

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

60709

Deuxième édition
Second edition
2004-11

**Centrales nucléaires de puissance –
Systèmes d'instrumentation et de
contrôle commande importants
pour la sûreté – Séparation**

**Nuclear power plants –
Instrumentation and control systems
important to safety – Separation**



Numéro de référence
Reference number
CEI/IEC 60709:2004

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/searchpub) 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/online_news/justpub) 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/searchpub) 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/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- Customer Service Centre

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

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

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

60709

Deuxième édition
Second edition
2004-11

**Centrales nucléaires de puissance –
Systèmes d'instrumentation et de
contrôle commande importants
pour la sûreté – Séparation**

**Nuclear power plants –
Instrumentation and control systems
important to safety – Separation**

© IEC 2004 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, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

R

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

SOMMAIRE

AVANT-PROPOS.....	4
INTRODUCTION.....	8
1 Domaine d'application	12
2 Références normatives.....	12
3 Termes et définitions	14
4 Principes généraux de séparation à l'intérieur de l'I&C importants pour la sûreté	16
4.1 Généralités.....	16
4.2 Erreurs de conception	18
4.3 Défaillances d'un système d'I&C	18
4.3.1 Défaillances uniques aléatoires	18
4.3.2 Défaillances multiples dues à une cause commune unique.....	18
4.4 Défaillances dans l'installation	20
4.4.1 Conditions d'ambiance	20
4.4.2 Interférences électromagnétiques (IEM).....	20
4.4.3 Défaillances des systèmes, des matériels ou des structures de l'installation	20
4.4.4 Erreurs humaines	20
4.5 Défaillances dues à des événements extérieurs à l'installation	20
4.5.1 Phénomènes naturels.....	20
4.5.2 Causes extérieures humaines.....	22
4.6 Conditions spéciales de fonctionnement.....	22
4.7 Problème de la séparation dans les installations existantes.....	22
5 Bases de conception	24
5.1 Protection incendie.....	24
5.2 Conditions d'ambiance durant et après les accidents.....	24
5.3 Dispositifs d'isolement.....	24
5.3.1 Généralités.....	24
5.3.2 Caractéristiques d'isolement.....	26
5.3.3 Priorités de mise en service.....	26
5.4 Indépendance du système de commande	28
6 Exigences en matière de séparation du câblage	30
6.1 Exigences générales	30
6.2 Séparation.....	30
6.2.1 Séparation des câbles redondants dans un système d'I&C importants pour la sûreté	30
6.2.2 Moindres distances de séparation	30
6.2.3 Circuits associés	32
6.2.4 Séparation du câblage des différentes catégories de sûreté	34
6.2.5 Séparation des câbles de commande des câbles de puissance	34
6.2.6 Séparation du câblage, des canalisations et de la tuyauterie	34
6.2.7 Généralités sur le cheminement des câbles.....	34
6.2.8 Armoires de commande, pupitres, panneaux et câbles attachés	34
6.3 Protections physique et thermique.....	38
6.4 Protection incendie.....	38
6.5 Identification.....	38

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	9
1 Scope.....	13
2 Normative references	13
3 Terms and definitions	15
4 General principles for separation within I&C systems important to safety.....	17
4.1 General.....	17
4.2 Design errors	19
4.3 I&C system failure events.....	19
4.3.1 Single random failure.....	19
4.3.2 Multiple failures from a single common cause	19
4.4 Plant failure events.....	21
4.4.1 Environmental conditions.....	21
4.4.2 Electromagnetic interference	21
4.4.3 Failure of plant systems, equipment or structures.....	21
4.4.4 Operator error	21
4.5 External failure events.....	21
4.5.1 Natural events	21
4.5.2 External man-made causes	23
4.6 Special operating conditions.....	23
4.7 Separation issues at existing plants	23
5 Design basis.....	25
5.1 Fire protection	25
5.2 Environmental conditions during and after accidents	25
5.3 Isolation devices	25
5.3.1 General.....	25
5.3.2 Isolation characteristics	27
5.3.3 Actuation priority	27
5.4 Independence from control systems	29
6 Requirements for cabling separation	31
6.1 General requirement	31
6.2 Separation.....	31
6.2.1 Separation of redundant cables inside the I&C system important to safety	31
6.2.2 Lesser separation distances	31
6.2.3 Associated circuits.....	33
6.2.4 Separation of system cables of different safety categories.....	35
6.2.5 Separation of signal cables from power cables	35
6.2.6 Separation of cables from tubes or pipes	35
6.2.7 General routing considerations	35
6.2.8 Control room cabinets, desks, panels and related cables.....	35
6.3 Thermal and physical protection.....	39
6.4 Fire protection	39
6.5 Identification.....	39

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE COMMANDE IMPORTANTES POUR LA SÛRETÉ – SÉPARATION

AVANT-PROPOS

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

La Norme internationale CEI 60709 a été établie par le sous-comité 45A: Instrumentation et contrôle commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition parue en 1981 et constitue une révision technique. Cette révision de la CEI 60709 vise à:

- ajuster le format du document afin d'être conforme aux directives CEI/ISO portant sur le style des normes;
- étendre le domaine de celle-ci pour couvrir tous les systèmes importants pour la sûreté, et la séparation entre et à l'intérieur des systèmes de catégories A, B, C et des systèmes non catégorisés;
- mettre en cohérence la norme avec les nouvelles révisions des documents de l'AIEA (remplaçant les D3 et D8) et élargir le domaine pour inclure de nouveaux aspects de l'indépendance;
- fournir des références normatives pertinentes;

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
INSTRUMENTATION AND CONTROL SYSTEMS
IMPORTANT TO SAFETY – SEPARATION**

FOREWORD

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

International Standard IEC 60709 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1981 and constitutes a technical revision. This revision of IEC 60709 is intended to accomplish the following:

- adjust the document format to follow current IEC/ISO directives on style of standards;
- expand to cover all systems important to safety, and separation between and within category A, B, C and un-categorised systems;
- align with the new revisions of IAEA documents (replacing D3 and D8) and broaden the scope to include other aspects of independence;
- provide references to relevant normative standards;

- couvrir de nouvelles technologies qui soit présentent des questions particulières de séparation, soit fournissent un moyen nouveau pour l'assurer;
- inclure les articles de la CEI 60639 (qui va être retirée en tant que norme) qui ne sont pas couvertes de façon appropriée dans la CEI 61513 ou qui nécessitent un développement, par exemple l'isolement, les interactions entre le contrôle et la protection, etc.;
- étendre le concept de perturbation électromagnétique en tant qu'initiateur de défaillance présentant potentiellement le caractère de DCC (défaillance de cause commune) ainsi que l'utilisation de la séparation comme moyen permettant de minimiser le risque d'interférence;
- améliorer les exigences et les conseils relatifs aux zones de câblage congestionnées, par exemple salle de commande, passages des chemins de câbles, etc.;
- introduire le concept de "circuits associés" (issu de la pratique américaine) pour prendre en compte les câbles non classés de sûreté qui ne sont pas séparés des câbles classés de sûreté;
- fournir des lignes directrices pour l'application des normes de qualification incendie des câbles importants pour la sûreté (telles que la série CEI 60332). Cela comprend les sujets suivants:
 - prise en compte des barrières comme alternative à la séparation,
 - assimilation des câbles à des barrières potentielles, et
 - concepts similaires tels que l'assimilation des fibres optiques à des barrières aux IEM (interférences électromagnétiques), assimilation des blindages de câbles à des barrières contre l'endommagement physique, etc.
- traiter des implications des circuits basse énergie, telles que l'utilisation possible de l'analyse pour réduire les distances minimales de séparation;
- faire la revue des exigences existantes, mettre à jour la terminologie et les définitions;
- fournir un guide d'application de la présente norme aux tranches en exploitation.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/537/FDIS	45A/545/RVD

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

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

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

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

- cover new technologies that either present unique separation issues or provide new means of achieving independence;
- include provisions from IEC 60639 (which will be withdrawn as a standard) that are not adequately covered in IEC 61513 or that required further expansion, e.g. isolation, control/protection interaction, etc.;
- expand concepts of electromagnetic disturbance as a failure initiator with CCF potential and the use of separation as a means to minimise risk of interference;
- enhance requirements and guidance for areas of cable congestion, e.g. control room, cable spreading galleries, etc.;
- introduce the concept of “associated circuits” (from US practice) to deal with non-safety cables that are not separated from safety cables;
- provide guidance for the application of fire qualification standards (such as the IEC 60332 series) to cables important to safety. This includes the topics:
 - barriers as an alternative to separation,
 - cables themselves as potential barriers, and
 - similar concepts such as fibre optics as a barrier to EMI, armour as a barrier to physical damage, etc.;
- address the implications of low energy circuits, such as the possible use of analysis to reduce the minimum separation distance;
- review existing requirements, update terminology and definitions;
- provide guidance for the application of the standard to existing plants.

