité requise pour la fonction.

Les règles d'affectation des fonctions définissent pour chaque catégorie de fonction une classe minimale de système d'I&C. Ces règles, ainsi que les exigences relatives à l'indépendance entre les fonctions d'un même groupe de sûreté (critère de défaillance unique, défense contre les DCC), permettent une estimation qualitative de la fiabilité de la fonction ou du groupe de fonctions dans un groupe de sûreté.

Une estimation quantitative de la fiabilité des fonctions d'application peut être nécessaire pour vérifier la conception du système et de la centrale (voir A2.2 de la CEI 60880). Cette estimation est normalement effectuée pour la conception du matériel du système (des méthodes bien rodées existent) mais aucune méthode unanimement reconnue n'existe pour l'évaluation quantitative de la fiabilité du logiciel (voir 6.1.3.1.2).

6.1.1.1.2 Fonctions de service

Les fonctions de service, à la différence des fonctions d'application, ne sont pas directement liées au procédé mais sont liées au système. Elles incluent les fonctions nécessaires à la configuration, à la validation, à la qualification, à l'installation, à la mise en service, à l'exploitation, aux essais périodiques, à la maintenance, à l'incorporation de modifications de la conception et à la sécurité.

Les exigences relatives aux fonctions de service sont définies par ceux qui spécifient le système. La précision de ces exigences est déterminée au cas par cas. Dans certains cas, elles peuvent être finalisées lors de la phase de spécification et de conception architecturale du système, après sélection d'une solution technique appropriée pour le matériel et le logiciel.

Il convient que les exigences relatives aux fonctions de service prennent en compte les interactions et contraintes pouvant provenir des plans du système (voir 6.2).

NOTE Par exemple, les commandes permettant la modification des paramètres doivent être en accord avec les dispositions spécifiées par le plan de sécurité du système (voir 6.2.2), le plan d'exploitation du système (voir 6.2.6) et le plan de maintenance du système (voir 6.2.7).

6.1.1.1.3 Fonctions du logiciel système

Les exigences relatives au système ne définissent normalement pas de manière explicite les fonctions du logiciel système. Ces fonctions, qui se rapportent au fonctionnement et à l'auto-surveillance du système, sont en fait particulières aux équipements préexistants (voir 6.1.2.1) et peuvent être définies de manière plus appropriée pendant la phase de spécification du système. Cependant, les exigences relatives au logiciel système sont implicitement définies par les exigences relatives à la fonctionnalité des fonctions d'application et par les exigences relatives aux contraintes de conception sur le système (voir 6.1.1.2.1).

Les exigences relatives aux fonctions du logiciel système doivent être explicitement spécifiées lorsqu'il y a un logiciel système qui fait l'objet d'un nouveau développement ou d'un nouvel approvisionnement.

6.1.1.2 Contraintes de conception

Les prescriptions suivantes définissent les contraintes qui limitent le choix de solutions potentielles pour la conception du système et l'affectation des fonctions dans le système. Ces contraintes dépendent de la classe du système et des catégories des fonctions et doivent être prises en compte pendant la spécification et la conception de l'architecture du système afin de

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

b) The requirements specification of each application function shall state its categorisation and whether there are independence constraints from other functions in a safety group. Such requirements implicitly define, in a qualitative way, the required reliability of the function.

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

An estimate of the quantitative reliability of the application functions may be required for verification of the system design and of the plant design basis (see A2.2 of IEC 60880). This estimation is normally performed for the system hardware design, where well established practices exist, but there is no generally recognised method available for the quantitative evaluation of software reliability (see 6.1.3.1.2).

6.1.1.1.2 Service functions

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

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

Service function requirements should take into account the interactions and constraints that can be derived from the system plans (see 6.2).

NOTE For example, the controls for the modification of parameters shall be consistent with the provisions specified by the system security plan (see 6.2.2), the system operation plan (see 6.2.6) and the system maintenance plan (see 6.2.7).

6.1.1.1.3 System software functions

The system requirements specification normally does not explicitly address the system software functions. In fact, these functions, which are related to the operation and self-monitoring of the system itself, are specific to the pre-existing equipment to be used (see 6.1.2.1) and may be more appropriately defined in the system specification phase. However, requirements on the system software are implicitly defined by the requirements on the functionality of the application functions and by the requirements on the design constraints on the system (see 6.1.1.2.1).

System software functions requirements shall be explicitly specified whether there is some system software to be newly developed or procured.

6.1.1.2 Design constraints

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

- satisfaire aux exigences relatives à la catégorisation des fonctions d'application;
- assurer que le système fonctionnera comme il a été spécifié;
- permettre ou faciliter la démonstration du fonctionnement correct du système.

6.1.1.2.1 Architecture du système

L'architecture du système dépend de la catégorie des fonctions à réaliser au sein du système (voir 5.3.2) et du concept de défense en profondeur (voir 5.2 et 7.8.1 de l'AIEA 50-SG-D3).

a) Le système peut réaliser des fonctions de la catégorie la plus élevée permise pour sa classe (voir 5.3.2) et des fonctions de catégories inférieures. Le système peut contenir des sous-systèmes appartenant à des classes inférieures, à condition que les prescriptions suivantes soient respectées:

   1) les exigences relatives à la conception de chaque sous-système ne doivent pas être plus faibles que celles requises pour la fonction de la catégorie la plus élevée supportée par le sous-système;

   2) la conception du système doit garantir que les exigences des sous-systèmes ou équipements des classes supérieures sont remplies, même en cas de défaillance d'équipements de classes inférieures.

b) La conception du système doit inclure les redondances et les autres caractéristiques nécessaires à la tolérance à la défaillance (voir 6.1.2.2.3) et à l'affectation des fonctions d'application importantes pour la sûreté (voir 6.1.2.4).

   NOTE Le système peut également contenir une redondance afin de satisfaire aux exigences de disponibilité. Le besoin pour de telles redondances est défini au niveau de la conception du système.

c) La conception du système doit satisfaire à toutes les exigences d'indépendance (voir 6.1.2.2.2) afin d'éviter la propagation de défaillances

   - provenant de systèmes moins importants pour la sûreté;
   - entre les voies redondantes des fonctions de catégorie A.

d) La conception des systèmes de classe 1 doit inclure les redondances nécessaires pour que les fonctions de catégorie A satisfassent au critère de défaillance unique pendant l'exploitation et la maintenance (voir point f) de 6.1.2.4).

   NOTE Les défaillances dues au logiciel sont des défaillances systématiques et non aléatoires. Ainsi, le critère de défaillance unique ne peut pas être appliqué à la conception du logiciel comme il l'est pour la conception du matériel. Les effets possibles de DCC dues au logiciel à l'intérieur de chaque ligne de défense et entre des lignes de défense redondantes sont à prendre en compte au niveau de chaque système et de l'architecture de l'I&C (voir 4.1.1 de la CEI 60880-2).

6.1.1.2.2 Comportement interne du système

a) Il convient que la conception d'un système informatique assure un comportement déterministe en accord avec les exigences de performance des fonctions mises en œuvre.

   NOTE 1 Un système informatique peut être déclaré comme ayant un comportement déterministe si la période de temps entre le stimulus et la réponse a un maximum et un minimum garantis dans toutes les conditions d'utilisation prévues (définition dérivée de la référence bibliographique [4]).

b) Les technologies de communication doivent être choisies et dimensionnées afin de satisfaire aux exigences de performance dans toutes les conditions de charge de données générés par les régimes transitoires prévisibles de la centrale (par exemple changements d'état très nombreux en cas de perte générale des alimentations électriques).

c) Afin de garantir avec un haut degré de confiance le comportement déterministe, il convient que les systèmes de classe 1 soient développés avec des techniques telles que celles mentionnées à l'annexe B de la CEI 60880 (notamment B2.*d* sur le temps d'exécution et B2.*e* sur les interruptions). Les techniques utilisant un séquencement statique des instructions (voir note 2) sont préférables à celles utilisant des interruptions.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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

6.1.1.2.1 System architecture

The architecture of the system is constrained by the category of functions to be implemented within the system (see 5.3.2) and the defence in-depth concept (see 5.2 and see 7.8.1 of IAEA 50-SG-D3).

a) The system may implement functions of the highest category allowed for its class (see 5.3.2) and functions of lower categories. The system may include subsystems of lower classes provided that the following requirements are fulfilled.

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

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

b) The design of the system shall include redundancy and other features necessary to provide tolerance to failure (see 6.1.2.2.3) and to accommodate the assignment of the application functions important to safety (see 6.1.2.4).

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

c) The design of the system shall satisfy any independence requirements (see 6.1.2.2.2) to

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

d) The design of class 1 systems shall include sufficient redundancy to meet the single-failure criterion for category A functions during operation and maintenance (see item f) of 6.1.2.4).

   NOTE Failures due to software are systematic and not random failures. Therefore, the single-failure criterion cannot be applied to the software design of a system in the same manner as it can be applied for hardware design. Possible effects of CCF due to software inside each defence layer and between redundant layers have to be considered at the level of each system and of the I&C architecture (see 4.1.1 of IEC 60880-2).

6.1.1.2.2 Internal behaviour of the system

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

   NOTE 1 A CB system may be said to have a deterministic behaviour if the time delay between stimulus and response has a guaranteed maximum and minimum under all required conditions (definition derived from bibliographical reference [4]).

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

c) In order to provide a high degree of assurance of deterministic behaviour, class 1 systems should be developed using techniques such as those of appendix B of IEC 60880 (notably B2.*d* on execution time and B2.*e* on interrupts). Techniques using static scheduling of operations (see note 2) are preferable to those using interrupts.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

NOTE 2 Statique se définit comme relatif à un événement ou processus intervenant sans l'exécution du programme informatique (IEEE 610). Ainsi, avec cette technique, la séquence des instructions ne dépend pas du fonctionnement de l'ordinateur, bien qu'il puisse y avoir un nombre fini de séquences différentes dépendant du chemin d'exécution.

NOTE 3 Voir l'article 1 de la CEI 60880 concernant le rôle des annexes à la norme et les prescriptions applicables si les pratiques diffèrent de celles mentionnées dans les annexes.

d) Les systèmes de classe 2 peuvent être développés avec des techniques autres que celles définies au point c). Dans ce cas, il convient que la conception du système garantisse un comportement adéquat dans toutes les conditions d'exploitation prévues de la centrale.

e) Pour augmenter l'aptitude des systèmes de classe 1 et 2 à supporter des situations imprévues:

- la suffisance des marges de conception fixées pour l'utilisation des ressources (du type puissance de l'unité centrale, mémoire, largeur de la bande de communication, ressources des systèmes opérationnels), ainsi que les temporisations internes au sein du système doit être justifiée;
- il convient que des dispositifs soient prévus pour surveiller tout écart au comportement déterministe et pour reconstituer l'état réel de la centrale en cas de pertes temporaires des informations d'entrée, par exemple chiens de garde, rafraîchissement cyclique en parallèle à la détection des événements sur changement d'état.

6.1.1.2.3 Auto-surveillance et tolérance aux défaillances

a) Il convient que les systèmes soient conçus de telle manière que les erreurs et défaillances soient détectées suffisamment tôt pour assurer la disponibilité requise pour le système, et que la détection des défaillances par les dispositifs d'autocontrôle soit mise en regard de la complexité supplémentaire qui est introduite. Il convient que les exigences de 4.8 et de A2.8 de la CEI 60880 relatives à l'auto-surveillance soient remplies autant que possible pour chaque classe de système.

b) Il convient que des informations adéquates, opportunes et correctement mises en valeur concernant les défaillances soient transmises aux opérateurs de la centrale afin qu'ils puissent prendre les mesures correctives appropriées.

c) Il convient que la conception du système garantisse l'établissement d'un mode de fonctionnement approprié en cas de détection de défaillances (dégradation progressive).

d) Pour les systèmes de classe 1, les installations d'autocontrôle doivent être conformes aux prescriptions de la CEI 60880 et de la CEI 60987.

6.1.1.2.4 Testabilité

a) Les systèmes doivent être munis de dispositifs permettant de vérifier qu'ils sont en mesure d'accomplir leurs fonctions importantes pour la sûreté.

NOTE 1 Conformément à l'AIEA (voir 4.12 de l'AIEA 50-SG-D8), les essais sont de préférence des vérifications d'ensemble depuis les capteurs en entrée jusqu'aux actionneurs en sortie, mais les essais de chevauchement sont acceptables. Les essais incluent notamment

a) la modification de l'état ou de la valeur de tout signal d'entrée et la surveillance des modifications au niveau de l'équipement récepteur;

b) l'interruption de la transmission, et la confirmation que l'équipement récepteur détecte cette interruption et effectue une action appropriée;

c) le contrôle et l'étalonnage des capteurs (voir 7.10.2 de l'AIEA 50-SG-D3);

d) le contrôle de la mise en marche des actionneurs en sortie (voir 7.10.3 de l'AIEA 50-SG-D3).

b) Les intervalles de temps entre les essais doivent être spécifiés par les plans d'exploitation et de maintenance du système (voir 6.2), en accord avec la fiabilité requise pour les fonctions (voir 4.5 de AIEA 50-SG-D8), la fiabilité des composants et le taux estimé de dérive de l'étalonnage.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

NOTE 2 Static is defined as pertaining to an event or process that occurs without computer program operation (IEEE 610). Thus, in static scheduling, the scheduling of an instruction does not depend upon the computer operation – although there might be a finite number of different schedules depending upon the execution path.

NOTE 3 See clause 1 of IEC 60880 concerning the role of the appendices to the standard and what is required if practices differing from those of the appendices are used.

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

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

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

6.1.1.2.3 Self-monitoring and tolerance to failures

a) Systems should be designed so that errors and failures are detected sufficiently early to maintain the required system availability. The detection of failures by self-test facilities should be balanced against the complexity that is introduced. The requirements of 4.8 and A2.8 of IEC 60880 on self-supervision should be supported as far as possible for each class of system.

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

c) The design of the system should enable the safe restoration to an appropriate back-up mode of operation when failures are detected (graceful degradation).

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

6.1.1.2.4 Testability

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

NOTE 1 In accordance with IAEA (see 4.12 of IAEA 50-SG-D8), tests are preferably overall checks from the input sensors to the output actuation, but overlapping tests are acceptable. Tests include notably

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

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

c) testing and calibration of sensors (see 7.10.2 of IAEA 50-SG-D3);

d) testing of output actuation (see 7.10.3 of IAEA 50-SG-D3).

b) Test intervals shall be specified by the system operation and maintenance plans (see 6.2), based on the required reliability of the functions (see 4.5 of IAEA 50-SG-D8), the equipment reliability, and expected calibration drift rate.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

c) Lorsque les intervalles de temps entre les essais sont tels qu'un contrôle périodique du système pendant l'exploitation est nécessaire, la conception du système doit inclure des dispositifs permettant ces essais et étalonnages en exploitation.

NOTE 2 L'utilisation de dispositifs automatiques facilite le contrôle périodique. Ce type de dispositif permet d'injecter en entrée des signaux simulés, d'enregistrer les sorties obtenues et de comparer les sorties observées et prévues.

d) La conception des systèmes de classe 1 ainsi que leurs moyens d'essai doivent assurer la sûreté de la centrale pendant les essais. Il convient de minimiser le risque de déclenchement inopportun d'une action de sauvegarde et tout autre effet négatif des essais sur la disponibilité de la centrale. La méthode d'essai doit minimiser la durée pendant laquelle une voie de protection n'est plus en service.

6.1.1.2.5 Maintenabilité

a) Le système doit être conçu de telle manière qu'il facilite la maintenance et, en cas de défaillance, un diagnostic aisé, une réparation ou remplacement sûr et le ré-étalonnage (voir 4.5 de l'AIEA 50-SG-D8).

b) Les capacités et limites humaines en regard des facteurs environnementaux doivent être prises en compte afin de minimiser le risque et la charge de travail pour le personnel pendant la maintenance.

c) Le système doit être conçu de manière à permettre la vérification de la réparation et du ré-étalonnage. Il convient que cela inclue la vérification de

- la restauration correcte de la continuité des circuits;
- l'étalonnage correct des mesures analogiques et de tout seuil d'alarme associé;
- l'aptitude du système à effectuer ses fonctions importantes pour la sûreté comme prévu dans les spécifications.