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

FDIS	Report on voting
45A/537/FDIS	45A/545/RVD

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

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

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

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

INTRODUCTION

Contexte technique, questions importantes et structure du document

Les systèmes d'I&C (Instrumentation et Contrôle commande) importants pour la sûreté des centrales nucléaires de puissance doivent tolérer les effets liés aux défaillances des matériels de la centrale comme ceux liés aux risques internes et externes. Différentes techniques sont disponibles pour augmenter le niveau de tolérance des systèmes d'I&C à de tels effets, comprenant les dispositions d'indépendance prises aux niveaux des systèmes, des sous-systèmes, des matériels. Pour prétendre à l'indépendance de systèmes ou de matériels, il faut qu'une séparation appropriée soit prévue et maintenue. Cette norme fournit des exigences techniques et des recommandations pour la mise en œuvre de la séparation lors de la conception des systèmes d'I&C.

L'objet de cette norme est le suivant:

- à l'Article 4, identifier un certain nombre de causes possibles de défaillances et, considérant celles-ci, stipuler un ensemble d'exigences à satisfaire lors de la conception des systèmes d'I&C importants pour la sûreté de façon à assurer qu'ils remplissent de la meilleure façon possible les missions auxquelles ils sont destinés. Ces exigences s'appliquent au système d'I&C comme un tout. L'Article 4 présente aussi des lignes directrices relatives à la séparation dans le cadre de la modernisation de systèmes d'I&C dans des centrales nucléaires de puissance existantes;
- à l'Article 5, établir les critères de base de la conception des systèmes d'I&C importants pour la sûreté qui prennent en compte les causes de défaillances identifiées à l'Article 4;
- à l'Article 6, donner les exigences devant être satisfaites pour la séparation du câblage des systèmes d'I&C importants pour la sûreté.

Position du présent document dans la série de normes du SC 45A

La CEI 60709 est un document du deuxième niveau qui est directement référencé par la CEI 61513 pour ce qui concerne les séparations électrique et physique exigées entre les sous-systèmes des différents trains de sûreté des systèmes d'I&C importants pour la sûreté et entre les systèmes I&C importants pour la sûreté et ceux qui ne sont pas importants pour la sûreté.

La CEI 61226 établit les principes de catégorisation des fonctions, des systèmes et des matériels d'I&C suivant leur niveau d'importance pour la sûreté. Elle exige qu'une séparation appropriée soit prévue entre les fonctions des différentes catégories. La CEI 61226 fait référence à la CEI 60709 comme la norme traitant des exigences de séparation.

Pour plus de détails sur la série de normes du SC 45A, voir le dernier paragraphe de cette introduction.

Recommandations et limites relatives à l'application de cette norme

La CEI 60709 est applicable aux matériels et systèmes d'I&C importants pour la sûreté. Elle donne les exigences de séparations physique et électrique qui constituent un moyen permettant d'assurer l'indépendance entre les fonctions implantées dans ces matériels et ces systèmes. Les autres aspects relatifs à l'indépendance qu'il peut être nécessaire de considérer en ce qui concerne les défaillances de cause commune ne sont pas couverts par cette norme.

Par ailleurs cette norme ne fournit aucune prescription complémentaire liée à la disponibilité, ni aucune exigence détaillée portant sur l'élimination des interférences électriques.

INTRODUCTION

Background, main issues and organization of the standard

I&C systems important to safety in nuclear power plants need to tolerate the effects of plant / equipment faults as well as internal and external hazards. Various techniques are available to increase the level of tolerability of I&C systems to such effects, including the provision of independent systems, subsystems and equipment. For claims to be made of independence between such systems and equipment, adequate separation must be provided and maintained. This standard provides technical requirements and recommendations for the implementation of separation in the design of I&C systems.

The object of this standard is as follows:

- in Clause 4, to identify a certain number of possible causes of failures and to lay down, taking these causes into consideration, a set of requirements to be followed when designing an I&C system important to safety in order to ensure that its purpose is fulfilled in the best possible way. These requirements apply to the I&C system as a whole. Clause 4 also presents guidance on separation when modernising I&C systems at existing nuclear power plants;
- in Clause 5, to establish design basis criteria for I&C systems important to safety that take the causes of failure identified in Clause 4 into consideration;
- in Clause 6, to give requirements to be fulfilled for cabling separation within an I&C system important to safety.

Situation of the current standard in the structure of the SC 45A standard series

IEC 60709 is a document of the second level, directly referenced by IEC 61513 in regard to physical and electrical separation being required between subsystems of different safety trains of I&C systems important to safety, and between I&C systems important to safety and those that are not important to safety.

IEC 61226 establishes the principles of categorization of I&C functions, systems and equipment according to their level of importance to safety. It then requires that adequate separation be provided between functions of different categories. IEC 61226 refers to IEC 60709 as the normative standard regarding requirements of separation.

For more details on the structure of the SC 45A standard series, see the last paragraph of this introduction.

Recommendations and limitations regarding the application of the Standard

IEC 60709 applies to I&C systems and equipment important to safety. It establishes requirements for physical and electrical separation as one means to provide independence between the functions performed in those systems and equipment. Other aspects of independence that may be required to address concerns of common cause failure are not included in this standard.

Additional requirements relating to availability and detailed requirements for the elimination of electrical interference are not given in this standard.

Description de la structure de la série des normes du SC 45A et relations avec les documents de la CEI, de l'AIEA et de l'ISO

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

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

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

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

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, publication fondamentale de sécurité, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales des parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur d'application nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier le guide NS-R-1 "Safety of Nuclear Power Plants: Design – Requirements" et le guide NS-G-1.3 "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants – Safety Guide". La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Description of the structure of the SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top level document of the SC 45A standard series is IEC 61513. It provides general requirements for instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs). IEC 61513 structures the SC 45A standard series.

IEC 61513 refers directly to other SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer based systems, hardware aspects of computer based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, SC 45A standards generally not directly referenced by IEC 61513 are standards related to specific equipment, technical methods or specific activities. Usually these documents, which make reference to second level documents for general topics, can be used on their own.

A fourth level extending the SC 45A standard series corresponds to the technical reports, which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508-1, -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. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA 50-C-QA for topics related to quality assurance.

The SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA Code on the safety of nuclear power plants and in the IAEA safety series, in particular the Requirements NS-R-1, "Safety of Nuclear Power Plants: Design" and the Safety Guide NS-G-1.3, "Instrumentation and control systems important to safety in Nuclear Power Plants". The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE COMMANDE IMPORTANTS POUR LA SÛRETÉ – SÉPARATION

1 Domaine d'application

La présente norme est applicable aux systèmes d'instrumentation et de contrôle commande (I&C) des centrales nucléaires ainsi qu'à leurs câbles importants pour la sûreté, telle que définie dans le guide de sûreté de l'AIEA NS-G-1.3. Elle est aussi applicable aux installations temporaires qui font partie de ces systèmes d'I&C importants pour la sûreté (par exemple l'équipement auxiliaire pour les essais de mise en service et l'expérimentation). L'Article 6 traite plus particulièrement du câblage des systèmes importants pour la sûreté.