NOTE Les prescriptions relatives à la maintenance et aux essais de l'article 10 de la CEI 60987 s'appliquent aux systèmes informatiques importants pour la sûreté. Les articles 7.10 (Testabilité), 7.11 (Contournements opérationnels), 7.12 (Contrôle d'accès) de l'AIEA 50-SG-D3 s'appliquent aux systèmes informatiques de classe 1. Les articles 4.5 (Testabilité) et 4.6 (Maintenabilité) de l'AIEA 50-SG-D8 s'appliquent aux systèmes informatiques de classe 2.

6.1.1.3 Limites et interfaces avec les autres systèmes et outils

Afin d'assurer l'intégration du système dans l'architecture de l'I&C, les aspects suivants doivent être spécifiés conformément aux prescriptions correspondantes de l'article 5:

- l'emplacement prévu et les contraintes physiques relatives à l'installation du système dans la centrale (voir 5.1.3);
- les interfaces physiques et fonctionnelles du système avec les systèmes et équipements de soutien (voir 5.1.3);
- les interfaces physiques et fonctionnelles du système avec les autres systèmes et équipements avec lesquels il échange des informations (voir 5.3.1.3);
- les interfaces avec les outils logiciels utilisés pour définir les échanges de données entre systèmes et pour vérifier la cohérence de ces données (voir 5.3.1.4).

6.1.1.4 Interfaces avec les utilisateurs

Les exigences relatives à l'IHM doivent minimiser le risque d'erreur humaine, par exemple les erreurs d'inadvertance, oublis et omissions, pendant l'installation, l'exploitation, les essais et la maintenance du système et de la centrale, ou lors de l'introduction de modifications.

NOTE La protection contre les modifications malintentionnées est traitée dans le plan de sécurité (voir 6.2.2).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

c) When test intervals are such that periodic testing of the system during operation is required, the system design shall include test and calibration facilities which enable such in-service tests.

NOTE 2 The use of automatic equipment facilitates periodic testing. This type of equipment may inject simulated input signals, record the resulting output states, and compare the observed and expected outputs.

d) The design of class 1 systems and their test provisions shall ensure the safety of the plant during the actual testing and should minimise spurious initiation of any safety action and any other adverse impact of the test on the plant availability. The test method shall minimise the time during which a line of protection is removed from service.

6.1.1.2.5 Maintainability

a) The system shall be designed in such a way that it facilitates maintenance and, in case of failure, easy diagnosis, safe repair or replacement, and re-calibration (see 4.5 of IAEA 50-SG-D8).

b) Human capabilities and limitations in relation to the environmental factors shall be taken into account to minimise the risk to, and workload on personnel during maintenance.

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

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

NOTE The maintenance and testing requirements of clause 10 of IEC 60987 apply to CB systems important to safety. Clauses 7.10 (Testability), 7.11 (Operational bypasses), 7.12 (Control of access) of IAEA 50-SG-D3 apply to CB systems of class 1. Clauses 4.5 (Testability), and 4.6 (Maintainability) of IAEA 50-SG-D8 apply to CB systems of class 2.

6.1.1.3 Boundaries and interfaces with other systems and tools

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

- the intended location and the physical constraints relevant to the installation of the system in the plant (see 5.1.3);
- the physical and functional interfaces of the system with the supporting systems and equipment (see 5.1.3);
- the physical and functional interfaces of the system with other systems and equipment with which it exchanges information (see 5.3.1.3);
- the interfaces with software tools used to define the exchange of data between systems and the verification of consistency of such data (see 5.3.1.4).

6.1.1.4 Interfaces with users

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

NOTE Protection against malicious modifications is handled in the security plan (see 6.2.2).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

6.1.1.5 Conditions liées à l'environnement

Les plages de variation normale et extrême des conditions environnementales auxquelles le système est tenu de résister doivent être spécifiées en fonction des contraintes imposées par la centrale (voir 5.1.3). Les conditions à spécifier incluent

- les conditions ambiantes, notamment la température, l'humidité, la pression, le rayonnement et les interférences électromagnétiques pendant le fonctionnement normal et les situations accidentelles;

  NOTE 1 Les conditions ambiantes pour l'IEM sont définies conformément aux CEI 61000-4-1 à CEI 61000-4-6.

- les conditions ambiantes imposées par les événements dangereux potentiels externes au système, en particulier les séismes;
- les conditions de l'alimentation électrique et de l'évacuation de la chaleur.

  NOTE 2 Les prescriptions relatives aux alimentations électriques des systèmes d'I&C importants pour la sûreté sont définies conformément à la CEI 61225.

6.1.1.6 Qualification

Les systèmes de la classe 1 et 2 doivent être qualifiés. Pour les systèmes informatiques, cette qualification comprend le matériel, le logiciel système et le logiciel d'application, tous deux intégrés dans le matériel (voir 6.4).

6.1.2 Spécification du système

L'objectif de cette phase est de fournir une description optimale de l'architecture du matériel et du logiciel du système, de spécifier les équipements à utiliser ou développer pour sa mise en œuvre et d'affecter les fonctions d'application.

Les exigences relatives au système et la documentation des composants candidats préexistants font partie des informations pour la spécification du système.

La documentation résultant de cette phase (voir 6.3.2) constitue une entrée pour la réalisation du système (matériel et logiciel) au cours des phases ultérieures du cycle de vie du système.

Conformément à l'article A.1 de la CEI 60880, cette phase inclut les activités nécessaires à la définition des exigences relatives au logiciel, au matériel et à l'intégration du système.

La spécification du système doit définir

- les composants à utiliser;
- l'architecture du système;
- les exigences relatives au logiciel;
- l'affectation des fonctions d'application dans les sous-systèmes.

6.1.2.1 Sélection des composants préexistants

Il n'est pas rare d'utiliser des composants préexistants (composants matériels ou logiciels spécifiques ou composants d'une famille d'équipements) pour réaliser tout ou partie d'un «nouveau» système.

NOTE 1 Les composants préexistants peuvent être des composants sur étagère du commerce (également appelés «COTS») ou des produits utilisés en interne par des fabricants.

NOTE 2 Le paragraphe 4.3 de la CEI 60880-2 traite des critères d'acceptation de logiciels préexistants réutilisables pour les fonctions de catégorie A.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

6.1.1.5 Environmental conditions

The normal and extreme ranges of environmental conditions that the system is required to withstand shall be specified in accordance with the constraints imposed from the plant context (see 5.1.3). Environmental conditions to be specified include

- ambient conditions, including, temperature, humidity, pressure, radiation, and electro-magnetic interference, during normal operation and accident conditions;

  NOTE 1 Ambient conditions for EMI are defined in accordance with IEC 61000-4-1 to IEC 61000-4-6.

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

  NOTE 2 Requirements for electrical supplies of I&C systems important for safety are defined in accordance with IEC 61225.

6.1.1.6 Qualification

Class 1 and 2 systems shall be qualified. For CB systems, this qualification includes the hardware, the system software and the application software, both integrated in the hardware (see 6.4).

6.1.2 System specification

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

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

The output documentation of this phase (see 6.3.2) forms the input for the activities which are to implement the combined hardware and software system during the subsequent phases of the system life cycle.

In accordance with clause A.1 of IEC 60880, this phase includes the activities necessary to produce the software requirements, the hardware requirements, and the integration requirements of the system.

The system specification shall define

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

6.1.2.1 Selection of pre-existing components

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

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

NOTE 2 Subclause 4.3 of IEC 60880-2 addresses acceptance criteria for reusable pre-existing software for category A functions.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

a) L'adéquation des composants candidats doit être évaluée et estimée afin de démontrer que leurs caractéristiques sont conformes aux exigences du système.

b) Il convient que l'évaluation et l'estimation des composants candidats reposent sur la comparaison de deux séries de documents: les spécifications des exigences du système et la documentation des composants préexistants. Cette dernière inclut les spécifications et (si disponibles) les rapports de qualification.

c) Les prescriptions suivantes s'appliquent:

- la documentation doit définir explicitement les fonctionnalités et les propriétés de tous les composants;

NOTE Cela inclut les temps d'exécution et les besoins en mémoire des composants logiciels, les taux de défaillance des composants matériels, les conditions environnementales du système et les exigences relatives au montage des armoires, au câblage et aux connexions à l'alimentation électrique, à la consommation électrique et aux outils de service.

- les propriétés qui, initialement, ne sont pas définies explicitement doivent le devenir après détermination par analyses ou essais;
- la documentation doit permettre de déterminer la fiabilité et la performance des fonctions d'application de la centrale dans la ou les configurations prévues des composants;
- la documentation doit définir la fonctionnalité et les propriétés des méthodes et outils d'ingénierie logicielle associés;
- les fonctions non utilisées (c'est-à-dire celles contenues dans des équipements mais qui ne seront pas utilisées) doivent être identifiées. Il doit être démontré que ces fonctions ne peuvent compromettre les fonctions demandées.

d) Lorsque des différences entre les exigences du système et la spécification des composants candidats sont identifiées et rendent les composants inadaptés à la classe du système, ceux-ci doivent être rejetés. L'estimation de l'adéquation doit établir que la spécification des composants candidats est conforme à leur utilisation prévue comme défini par les exigences du système (voir 6.3.2.2).

e) Pour les systèmes de classe 1 et 2, la faisabilité de la qualification conformément aux exigences de 6.4 doit être vérifiée.

f) Si une pré-qualification est mise en avant, les propriétés démontrées doivent être identifiées explicitement. Le supplément de travail nécessaire pour la qualification spécifique à la centrale doit également être identifié.

6.1.2.2 Architecture du système

L'architecture divise le système en sous-systèmes et composants interconnectés qui fournissent la redondance requise et des capacités de reconfiguration. L'objectif de cette partition est de parvenir à une configuration optimale simple du matériel et du logiciel qui satisfasse aux exigences de fonctionnalité et de performances et qui soit conforme aux exigences de fiabilité et de maintenance.

L'organisation des sous-systèmes doit

- satisfaire aux prescriptions de 6.1.1.2;
- permettre la conformité aux exigences relatives à l'affectation des fonctions d'application (voir 6.1.2.4);
- être en accord avec les exigences de fiabilité des fonctions d'application importantes pour la sûreté (voir 6.1.1.1.1).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

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

c) The following requirements apply:

- the documentation supplied shall define explicitly the functionality and properties of all components;

NOTE This includes run time and memory consumption of software components, failure rates for the components, environmental conditions for the system configuration, requirements for the mounting in cabinets, for wiring and connections to power supply, power consumption, service tools.

- those properties that are not explicitly defined shall be determined by analysis or test and made explicit;
- the documentation shall allow the reliability and performance to be determined for the plant application functions in the anticipated configuration(s) of components;
- the documentation shall define the functionality and properties of the associated software engineering methods and tools;
- unused functions (i.e. functions that are included in the equipment, but that are not going to be used) shall be identified. It shall be demonstrated that these functions cannot jeopardise the required functions.

d) If discrepancies between the requirements specification of the system and the equipment family specification are identified which render the equipment unsuitable for the intended system class, the equipment shall be rejected. The assessment of the suitability shall establish that the specification of the candidate equipment complies with its intended use as defined by the system requirements specification (see 6.3.2.2).

e) For class 1 and 2 systems, the feasibility of qualification in accordance with the requirements of 6.4 shall be verified.

f) If pre-qualification is claimed, the properties included in this qualification shall be explicitly identified. The additional work necessary for plant specific qualification shall also be identified.

6.1.2.2 System architecture

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

The arrangement of system subsystems shall

- satisfy the design constraints of 6.1.1.2;
- allow the requirements on functional assignment of the application functions to be met (see 6.1.2.4);
- be consistent with the reliability requirements of the application functions important to safety (see 6.1.1.1.1).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.1.2.2.1 Répartition géographique des sous-systèmes (centralisés/décentralisés)

a) Lors de la définition des emplacements géographiques des sous-systèmes dans la centrale et des chemins de transmission de données entre ces sous-systèmes, il convient que les facteurs suivants soient pris en compte:

- la séparation des voies redondantes d'un équipement dont le vote est majoritaire peut être nécessaire afin de réduire l'effet d'événements dangereux localisés tels que les incendies, et de respecter le critère de défaillance unique lorsqu'il est demandé (voir 6.1.1.2.1);
- la centralisation des fonctions importantes pour la sécurité peut être nécessaire pour respecter la prescription relative au contrôle des accès non autorisés (voir 5.4.2);
- la centralisation des composants complexes peut faciliter l'exploitation, les essais périodiques, la maintenance et la maîtrise des conditions d'environnement;
- l'utilisation de transmissions de données multiplexées peut réduire la complexité du câblage.

b) Pour les systèmes de classe 1, il convient d'utiliser des transmissions de données redondantes pour les informations provenant d'endroits auxquels on ne peut normalement pas accéder (par exemple l'enceinte de confinement du réacteur). Les prescriptions relatives au multiplexage figurent dans la CEI 61500.

6.1.2.2.2 Indépendance

Le principe d'indépendance prévoit des dispositions pour éviter les interactions néfastes entre les sous-systèmes du système, ou avec d'autres systèmes, dues à un fonctionnement anormal ou à la défaillance de composants du système ou de sous-systèmes. Ces interactions peuvent aussi être causées par l'induction électromagnétique, des courts-circuits, des défauts de mise à la terre, des incendies, des explosions chimiques, des chutes d'avion et la propagation de données altérées.

a) Lorsque l'indépendance est demandée (voir 6.1.1.2.1), il convient qu'elle soit atteinte en utilisant

- l'isolation électrique, qui peut être réalisée par des fibres optiques, des isolateurs optiques et le blindage des câbles;
- la séparation physique, qui peut être réalisée par la mise à distance, des barrières ou bien une combinaison des deux;
- pour les systèmes informatiques, l'indépendance des communications, qui peut être réalisée en sélectionnant des architectures et protocoles de communication appropriés (voir également 5.3.1.3).

NOTE 1 Les prescriptions relatives à l'isolation électrique et à la séparation physique figurent en 4.3 de l'AIEA 50-SG-D8 et en 7.8 de l'AIEA 50-SG-D3.

b) Dans un système de classe 1, la séparation physique et l'isolation électrique entre sous-systèmes de différentes voies doivent être conformes aux prescriptions de la CEI 60709.

c) La séparation et l'isolation entre un système de classe 1 et les systèmes et composants non importants pour la sûreté doivent être conformes aux exigences de la CEI 60709.

NOTE 2 La méthode privilégiée pour la séparation physique et la protection des câbles d'un système de sûreté, véhiculant ou non des signaux électriques ou optiques, est l'utilisation de boîtiers ou de goulottes de câbles particuliers garantissant une protection totale contre les événements dangereux.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.1.2.2.1 Geographical distribution of subsystems (centralised/decentralised)

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

- the separation of redundant channels of majority voted equipment may be necessary to reduce the effect of localised hazards such as fire, and to meet the single failure criterion when this is required (see 6.1.1.2.1);
- the centralisation of functions important to security may be necessary to meet the requirement on control of unauthorised access (see 5.4.2);
- the centralisation of complex equipment may facilitate operation, periodic testing, maintenance, and environmental control;
- the use of multiplexed data transmission may reduce cabling complexity.

b) For class 1 systems, redundant means of data transmission should be used for information from locations which cannot normally be accessed (for example the reactor containment). The requirements for multiplexed transmission are given in IEC 61500.

6.1.2.2.2 Independence

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

a) When independence is required (see 6.1.1.2.1), it should be achieved by using

- electrical isolation, which can be achieved by fibre optics, optical isolators, cable shields;
- physical separation, which can be achieved by distance, barriers, or combination of the two;
- independence of communication for CB systems, which can be achieved by selecting appropriate data communication architectures and protocols (see also 5.3.1.3).

NOTE 1 Requirements for electrical isolation and physical separation are given in 4.3 of IAEA 50-SG-D8 and 7.8 of IAEA 50-SG-D3.

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

c) The separation and isolation between a class 1 system, and systems and equipment not important to safety, shall meet the requirements of IEC 60709.

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.1.2.2.3 Défense contre la propagation et les effets secondaires des défaillances

Outre la propagation de défaillances, qui peut être évitée par l'indépendance, d'autres types de propagation de défaillances doivent être pris en compte pour les systèmes informatiques. Par exemple:

- la préemption non intentionnelle de ressources partagées (puissance de traitement, largeur de bande de communication, mémoire, ressources des systèmes d'exploitation, etc.);
- la non-libération des ressources préemptées;
- la perte de la synchronisation au sein du système ou de l'architecture de l'I&C.