Cette norme s'applique à l'I&C des nouvelles centrales nucléaires comme aux I&C modernisés ou rénovés de centrales existantes. Pour les centrales existantes, seul un sous-ensemble des exigences est applicable; ce sous-ensemble est à identifier au début de chaque projet.

Lorsque l'indépendance est exigée par une norme de sûreté telle que les guides sûreté AIEA ou la CEI 61513, un des moyens pour atteindre l'indépendance est la séparation physique des systèmes et des matériels qui réalisent des fonctions importantes pour la sûreté.

Cette norme définit les exigences techniques qui doivent être satisfaites par les systèmes d'instrumentation et de contrôle commande importants pour la sûreté et leurs câbles, ainsi que les contrôles nécessaires afférents, de façon à obtenir une séparation physique appropriée entre les parties redondantes de système ou entre un système et un autre système. Cette séparation est nécessaire pour prévenir ou minimiser l'impact sur la sûreté qui pourrait résulter de fautes ou de défaillances qui pourraient être propagées ou qui pourraient affecter plusieurs parties d'un système ou de plusieurs systèmes.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60332 (toutes les parties), *Essais des câbles électriques soumis au feu*

CEI 60964, *Conception des salles de commande des centrales nucléaires de puissance*

CEI 61000 (toutes les parties), *Compatibilité électromagnétique (CEM)*

CEI 61000-6-5, *Compatibilité électromagnétique (CEM) – Partie 6-5: Normes génériques – Immunité pour les environnements de centrales électriques et de postes*

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

CEI 61513, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

CEI 62096, *Centrales nucléaires – Système de contrôle commande et d'instrumentation – Guide pour décider d'une modernisation*

AIEA Guide de Sûreté NS-G-1.3, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants – Safety Guide* (en anglais seulement)

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SEPARATION

1 Scope

This standard is applicable to nuclear power plant instrumentation and control (I&C) systems, and their cables, that are important to safety, as defined in IAEA Safety Guide NS-G-1.3. It is also applicable to temporary installations which are part of those I&C systems important to safety (for example, auxiliary equipment for commissioning tests and experiments). Clause 6 is intended particularly for the cabling of the I&C systems important to safety.

This standard applies to the I&C of new nuclear power plants as well as to I&C upgrading or back-fitting of existing plants. For existing plants, only a subset of the requirements is applicable; this subset is to be identified at the beginning of any project.

Where independence is required by general safety standards such as IAEA safety guides or IEC 61513, one aspect of achieving this independence is physical separation between the systems and their equipment that perform functions important to safety.

This standard defines the assessments needed and the technical requirements to be met for I&C systems important to safety and their cables, in order to achieve adequate physical separation between redundant sections of a system and between a system and another system. This separation is needed to prevent or minimise the impact on safety that could result from faults and failures which could be propagated or affect several sections of a system or several systems.

2 Normative references

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

IEC 60332 (all parts), *Tests on electric cables under fire conditions*

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

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61000-6-5, *Electromagnetic compatibility (EMC) – Part 6-5: Generic standards – Immunity for power station and substation environments*

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

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 62096, *Nuclear power plants – Instrumentation and control – Guidance for the decision on modernisation*

IAEA Safety Guide NS-G-1.3, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

3 Termes et définitions

Pour les besoins du présent document, les définitions suivantes sont applicables.

3.1

circuit associé

circuit de catégorie de sûreté inférieure qui n'est pas physiquement séparé ou qui n'est pas électriquement isolé des circuits de catégorie supérieure par des distances de séparation acceptables, des structures de classe de sûreté, des barrières, ou des dispositifs d'isolement électrique, mais qui satisfait aux critères appropriés de sûreté

3.2

barrière

dispositif ou structure interposé entre des matériels ou des circuits redondants importants pour la sûreté ou entre des matériels ou des circuits importants pour la sûreté et une source potentielle de dommage afin de limiter à un niveau acceptable ceux concernant le système d'I&C importants pour la sûreté

3.3

chemin de câbles

cheminement physique dans la centrale suivant lequel de nombreux câbles peuvent être tirés, tel qu'un local ou une buse dans un bâtiment de la centrale, ou un tube, un plateau ou une gaine métallique ou une alvéole (câbles souterrains) ou une gaine aérienne de franchissement routier

3.4

défaillance de cause commune (DCC)

défaillance de deux ou de plusieurs structures, systèmes ou composants due à une cause ou à un événement spécifique unique

[AIEA NS-G-1.3]

3.5

dispositif d'isolement

dispositif d'un circuit qui empêche que des dysfonctionnements dans une partie de celui-ci n'aient des conséquences inacceptables sur les autres parties du circuit ou sur d'autres circuits

3.6

événement initiateur hypothétique (EIH)

événement identifié durant la conception comme capable d'entraîner des incidents de fonctionnement prévus et des situations accidentelles

[AIEA NS-G-1.3]

3.7

redondance

mise en place de structures de remplacement (identiques ou différentes), systèmes ou composants, afin qu'un élément quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément

[AIEA NS-G-1.3]

3.8

groupe de sûreté

assemblage de matériels destiné à réaliser toutes les actions nécessitées par un événement initiateur hypothétique particulier pour assurer que les limites spécifiées lors de la conception de base pour les incidents de fonctionnement et les accidents de référence ne sont pas dépassées

[AIEA NS-G-1.3]

3 Terms and definitions

For the purposes of this document, the following definitions apply.

3.1

associated circuit

circuit of a lower safety category that is not physically separated or is not electrically isolated from the circuit(s) of the higher category by acceptable separation distances, safety class structures, barriers, or electrical isolation devices but meets suitable criteria for safety

3.2

barrier

device or structure interposed between redundant equipment or circuits important to safety, or between equipment or circuits important to safety and a potential source of damage to limit damage to the I&C system important to safety to an acceptable level

3.3

cable route

physical pathway through the plant along which multiple cables can be laid, such as through a room or duct in the plant building, or a metal duct, tray, or tube, or a duct below or gantry over roads

3.4

common cause failure (CCF)

failure of two or more structures, systems or components due to a single specific event or cause

[IAEA NS-G-1.3]

3.5

isolation device

device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits

3.6

postulated initiating event (PIE)

event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[IAEA NS-G-1.3]

3.7

redundancy

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

[IAEA NS-G-1.3]

3.8

safety group

assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

[IAEA NS-G-1.3]

4 Principes généraux de séparation à l'intérieur de l'I&C importants pour la sûreté

4.1 Généralités

La CEI 61226 définit la façon de classer les fonctions de sûreté par rapport à leur importance au niveau de la sûreté, et exige une séparation physique afin d'assurer la protection contre la propagation des défaillances dues aux effets physiques, et de contrer les mises en péril simultanées des systèmes redondants.

Un système d'I&C peut réaliser des fonctions appartenant à plus d'une catégorie. Dans ce cas, la catégorie attribuée au système doit correspondre à la catégorie de la fonction la plus haute réalisée par le système. Par exemple, lorsqu'un système supporte en même temps des fonctions de catégories A et B, ce système est de catégorie A.

Lors de la conception des systèmes d'I&C importants pour la sûreté, les principes généraux suivants doivent être appliqués pour maintenir l'indépendance des systèmes redondants ainsi que l'indépendance entre les différents systèmes, et pour assurer que la redondance et la diversité (prévues pour assurer une grande disponibilité des systèmes importants pour la sûreté) sont efficaces.

- Les systèmes réalisant des fonctions de catégorie A doivent être protégés des effets physiques résultants de fautes ou d'actions normales situées à l'intérieur
 - a) de parties redondantes de ces systèmes, et
 - b) de systèmes de catégorie inférieure.

Les fautes à prendre en compte doivent comprendre les fautes internes au système d'I&C et à son système d'alimentation, aussi bien que les fautes qui surviennent comme le résultat d'événements externes aux systèmes d'I&C.

Dans certains cas, il peut être nécessaire de mettre en place une séparation physique entre différents systèmes réalisant des fonctions de catégorie A, lorsqu'il est exigé que ces fonctions soient indépendantes.

- Les systèmes réalisant des fonctions de catégorie B doivent être protégés des effets physiques résultant de fautes ou d'actions normales situées à l'intérieur
 - a) de parties redondantes de ces systèmes, et
 - b) de systèmes de catégorie inférieure.

Les fautes à prendre en compte doivent comprendre les fautes internes au système d'I&C et à son système d'alimentation mais elles peuvent exclure celles qui surviennent comme le résultat d'événements externes aux systèmes d'I&C. Dans le cas où il est acté que des fonctions de catégorie B assurent une protection contre des événements spécifiques dangereux, alors les systèmes en question doivent suivre les principes de la catégorie A. Par exemple, dans certains pays, tous les systèmes nécessaires pour atteindre et maintenir l'état d'arrêt long terme doivent être protégés contre le risque incendie quelque soit leur catégorie.

- Il peut être nécessaire de protéger certains systèmes réalisant des fonctions de catégorie C des conséquences des fautes survenant dans d'autres systèmes. Cela doit être déterminé au cas par cas.
- Il n'est pas nécessaire de protéger les systèmes non catégorisés des conséquences des fautes situées dans d'autres systèmes.

La séparation prévient

- a) la propagation de défaillance de système à système,
- b) la propagation de défaillance entre les parties redondantes à l'intérieur des systèmes,
- c) les défaillances de cause commune dues aux risques internes communs.

4 General principles for separation within I&C systems important to safety

4.1 General

IEC 61226 defines how safety functions are classified according to their significance to safety, and requires physical separation to provide protection against propagation of failures due to physical effects, and against jeopardising redundant systems simultaneously.

An I&C system may perform functions in more than one category. In such a case, the category designation of the system shall be of the highest category function performed by it. For example, a system performing both category A and B functions is identified as a category A system.

As a design basis for the I&C systems that are important to safety, the following general principles shall be applied to maintain the independence of redundant systems and between different systems, and to ensure that the redundancy and diversity (provided to achieve high reliability of systems important to safety) are effective.

- Systems performing category A functions shall be protected from consequential physical effects caused by faults and normal actions within
 - a) redundant parts of those systems, and
 - b) systems of a lower category.

The faults considered shall include those internal to the I&C system and its power supply as well as those that occur as a result of events external to the I&C systems.

In some cases, it may be necessary to provide physical separation between different systems performing category A functions where those functions are required to be independent.

- Systems performing category B functions shall be protected from consequential physical effects caused by faults and normal actions within
 - a) redundant parts of those systems, and
 - b) systems of a lower category.

The faults considered shall include those internal to the I&C system and its power supply, but may exclude those that occur as a result of events external to the I&C systems. In cases where category B functions are claimed to provide protection in the event of specific hazards, then those systems shall follow the principles of category A. For example, in some countries, all systems required to achieve and maintain long-term shutdown must be protected against fire hazard regardless of their category.

- Certain systems performing category C functions may need to be protected from the influences of faults in other systems. This shall be determined on a case-by-case basis.
- Un-categorised systems need not be protected from influences of faults in other systems.

Separation prevents

- a) propagation of failures from system to system,
- b) propagation of failures between redundant parts within systems,
- c) common cause failures due to common internal plant hazards.

Lorsque la séparation physique est exigée, on doit se prémunir contre la propagation des défaillances

- survenant simultanément dans des composants de système multiples comme conséquence d'un EIH;
- entre des systèmes d'une même catégorie de sûreté;
- entre des groupes de sûreté redondants du même système d'I&C importants pour la sûreté, et;
- de systèmes de catégorie inférieure vers des systèmes de catégorie supérieure et dans certains cas particuliers de systèmes de catégorie supérieure vers des systèmes de catégorie inférieure.

Les types possibles d'événements initiateurs de défaillances contenus dans les paragraphes suivants doivent être considérés (à savoir identifiés, documentés et justifiés). Des mesures appropriées doivent être prises dans les systèmes d'I&C importants pour la sûreté pour limiter les effets possibles de ces événements à un niveau acceptable. Il est recommandé de considérer les effets des combinaisons de défaillances.

4.2 Erreurs de conception

Au stade de la conception, on ne peut écarter l'existence potentielle d'erreurs dans la spécification des exigences des systèmes d'I&C importants pour la sûreté. De telles erreurs de conception peuvent entraîner la propagation de fautes entre les systèmes, par exemple un isolement insuffisant au niveau du câblage, un dimensionnement inapproprié des conducteurs, etc. Les moyens permettant de prendre en compte ce genre de défaillance comprennent généralement des mesures de précaution au niveau de la conception concernant la séparation physique et l'isolement électrique.

4.3 Défaillances d'un système d'I&C

Les événements initiateurs de défaillances qui ont leurs causes à l'intérieur de chaque système d'I&C important pour la sûreté doivent être pris en considération. Ces événements sont généralement caractérisés par des effets mécaniques et électriques localisés qui peuvent avoir différentes conséquences fonctionnelles. Des défaillances uniques dans des processeurs centraux ou dans des interfaces de communication multiplexées peuvent aussi potentiellement entraîner des défaillances multiples. Les défaillances dans le domaine de l'I&C peuvent être réparties comme suit.

4.3.1 Défaillances uniques aléatoires

On doit prendre en compte toutes les défaillances uniques aléatoires d'un système d'I&C, y compris celle de son alimentation en énergie, normale ou auxiliaire, qui peuvent entraîner un mauvais fonctionnement d'un composant, un court-circuit, une ouverture de circuit, une mise à la terre, un changement de tension ou de fréquence, une défaillance de composant mécanique ou un incendie local. De tels événements peuvent être la conséquence d'une surcharge, d'une perte ou d'une insuffisance de réfrigération, d'endommagements mécaniques, d'erreurs de maintenance ou de réparation, d'endommagements chimiques, de défaillances aléatoires dues à des défaillances de matériels et d'autres événements.

4.3.2 Défaillances multiples dues à une cause commune unique

On doit prendre en compte les conséquences de défaillances, dues à une cause commune unique, telle qu'une erreur de maintenance, un endommagement mécanique ou une interférence électrique, situées dans deux composants ou plus, affectant des groupes de sûreté redondants. Les effets environnementaux, l'endommagement dû aux radiations et autres facteurs physiques communs potentiels doivent être pris en considération.

Where physical separation is required, prevention of failure propagation shall be considered for failures

- occurring simultaneously to multiple system components as a consequence of PIEs;
- between systems of the same safety category;
- between redundant safety groups of the same I&C system important to safety, and;
- from systems of lower category to systems of higher category and in some specific cases from systems of higher category to systems of lower category.

The types of possible failure-initiating events contained in the following subclauses shall be taken into consideration (i.e. identified, documented and justified). Adequate provisions shall be made in the I&C systems important to safety to limit the possible effects of these events to an acceptable level. Consideration should be given to the effects of a combination of failure events.

4.2 Design errors

The potential for errors in the specifications of the requirements for the I&C systems important to safety cannot be ignored. Such design errors could lead to propagation of faults between systems, for example, insufficient insulation on cabling, inadequate sizing of conductors, etc. Means to address this type of fault generally include conservative design of physical separation and electrical isolation.