Par ailleurs, un défaut dans le logiciel d'un programme, qui l'empêche d'accomplir une fonction particulière, peut engendrer des défaillances dans d'autres programmes supportant d'autres fonctions dans le même système (effets secondaires). La défaillance peut provenir d'erreurs dans les données, les programmes, ou les matériels partagés par des fonctions différentes. Par exemple, un processeur provoque la défaillance d'autres fonctions en raison d'exceptions ou de boucles sans fin dans une fonction.

Il convient que l'architecture du système minimise le risque et les conséquences de la propagation et des effets secondaires des défaillances. On peut considérer les techniques suivantes:

- l'isolation interne, qui bloque la propagation des défaillances par le manque de chemins de propagation et de ressources partagées;
- la surveillance du système par des moyens internes (c'est-à-dire l'auto-surveillance) ou externes (c'est-à-dire d'autres systèmes ou l'opérateur), permettant une détection rapide des données altérées et/ou des ressources détériorées;
- les interfaces défensives, permettant au système et à ses sous-systèmes d'identifier les informations d'entrée altérées et/ou les interactions erronées;
- la validation en ligne des signaux d'entrée redondants utilisés comme informations d'entrée pour les traitements suivants;
- les modes de comportement bien définis qu'il convient d'utiliser lorsque des défaillances sont détectées, permettant au système de réduire son potentiel de propagation de défaillances et/ou de leurs effets.

NOTE Les prescriptions détaillées pour éviter les structures logicielles prédisposées aux erreurs et pour vérifier et tester les modules logiciels figurent dans la CEI 60880 et la CEI 60880-2.

6.1.2.3 Spécification du logiciel

La spécification du logiciel contient

- la spécification des fonctions d'application (spécifications du logiciel d'application);
- la spécification de l'architecture du logiciel système;

  NOTE 1 L'architecture du logiciel définit les principaux composants et sous-systèmes du logiciel, leur interconnexion et la manière dont les caractéristiques exigées seront atteintes. Les prescriptions relatives à l'architecture du logiciel sortent du cadre de la présente norme (pour les systèmes de classe 1, se référer à la CEI 60880 et la CEI 60880-2).

- la spécification des fonctions de service et des fonctions du logiciel système.

  NOTE 2 Lorsque des familles d'équipements préexistants sont utilisées, les spécifications du logiciel système font essentiellement partie de la documentation des équipements.

a) Afin de faciliter la spécification, la vérification et la validation des fonctions d'application, il convient que l'architecture du logiciel prévoie une séparation claire entre le logiciel d'application et le logiciel système (voir B2.*a* de la CEI 60880). Dans ce cas, la vérification et la validation de la spécification du logiciel d'application peuvent être effectuées indépendamment.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.1.2.2.3 Defence against propagation and side-effects of failures

Beside propagation of failures, which may be prevented by independence, other types of failure propagation have to be considered in CB systems, for example:

- unintended pre-emption of shared resources (processing power, communication bandwidth, memory, operating system resources, etc.);
- failure to release pre-empted resources;
- disruption of synchronisation within the system or within the I&C architecture.

Furthermore, a fault in a software program, which prevents it performing a particular function, may lead to failures of other programs implementing other functions in the same system (side-effects). The failure may result from faults in the common data, programs or hardware used for different functions, for example, a processor causes other functions to fail due to exceptions or endless loops of one function.

The system architecture should minimise the risk and the consequences of failure propagation and side-effects of failures. The following techniques may be considered:

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

NOTE Detailed requirements for avoidance of error-prone software structures and for verification and tests of software modules are given in IEC 60880 and IEC 60880-2.

6.1.2.3 Software specification

The software specification includes

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

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

- specification of the service functions and system software functions.

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

a) In order to facilitate the specification, verification and validation of the application functions, the software architecture should provide a clear separation between the application software and the system software (see B2.*a* of IEC 60880). In such cases, the verification and validation of the application software may be performed independently.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

b) La spécification du logiciel d'application doit être déduite des exigences relatives aux fonctions d'application (voir 6.1.1.1). Elle est complétée, lorsque nécessaire, en introduisant les relations avec les fonctions de commande et de surveillance du système.

c) Afin de réduire les erreurs de spécification et l'effort de vérification, il convient que le logiciel d'application soit spécifié autant que possible à l'aide de fonctions élémentaires standard.

NOTE 3 Avec des équipements préexistants, le logiciel d'application peut être bien souvent spécifié et développé avec des outils appropriés et en utilisant des composants préexistants réutilisables d'une bibliothèque d'application logicielle.

d) Le filtrage des signaux, leur validation et les verrouillages doivent être spécifiés pour la réalisation des modes de secours et la minimisation du risque d'actions inopportunes.

6.1.2.4 Affectation des fonctions d'application dans le système

Cela inclut l'affectation

- des signaux d'entrée aux fonctions et des fonctions à des processeurs spécifiques;
- du processus de vote, de la gestion des priorités, des fonctions de protection des composants;
- des liens entre les actions de commande des sorties et les actionneurs.

a) L'affectation des fonctions d'application importantes pour la sûreté au système et aux sous-systèmes doit respecter la spécification des exigences de fonctionnalité, performance et catégorisation des fonctions (voir 6.1.1.1.1).

b) L'affectation doit être effectuée en tenant compte du confinement des défaillances.

c) Il convient que les fonctions redondantes et les signaux importants pour la sûreté ne soient pas traités dans le même sous-système ni envoyés via la même voie de transmission multiplexée afin qu'en cas de survenance d'une défaillance ou d'un événement dangereux localisé dans une voie, le système puisse encore accomplir ses fonctions.

d) Les fonctions de différentes catégories affectées au même système ou sous-système doivent toutes être considérées comme appartenant à la catégorie de sûreté la plus élevée, sauf s'il est démontré que des données et fonctions de catégories inférieures ne peuvent compromettre les fonctions des catégories supérieures, par exemple arrêter ou déclencher de manière intempestive l'une de ces dernières. Cela peut conduire à répartir les fonctions dans différents sous-systèmes, ou à affecter les fonctions de catégories inférieures dans d'autres systèmes (itération avec l'allocation des fonctions d'I&C – voir 5.3).

e) Pour les fonctions de catégorie A, les traitements redondants ne doivent pas être effectués dans les mêmes sous-systèmes et les données redondantes ne doivent pas être envoyées via les mêmes voies de transmission.

f) Pour les fonctions de catégorie A, le critère de défaillance unique doit être rempli au cours de l'exploitation, même lorsqu'une voie redondante est isolée pour cause de maintenance.

6.1.3 Conception détaillée et réalisation du système

L'objectif de cette phase est de

- développer et obtenir la conception détaillée du matériel du système;
- développer (conception et codage) et obtenir les programmes informatiques qui constituent le logiciel système opérationnel et de soutien;

NOTE 1 La situation normale (voir 6.1.2.2) veut que les nouveaux développements soient limités, par exemple interfaces avec les autres systèmes.

- développer (conception et codage) et produire le logiciel d'application du système.

NOTE 2 En utilisant des familles d'équipements préexistants, le code du logiciel d'application est bien souvent généré automatiquement à partir de la spécification du logiciel d'application (voir 6.1.2.3).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

b) Specification of the application software shall be derived from the application functions requirements specification (see 6.1.1.1). The specification is expanded, where appropriate, by introducing the relations with the control and monitoring functions of the system.

c) In order to reduce specification errors and the verification effort, the application software of the individual application functions should be specified as far as possible by configuration and instantiation of components of standard proven functionality.

NOTE 3 It is common with pre-existing equipment that the application software may be specified and developed with appropriate tools using pre-existing reusable components of an application software library.

d) Appropriate signal filtering, signal validation and interlocks shall be specified to implement back-up modes of operation and to minimise the potential of spurious actions.

6.1.2.4 Assignment of the application functions in the system

This includes assignment of

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

a) The assignment of the application functions important to safety to the system and subsystems shall meet the functional, performance and categorization requirements specification of the functions (see 6.1.1.1.1).

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

c) Redundant functions and signals important to safety should not be processed in the same subsystem so that if a failure or a localised hazard occurs in one channel, the system can still perform its functions.

d) Functions of different categories assigned to the same system or subsystem shall all be considered as being of their highest safety category, except if it can be demonstrated that lower category data and functions cannot jeopardise higher category functions, for example, by stopping or causing spurious actuation of the higher category function. This may lead to the separation of the functions in different subsystems or to the decision to implement the lower category functions in other systems (iteration process with the overall assignment – see 5.3).

e) For category A functions, redundant processing shall not be performed in the same subsystems and redundant data shall not be sent over the same transmission paths.

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

6.1.3 System detailed design and implementation

The objective of this phase is

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

NOTE 1 The normal situation (see 6.1.2.2) is that there are only limited new developments, for example, interfaces to other systems.

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

NOTE 2 It is common, when using pre-existing equipment families, that the application software code is automatically generated by tools from the application software specification (see 6.1.2.3).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

La documentation de spécification du système et le plan d'intégration du système sont les principales informations pour la phase de conception détaillée et de réalisation.

Les résultats de cette phase sont

- les sous-systèmes et composants matériels et logiciels pour la phase suivante d'intégration du système;
- les programmes informatiques.

Le développement et l'obtention du matériel et du logiciel font partie des cycles de vie du matériel et du logiciel et sortent ainsi du cadre de la présente norme.

Pour les systèmes de classe 1, les prescriptions relatives au développement du logiciel figurent dans la CEI 60880 et la CEI 60880-2, et les prescriptions relatives au matériel dans la CEI 60987.

6.1.3.1 Analyses requises

6.1.3.1.1 Validation fonctionnelle de la spécification des exigences relatives aux fonctions d'application

La validation fonctionnelle a pour objectif de détecter les erreurs ou omissions dans la spécification des fonctions d'application qui peuvent ne pas être détectées par la validation du système (voir 6.1.5). La validation fonctionnelle implique la modélisation des actionneurs et de l'exploitation de la centrale nucléaire.

a) Il convient que la conformité de la spécification des fonctions d'application aux exigences de fonctionnalité et de performance des fonctions la centrale (voir 5.1.1) soit validée pour les fonctions de catégorie A.

b) Le logiciel d'application final produit par la conception détaillée ainsi qu'un environnement matériel adéquat doivent être utilisés pour cette tâche.

6.1.3.1.2 Estimation de la fiabilité

a) La fiabilité des fonctions d'application supportées par le système doit être justifiée, et il convient que la rigueur de la démonstration soit plus forte pour les fonctions de la catégorie la plus élevée:

   - il convient que la démonstration repose sur un équilibre entre critères déterministes et analyse quantitative de la fiabilité;
   - l'effet d'éventuelles défaillances du matériel sur la fiabilité de la fonction doit être déterminé par une analyse probabiliste quantitative reposant sur le taux de défaillances des composants. L'analyse englobe l'architecture du système et les composants, et il convient qu'elle prenne en compte les défaillances permanentes et transitoires;
   - il convient que l'estimation des effets des erreurs de conception potentielles du logiciel sur la fiabilité de la fonction repose sur une évaluation qualitative, tenant compte de la complexité de la conception, de la qualité du processus de développement et du retour d'informations sur l'expérience opérationnelle. Il convient que l'évaluation repose sur une méthode préalablement convenue et démontre que la qualité du logiciel correspond à la fiabilité voulue.

   NOTE Les résultats de l'analyse et des essais de simulation pourraient être utilisés pour une évaluation quantitative, mais il n'existe aucune méthode reconnue qui puisse être utilisée. Pour les systèmes câblés, aucune quantification des défaillances provenant de défauts de conception n'a généralement été donnée.

b) La capacité des fonctions de service du système à perturber les fonctions d'application doit être analysée avec une rigueur adaptée à l'importance pour la sûreté des fonctions d'application.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

The outputs of this phase are

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

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

For class 1 systems, requirements on software development are established in IEC 60880 and IEC 60880-2, the hardware requirements are in IEC 60987.

6.1.3.1 Required analysis

6.1.3.1.1 Functional validation of the application functions requirements specification

Functional validation aims to detect errors or omissions in the application function specification which may not be detected by the system validation (see 6.1.5). Functional validation involves modelling of actuation equipment and NPP operation.

a) The correctness of the application function specification versus the functional and performance requirements of the plant functions (see 5.1.1) should be validated for functions of category A.

b) The final application software generated in the detailed design and an adequate hardware environment shall be used for the validation.

6.1.3.1.2 Reliability assessment

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

c) Si la fonction réalisée par le système fait partie d'un groupe de sûreté et que des exigences de fiabilité sont demandées à ce groupe par l'architecture de l'I&C (voir 5.3.3.1), l'analyse de fiabilité doit prendre en compte les effets des défaillances uniques, des DCC et de la propagation des défaillances au sein de tous les systèmes contribuant à ce groupe.

d) Pour les systèmes de classe 1, l'analyse de fiabilité doit également estimer la conformité des dispositifs de test du système aux prescriptions de 6.1.1.2.4.

6.1.4 Intégration du système

L'objectif de cette phase est d'assembler les modules matériels et logiciels et de vérifier la compatibilité du logiciel chargé dans le matériel (voir l'article 7 de la CEI 60880).

Les sous-systèmes et composants du système, la documentation de conception détaillée et le plan d'intégration du système constituent les principales informations pour la phase d'intégration du système.

Le système intégré fait partie des résultats de cette phase.

a) L'intégration doit être réalisée conformément au plan d'intégration défini en 6.2.3.

b) Les exigences de performance doivent être vérifiées lorsque tous les logiciels d'application (développés avec les outils de la famille d'équipements ou bien développés spécialement) ont été intégrés dans le système.

c) Au cours de la phase d'intégration, des cas de test doivent démontrer que chaque fonction d'application accomplit sa tâche.

NOTE En fonction des techniques de conception utilisées pour assurer le comportement déterministe du système (voir 6.1.1.2.2), il peut être nécessaire de passer des cas de test prévoyant des données aléatoires avec des variations importantes en entrée des autres fonctions du système.

6.1.5 Validation du système

L'objectif de cette phase est de tester le système intégré afin de démontrer la conformité aux spécifications de fonctionnalité, de performance et d'interface (voir l'article 8 de la CEI 60880).

Le système intégré, la spécification du système et le plan de validation du système constituent les principales informations pour la phase de validation du système.

a) La validation doit être réalisée conformément au plan de validation défini en 6.2.4.

b) Les prescriptions de l'article 8 de la CEI 60880 doivent être appliquées pour valider les fonctions de catégorie A.

c) Les prescriptions de l'article 8 de la CEI 60880 doivent être appliquées pour valider les fonctions de catégorie B et C, avec les amendements suivants:

- le même niveau de détail doit être appliqué mais l'étendue des essais peut être réduite conformément aux objectifs de sûreté des fonctions importantes pour la sûreté;
- l'indépendance entre l'équipe en charge de l'analyse des essais de validation et les l'équipe de conception n'est pas demandée.

6.1.6 Installation du système

L'objectif de cette phase est d'installer, d'interconnecter et de tester le système sur site.

Les activités suivantes, relatives à l'intégration globale du système aux autres systèmes et à la mise en service globale font partie du cycle de vie et de sûreté global de l'I&C (voir l'article 7).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

c) Where the function performed by the system is part of a safety group and there are reliability requirements placed by the I&C architecture on this safety group (see 5.3.3.1), the reliability analysis shall take into account the effects of single failures, CCFs and propagation of failures within all the systems contributing to this safety group.

d) For class 1 systems, the reliability analysis shall also assess the adequacy of the test facilities of the system with respect to the requirements of 6.1.1.2.4.

6.1.4 System integration

The objective of this phase is to assemble the hardware and software modules and to verify compatibility of the software loaded into the hardware (see clause 7 of IEC 60880).

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

The outputs of this phase include the integrated system.

a) Integration shall be performed in accordance with the integration plan defined in 6.2.3.

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

c) In the integration phase, there shall be test cases which demonstrate that each selected application function performs its task.

NOTE Depending on the design techniques used to ensure the deterministic behaviour of the system (see 6.1.1.2.2), test cases including random data with high rates of change as inputs of the other functions inside the same CB system may be necessary.

6.1.5 System validation

The objective of this phase is to test the integrated system to demonstrate compliance with the functional, performance and interface specifications (see clause 8 of IEC 60880).

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

a) System validation shall be performed in accordance with the validation plan defined in 6.2.4.

b) The requirements of clause 8 of IEC 60880 shall apply to validation of category A functions.

c) The requirements of clause 8 of IEC 60880 shall apply to validation of category B and C functions, with the following amendments:

- the same level of detail shall apply but the extent of the testing may be reduced in accordance with the safety goals of the functions important to safety;
- independence between the team responsible for the evaluation of the validation tests and the designers is not required.

6.1.6 System installation

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

a) L'installation du système doit être réalisée conformément au plan d'installation défini en 6.2.5.

b) Des moyens appropriés, par exemple l'étiquetage ou le codage couleur, doivent être utilisés pour identifier le système de manière unique et pour réduire la probabilité d'erreurs d'installation, d'exploitation et de maintenance.

6.1.7 Modifications de la conception

Des modifications de la conception du système peuvent être demandées en raison de l'identification de nouvelles exigences relatives au système ou de la découverte de défauts de conception du système.

a) L'intégration d'une modification à un système doit être réalisée conformément aux procédures définies (voir 6.3.6).

b) Un contrôle du bon fonctionnement du système doit être effectué après une modification.

c) Aucune modification matérielle ou logicielle autre que celles spécifiées dans les procédures de maintenance ne peut être apportée dans le cadre des opérations de routine.

d) Si un remplacement de matériel est nécessaire, il doit être démontré/justifié que le matériel de remplacement respecte la spécification du matériel d'origine.

e) Pour les systèmes de classe 1, les processus de modification du logiciel et du matériel doivent être conformes respectivement à l'article 9 de la CEI 60880 et à l'article 11 de la CEI 60987.

6.2 Planification du système

L'objectif des prescriptions du présent paragraphe est de développer les plans du système afin d'assurer que les exigences sur les fonctions d'I&C importantes pour la sûreté supportées par le système seront respectées et maintenues.

Les prescriptions de 5.4 s'appliquent aux plans globaux. Ces plans spécifient des dispositions complémentaires relatives aux fonctions réparties au sein des systèmes interconnectés.

NOTE Les prescriptions suivantes relatives aux plans n'excluent pas le fait que ceux-ci puissent être organisés dans plusieurs documents différents.

Les plans du système doivent être établis tôt dans le cycle de vie du système, avant le commencement des activités concernées.

6.2.1 Plan d'assurance qualité du système

a) Un plan d'assurance qualité, couvrant chaque activité du cycle de vie et de sûreté du système, doit être établi et mis en œuvre. Les prescriptions relatives au plan d'assurance qualité du système sont dérivées de l'AIEA 50-C-QA (Rév. 1) et de l'ISO 9001.

b) Le plan d'assurance qualité du système doit englober les activités nécessaires à l'obtention d'une qualité appropriée du système, celles nécessaires à la vérification que la qualité désirée est bien atteinte, et celles permettant de fournir des preuves objectives à cet effet (voir article 102 de l'AIEA 50-C-QA (Rév.1)). Les exigences relatives aux activités de vérification figurent dans le plan de vérification du système (voir 6.2.1.1).

c) Le plan d'assurance qualité du système doit traiter de la qualité du système et des aspects de la qualité liés à l'intégration du matériel et du logiciel. Les plans d'assurance qualité spécifiques au matériel et au logiciel sortent du cadre de la présente norme.

NOTE Les prescriptions relatives au plan d'assurance qualité du logiciel des systèmes de sûreté sont définies à l'article 3 de la CEI 60880.

d) Le plan d'assurance qualité du système doit contenir

- l'identification des normes et procédures devant être appliquées pour le projet (selon 4.2.2 de l'ISO 9001);

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

a) System installation shall be performed in accordance with the installation plan defined in 6.2.5.

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

6.1.7 System design modification

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

a) The implementation of a modification to a system shall be carried out in accordance with defined procedures (see 6.3.6).

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

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

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

e) For class 1 systems, the modification process of software shall be in accordance with clause 9 of IEC 60880 and the modification process of hardware in accordance with clause 11 of IEC 60987.

6.2 System planning

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

The requirements of 5.4 address complementary overall plans for functions distributed within interconnected systems.

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

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

6.2.1 System quality assurance plan

a) A quality assurance plan shall be established and implemented to cover each of the activities of the system safety life cycle. The requirements for the system quality assurance plan are derived from IAEA 50-C-QA (Rev. 1) and ISO 9001.

b) The system quality assurance plan shall include the activities that are necessary to, achieve the appropriate quality of the system, for verifying that the required quality is achieved, and to provide objective evidence to that effect (see clause 102 of IAEA 50-C-QA (Rev. 1)). The requirements on verification activities are established in the system verification plan (see 6.2.1.1).

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

NOTE The requirements for software quality assurance plan of safety systems are defined in clause 3 of IEC 60880.

d) The system quality assurance plan shall include:

- identification of the governing standards and procedures to be used for the project (according to 4.2.2 of ISO 9001);

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

- l'identification des phases du cycle de vie du système, les activités élémentaires et les résultats attendus de chaque phase (selon 4.4.2 de l'ISO 9001);
- la description des relations et des interactions entre les différentes activités (selon 4.4.3 de l'ISO 9001);
- la description de la structure organisationnelle (selon 4.1.2 de l'ISO 9001);
- l'approvisionnement des composants auprès des fournisseurs externes (selon 4.6 et 4.7 de l'ISO 9001);
- l'identification et la traçabilité du produit (selon 4.8 de l'ISO 9000-3). Les exigences correspondantes figurent dans le plan de gestion de la configuration (voir 6.2.1.2);
- l'identification de toutes les procédures d'inspection et d'essai (selon 4.10 de l'ISO 9001);
- l'identification des activités et tâches d'assurance qualité;
- l'identification du personnel et des organisations responsables des activités et tâches d'assurance qualité, et leurs garanties d'indépendance (selon l'AIEA 50-C-QA (Rév. 1));
- les procédures de déclaration et de résolution des non-conformités aux exigences, normes et procédures. Les procédures doivent inclure la prise en compte de l'impact sur la sûreté de la centrale nucléaire et doivent assurer que tous les effets des non-conformités sont identifiés, par exemple l'interchangeabilité, la maintenance, les pièces de rechange, la notice de fonctionnement, etc. (selon 4.13 de ISO 9001).

e) Le plan d'assurance qualité doit être établi tôt dans le cycle de vie du système et doit être prévu dans le programme général des autres activités du cycle de vie et de sûreté de l'I&C. Le plan peut soit faire partie de la spécification du système, soit constituer un document associé (voir 3.2 de la CEI 60880).

6.2.1.1 Plan de vérification du système

a) Un plan de vérification du système doit être établi et doit décrire
   - le processus de vérification au cours de toutes les phases du cycle de vie et de sûreté du système;
   - l'organisation et les responsabilités correspondantes.

b) Les résultats de chaque phase du cycle de vie et de sûreté du système doivent être vérifiés par rapport à ses entrées identifiées.

c) Chaque étape de vérification doit conduire à un rapport sur l'analyse effectuée et les conclusions atteintes. Lorsqu'une phase est achevée, un rapport final doit être rédigé, montrant la conformité des résultats de la phase aux exigences initiales et la résolution des anomalies.

d) La vérification doit être réalisée par des personnes compétentes dans les sujets concernés et possédant une bonne compréhension des informations d'entrée vis à vis desquelles la vérification est effectuée.

e) La minutie apportée au plan de vérification doit être proportionnelle à la classe de sûreté du système. Le plan de vérification doit souligner les aspects importants à vérifier pour la sûreté et il convient qu'il prenne en compte le fait que la probabilité d'une erreur ou omission dans les sujets complexes est plus importante que dans les plus simples.

f) Les documents soumis à une vérification doivent être identifiés dans le plan d'assurance qualité du système.

g) Les documents associés à une vérification, c'est-à-dire les entrées et sorties des activités, les rapports de vérification et, éventuellement, les outils utilisés, doivent être gérés en configuration.

h) Pour les systèmes de classe 1, le plan de vérification doit être réalisé par des personnes indépendantes de celles ayant conçu le système (selon 6.2.1 de CEI 60880).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- identification of the phases of the system life cycle, the elementary tasks and the expected results of each phase (according to 4.4.2 of ISO 9001);
- description of relationships and interactions between the different tasks (according to 4.4.3 of ISO 9001);
- description of the organisational structure (according to 4.1.2 of ISO 9001);
- procurement of components from external suppliers (according to 4.6 and 4.7 of ISO 9001);
- product identification and traceability (according to 4.8 of ISO 9000-3). The corresponding requirements are established in the configuration management plan (see 6.2.1.2);
- identification of all inspection and testing procedures (according to 4.10 of ISO 9001);
- identification of QA activities and tasks;
- identification of personnel/organisations responsible for QA activities and tasks, including assurance of independence (according to IAEA 50-C-QA (Rev. 1));
- procedures for reporting and disposition of non-conformance to requirements, standards and procedures. The procedures shall include consideration of the impact upon NPP safety and shall ensure that all effects of the non-conformance are identified, for example interchangeability, maintenance, spares, operating instructions, etc. (according to 4.13 of ISO 9001).

e) The quality assurance plan shall be established at an early stage of the system life cycle and shall be planned within the general schedule of the other activities of the I&C safety life cycle. The plan may be either a part of the system specification or a companion document (see 3.2 of IEC 60880).

6.2.1.1 System verification plan

a) A system verification plan shall be developed describing
   - the verification process across all the phases of the system safety life cycle;
   - the corresponding organisation and responsibilities.

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

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

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

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

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

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

h) For class 1 systems, the verification plan shall be executed by individuals independent of the designers of the system (according to 6.2.1 of IEC 60880).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.2.1.2 Plan de gestion de configuration du système

NOTE Une partie des exigences suivantes relatives au plan de gestion de configuration du système est inspirée de l'IEEE 828 [3].

a) Identification de la configuration:

- des unités de configuration appropriées doivent être définies en des points de contrôle au cours du cycle de vie du système et les éléments à contrôler doivent être définis. Les éléments contrôlés peuvent être des résultats intermédiaires et finals (tels que la documentation du matériel, du logiciel ou de vérification, le manuel de l'utilisateur) et des éléments de l'environnement de soutien (tels que les compilateurs, outils, bancs d'essai);
- tous les éléments à contrôler doivent être identifiés. Chaque élément doit avoir une référence unique et les versions différentes doivent être identifiées;
- les liens entre les éléments d'une unité de configuration et les éléments à partir desquels ils ont été développés doivent être établis et enregistrés;
- le système de gestion de configuration doit être capable de reconstituer la configuration de toutes les unités de configuration du système;
- il convient que des moyens de recherche soient disponibles afin que des liens et des occurrences multiples d'éléments puissent être facilement identifiés.

b) Contrôle de configuration:

- le contrôle de configuration doit permettre de geler un état de la conception. Les procédures et l'autorité requises pour toute modification après le gel doivent être définies;
- l'état de chaque élément contrôlé doit faire l'objet d'un suivi; cela inclut les informations sur la version initiale approuvée, la nature des changements demandés et la réalisation des changements approuvés.

c) Le plan de gestion de configuration doit être défini au début du projet du système et doit être conservé pendant tout le cycle de vie du système.

6.2.2 Plan de sécurité du système

Le plan de sécurité du système est défini en accord avec le plan global de sécurité (voir 5.4.2).

a) Pendant la spécification et la conception du système, il convient que les exigences relatives aux contre-mesures techniques identifiées pour le système dans le plan de sécurité (voir 5.4.2) soient converties en exigences de conception techniques et soient documentées.

b) Une évaluation de la documentation de la conception doit avoir lieu afin de vérifier que les contre-mesures identifiées dans le cadre de l'analyse de sécurité du système ont été mises en œuvre correctement.

c) Pendant la vérification et la validation du système, l'efficacité des fonctions de sécurité doit être démontrée par des essais appropriés, le système étant dans sa configuration finale.

6.2.3 Plan d'intégration du système

Le plan d'intégration du système traite des mesures administratives et techniques pour intégrer les sous-systèmes au système et pour intégrer le matériel et le logiciel. Il couvre les activités décrites en 7.4 de la CEI 60880.

a) Un plan d'intégration du système doit être préparé et doit définir les types d'essais à effectuer, l'environnement des essais et les critères d'acceptation.

b) Les essais d'intégration doivent être fondés sur un concept d'intégration progressive.

IECNORM.COM: Click to view the full PDF of IEC 61513:2001

6.2.1.2 System configuration management plan

NOTE Part of the following requirements for system configuration management plan are derived from IEEE 828 [3].

a) Configuration identification:

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

b) Configuration control:

- the configuration control shall provide the facilities required to initiate a design freeze. Procedures and authority required for any further modification following a design freeze shall be defined;
- the status of each controlled item shall be tracked; this includes information on the initial approved version, the status of requested changes, and the implementation of approved changes.

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

6.2.2 System security plan

The system security plan is defined to be consistent with the overall security plan (see 5.4.2).

a) During system specification and design the requirements for technical counter-measures identified for the system in the overall security plan (see 5.4.2) should be transformed into technical design requirements and documented.

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

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

6.2.3 System integration plan

The system integration plan addresses the procedural and technical measures used to integrate subsystems into the system and to integrate hardware and software. It covers the activities described in 7.4 of IEC 60880.

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

c) Il convient de faire la distinction entre les essais propres au système (fonctions du logiciel système et du matériel) et les essais spécifiques à la centrale (fonctions d'application).

NOTE Les essais des modules (matériel, logiciel, modules combinés) réalisés lors des essais de tête de série ou des projets antérieurs peuvent être utilisés afin d'éviter la répétition de cas d'essais identiques ou inutiles.

6.2.4 Plan de validation du système

Le plan de validation du système traite des mesures administratives et techniques pour démontrer que le système est conforme à sa spécification et à ses exigences. La validation des exigences relatives aux fonctions d'application est traitée dans la phase de validation fonctionnelle (voir 6.1.3.1.1).

a) Un plan de validation du système doit être établi et doit décrire la ou les configurations du système pour sa validation, les essais et analyses à réaliser et les rapports à produire.

   1) Les documents relatifs aux essais de validation doivent spécifier la configuration du système à soumettre aux essais, les informations d'entrée, les méthodes, outils et étalonnages à utiliser et les critères d'acceptation appropriés. Si cela est pertinent, il convient que la précision et l'influence des outils d'observation sur le comportement du système soient estimées.

   2) Les documents relatifs aux analyses de validation doivent spécifier ce que les analyses doivent démontrer, les résultats attendus et les critères d'acceptation appropriés.

b) Pour des fonctions de catégorie A, le plan de validation du système doit être établi et les activités de validation réalisées par des équipes indépendantes de celles qui ont conçu, réalisé et/ou modifié le système (voir article 8 de la CEI 60880).

   NOTE L'indépendance n'est pas demandée pour les personnes participant à la réalisation du plan de validation et à la production du rapport de validation.

c) Pour les fonctions de catégorie B, l'équipe de développement du plan de validation du système doit inclure, et être sous la responsabilité, de personnes qui n'ont pas participé à la conception, à la réalisation et/ou à la modification du système.

d) Pour les fonctions de catégorie A et B, le plan de validation du système doit prévoir la traçabilité entre la spécification et les essais et analyses correspondants.

e) Pour les fonctions de catégorie C, il convient que le plan de validation du système prévoie la traçabilité entre la spécification et les essais et analyses correspondants.

6.2.5 Plan d'installation du système

Le plan d'installation du système traite des mesures administratives et techniques pour l'installation du système sur site et pour le contrôle d'aptitude à une utilisation opérationnelle. Le plan est complété par les plans d'intégration et de mise en service globales (voir 5.4.3).

a) Un plan d'installation du système doit être établi et décrire les mesures à prendre afin d'assurer et vérifier que la configuration du système et de tous les paramètres modifiables est correcte, que le système est complet, correctement installé, assemblé et connecté, et fonctionne comme prévu et spécifié.

b) Pour les systèmes de classe 1, le plan d'installation doit être conforme aux prescriptions des articles 9 de la CEI 60987 et 10.1.1 de la CEI 60880.

c) Pour les fonctions de catégorie A, l'aptitude de chaque voie à remplir ses fonctions doit être démontrée sur site.