4.3 I&C system failure events

Failure initiating events having their cause within each I&C system important to safety shall be taken into consideration. These events are generally characterised by locally restricted mechanical and electrical effects that may have different functional consequences. Single failures within I&C central processing units and on multiplexed communications interfaces may also have the potential to generate multiple failures. I&C failure events can be subdivided as follows.

4.3.1 Single random failure

A single random failure of an I&C system component, including its energy or other auxiliary supply, which can lead to component malfunction, short-circuits, interruption of circuit continuity, ground-contact, voltage or frequency changes, mechanical failure of components or local fire shall be taken into consideration. Such an event may have its cause in overloading, loss of or insufficient cooling, mechanical damage, errors during maintenance and repair, chemical damage, random failure due to material deficiency and other events.

4.3.2 Multiple failures from a single common cause

Consideration shall be given to the consequences of failures in two or more components, affecting redundant safety groups, due to a single common cause such as maintenance error, mechanical damage or electrical interference. Environmental effects, radiation damage and other potential common physical factors shall be taken into consideration.

4.4 Défaillances dans l'installation

Les événements initiateurs de défaillances qui peuvent avoir leurs origines dans des conditions opérationnelles de l'installation peuvent entraîner des défaillances de composants d'un système d'I&C. Ces incidents sont caractérisés par une libération d'énergie relativement importante et par une gamme d'effets affectant l'ensemble d'un local ou des parties de bâtiments. Ces événements peuvent être répartis comme suit.

4.4.1 Conditions d'ambiance

On doit prendre en compte la variation des conditions d'ambiance telles que les rayonnements, la température, le taux d'humidité en exploitation normale et en conditions accidentelles. Le feu et la fumée pouvant affecter un local matériel ou un chemin de câbles, est une condition d'ambiance importante. On doit aussi prendre en compte le fonctionnement intempestif des systèmes de lutte incendie.

4.4.2 Interférences électromagnétiques (IEM)

Le matériel d'I&C produit et transmet par nature des signaux électromagnétiques. Ces signaux sont susceptibles d'être modifiés ou dégradés par inadvertance par des sources externes. Les avancées technologiques dans les systèmes d'I&C, en particulier la réduction de la tension des signaux peut rendre les systèmes plus sensibles au mauvais fonctionnement et à la dégradation. Ainsi, on doit prendre en compte les IEM comme une source de DCC pour les groupes de sûreté redondants d'I&C. La séparation est une approche préservant l'indépendance des signaux d'I&C et permettant de se protéger de l'impact d'une DCC potentielle due aux IEM.

La série CEI 61000 donne des lignes directrices pour prendre en compte les IEM durant la conception et les tests.

4.4.3 Défaillances des systèmes, des matériels ou des structures de l'installation

On doit prendre en compte les EIH survenant dans les systèmes, les matériels ou les structures de la centrale, tels que l'incendie, l'impact de projectile, le fouettement de canalisation, les effets mécanique et thermique, les explosions de canalisation, les fuites d'eau, de vapeur, de métal en fusion, de gaz, d'huile et les autres événements qui peuvent potentiellement endommager les matériels.

4.4.4 Erreurs humaines

On doit prendre en compte les EIH qui sont la conséquence d'une action erronée du personnel en fonctionnement normal et plus particulièrement en conditions accidentelles.

4.5 Défaillances dues à des événements extérieurs à l'installation

Des défaillances des composants des systèmes d'I&C peuvent résulter d'événements initiateurs ayant des causes extérieures à la centrale. Ces événements sont caractérisés par une libération d'énergie importante et par des effets affectant des parties de bâtiments ou des bâtiments entiers. Ces événements peuvent être subdivisés comme suit:

4.5.1 Phénomènes naturels

On doit prendre en compte les phénomènes naturels tels que les tremblements de terre, les inondations, les tornades, la foudre, les raz-de-marée ou tsunami pouvant survenir sur le site de l'installation.

4.4 Plant failure events

Failure initiating events that have their cause in plant conditions may result in the failure of I&C system components. These events are characterised by a medium to large energy release and by a range of effects involving individual rooms and parts of a building. These events can be subdivided as follows.

4.4.1 Environmental conditions

Variation of environmental conditions such as radiation-, temperature-, pressure-, humidity-fields during normal operation and under accident conditions shall be considered. Fire or smoke affecting an equipment room or cable route is an important environmental condition. Also, the spurious operation of fire suppression systems shall be considered.

4.4.2 Electromagnetic interference

I&C equipment by its nature involves the generation and transmission of electromagnetic signals. These signals may be susceptible to inadvertent modification or corruption from external sources. Technology advances in I&C systems, particularly the reduction in signal voltage, may make systems ever more susceptible to malfunction and corruption. Therefore, EMI shall be considered as a potential for CCF of I&C redundant safety groups. Separation is one approach to preserve the independence of I&C signals and to guard against the potential CCF impact of EMI.

The IEC 61000 series provides guidance in the design and testing for EMI.

4.4.3 Failure of plant systems, equipment or structures

PIEs in plant systems, equipment or structures such as fire, missile impact, pipe whipping, mechanical and thermal effects, explosion or leakage of water, of steam, of liquid metal, of gas, of oil, and other events that have a potential to cause equipment damage shall be considered.

4.4.4 Operator error

PIEs which have their cause due to erroneous operator action in normal operation and especially under accident conditions shall be considered.

4.5 External failure events

Failure initiating events that have their cause external to the plant may result in the failure of I&C system components. These events are characterised by a very large energy release and by effects on parts of buildings or whole buildings. These events may be subdivided as follows.

4.5.1 Natural events

Natural events such as earthquakes, floods, tornadoes, lightning, tidal surge or tsunami, as appropriate to the site of the plant shall be considered.

4.5.2 Causes extérieures humaines

On doit prendre en compte les événements intérieurs et extérieurs à la centrale dus à des causes extérieures humaines telles que les explosions, l'incendie, les chutes d'aéronefs ou le sabotage.

4.6 Conditions spéciales de fonctionnement

Durant la conception et la construction, on doit prendre en compte les événements qui provoquent des EIH, pouvant résulter de conditions de fonctionnement spéciales telles que la mise en service, les modifications, la maintenance et les réparations, la conception et les procédures de contrôle administratives, afin de réduire les risques à des niveaux acceptables.

4.7 Problème de la séparation dans les installations existantes

Dans les centrales nucléaires de puissance existantes, la séparation physique des systèmes d'I&C réalisant des fonctions importantes pour la sûreté est souvent imparfaite; en effet des fonctions qui initialement étaient non classées de sûreté ont pu être classées comme importantes pour la sûreté, en particulier parce que les normes de conception ont changé. Lors d'une rénovation d'une installation existante, il convient de justifier les conséquences potentielles de la non-application, pour des considérations pratiques, de cette norme à quel que niveau que ce soit par rapport aux gains de sûreté apportés par la modernisation prise dans son ensemble. Les arguments de justification suivants peuvent être admis:

- les structures de génie civil ou l'espace physique disponible dans l'installation peuvent ne pas permettre de satisfaire aux exigences de séparation. Il est recommandé de faire une revue des contraintes physiques lors du repérage du lieu d'implantation du système d'I&C rénové;
- les principales faiblesses de l'I&C existant doivent être identifiées, considérant la séparation telle qu'elle existe et les gains de sûreté qui peuvent être obtenus par la rénovation;
- la séparation telle qu'elle existe et les améliorations possibles doivent être évaluées à l'aide d'une méthodologie présentant un caractère systématique et permettant d'identifier les points forts particuliers ou les solutions alternatives aux exigences de cette norme;
- un autre ensemble comparable de règles de séparation peut être établi, prenant en compte et justifiant les conditions existantes validées par des rapports relatifs à l'expérience opérationnelle de l'installation;
- d'autres technologies doivent être présentées et évaluées dans le cas de situations spéciales de l'installation, par exemple franchissements de barrière, câblage optique, systèmes d'I&C distribués.

On doit plus particulièrement s'intéresser au problème de la séparation durant la phase traitant de la stratégie d'implantation de la modernisation de l'installation. Les questions suivantes font partie de celles à prendre en compte:

- séparation dans les configurations intermédiaires lorsque le nouveau système d'I&C est installé en plusieurs étapes;
- identification des sous-systèmes qui peuvent être séparés sans besoin d'interfaces intermédiaires;
- pertinence de la séparation existante pour la nouvelle technologie d'I&C (principalement concernant le caractère sensible des systèmes numériques d'I&C aux IEM, exigences spéciales concernant la température ou la susceptibilité aux radiations);
- limitations liées au câblage et évaluation des besoins propres aux nouvelles technologies pour des chemins de câbles spéciaux pour fibres optiques, pour bus et les exigences de séparation.

La CEI 62096 peut fournir des lignes directrices pour décider de la mise à niveau et de la modernisation d'I&C.

4.5.2 External man-made causes

Events inside or outside the plant due to external man-made causes such as explosion, fire, aircraft crashes, sabotage shall be considered.

4.6 Special operating conditions

PIEs, which may have their cause in special operating conditions such as commissioning, modification, maintenance and repair, design and administrative control procedures, shall be considered during design and construction to reduce them to acceptable levels.

4.7 Separation issues at existing plants

The physical separation of I&C systems performing functions important to safety in existing nuclear power plants is often incomplete because functions that had initially no safety classification may need to be classified as important to safety and because design standards have changed. When upgrading existing plants, the potential consequences of not following this standard in all aspects due to practical considerations should be justified against the added safety gained through the upgrade taken as a whole. The following justification arguments may be admissible:

- the civil structures or physical space available at the plant may not allow the required separation. Physical constraints should be reviewed in locating the upgraded I&C systems;
- the major weaknesses of existing I&C shall be identified with respect to both existing separation and safety improvements possible through upgrading;
- the existing separation, or feasible improvements of separation, shall be evaluated through a systematic methodology recognising particular strengths or alternatives to the requirements of this standard;
- an alternative set of separation rules may be established, recognising and justifying existing conditions proven through records of plant operation;
- alternative technologies shall be presented and evaluated in the case of special plant situations; e.g. through use of barriers, optical cabling, distribution of the I&C systems.

Separation issues shall be particularly addressed in the implementation strategy of the plant upgrading. Issues which shall be considered include

- separation in intermediate configurations when new I&C is installed through a phased programme;
- identification of subsystems, which can be separated without the need of intermediate interfaces;
- suitability of the existing separation to the new I&C technology (mainly sensitivity of digital I&C to EMI, special temperature requirements and susceptibility to radioactive radiation);
- cable routing limits and an evaluation of the needs coming from new technologies for special cable trays for fibre optic cables, bus cables and requirements for separation.

Guidance for the decision on upgrading and modernisation of I&C can be found in IEC 62096.

5 Bases de conception

Pour concevoir le système d'I&C important pour la sûreté, on doit appliquer les règles fondamentales exposées ci-dessous, en prenant en considération les causes possibles de défaillances mises en évidence dans l'Article 4.

5.1 Protection incendie

Une analyse des risques incendie doit être menée lors de la conception de la centrale sous l'angle de la sûreté nucléaire afin de s'assurer que les exigences concernant la séparation physique mentionnées dans l'Article 6 sont remplies.

On doit placer des détecteurs incendie suffisamment sensibles et des dispositifs d'alarme aux endroits sans surveillance où sont installés les systèmes et les câbles.

Les matériels des systèmes d'I&C redondants doivent parfois être placés dans la zone protégée par un système de protection incendie fixe. Lorsque c'est le cas, la conception des systèmes d'I&C et de leurs matériels et du système de protection incendie doit être coordonnée de telle façon que la mise en service du système de protection incendie n'affecte pas l'indépendance des groupes de sûreté redondants.

L'efficacité des groupes redondants ne doit pas être compromise par le feu ou les fumées d'origine extérieure aux systèmes d'I&C importants pour la sûreté. Cela doit être assuré par l'éloignement, par des barrières ou par les deux à condition de satisfaire aux exigences suivantes:

- a) l'espace entre les systèmes redondants ou les câbles ne doivent pas contenir de matériaux, d'équipements ou de structures interposés qui pourraient aider à la propagation de l'incendie;
- b) lorsqu'elles sont utilisées entre des systèmes redondants ou des câbles, les barrières doivent avoir une classification au feu compatible avec la protection contre le risque incendie.

5.2 Conditions d'ambiance durant et après les accidents

Les matériels des systèmes d'I&C doivent être conçus, spécifiés et installés de façon à garantir leur capacité fonctionnelle dans les conditions résultant des événements décrits en 4.4 et 4.5, ainsi qu'après la disparition de celles-ci.

5.3 Dispositifs d'isolement

5.3.1 Généralités

Lorsque des signaux sont produits par des matériels de système de catégorie A et qu'ils sont fournis à des systèmes de catégorie inférieure, la transmission de ces signaux doit se faire au travers de dispositifs d'isolement qui sont inclus dans le système de catégorie A. Le dispositif d'isolement doit être tel que les défaillances ou les conditions prévalant à ses sorties (qui sont connectées aux systèmes de catégorie inférieure) ne peuvent empêcher l'action du système ou du sous-système de sûreté de catégorie A auquel le dispositif d'isolement est connecté. Par exemple, un circuit de catégorie A peut être surveillé au niveau alarmes par un relais de la même catégorie dont les contacts produiront des alarmes pour des catégories inférieures. L'isolement électrique réalisé doit satisfaire aux exigences de 5.3.2.

Les branchements temporaires aux systèmes supportant des fonctions de catégorie A mis en place pour des raisons de maintenance doivent être autorisés s'ils sont connectés à une seule voie de redondance à un instant donné, s'ils sont déconnectés après utilisation, et si le système est capable de résister à un défaut introduit par une défaillance ou par l'utilisation d'un branchement.

5 Design basis

Taking into consideration possible causes of failures identified in Clause 4, the following basic rules shall be followed when designing an I&C system that is important to safety.

5.1 Fire protection

A fire hazard analysis based on nuclear safety considerations shall be performed in the design phase of the nuclear power plant to ensure that the physical separation requirements as resulting from Clause 6 are met.

Fire and smoke detectors of suitable sensitivity and alarms shall be provided for unattended areas where cables or systems are installed.

Redundant equipment of I&C systems must sometimes be placed within the influence area of a fixed fire protection system. When this is so, the design of I&C systems and their equipment and the fire protection system shall be such that the operation of this fire protection system will not affect the independence of redundant safety groups.

The performance of redundant safety groups shall not be compromised by fires or smoke generated externally to the I&C system important to safety. This shall be achieved by spatial separation, barriers or a combination thereof, while keeping the following requirements:

- a) space between redundant systems or cables shall not contain interposing structures, equipment or materials that could assist in the propagation of the fire;
- b) barriers when used between redundant systems or cables shall have a fire rating commensurate with the fire hazard protection requirements.

5.2 Environmental conditions during and after accidents

I&C system equipment shall be designed, specified and installed in such a manner as to assure its functional capability under and following the expected environmental conditions arising from events as described in 4.4 and 4.5.

5.3 Isolation devices

5.3.1 General

Where signals are extracted from category A system equipment and provided to systems of a lower category, the transmission of these signals shall be through isolation devices that are included within the category A system. The isolation device shall be such that failures or conditions at their output terminals (which are connected to the lower category system) cannot prevent the safety action of the category A system or sub-system to which the isolation device is connected. As an example, a circuit at category A may be monitored for alarms by a relay in that circuit at that category whose contacts provide alarms at a lower category. The electrical isolation provided shall meet the requirements of 5.3.2.