6.2.6 Plan d'exploitation du système

Le plan d'exploitation du système traite de la manière dont le système doit être exploité et des exigences qui lui sont applicables pendant son fonctionnement.

a) Un plan d'exploitation du système doit spécifier la manière dont le système doit être exploité dans tous ses modes de fonctionnement. Le plan doit être en accord avec le plan de maintenance du système (voir 6.2.7) et avec les plans d'exploitation et de maintenance globales (voir 5.4.4 et 5.4.5).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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

NOTE Tests of modules (hardware, software, combined modules) performed during type testing or preceding projects may be used in order to avoid repetition of identical or unnecessary test cases.

6.2.4 System validation plan

The system validation plan addresses the procedural and technical measures taken to demonstrate that the system meets its system specification and its system requirements specification. The validation of the application functions requirements is considered in the functional validation phase (see 6.1.3.1.1).

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

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

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

b) For category A functions, the system validation plan shall be developed and validation activities performed by teams independent from the ones who designed, implemented, and or modified the system (see clause 8 of IEC 60880).

   NOTE Independence is not required for individuals included in the execution of the validation plan and the production of the validation report.

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

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

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

6.2.5 System installation plan

The system installation plan addresses the procedural and technical measures for installation of the system on site and for the checking needed to provide assurance that the system is ready for operational use. The plan is complemented by the overall integration and commissioning plans (see 5.4.3).

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

b) For class 1 systems, the installation plan shall meet the requirements of clause 9 of IEC 60987 and 10.1.1 of IEC 60880.

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

6.2.6 System operation plan

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

a) A system operation plan shall specify how the system is to be operated in all modes of operation. The plan shall be consistent with the system maintenance plan (see 6.2.7) and the overall operation and maintenance plans (see 5.4.4 and 5.4.5).

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

b) Il convient que le plan d'exploitation du système spécifie les conditions à remplir avant la mise en exploitation du système. En particulier:

- l'installation, l'intégration et la décision de mise en service du système doivent être achevées (voir 5.4.3);
- le plan de maintenance du système (voir 6.2.7) et le manuel d'utilisation doivent être disponibles.

c) Lorsque des essais périodiques sont prévus (voir 6.1.1.2.4), le plan d'exploitation du système doit spécifier

- la fréquence et la durée de chaque essai, les conditions à remplir avant la mise en œuvre d'un essai et les effets, le cas échéant, sur l'exploitation du système et de la centrale;
- les étapes nécessaires pour réaliser chaque essai, les outils à utiliser et leurs étalonnages, l'analyse de la justesse des résultats;
- la vérification du retour complet à l'état normal, si des modifications provisoires du système sont requises.

NOTE Les essais périodiques concernent aussi bien l'équipe opérationnelle que celle chargée de la maintenance. Cette activité peut également être considérée comme faisant partie de la maintenance de routine (voir 6.2.7).

d) Le plan d'exploitation du système doit spécifier les enregistrements devant être tenus à jour pendant le fonctionnement du système. Ceux-ci doivent contenir les détails des défaillances, les enregistrements des essais du système et un enregistrement des demandes affectant le système.

e) Le plan d'exploitation du système doit être pris en compte pour l'impact qu'il pourrait avoir sur la sûreté de la centrale.

f) Pour un système de classe 1 ou 2, le plan d'exploitation du système doit exiger un contrôle périodique du système, en accord avec les exigences résultant de l'analyse probabiliste.

g) Pour un système de classe 3, le plan d'exploitation du système doit spécifier le contrôle périodique du système, avec des intervalles appropriés, si le fonctionnement continu ne garantit pas la détection des défaillances.

6.2.7 Plan de maintenance du système

Le plan de maintenance du système comprend des mesures administratives et techniques à prendre pour conserver la fonctionnalité du système opérationnel. Il est établi de manière à être en accord avec le plan d'exploitation du système et avec les plans d'exploitation et de maintenance globales (voir 5.4.4 et 5.4.5).

a) Un plan de maintenance du système doit être établi et spécifier

- les mesures de routine et les procédures qui seront suivies pour détecter les défaillances du système et pour maintenir la performance fonctionnelle et la fiabilité du système «comme prévues à la conception» (maintenance préventive);
- les mesures et procédures qui doivent être suivies afin de remettre le système dans un état totalement opérationnel (maintenance corrective).

b) Il convient que l'étendue de la maintenance préventive soit déterminée par une méthode d'analyse systématique telle que l'analyse des modes de défaillance et leur conséquences, ou par l'application d'un modèle de maintenance axée sur la fiabilité, ou par l'examen des arbres de défaillances des fonctions du système.

c) Les procédures de remplacement des composants doivent assurer que

- les composants de rechange sont fonctionnellement identiques à ceux qui sont remplacés et qu'ils sont conformes aux exigences relatives à la qualité;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

- the system shall have completed installation, integration and commissioning (see 5.4.3);
- the system maintenance plan (see 6.2.7) and user documentation shall be available.

c) When periodic testing is required (see 6.1.1.2.4), the system operation plan shall specify

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

NOTE Periodic testing involves both the operation and maintenance teams. This activity may also be considered as part of routine maintenance (see 6.2.7).

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

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

f) For a class 1 or 2 system, the system operation plan shall require periodic testing of the system, consistent with any requirements arising from probabilistic analysis.

g) For a class 3 system, the system operation plan shall specify periodic testing of the system, at appropriate intervals, if continuous operation does not guarantee the detection of failures.

6.2.7 System maintenance plan

System maintenance includes the procedural and technical measures to be taken to maintain the functionality of the operational system. The system maintenance plan is developed to be consistent with the system operation plan and the overall operation and maintenance plans (see 5.4.4 and 5.4.5).

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

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

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

c) The procedures for replacement of components shall ensure that

- replacement components are functionally identical to those being replaced and meet the quality requirements;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- si le remplacement est effectué en marche, son impact sur la fonctionnalité du système est estimé et documenté avant de procéder au remplacement;
- un enregistrement de tous les remplacements, permettant de satisfaire aux exigences de traçabilité, est tenu à jour.

d) Les procédures de ré-étalonnage doivent assurer que

- le nouvel étalonnage se trouve dans des limites définies (lorsque ces limites sont appliquées par le système, il n'est pas nécessaire d'imposer de contraintes formelles au personnel de maintenance);
- si le ré-étalonnage est effectué en marche, son impact sur la fonctionnalité du système est estimé et documenté avant de procéder au réétalonnage;
- un enregistrement de tous les réétalonnages, permettant de satisfaire aux exigences de traçabilité, est tenu à jour.

6.3 Prescriptions relatives à la documentation

Le présent paragraphe définit la documentation de sortie des phases du cycle de vie du système: contenu, caractéristiques et principaux points devant être vérifiés.

La documentation de sortie doit constituer un ensemble de documents, correctement référencés et cohérents entre eux, assurant la traçabilité de la conception finale depuis les exigences initiales.

6.3.1 Documentation de spécification des exigences sur le système

6.3.1.1 Contenu

La documentation de spécification des exigences sur le système doit être complète et doit fournir toutes les informations nécessaires aux activités suivantes du cycle de vie et de sûreté du système et à la qualification du système.

6.3.1.2 Caractéristiques

Caractéristiques de la documentation de spécification des exigences du système:

a) les exigences doivent être vérifiables;

NOTE 1 Le paragraphe 4.3 de l'IEEE 830 [2] fournit des conseils pour la vérifiabilité des exigences.

b) il convient que les exigences soient claires et précises afin qu'elles puissent être comprises sans ambiguïté par tous les lecteurs prévus, notamment les vérificateurs et les personnes en charge de la spécification du système et de la validation fonctionnelle;

NOTE 2 Par exemple, le document facilite l'identification précise et complète des exigences, au lieu de les noyer dans des explications et autres informations secondaires, afin de limiter le risque d'interprétations différentes. La manière la plus appropriée d'atteindre ces objectifs est de rédiger des exigences conformément aux recommandations de documents tels que l'IEEE 830 [2] et l'EWICS n° 6 [5].

c) il convient que les exigences relatives aux fonctions d'application soient spécifiées en termes fonctionnels plutôt qu'informatiques afin de permettre la vérification par les ingénieurs de fonctionnement et par les opérateurs de la centrale qui peuvent n'avoir que des connaissances limitées en technologie informatique;

d) il convient que les exigences soient spécifiées en utilisant des méthodes, outils et directives documentés;

NOTE 3 Les prescriptions détaillées relatives aux outils logiciels pour les systèmes de classe 1 figurent en 4.2 de la CEI 60880-2.

e) il convient que les exigences soient rédigées et organisées de manière à faciliter l'estimation de la conformité des spécifications du système et à constituer une référence pour le plan de qualification du système.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

- if replacement is performed on line, its impact upon the functionality of the system is assessed and documented prior to replacement;
- a record is maintained of all replacements, enabling any requirements for traceability to be achieved.

d) The procedures for re-calibration shall ensure that

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

6.3 Output documentation

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

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

6.3.1 System requirements specification documentation

6.3.1.1 Content

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

6.3.1.2 Characteristics

Characteristics of the system requirements specification document:

a) the requirements shall be verifiable ;

NOTE 1 Subclause 4.3 of IEEE 830 [2] provides guidance to check for verifiability of requirements.

b) the requirements should be clear and precise so that they can be understood unambiguously by all intended readers, including the reviewers and those in charge of the system specification and the functional validation;

NOTE 2 For example, the document facilitates a precise and comprehensive identification of requirements, as opposed to providing extensive explanations and other ancillary information, so as to limit the risk of diverging interpretations. The most appropriate way to achieve these objectives is to write a system requirements specification according to guidance documents such as IEEE 830 [2] and EWICS position paper No. 6 [5].

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

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

NOTE 3 Detailed requirements regarding software tools for class 1 systems are given in 4.2 of IEC 60880-2.

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.3.1.3 Vérification

Les points suivants doivent être vérifiés:

a) les exigences doivent être traçables et cohérentes avec celles établies lors de la conception de l'architecture et de l'affectation des fonctions et concernant le système (voir 5.5);

b) les exigences relatives aux interfaces doivent être cohérentes avec celles des systèmes et équipements connectés au système;

c) il convient que les exigences qui augmentent inutilement la complexité du système soient identifiées (la complexité peut accroître le risque d'erreurs dans la spécification des exigences du système et/ou dans le système lui-même).

6.3.2 Documentation de la spécification du système

6.3.2.1 Contenu

a) La documentation de spécification du système doit être complète et doit fournir toutes les informations nécessaires aux activités suivantes dans le cycle de vie et de sûreté du système, notamment pour les phases de conception et de validation du système.

b) La documentation de spécification du système doit identifier les équipements à utiliser, c'est-à-dire les équipements préexistants ou bien ceux à développer. L'adéquation des équipements choisis doit être justifiée.

c) La documentation de spécification du système doit décrire l'architecture du système:

- la décomposition du système en sous-systèmes et/ou en composants matériels et logiciels;
- le comportement interne du système (voir 6.1.1.2.2), y compris la description des principaux événements internes au système et sa réaction face à ces événements (voir 6.1.2.2.3);
- les limites, les conditions environnementales, la fiabilité attendue du matériel, le comportement, les fonctions, les performances et interfaces de chaque sous-système;
- la classification de chaque sous-système; il convient qu'une justification soit apportée si la classe d'un sous-système est inférieure à celle du système ou du sous-système dans lequel il est inclus;
- les conditions d'utilisation et la connexion des sous-systèmes identifiés dans le système.

NOTE La description des sous-systèmes peut être réalisée hiérarchiquement, afin de faciliter la compréhension, en partant d'une vue d'ensemble et en descendant jusqu'aux sous-systèmes élémentaires (c'est-à-dire les sous-systèmes qui, dans la documentation, ne sont pas décomposés). Des informations «horizontales» peuvent également s'avérer utiles.

d) La documentation de spécification du système doit contenir la spécification du logiciel (voir 6.1.2.3).

e) Dans un système de la classe 1 ou 2, l'affectation des fonctions aux sous-systèmes doit être précisée, c'est-à-dire que la spécification du système doit indiquer les sous-systèmes qui contribuent et/ou sont nécessaires à la réalisation d'une fonction donnée.

6.3.2.2 Caractéristiques

Caractéristiques de la documentation de spécification du système:

a) il convient que la documentation soit claire et précise afin qu'elle puisse être comprise sans ambiguïté par tous les lecteurs prévus, notamment les vérificateurs et les personnes en charge de la conception du système et de l'intégration et de la validation;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

6.3.1.3 Verification

The following points shall be verified:

a) requirements shall be traceable and consistent with the requirements for the system established in the architectural design and functional assignment (see 5.5);

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

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

6.3.2 System specification documentation

6.3.2.1 Content

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

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

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

- the decomposition of the system into subsystems, and/or into hardware and software components;
- the internal behaviour of the system (see 6.1.1.2.2), including the description of the main events internal to the system and its defence to these events (see 6.1.2.2.3);
- the boundaries, environmental conditions, expected hardware reliability, behaviour, functions, performances and interfaces of each subsystem;
- the classification of each subsystem; justification should be provided if the subsystem class is lower than the class of the system or subsystem in which it is included;
- the conditions of use and the connection of the identified subsystems within the system.

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

d) The system specification documentation shall include the software specification (see 6.1.2.3).

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

6.3.2.2 Characteristics

Characteristics of the system specification documentation:

a) the documentation should be clear and precise so that it can be understood unambiguously by all intended readers, particularly the reviewers and those producing the system design, and completing integration and validation;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

b) il convient que la spécification des fonctions d'application soit rédigée en des termes tels que la vérification et la compréhension, effectuée aussi par les ingénieurs de fonctionnement de l'I&C et par les opérateurs de la centrale, soit facilitée;

c) il convient que la spécification du système soit développée avec des méthodes, outils et directives documentés. Il convient que ces méthodes, outils et directives comblent les «lacunes» des méthodes, outils et directives utilisés pour la spécification des exigences du système;

NOTE Les méthodes et outils d'ingénierie logicielle peuvent améliorer la qualité de la spécification de la conception du système final, même comparée à la spécification de la conception d'un système câblé.

d) il convient que la spécification du système soit rédigée et structurée afin de faciliter l'estimation de la cohérence avec les exigences du système et de constituer un outil de référence efficace pour la validation du système, c'est-à-dire qu'elle devrait faciliter une identification complète des spécifications (au lieu de les noyer dans des explications et autres informations secondaires).

6.3.2.3 Vérification

a) Il convient que la vérification de la spécification du système par rapport aux exigences sur le système soit effectuée avant l'achèvement de l'activité de conception détaillée. Il convient qu'elle permette la prise de mesures correctives avant la réalisation et l'intégration du système.

b) Il convient d'établir une communication forte entre l'équipe chargée de la spécification du système et les fournisseurs afin de permettre la vérification de l'adéquation des équipements choisis.

c) La vérification doit documenter la cohérence et signaler toute non-conformité de la spécification du système relativement aux exigences du système.

d) La traduction correcte des exigences des fonctions d'application dans la spécification du logiciel d'application doit être vérifiée.

e) Pour les systèmes de classe 1 et 2, toute non-conformité doit être corrigée ou doit être justifiée eu égard à la sûreté, en tenant compte d'éventuelles mesures de compensation.

f) Pour les systèmes de classe 1 et 2, les caractéristiques qui augmentent la complexité du système et qui ne sont pas déduites des exigences sur le système doivent être identifiées et justifiées par rapport à la sûreté.

NOTE La présence de caractéristiques non exigées par la spécification des exigences du système peut accroître considérablement la complexité du système, ce qui pourrait potentiellement diminuer la confiance en son bon fonctionnement.

6.3.3 Documentation de la conception et réalisation détaillées du système

La conception détaillée peut être effectuée par un certain nombre d'itérations. Les prescriptions du présent paragraphe traitent de la documentation finale du système, qui est disponible lorsque la conception, la réalisation, l'intégration et la validation du système sont achevées et que celui-ci est prêt à être livré et installé sur le site.

La documentation de conception détaillée du système peut généralement être répartie en quatre groupes de documents. A savoir:

- les documents relatifs à la conception du système;
- les analyses requises (voir 6.1.3.1);
- les documents relatifs à la conception du logiciel d'application;
- les documents relatifs à la conception du logiciel système et des composants du matériel du système.