Temporary connections for maintenance to systems performing category A functions without isolation devices shall be permitted provided that they are connected to only a single redundancy at any given time, that they are disconnected after use, and that the system is capable of withstanding a fault introduced through failure or use of the connection.

5.3.2 Caractéristiques d'isolement

Les défaillances et les conditions contre lesquelles on doit se prémunir sont

- a) les courts-circuits entre sorties ou les mises à la terre;
- b) les ouvertures de circuits;
- c) l'application de la tension alternative ou continue maximale qui peut raisonnablement survenir, considérant les potentiels et les sources disponibles dans les systèmes de catégorie A et non classés de catégorie A;
- d) interférences électrostatiques et électromagnétiques.

Le dispositif d'isolement doit avoir les propriétés suivantes:

- tolérance et isolement des pointes et défauts électriques définis dans la CEI 61000-6-5;
- tolérance et isolement aux IEM définies dans la CEI 61000-6-5;
- simple barrière entre les sorties proches ou adjacentes ou les groupes de contacts sur les matériels à relais utilisés pour l'isolement électrique;
- prévention contre la transmission de tensions excessivement hautes ou pouvant endommager.

Dans ce contexte, il est recommandé de faire une évaluation de la tension maximale prévisible en conditions de fonctionnement normal et de défaut, ainsi que des effets potentiels sur les matériels importants pour la sûreté lorsque cela survient aux sorties du dispositif d'isolement connectées au circuit le moins important pour la sûreté.

Il est aussi recommandé de prendre des précautions minimisant la probabilité qu'une défaillance dans un système non classé de catégorie A entraîne le déclenchement intempestif ou prématuré d'une fonction de catégorie A.

5.3.3 Priorités de mise en service

Lorsqu'un matériel de tranche commandé par un système de catégorie A est aussi commandé par des signaux issus de systèmes de catégorie inférieure, on doit prévoir un dispositif d'isolement qui garantit la priorité des actions du système de catégorie A sur celles des systèmes de catégorie inférieure. Les actions liées au fonctionnement normal d'un système de catégorie inférieure ainsi que ses défaillances ne doivent pas interférer avec les fonctions de catégories A lorsque celles-ci sont requises par les conditions opérationnelles de l'installation. On doit classer la partie priorité du dispositif d'isolement comme composant du système de catégorie A.

Les défaillances et les mauvais fonctionnements des systèmes non classés en catégorie A ne doivent entraîner aucun changement en matière de réponse, de dérive, de précision, de sensibilité au bruit ou autres caractéristiques d'un système de catégorie A qui pourrait compromettre l'aptitude du système à réaliser ses fonctions de sûreté.

Lorsque des signaux sont produits dans des systèmes de catégories B et C pour être utilisés dans des systèmes de catégorie inférieure, les systèmes d'isolement peuvent ne pas être requis; cependant il est recommandé de suivre l'état de l'art en ingénierie afin de se protéger contre la propagation des défaillances. Dans le cas où des systèmes réalisant des fonctions de catégories B revêtent dans leur fonctionnement des aspects propres à la catégorie A, l'isolement est exigé.

La communication par fibre optique est un moyen très efficace d'isolement électrique, et il est recommandé d'y avoir recours partout où cela est possible.

5.3.2 Isolation characteristics

Failures and conditions that shall be protected against include

- a) short-circuits between terminals or to ground;
- b) open circuits;
- c) application of the maximum a.c. or d.c. potential that could reasonably occur, considering potentials and sources available in both the category A and non-category A systems;
- d) electromagnetic and electrostatic interference.

The properties of an isolation device shall include

- tolerance of and isolation for the electrical surges and spikes defined in IEC 61000-6-5;
- tolerance and isolation for EMI to IEC 61000-6-5;
- simple barriers between close or adjacent terminals or contact groups on relay equipment used for electrical isolation;
- prevention of transmission of excessively high or damaging voltages.

In this context, an assessment should be done of the maximum voltage that could be envisaged under normal and faulted conditions, and its potential effects on the equipment important to safety when applied to the isolation device terminals of the circuit of lesser importance to safety.

Precautions should also be taken to minimise the possibility that failure in a non-category A system causes spurious or premature actuation of a category A function.

5.3.3 Actuation priority

Where plant equipment that is controlled by a category A system is also controlled by signals from a lower category system, isolation devices shall be provided which ensure priority of the category A system actions over those of the lower category system. Failures of, or normal actions by, the lower category system shall not interfere with the category A functions under plant conditions requiring success of those category A functions. The priority isolation devices shall be categorised as part of the category A system.

Failures and mal-operations in the non-category A systems shall cause no change in response, drift, accuracy, sensitivity to noise, or other characteristics of the category A system which might impair the ability of the system to perform its safety functions.

Where signals are extracted from category B or C systems for use in lower category systems, isolation devices may not be required; however, good engineering practices should be followed to prevent the propagation of faults. In cases where systems performing category B functions need to take on the aspects of category A systems due to the functions performed, isolation shall be applied.

Fibre optic communications provide a very effective means of achieving electrical isolation, and should be applied wherever practical.

5.4 Indépendance du système de commande

L'utilisation de signaux issus de systèmes de catégorie A dans les systèmes de commande (sans égard à la catégorisation) demande des précautions qui vont au-delà de celles observées lorsque les signaux sont utilisés seulement à des fins de surveillance et de protection. Suite à une défaillance capteur, une valeur externe mesurée d'un système de commande peut produire une demande hors tolérance, et déclencher en conséquence une commande dangereuse, tout en empêchant la détection des conditions dangereuses par le système de protection.

Les conceptions du système de commande et du système de protection sont telles qu'une défaillance hypothétique unique, comprenant les défauts consécutifs à celle-ci portant sur les signaux échangés entre ces deux systèmes, ne puisse causer un accident ou un transitoire nécessitant le déclenchement d'une action de sûreté et, en même temps, n'entraîne une dégradation inacceptable d'un système de catégorie A.

Lorsqu'une défaillance aléatoire unique d'un système de catégorie A ou les défauts consécutifs à celle-ci peuvent déclencher l'action d'un système de commande susceptible de créer les conditions initiatrices d'une action de sûreté, alors il convient que le système de catégorie A soit capable de réaliser cette action même en prenant en compte une deuxième défaillance aléatoire. On doit prendre des mesures pour que cette exigence puisse être satisfaite même si un composant ou un ensemble est inhibé ou mis hors service pour quelque raison que ce soit, incluant les essais et la maintenance.

Les précautions acceptables dépendront du type de réacteur et des défaillances possibles. Celles-ci comprennent

- la réduction de la logique majoritaire de votes identiques, lorsqu'une défaillance capteur ou une panne matérielle sont détectées,
- l'abandon de signaux de commande pris dans des ensembles ou des composants redondants, lorsqu'il est connu que les signaux ne représentent pas les conditions réelles,
- l'initiation des actions de sûreté à partir des ensembles de logique de sûreté, plaçant ainsi la centrale dans un état qui ne peut plus être dégradé par une action du système de commande,
- déclenchement de protection à partir de différents paramètres physiques.

Un système de protection incluant une logique de vote un sur deux produisant les signaux de commande nécessitera une justification des arguments de compromis (voir 4.7), même si on fait état de preuve d'essai de la fiabilité des matériels, des capteurs et de contournements efficaces. Un système à logique de vote deux sur trois peut satisfaire aux exigences associées aux matériels à position de repli sécurisée et de détection des capteurs défaillants si des dispositifs de contournement sont utilisés en maintenance.

Lorsqu'il peut être montré que la défaillance simultanée d'ensembles redondants de surveillance de sûreté due à un événement original est improbable, on peut installer des ensembles de surveillance de sûreté comparant les signaux. Ces ensembles de surveillance de sûreté doivent fournir une indication, une alarme ou un signal d'initiation d'action de sûreté ou modifier de façon sécuritaire les logiques lorsqu'un signal dévie de façon excessive d'autres signaux redondants concernant les conditions opérationnelles de l'installation ou d'un paramètre. L'ensemble de surveillance de sûreté qui réalise la comparaison doit être isolé de façon appropriée afin de prévenir les interactions entre les canaux redondants. De telles méthodes par exemple transmettent toutes les valeurs de tous les capteurs à tous les canaux redondants des systèmes de sûreté. Chaque canal compare alors les valeurs afin de détecter les valeurs anormales ou hors service. Chaque canal peut alors utiliser toutes les valeurs des capteurs ou bien on peut ne retenir que la valeur la plus pénalisante dans chaque canal pour le vote. Il convient de signaler à l'aide d'alarmes les capteurs identifiés comme défaillants, et les valeurs doivent être mises à disposition pour affichage.

5.4 Independence from control systems

The use of category A system signals in control systems (regardless of category) requires precautions beyond those required when category A system signals are used only for monitoring or protection purposes. A sensor failure could cause a control system measured value outside the demand tolerance, and a consequent unsafe control action, while preventing detection of the unsafe condition by the protection system.

The protection system and the control system shall be designed so that a postulated single failure including consequential failures concerning signals transferred between these two systems cannot cause an accident or transient requiring safety action and, at the same time, cause unacceptable degradation of the category A system.

For the case where a single random failure, and any consequential failures, within the category A system could cause a control system action that results in a condition requiring safety action, then the category A system should be capable of providing this action even when degraded by a second random failure. Provisions shall be included so that this requirement can still be met if a component or assembly is by-passed or removed from service for any reason including test or maintenance purposes.

Acceptable provisions will depend on the type of reactor and on the possible failures. They include

- reducing the required majority voting coincidence when sensor failure or equipment faults are detected,
- removing the control signals taken from the redundant components or assemblies when the signals are determined to not represent the true process condition,
- initiating a safety action from the safety logic assembly, thus putting the plant in a state no longer adversely impacted by the control system action,
- providing protection by use of different physical parameters.

A one from two voted protection system providing control signals will require justification by trade-off arguments (see 4.7), even if effective bypasses and high sensor and equipment reliability with proof testing is claimed. A two from three voted system can meet the requirements with fail-safe equipment and automatic detection of failed sensors if suitable bypass facilities are used during maintenance.

Where it can be shown that, due to the original event, the simultaneous failure of redundant safety monitoring assemblies is unlikely, safety monitoring assemblies which compare signals may be provided. These safety monitoring assemblies shall provide an indication, alarm or safety action signal or make the logic more restrictive when one signal deviates excessively from other redundant signals of the same plant condition or parameter. The safety monitoring assemblies which perform the comparison shall be provided with adequate isolation to prevent interaction between redundant channels. An example of this involves sending all sensor values to each redundant safety system channel. Each channel then compares the values to detect out-of-line or abnormal values. Each channel may then vote all sensors values, or detect the most adverse sensor in each channel for the voted action. The sensors which are detected as faulty should be alarmed and the values may be made available for display.

6 Exigences en matière de séparation du câblage

6.1 Exigences générales

On doit concevoir et installer les parties redondantes des systèmes de catégorie A de façon que les événements spécifiés dans les paragraphes de l'Article 4 ne puissent entraîner une défaillance de fonction de catégorie A.

On doit concevoir et installer les parties redondantes des systèmes de catégorie B de façon que les événements uniques spécifiés en 4.2 et 4.3 ne puissent entraîner une défaillance de fonction de catégorie B. On doit prendre en compte les événements spécifiés en 4.4 et 4.5 au cas par cas comme indiqué dans les principes généraux (Article 4).

On doit prendre en compte les éléments contenus dans les paragraphes suivants.

6.2 Séparation

On doit séparer les câbles en utilisant des structures de sûreté, des barrières ou des espace-ments ou toutes combinaisons de ces méthodes.

6.2.1 Séparation des câbles redondants dans un système d'I&C importants pour la sûreté

Les exigences suivantes s'appliquent aux câbles redondants dans un système d'I&C importants pour la sûreté:

- on doit fournir pour chaque groupe redondant des chemins de câbles, des tablettes, des buses, des gaines et des traversées physiquement séparés;
- tous les chemins de câble, tablettes, buses, gaines, gaines verticales ou traversées doivent uniquement supporter ou contenir des câbles du même groupe redondant;
- pour les événements initiateurs concernant le système d'I&C qui ont leurs origines dans le système de câblage, tels que les arcs électriques ou les surchauffes dus à des courts-circuits, les surcharges ou les transitoires de tension, etc. (voir 4.3), un degré faible de séparation physique peut être suffisant. On doit maintenir au minimum une distance horizontale de 30 cm et une distance verticale de 80 cm. Lorsque la distance minimale de séparation n'est pas respectée, les câbles doivent emprunter des chemins de câbles qualifiés en tant que barrière ou des justifications concernant ces distances plus faibles peuvent être fournies;
- concernant les défaillances dues à des événements extérieurs ou des défaillances de l'installation (voir 4.4 et 4.5), tels que l'incendie ou l'effondrement de structure, on doit appliquer des règles de séparation physique renforcées faisant intervenir des barrières et/ou des structures de sûreté.

6.2.2 Moindres distances de séparation

Des distances de séparation moindres que celles spécifiées en 6.2.1 peuvent être établies par l'analyse du câblage proposé pour l'installation. Il est recommandé que l'analyse soit basée sur des essais de détermination des caractéristiques du câblage à ralentir la propagation du feu, considérant des points tels que les matériaux isolants et de couverture, le taux de remplissage des chemins de câble, leurs types, et leurs configurations. Il est recommandé de prendre en compte dans les zones exposées le niveau des risques (tel que la taille d'incendie ou de brèche) et les moyens de mitigation (tels que les extincteurs).

6 Requirements for cabling separation

6.1 General requirement

Redundant portions of category A systems shall be designed and installed in such a way that the single events specified in all subclauses of Clause 4 cannot result in a failure of the category A function.

Redundant portions of category B systems shall be designed and installed in such a way that the single events specified in 4.2 and 4.3 cannot result in a failure of the category B function. Treatment of failure initiating events specified in 4.4 and 4.5 to category B systems shall be on a case by case basis as discussed in the general principles (Clause 4).

The items in the following subclauses shall be taken into account.

6.2 Separation

Separation shall be achieved by safety structures, barriers or physical distance or by any combination of these methods.

6.2.1 Separation of redundant cables inside the I&C system important to safety

For redundant cables within an I&C system important to safety, the following apply:

- each redundant group shall be provided with physically separate cable routes, trays, conduits, ducts and penetrations;
- any given route, tray, conduit, duct, vertical duct or penetration shall carry or contain only cables of the same redundant group;
- for the I&C system failure-initiating events that have their cause in the cabling system, such as arcing or overheating due to shorts, overloads, voltage transients, etc. (see 4.3), a low degree of physical separation may be sufficient. A horizontal distance of 30 cm and a vertical distance of 80 cm shall be maintained as a minimum. Where the minimum separation distance is not maintained, the redundant cables shall be run in enclosed raceways that qualify as barriers or a justification of lower distances shall be provided;
- for plant failure and external failure events (see 4.4 and 4.5), such as fire or structure collapse, greater physical separation including barriers and/or safety structures shall be applied.

6.2.2 Lesser separation distances

Lesser separation distances than those specified in 6.2.1 may be established by analysis of the proposed cable installation. The analysis should be based on tests performed to determine the flame retardant characteristics of the proposed cable installation considering features such as insulation and jacket materials, raceway fill, raceway types, and arrangements. For lesser separation distances in hazardous areas, the degree of hazards (such as size of the fire or pipe break) and mitigating measures (such as sprinklers) should be considered.