NOTE 1 Si le système est réalisé avec des équipements préexistants, les documents relatifs à la conception du logiciel système et du matériel du système font partie de la documentation des équipements préexistants.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

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

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

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

6.3.2.3 Verification

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

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

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

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

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

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

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

6.3.3 System detailed design documentation

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

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

- the system design documents;
- the required analysis (see 6.1.3.1);
- the application software design documents;
- the system hardware components and system software design documents.

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

Seuls les deux premiers points sont traités, dans la mesure où la conception du logiciel et du matériel sort du cadre de la présente norme (voir 6.1.3).

NOTE 2 Pour les systèmes de classe 1, les prescriptions relatives à la documentation du logiciel figurent dans la CEI 60880 et la CEI 60880-2, et les prescriptions relatives à la documentation du matériel dans la CEI 60987.

6.3.3.1 Contenu

a) Les documents relatifs à la conception du système doivent être complets et doivent apporter toutes les informations nécessaires aux activités suivantes dans le cycle de vie et de sûreté du système, en particulier intégration, validation, installation, exploitation et maintenance.

b) Les documents relatifs à la conception du système prolongent les documents relatifs à la spécification et doivent fournir une description détaillée de la structure interne et du comportement interne du système. Le niveau de détail de cette description peut s'adapter à la classe de sûreté du système.

c) Les documents relatifs à la conception du système doivent contenir la description de l'installation des équipements dans la centrale et des dispositions relatives aux essais du système.

d) Les documents relatifs à la conception du système doivent contenir la description de la fonctionnalité et de la performance qui ont été validées pour le système, en particulier le temps de réponse attendu dans les différentes conditions d'exploitation de la centrale, les réglages de sûreté nominaux des points de réglage et des algorithmes de contrôle, les marges des réglages de sûreté.

6.3.3.2 Caractéristiques

Caractéristiques de la documentation de conception du système:

a) Il convient que la documentation soit claire et précise afin que chacune de ses parties puisse être comprise sans ambiguïté par ses lecteurs prévus, notamment les auteurs et vérificateurs des plans d'intégration, de qualification, d'installation, d'exploitation et de maintenance du système, le personnel de maintenance, les auteurs et vérificateurs des modifications.

b) La documentation de conception détaillée doit être mise à jour pendant le développement du système afin d'assurer que la version finale des documents est conforme à l'exécution.

6.3.3.3 Vérification

a) Il convient que la vérification de la conception détaillée du système et de sa documentation soit réalisée avant la réalisation de nouveaux matériels et logiciels, et qu'un délai suffisant soit accordé pour permettre, le cas échéant, la mise en œuvre de mesures correctives suite à la vérification.

b) Il convient que les exigences relatives à la fiabilité des fonctions d'application du système (voir 6.1.3.1.1) soient, tôt dans la phase de conception détaillée, vérifiées comme étant réalisables.

NOTE L'analyse de fiabilité du système peut nécessiter la modification de la conception détaillée, de l'architecture du système, par exemple le degré de redondance, voire même le choix des solutions de l'architecture globale de l'I&C.

c) Les possibilités de perturbation des fonctions d'application par les fonctions de service du système doivent être vérifiées par une analyse rigoureuse à l'aide de moyens adaptés pour la sûreté des fonctions d'application.

d) Les hypothèses faites lors de la vérification de la conception détaillée doivent être explicitées et documentées.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

Only the first two groups are addressed, as software and hardware design is outside of the scope of this standard (see 6.1.3).

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

6.3.3.1 Content

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

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

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

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

6.3.3.2 Characteristics

Characteristics of the system design documentation:

a) The documentation should be clear and precise so that each part can be understood unambiguously by its intended readers, including the authors and reviewers of the system integration plan, the system qualification plan, the system installation and commissioning plan, and the system maintenance plan, maintenance staff, authors and reviewers of design modifications.

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

6.3.3.3 Verification

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

b) The reliability requirements specified for the application functions of the system (see 6.1.3.1.1) should be verified as achievable at an early stage of the detailed design.

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.3.4 Documentation de l'intégration du système

6.3.4.1 Contenu

La documentation d'intégration du système doit contenir le plan d'intégration, les rapports d'essais d'intégration et toutes les informations nécessaires à la phase suivante de validation.

6.3.4.2 Caractéristiques

a) Les rapports d'essais d'intégration doivent contenir les informations suivantes:

- les versions des modules matériels et logiciels, de la spécification des essais utilisée, des outils et équipements utilisés, et toute valeur d'étalonnage appropriée;
- les résultats de chaque essai indiquant tout écart entre résultats attendus et obtenus et, pour chaque écart, un enregistrement de l'analyse faite et des décisions prises quant à la poursuite de l'essai ou la mise en route d'une modification.

b) Pour les systèmes de classe 1, les prescriptions de 7.7 de la CEI 60880 s'appliquent.

6.3.4.3 Vérification

a) Il convient que la vérification des rapports d'intégration du système relativement au plan d'intégration du système soit réalisée avant l'activité de validation.

b) Pour un système de classe 1, la traçabilité entre la documentation de conception détaillée et les essais et analyses des composants et de l'intégration correspondants doit être réalisée, de manière à permettre l'évaluation des essais et analyses relativement à leur étendue.

c) Pour les systèmes de classe 2, il convient que la traçabilité entre la documentation de conception détaillée et les essais et analyses des composants et de l'intégration correspondants soit réalisée, de manière à permettre l'évaluation des essais et analyses relativement à leur étendue.

6.3.5 Documentation de la validation du système

6.3.5.1 Contenu

La documentation de validation du système doit contenir le plan de validation, les rapports d'essais de validation et toutes les informations nécessaires à la qualification du système.

6.3.5.2 Caractéristiques

Pour les systèmes de classe 1, les prescriptions de 8.1 de la CEI 60880 s'appliquent.

6.3.5.3 Vérification

Les résultats des essais et analyses de validation doivent être documentés et comparés aux exigences figurant dans le plan de validation du système afin de confirmer que la performance fonctionnelle du système est bien conforme à ces exigences.

NOTE La documentation de validation ainsi que la documentation de validation fonctionnelle (voir le point d) de 6.3.3.1) confirment la conformité du système à la fois à la spécification du système et à la spécification des exigences du système.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.3.4 System integration documentation

6.3.4.1 Content

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

6.3.4.2 Characteristics

a) Integration test reports shall contain the following information:

- the versions of the hardware and software modules, the test specification used, the tools and equipment used, together with any relevant calibration data;
- the results of each test listing any discrepancies between the expected and actual results, and, for each discrepancy, a record of the analysis made and the decisions taken on whether to continue the test or implement a change.

b) The requirements of 7.7 of IEC 60880 apply for class 1 systems.

6.3.4.3 Verification

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

b) For a class 1 system, traceability from the detailed design documentation to the corresponding component and integration tests and analyses shall be provided, so as to enable the assessment of the tests and analyses with respect to test coverage.

c) For class 2 systems, traceability from the detailed design documentation to the corresponding component and integration tests and analysis should be provided, so as to enable the assessment of the tests and analyses with respect to test coverage.

6.3.5 System validation documentation

6.3.5.1 Content

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

6.3.5.2 Characteristics

The requirements of 8.1 of IEC 60880 apply for class 1 systems.

6.3.5.3 Verification

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

NOTE The validation documentation together with the functional validation documentation (see d) of 6.3.3.1) confirms the system compliance with both system specification and system requirements specification.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.3.6 Documentation des modifications du système

6.3.6.1 Contenu

a) Demande de modification

Ce document doit indiquer

- la justification de la modification et l'effet (le cas échéant) sur la sûreté de la centrale nucléaire;
- la description fonctionnelle de la modification (avec des dessins légendés, des schémas mécaniques, un dessin de configuration, etc.) et les moyens proposés pour mettre en œuvre la modification;
- les relations entre la modification et toute autre modification concernant la centrale.

b) Lot de modification

Lorsque la modification de conception est achevée, c'est-à-dire lorsque les composants logiciels, les composants matériels et la documentation sont le reflet exact de la nouvelle conception, il convient de construire un lot de modification permettant l'introduction de la modification dans le système opérationnel. La documentation du lot de modification doit décrire les modules matériels, les modules logiciels et les moyens pour introduire la modification, c'est-à-dire les équipements qui devraient être mis hors tension, la procédure qui doit être suivie pour charger le nouveau logiciel, ou bien aussi la référence qui peut être faite à des procédures de modification déjà existantes.

6.3.6.2 Caractéristiques

La demande de modification doit être identifiée de manière unique et doit être évaluée par le personnel compétent. Le résultat de cette évaluation (accord ou refus) doit être enregistré.

6.3.6.3 Vérification

a) Pour les systèmes de classe 1, il convient que le caractère exhaustif et la correction technique du lot de modification soient examinés par une équipe n'ayant pas été directement impliquée dans la réalisation de la modification mais qui soit techniquement compétente pour l'évaluer.

b) Le lot de modification ne doit pas être incorporé dans le système avant l'évaluation de la modification.

6.4 Qualification du système

Le présent article établit les prescriptions relatives au processus de qualification des systèmes d'I&C de classe 1 et 2 (voir 6.1.1.6). Ce processus garantit qu'un système d'I&C est en mesure de satisfaire, sur une base permanente, aux exigences de performance de base, imposées par la conception aux fonctions importantes pour la sûreté lorsque ce système est soumis aux conditions d'environnement spécifiées.

6.4.1 Plan de qualification

Un plan de qualification, identifiant tous les aspects à évaluer et à estimer afin d'obtenir et de conserver la qualification du système et des fonctions importantes pour la sûreté qu'il met en œuvre, doit être élaboré.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.3.6 System modification documentation

6.3.6.1 Content

a) Modification request

This document shall state

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

b) Modification package

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

6.3.6.2 Characteristics

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

6.3.6.3 Verification

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

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

6.4 System qualification

This subclause sets out requirements for the qualification process for class 1 and 2 I&C systems (see 6.1.1.6). This process provides assurance that an I&C system is capable of meeting, on a continuing basis, the design basis performance requirements needed for the functions important to safety while subject to the specified environmental conditions.

6.4.1 Qualification plan

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.4.1.1 Qualification fonctionnelle et environnementale

NOTE La qualification fonctionnelle et environnementale est également appelée «qualification du matériel».

Plusieurs techniques peuvent être utilisées pour démontrer la qualification fonctionnelle et environnementale du système, notamment l'essai de type, l'essai fonctionnel, les analyses théoriques et l'expérience opérationnelle en des applications similaires. L'essai de type est la méthode privilégiée (voir 4.1 de la CEI 60780).

a) Le système doit être qualifié pour ses conditions environnementales conformément aux prescriptions de la CEI 60780 et de la CEI 60987. Les conditions environnementales doivent inclure celles prescrites en 6.1.1.5.

b) Des séquences d'essais doivent être définies pour les essais de type des composants, de configurations de composants ou du système entier selon les cas, afin de:

- vérifier les caractéristiques fonctionnelles dans les conditions ambiantes normales et dans toutes les conditions extrêmes d'exploitation spécifiées;
- démontrer la résistance aux conditions sismiques.

6.4.1.2 Evaluation et estimation des logiciels

NOTE 1 L'évaluation et l'estimation du logiciel sont également appelées «qualification du logiciel».

L'évaluation et estimation du logiciel prennent en compte la rigueur du processus de développement du logiciel et l'étendue des essais et de la validation effectués sur le système intégré. Pour les logiciels prédéveloppés (LPD), le retour d'informations sur l'expérience opérationnelle peut constituer, sous certaines conditions, un facteur de compensation du manque d'information sur le processus de développement.

Les logiciels du système informatique à qualifier incluent

- le logiciel système, qui peut être un logiciel prédéveloppé non spécifique à la centrale;
- le logiciel d'application intégré au système, qui est spécifique à la centrale.

a) La qualification doit évaluer et estimer le logiciel système et le logiciel d'application afin de garantir que la qualité des logiciels est appropriée à l'obtention de la fiabilité requise pour les fonctions accomplies par le système.

b) Pour les systèmes de classe 1, les nouveaux logiciels doivent être évalués et estimés conformément aux prescriptions de la CEI 60880.

c) Il convient que les logiciels des équipements préexistants sélectionnés pour les systèmes de classe 1 aient été élaborés conformément à des directives et normes reconnues et appropriées au niveau de qualité élevé requis pour les fonctions de catégorie A (voir 8.1.2 de la CEI 61226). En particulier, les prescriptions de la CEI 60880-2 relatives aux logiciels et outils pré-développés et celles de la CEI 60987 doivent être respectées.

NOTE 2 La CEI 60880-2 définit des critères d'acceptation et des restrictions quant à l'utilisation de retours d'informations documentés sur l'expérience en matière de processus de qualification.

d) Il convient que les logiciels des équipements préexistants sélectionnés pour les systèmes de classe 2 aient été développés et fabriqués conformément à des directives et normes reconnues. Dans le cas contraire, des logiciels d'équipements sur étagère qualifiés, disposant d'un historique de leurs utilisations passées faisant état de leur fonctionnement satisfaisant dans des applications similaires, peuvent être utilisés (voir 8.1.2 de la CEI 61226).

NOTE 3 Les critères d'acceptation pour les logiciels des équipements sur étagère de classe 2 faisant état d'un fonctionnement satisfaisant rentrent dans le cadre d'une future norme CEI relative aux logiciels de classe 2.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

6.4.1.1 Functional and environmental qualification

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

Several techniques may be used to demonstrate the functional and environmental qualification of the system. These include type-testing, functional testing, theoretical assessments, and operating experience in similar applications. Type testing is the preferred method (see 4.1 of IEC 60780).

a) The system shall be qualified for its environmental conditions in accordance with the requirements of IEC 60780 and IEC 60987. Environmental conditions shall include those specified in 6.1.1.5.

b) Test sequences shall be defined for the type testing of components or configurations of components or the whole system as appropriate in order to

- check the functional characteristics under normal ambient conditions and at all specified limits of operation;
- demonstrate the resistance to seismic conditions.

6.4.1.2 Software evaluation and assessment

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

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

The software of the CB system to be qualified includes

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

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

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

c) Software of pre-existing equipment selected for class 1 systems should have been developed according to recognised guides and standards appropriate to the high level of quality required for category A functions (see 8.1.2 of IEC 61226). In particular, the requirements of IEC 60880-2 on pre-developed software and tools and the requirements of IEC 60987 shall be met.

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

d) Software of pre-existing equipment selected for class 2 systems should have been developed and manufactured according to recognised guides and standards. Otherwise, software of qualified off-the-shelf equipment with a documented history of satisfactory operation in similar applications may be used (see 8.1.2 of IEC 61226).

NOTE 3 Acceptance criteria for software of class 2 off-the-shelf equipment with documented satisfactory operation are in the scope of a future IEC standard on class 2 software.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

6.4.1.3 Qualification liée au produit et qualification spécifique à la centrale

Comme illustré à la figure 6, la qualification du système inclut

- des aspects liés aux produits pouvant ne pas être spécifiques à la centrale et pouvant avoir été précédemment évalués;
- des aspects spécifiques au système devant être estimés pendant le cycle de vie du système utilisé dans la centrale.

a) La qualification du matériel et du logiciel système d'un système réalisé à partir d'une famille d'équipements (voir 6.1.2.1) peut être déduite de la qualification précédemment réalisée sur des composants et des configurations de composants interconnectés. Dans ce cas, une analyse doit être menée afin de démontrer que le processus de qualification couvre la configuration finale du système utilisée dans la centrale, y compris pour l'implantation du montage et la répartition de la charge et de la température à l'intérieur des armoires.

b) Sur la base de l'analyse antérieure, il convient que le plan de qualification identifie toutes les nouvelles caractéristiques de conception du système et détermine la nécessité de mener des essais de qualification et des évaluations complémentaires.

6.4.2 Qualification supplémentaire des systèmes interconnectés

a) Un plan doit être établi pour les essais supplémentaires qui peuvent être exigés pour les systèmes d'I&C interconnectés, afin de compléter leur qualification propre, par exemple des essais d'interférence électromagnétique des interfaces pour l'implantation et la mise à la terre spécifiques.

b) La faisabilité et la cohérence des essais supplémentaires doivent être vérifiées dans le cadre de la vérification de la conception de l'architecture de l'I&C.

6.4.3 Maintien de la qualification

a) Un plan complémentaire doit être établi pour maintenir la qualification pendant le fonctionnement et la maintenance du système, lorsque certaines pièces sont remplacées par des pièces qui ne sont pas identiques et en cas de modifications fonctionnelles.

b) Le plan complémentaire doit permettre l'identification des modules qui réalisent des fonctions de catégorie A ou B, afin d'assurer la cohérence avec les versions validées.

6.4.4 Documentation

a) Il convient que les informations qui seront communiquées à l'autorité délivrant les licences figurent dans une liste.

b) Il convient que la liste fasse la distinction entre les informations nécessaires avant l'installation d'un système et les informations que doit fournir le candidat à la licence parallèlement à l'installation et à la mise en service, par exemple les rapports d'essais. Parmi les types d'informations pouvant être demandés figurent notamment

   - les descriptions (représentations détaillées des faits);
   - les explications (représentations des faits et raisonnements);
   - les démonstrations;
   - les justifications;
   - les preuves (déclarations vérifiables prouvant les assertions).

c) La documentation peut être regroupée en fonction de l'utilisation pour laquelle elle est nécessaire, mais dans son contenu doivent figurer

   - le rapport d'analyse préliminaire de sûreté et les documents récapitulatifs, afin d'estimer la conception préliminaire du système;

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.4.1.3 Product-related and plant-specific qualification

As illustrated in figure 6, the qualification of the system includes

- product-related aspects that may be not specific of the plant and which may have been previously assessed;
- system specific aspects to be assessed during the life cycle of the system used in the plant.

a) The qualification of the hardware and system software of a system built up by configuring an equipment family (see 6.1.2.1) may be derived from the qualification previously performed on individual components and configurations of interconnected components. In such cases, an analysis shall be completed to demonstrate that the qualification process covers the final configuration of the system used in the plant, including mounting arrangement, load and temperature distribution inside the cabinets.

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

6.4.2 Additional qualification of interconnected systems

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

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

6.4.3 Maintaining qualification

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

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

6.4.4 Documentation

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

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

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

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

- preliminary safety analysis report and summarising documents, in order to assess the conceptual and basic design of the system;

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

- des descriptions détaillées partielles ou de l'ensemble du système, afin de permettre une vérification et une validation indépendantes. Cette documentation peut contenir des informations détaillées sur les essais de tête de série des composants;
- des explications détaillées ou sommaires, des démonstrations ou des preuves, nécessaires pour justifier les décisions relatives à la conception et pour simplifier le processus de vérification et de validation indépendantes;
- des informations sur l'installation, l'intégration, la mise en service et les essais de réception réalisés en usine et sur site, afin de vérifier les étapes du cycle de vie et de sûreté qui se situent entre les phases de conception et d'exploitation;
- la documentation relative aux informations nécessaires à l'exploitation du système, afin de vérifier les procédures de maintien à long terme de la qualité du système.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

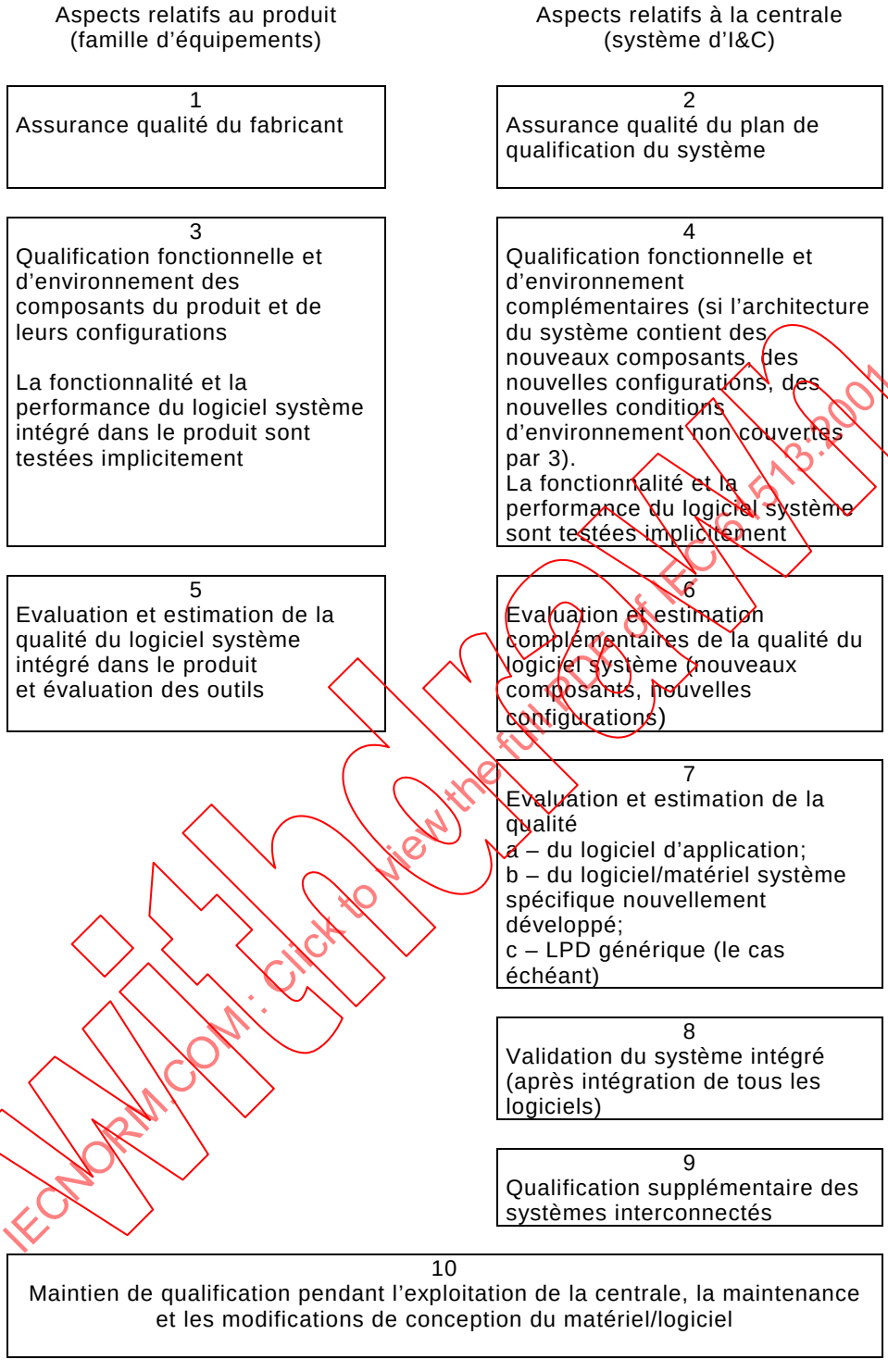


Figure 6 – Aspects devant être traités par le plan de qualification du système

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

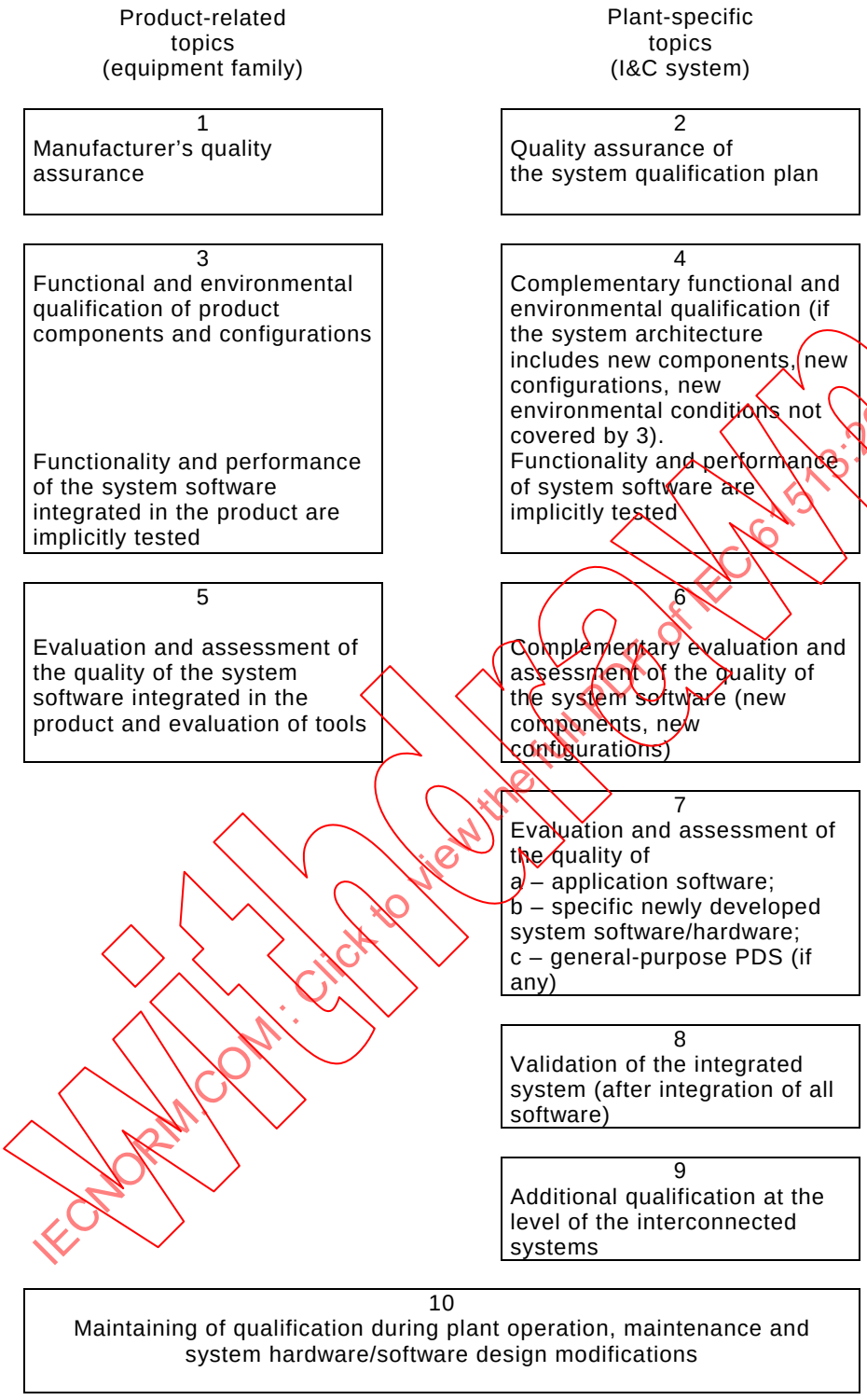


Figure 6 – Topics to be addressed in the system qualification plan

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.5 Résumé des principales prescriptions spécifiques aux différentes classes et catégories

Tableau 4 – Exigences relatives à la conception et à la qualification des systèmes et des équipements d'I&C

Classe 1	Classe 2	Classe 3
Equipements appropriés typiques		
Développés selon les normes CEI du secteur nucléaire (6.1.2.1)	COTS qualifiés et sélectionnés	COTS sélectionnés
Exigences relatives aux conditions préalables des équipements/famille d'équipements		
Permettre la séparation des redondances afin de satisfaire au critère de défaillance unique (6.1.1.2.1)		
Comportement déterministe par séquencement statique (6.1.1.2.2)	Comportement déterministe par méthodologie de dimensionnement (6.1.1.2.2)	
Minimiser la dépendance du fonctionnement du système vis à vis de la demande de la centrale (5.3.1.5.3)		
Moyens d'autosurveillance: CEI 60880 et CEI 60987 (6.1.1.2.3)		
Testabilité (6.1.1.2.4 et 6.1.3.1.2)		
Moyens pour mettre en œuvre l'indépendance: CEI 60709 (6.1.2.2.2)		
Exigences de qualification (6.4)		
Matériel: CEI 60780 Logiciel: CEI 60880 et CEI 60880-2	Matériel: CEI 60780 Logiciel	

Tableau 5 – Exigences relatives à la spécification et à la mise en œuvre des FSE

Catégorie A	Catégorie B	Catégorie C
Sous-systèmes indépendants pour les fonctions redondantes (6.1.2.4) Critère de défaillance unique pour l'exploitation et la maintenance (6.1.2.4)		
Indépendance vis à vis des moyens de commande de secours (5.3.1.5)		
Validation fonctionnelle (6.1.3.1.1)		
Analyse de fiabilité (6.1.3.1.2) (sa rigueur dépend de la catégorie)	Analyse de fiabilité (6.1.3.1.1) (sa rigueur dépend de la catégorie)	Analyse de fiabilité (6.1.3.1.1) (sa rigueur dépend de la catégorie)
Validation: CEI 60880 (6.2.4)	Validation: CEI 60880 avec exceptions possibles (6.2.4)	Validation: CEI 60880 avec exceptions possibles (6.2.4)
Vérification sur site de chaque voie de sûreté (6.2.5)		
Modifications de conception: CEI 60880 et CEI 60987 (6.1.7)		
Plans du système		
Equipe indépendante chargée du plan de vérification (6.2.1.1) Equipe indépendante chargée du plan de validation (6.2.4)	Personnes indépendantes dans l'équipe chargée du plan de validation (6.2.4)	Personnes indépendantes dans l'équipe chargée du plan de validation (6.2.4)
Documentation et vérifications		
Couverture des essais d'intégration exigée (6.3.4.3)	Couverture des essais d'intégration recommandée (6.3.4.3)	

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

6.5 Summary of main specific requirements for different classes and categories

Table 4 – Requirements for design and qualification of I&C systems and equipment

Class 1	Class 2	Class 3
Typical suitable equipment		
Developed according to IEC nuclear standards (6.1.2.1)	Selected qualified COTS	Selected COTS
Requirements on prerequisites of the equipment/equipment family		
Allow separation of redundancies to meet single-failure criterion (6.1.1.2.1)		
Deterministic behaviour by static scheduling (6.1.1.2.2)	Deterministic behaviour also by sizing methodology (6.1.1.2.2)	
Minimise dependencies of system operation from plant demand (5.3.1.5.3)		
Self-test facilities: IEC 60880 and IEC 60987 (6.1.1.2.3)		
Testability (6.1.1.2.4; 6.1.3.1.2)		
Features to implement independence: IEC 60709 (6.1.2.2.2)		
Qualification requirements (6.4)		
Hardware: IEC 60780 Software: IEC 60880 and IEC 60880-2	Hardware: IEC 60780 Software	

Table 5 – Requirements for the specification and implementation of the FSE

Category A	Category B	Category C
Independent subsystems for redundant functions (6.1.2.4) Single-failure criterion operation and maintenance (6.1.2.4)		
Independence from manual back-up control means (5.3.1.5)		
Functional validation (6.1.3.1.1)		
Reliability analysis (6.1.3.1.2) (rigour depends on category)	Reliability analysis (6.1.3.1.1) (rigour depends on category)	Reliability analysis (6.1.3.1.1) (rigour depends on category)
Validation: IEC 60880 (6.2.4)	Validation: IEC 60880 with possible exceptions (6.2.4)	Validation IEC 60880 with possible exceptions (6.2.4)
On-site verification of each safety channel (6.2.5)		
Design modifications : IEC 60880 and IEC 60987 (6.1.7)		
System planning		
Verification plan by independent team (6.2.1.1) Validation plan by independent team (6.2.4)	Validation plan including independent persons (6.2.4)	Validation plan including independent persons (6.2.4)
Documentation and verification		
Integration tests coverage required (6.3.4.3)	Integration tests coverage recommended (6.3.4.3)	

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

7 Intégration et mise en service globales

L'objectif de cette phase est d'intégrer sur site les systèmes d'I&C et d'assurer que toutes les fonctions d'I&C importantes pour la sûreté s'exécutent comme prévu pendant les essais de mise en service de la centrale. Le plan de mise en service des systèmes d'I&C est inclus dans le programme de mise en service des systèmes de la centrale (voir 4.4 de l'AIEA 75-INSAG-3).

7.1 Prescriptions relatives aux objectifs à atteindre

a) Les activités doivent être menées d'une manière systématique, selon une stratégie établie conformément aux plans d'installation des systèmes, aux plans d'intégration et de mise en service globales et aux plans de sécurité définis en 5.4 et 6.2.

b) Il convient que l'activité d'intégration globale soit effectuée avec tous les systèmes d'I&C concernés installés et contrôlés individuellement (voir 6.1.6).

c) Les bases de données doivent être chargées et les valeurs enregistrées doivent être justifiées et testées.

d) Le matériel et le logiciel des systèmes informatiques doivent être soumis à la gestion de configuration.

e) Pour les nouvelles centrales, il convient que la vérification et la validation sur site de toutes les fonctions importantes pour la sûreté soient achevées avant le chargement en combustible du réacteur.

7.2 Prescriptions relatives à la documentation

a) La documentation de l'intégration des systèmes d'I&C contenant les enregistrements de l'évolution chronologique des activités de vérification et de validation sur site doit être disponible avant l'étape d'exploitation.

b) Le rapport de mise en service globale doit confirmer que les systèmes d'I&C satisfont à toutes les attentes relatives à leur utilisation, et que les fonctions importantes pour la sûreté satisfont à leurs exigences (voir 5.2).

c) Les différences par rapport à la conception sont évaluées, corrigées et signalées à l'organisation en charge de l'exploitation, afin que tout effet sur le fonctionnement de la centrale puisse être pris en compte (voir 4.4.2 de l'AIEA 75-INSAG-3).

NOTE Les exigences exactes relatives à la documentation dépendront de l'organisation spécifique en charge de l'exploitation.

8 Exploitation et maintenance globales

L'exploitation des systèmes d'I&C peut débuter dès que l'évaluation des rapports de mise en service indique que l'étape a été franchie avec succès. L'exploitation peut continuer si les enregistrements relatifs à la maintenance n'exigent ni réparation ni modification. L'exploitation peut reprendre après une réparation ou une modification réussie et après l'évaluation des rapports correspondants.

Il convient que les conditions à respecter avant d'entrer dans la phase d'exploitation soient fixées au préalable. Les prescriptions suivantes sont indépendantes de cette recommandation:

- il convient que les systèmes aient été soumis à suffisamment d'essais pour confirmer que la fonctionnalité spécifiée a bien été obtenue. Si les essais ont identifié des défauts, ceux-ci doivent être documentés et, si possible, corrigés avant la mise à disposition;
- un manuel de l'utilisateur adéquat et les plans de maintenance doivent être disponibles.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

7 Overall integration and commissioning

The objective of this phase is to integrate the I&C systems on site and ensure that all I&C functions important to safety perform as expected during the commissioning tests of the plant. The commissioning plan of I&C systems is included in the commissioning programme of the plant systems (see 4.4 of IAEA 75-INSAG-3).

7.1 Requirements on the objectives to be achieved

a) The activities shall be carried out in a systematic way, with a strategy developed in accordance with the system installation plans, the overall integration and commissioning plans, and the security plans defined in 5.4 and 6.2.

b) The overall integration activity should be carried out with all the related I&C systems installed and individually tested (see 6.1.6).

c) Data bases shall be loaded, and stored values shall be justified and tested.

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

e) For new plants the on-site verification and validation of all functions important to safety should be completed before the reactor is fuelled.

7.2 Output documentation

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

b) The report on the overall commissioning activity shall confirm that the I&C systems satisfy all expectations for intended use and functions important to safety comply with the overall requirements specifications (see 5.2).

c) Variations from the design intent that are found are assessed, corrected and referred to the operating organisation so that any effect on plant operation can be taken into account (see 4.4.2 of IAEA 75-INSAG-3).

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

8 Overall operation and maintenance

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

8.1 Prescriptions relatives aux objectifs à atteindre

Les systèmes d'I&C sont exploités et entretenus afin que les exigences relatives aux fonctions d'I&C importantes pour la sûreté soient toujours remplies.

a) Les plans d'exploitation, de maintenance et de sécurité définis en 5.4 et 6.2 doivent être mis en œuvre.

b) Les procédures que doivent suivre les opérateurs de la centrale ou les équipes de maintenance dans les conditions d'exploitation normales et accidentelles doivent être disponibles dans la salle de commande ou à proximité. Il convient que leur présentation et leur contenu soient en accord avec la réglementation internationale ou nationale.

c) Pour les systèmes de classe 1, les procédures d'exploitation et de maintenance des logiciels de la CEI 60880 doivent être mises en œuvre.

8.2 Prescriptions relatives à la documentation

La documentation chronologique de l'exploitation, des réparations et de la maintenance doit être tenue à jour. Les enregistrements et les rapports d'exploitation doivent être analysés avec une périodicité définie afin d'identifier et réaliser toutes les activités de maintenance ou modifications qui pourraient s'avérer nécessaires.

NOTE Les exigences exactes relatives à la documentation dépendront de l'organisation spécifique en charge de l'exploitation.

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

8.1 Requirements on the objectives to be achieved

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

a) The plans for operation, maintenance and security defined in 5.4 and 6.2 shall be implemented.

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

c) For class 1 systems, the operation and maintenance procedures for software of IEC 60880 shall be implemented.

8.2 Output documentation

Chronological documentation of operation, repair and maintenance shall be maintained. Operation records and reports shall be evaluated with a defined periodicity in order to identify and initiate any maintenance or modification activities that might become necessary.

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001

Annexe A
(informative)

Problèmes de base de sûreté dans les centrales nucléaires

La présente annexe identifie les principaux concepts de sûreté qui sont pris en compte dans la présente norme pour la conception de l'I&C de la centrale nucléaire.

A.1 Objectifs de sûreté de la centrale

Toute activité industrielle présentant des risques pour le personnel, le public et l'environnement nécessite que l'exploitant prenne toutes les mesures réalisables afin de minimiser ces risques. Un risque typique de l'énergie nucléaire est le risque potentiel de rayonnement ionisant (voir article 201 de l'AIEA 50-C-D).

L'objectif général de la sûreté nucléaire est de protéger les personnes, la société et l'environnement en établissant et maintenant dans les centrales nucléaires une défense efficace contre le risque radiologique (voir 2.1 de l'AIEA 75-INSAG-3 et l'article 2 de l'AIEA 50-C-D).

L'objectif de la sûreté technique pour les centrales nucléaires existantes est une «probabilité cible» de survenance d'un endommagement grave du cœur inférieure à 10^{-4} événements par année d'exploitation de la centrale. La mise en œuvre de tous les principes de sûreté pour les futures centrales devrait permettre l'atteinte d'un meilleur objectif, à savoir moins de 10^{-5} événements par année d'exploitation de la centrale. Des mesures de gestion et d'atténuation des accidents graves devraient réduire, par un facteur au minimum de 10, la probabilité de survenance d'un important dégagement radiologique hors du site nécessitant une réponse extérieure au site (voir 2.3 de l'AIEA 75-INSAG-3).

A.2 Analyse de sûreté de la centrale

Une analyse de sûreté de la centrale nucléaire est réalisée afin d'établir et de confirmer la conception préliminaire des éléments importants pour la sûreté et d'assurer que la conception de la centrale est en mesure de respecter les limites et les niveaux de référence des doses et dégagements radiologiques fixés par les autorités de réglementation pour chaque condition d'exploitation de la centrale (voir article 6 de l'AIEA 50-SG-D11).

L'analyse de sûreté pourrait inclure

- la démonstration que les limites et conditions d'exploitation sont respectées lors de l'exploitation normale de la centrale;
- la caractérisation des EIH appropriés à la conception de la centrale et à son implantation;
- l'analyse et l'évaluation des séquences d'événements qui résultent des EIH;
- la comparaison des résultats de l'analyse avec les critères d'acceptation radiologique et les limites de conception;
- l'établissement et la confirmation de la conception préliminaire;
- la démonstration que la gestion des incidents de fonctionnement prévus et des situations accidentelles est possible par une réponse automatique du système de sûreté combinée avec les mesures prévues prises par l'opérateur.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

Annex A
(informative)

Basic safety issues in the NPP

This annex identifies the main safety concepts that are considered in this standard for the design of NPP I&C systems.

A.1 Plant safety objectives

Any industrial activity that presents risks to workers, members of the public and the environment requires the operator to take all reasonably practicable measures to keep these risks low. One typical risk of nuclear energy is the potential hazard of ionising radiation (see clause 201 of IAEA 50-C-D).

The general nuclear safety objective is to protect individuals, society and the environment by establishing and maintaining an effective defence against radiological hazard from NPPs (see 2.1 of IAEA 75-INSAG-3 and clause 2 of IAEA 50-C-D).

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

A.2 Plant safety analysis

A safety analysis of the nuclear plant design is performed to establish and confirm the design basis for the items important to safety and to ensure that the overall plant design is capable of meeting the limits and reference levels for radiological doses and releases set by the regulatory authority for each plant condition category (see clause 6 of IAEA 50-SG-D11).

The scope of the safety analysis might include

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

Ce processus d'analyse de sûreté de la centrale nucléaire est réalisé de manière itérative depuis le début de la conception de la centrale jusqu'à l'estimation finale de la sûreté de la centrale, et prend en compte tous les aspects relatifs à la configuration de la centrale qui peuvent avoir une influence sur la sûreté. L'analyse de sûreté de la centrale prend en compte le risque d'erreurs humaines au cours de l'exploitation et au cours de situations accidentelles.

Il convient que l'analyse démontre que les mesures devant être prises par les systèmes automatiques et les opérateurs permettront à la centrale de maintenir les doses de rayonnement reçues par le personnel du site et le public à un niveau inférieur aux limites prévues pour l'exploitation normale, les incidents de fonctionnement prévus et les situations accidentelles.

A.2.1 Analyse des séquences d'événements

L'objectif de l'analyse d'une séquence d'événements est l'identification systématique et détaillée de toutes les conséquences possibles d'un EIH sur la centrale, y compris celles concernant les systèmes auxiliaires et de soutien et celles dues à une éventuelle erreur de l'opérateur. Les résultats de cette analyse peuvent ensuite être utilisés pour déterminer si les exigences de sûreté établies dans le code de conception de l'AIEA ont été remplies (voir annexe de l'AIEA 50-C-D).

L'analyse (qualitative) d'un arbre d'événements et l'analyse (quantitative) de l'arbre de défaillances sont des outils analytiques utiles pour identifier les états possibles de la centrale après la survenance d'un EIH.

Il convient de noter qu'il n'est ni possible ni nécessaire d'inclure dans l'analyse de sûreté chaque séquence d'événements pouvant se produire. Cependant, l'analyse de sûreté doit identifier et évaluer de manière détaillée les EIH et les séquences d'événements qui conduisent à des cas limites de sûreté. L'expérience des centrales existantes doit être utilisée pour le choix de ces séquences d'événements.

Même avec les restrictions imposées aux cas limites décrits ci-dessus, une application rigoureuse de la méthode par arbre d'événements conduira, dans beaucoup de situations pratiques, à l'identification de nombreuses autres configurations de la centrale pour chaque EIH pouvant être analysées en détail. Ainsi, il est en général admissible de restreindre l'analyse détaillée à un certain nombre de séquences d'événements représentatives.

A.2.2 Estimation de la conception: méthodes déterministes et probabilistes

Des méthodes ont été élaborées afin d'évaluer l'atteinte des objectifs de sûreté (voir 3.3.4 de l'AIEA 75-INSAG-3).

Dans l'approche déterministe, des événements sont choisis pour déterminer une gamme d'événements initiateurs possibles, reliés entre eux et pouvant constituer un obstacle à la sûreté de la centrale.

L'analyse probabiliste est utilisée pour évaluer la probabilité d'apparition d'une séquence particulière et ses conséquences. Cette évaluation peut prendre en compte les effets des mesures d'atténuation internes et externes à la centrale.

Comparaison des méthodes: le manque de données sur le comportement des composants ou des systèmes et l'impossibilité de spécifier un mode approprié peuvent empêcher une approche probabiliste quantitative rigoureuse. Cependant, une approche probabiliste partielle peut souvent être complétée par un jugement technique qualitatif. D'autre part, une approche déterministe requiert un jugement d'ingénieur qui contient implicitement des considérations probabilistes qualitatives.

La pratique actuelle consiste à utiliser l'approche déterministe pour concevoir les systèmes et l'approche probabiliste pour optimiser des parties appropriées de la conception et pour évaluer la sûreté globale.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

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

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

A.2.1 Analysis of event sequences

The purpose of analysing an event sequence is to identify systematically and in detail all possible consequences of a PIE on the plant, including those arising from auxiliary and support systems and from possible operator error. The results of this event sequence analysis can then be used to determine if the safety requirements set down in the IAEA code of design have been met (see appendix of IAEA 50-C-D).

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

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

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

A.2.2 Assessment of design basis: deterministic/probabilistic methods

Methods have been developed to assess whether safety objectives have been met (see 3.3.4 of IAEA 75-INSAG-3).

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 61513:2001
Withdrawn

A.3 Défense en profondeur

Le concept de la défense en profondeur apporte une importante contribution à la notion de sûreté. Ce concept doit être appliqué à toutes les activités de sûreté, qu'elles concernent l'organisation, le comportement ou la conception, afin d'assurer que les dispositions de sûreté se recouvrent pour qu'en cas de défaillance, celle-ci soit compensée ou corrigée (voir article 2 de l'AIEA 50-C-D, 3.2 et annexe de l'AIEA 75-INSAG-3, 3.3 de l'AIEA 50-SG-D8 et 4.3 de l'AIEA 50-SG-D11).

Une première application du concept de défense en profondeur consiste à prévoir lors de la conception des ensembles indépendants mais complémentaires d'équipements et de procédures afin d'empêcher les accidents ou d'assurer une protection appropriée en cas de défaillance de la prévention. Exemples de niveaux de protection multiples:

- mise à disposition de moyens suffisants pour assurer chacune des fonctions de sûreté de base, c'est-à-dire le contrôle de la réactivité, l'évacuation de la chaleur et le confinement de la radioactivité;
- utilisation de dispositifs de protection fiables en complément des moyens de sûreté;
- amélioration de la commande de la centrale par des actions automatiques et manuelles;
- mise à disposition de composants et de procédures permettant d'atténuer les conséquences des accidents.

En règle générale, toutes les lignes de défense doivent être disponibles à tout moment pour les divers modes d'exploitation.

- L'objectif de la première ligne de défense est de maintenir une exploitation normale. Cela exige que la centrale soit conçue sur des bases solides et prudentes, et qu'elle soit construite et exploitée en accord avec des niveaux de qualité et des pratiques technologiques appropriés.
- L'objectif de la deuxième ligne de défense est de détecter et prendre en compte tout écart par rapport aux conditions normales d'exploitation afin d'empêcher les incidents de fonctionnement prévus de se transformer en situations accidentelles.
- Pour la troisième ligne de défense, il est supposé, bien que ce soit très improbable, que l'intensification de certains incidents de fonctionnement prévus ne peut être arrêtée par une ligne précédente. Des dispositifs et procédures supplémentaires sont alors prévus pour contrôler les conséquences des situations accidentelles qui en résultent. Un autre objectif essentiel de cette ligne de défense est de parvenir à une situation stable et acceptable suite à un accident.
- Au-delà de la troisième ligne de défense, il existe d'autres contributions à la protection du public par les caractéristiques complémentaires de la centrale (non importantes pour la sûreté), ainsi que des plans de préparation d'urgence, qui sont largement indépendants de la conception des réacteurs.

Une seconde application du concept de défense en profondeur consiste à construire et exploiter la centrale de manière que les matières radioactives soient confinées au sein d'une succession de barrières physiques. Ces barrières sont essentiellement passives et incluent généralement le combustible lui-même, la gaine du combustible, le périmètre du circuit de refroidissement primaire et l'enveloppe de confinement. La conception doit garantir l'efficacité appropriée et la protection de chacune de ces barrières.

IECNORM.COM : Click to view the full PDF of IEC 61513:2001

A.3 Defence in depth

A major contribution to the safety philosophy is provided by the defence-in-depth concept. This concept has to be applied to all safety activities, whether organisational, behavioural or design-related, to ensure that there are overlapping safety provisions so that if a failure does occur, it would be compensated for or corrected (see clause 2 of IAEA 50-C-D; 3.2 and appendix of IAEA 75-INSAG-3; 3.3 of IAEA 50-SG-D8 and 4.3 of IAEA 50-SG-D11).

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

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

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

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

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

Withdrawn
IECNORM.COM : Click to view the full PDF of IEC 61513:2001