IEC 60709

Edition 3.0 2018-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique importants pour la sûreté – Séparation

IEC 60709:2018-04(en-fr)

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

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

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

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

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

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 21 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC 60709

Edition 3.0 2018-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique importants pour la sûreté – Séparation

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-5582-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER 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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This third edition cancels and replaces the second edition published in 2004. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) include requirements referring to the separation principle in electrical systems important to safety;
b) define separation criteria for I&C and electrical systems in a generic way;
c) restructure the standard following the criteria;
d) consider interferences between I&C and electrical equipment from different safety classes;

e) align with the new revisions of IAEA documents and broaden the scope to include other aspects of separation;

f) cover new technologies that either present unique separation issues or provide new means of achieving separation;

g) enhance requirements and guidance for areas of cable congestion, e.g. control room, cable spreading galleries, etc;

h) introduce the concept of “associated circuits” (from US practice) to deal with equipment not important to safety and cables that are not separated from safety equipment and cables;

i) address the implications of low energy circuits, such as the possible use of analysis to reduce the minimum separation distance;

j) review existing requirements, update terminology and definitions;

k) provide guidance for the application of the standard to existing plants.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1185/FDIS	45A/1195/RVD

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

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Background, main issues and organization of the standard

I&C and electrical 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 and electrical 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 should be provided and maintained. This standard provides generic technical requirements and recommendations for the implementation of separation in the design of I&C and electrical systems.

The object of this standard is as follows:

– in Clause 5 to present the principles for separation of I&C and/or electrical systems. Subclause 5.4 focuses on modernization of existing nuclear power plants;

– in Clause 6, to define the separation design basis, including inputs, and to identify a certain number of possible causes of internal and external hazards;

– in Clause 7, to establish the electrical isolation measures for I&C and electrical systems important to safety and also requirements referring isolation devices;

– in Clause 8, to give requirements to be fulfilled for cabling and component separation within an I&C and electrical system important to safety.

b) 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 and IEC 63046 in regard to physical separation and electrical isolation being required between subsystems of different safety trains of I&C and electrical systems important to safety, and between I&C and electrical systems important to safety and those that are not important to safety and between different defence in depth levels.

IEC 61226, that is consistent with IAEA SSG-30, establishes the principles of categorization of I&C and electrical functions and the classification of structures, systems and components (SSC) according to their level of importance to safety. IEC 61226 refers to IEC 60709 as the normative standard regarding requirements for separation.

For more details on the relation of this standard to IAEA guidelines and IEC 61226, see Annex A to this standard.

c) Recommendations and limitations regarding the application of the Standard

IEC 60709 applies to I&C and electrical 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. Furthermore, separation criteria due to security requirements are also not considered.

The requirements given in this standard for the separation of safety classes can be applied to separation for other design constraints, such as the defence in depth concept. These rules shall be defined at the beginning of a project by a separation concept.

The separation of safety class 1 from other classes, as used in this standard, is only an example of the application of the requirements of the standard.

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

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC45A standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 will be published this NOTE 2 of the introduction of IEC SC 45A standards will be suppressed.

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

1 Scope

1.1 General

This document is applicable to nuclear power plant instrumentation and control (I&C) and electrical systems and equipment, whose functions are required to be independent due to their contribution to:

- a redundant or diverse safety group;
- different defence in depth levels;
- different safety classes and also with non-classified (NC) systems.

It is also applicable to temporary installations which are part of those I&C and electrical systems important to safety (for example, auxiliary equipment for commissioning tests and experiments or mobile power supply systems). Clause 7 is intended particularly for electrical isolation, Clause 8 is intended particularly for the cabling and the arrangement of equipment of I&C and electrical systems important to safety.

This document applies to I&C and electrical systems of new nuclear power plants and to I&C and electrical upgrading or back-fitting of existing plants. For existing plants see 1.2 and 5.4.

Where independence is required by general safety standards such as IAEA safety guides, IEC 61513 (for I&C), IEC 63046 (for electrical systems) and other project constraints, one aspect of achieving this independence is physical separation and electrical isolation between the systems and their equipment that perform safety functions. This document defines the assessments needed and the technical requirements to be met for I&C and electrical systems, equipment or cables for which separation is required. Those means are to achieve adequate physical separation and electrical isolation between redundant sections of a system and between a higher and lower class systems. 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.

The requirements for functions, and their associated systems and equipment, to be independent are normally defined in detail in the project documentation; the method of determining and defining these requirements is not the subject of this document.

Following IAEA SSR-2/1 Requirement 21, separation means by physical separation, electrical isolation, functional independence and independence of communication are considered. In this document physical separation and electrical isolation are treated. Functional independence and independence of communication are not considered in this document. More details referring to functional independence, independence from control systems and independence of communication are given in Annex D.

1.2 Application: new and pre-existing plants

This document applies to the I&C and electrical of new nuclear power plants as well as to up-grading or back-fitting of existing plants.

For existing plants, only a subset of requirements is applicable and this subset is normally specified and argued at the beginning of any project.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60071 (all parts), *Insulation co-ordination*

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

IEC 60364-4-41, *Low-voltage electrical installations – Part 4-41: Protection for safety – Protection against electric shock*

IEC 60364-5-52, *Low-voltage electrical installations – Part 5-52: Selection and erection of electrical equipment – Wiring systems*

IEC 60364-5-56, *Low-voltage electrical installations – Part 5-56: Selection and erection of electrical equipment – Safety services*

IEC 60909 (all parts), *Short-circuit currents in three-phase a.c. systems*

IEC 60964, *Nuclear power plants – Control rooms – Design*

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

IEC 61226, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61439-1, *Low voltage switchgear and controlgear assemblies – Part 1: General rules*

IEC 61500, *Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 61660 (all parts), *Short-circuit currents in d.c. auxiliary installations in power plants and substations*

IEC 62003, *Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*

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

IEC 62808, *Nuclear power plants – Instrumentation and control systems important to safety – Design and qualification of isolation devices*

IEC 63046*, Nuclear power plants – Electrical systems – General requirements*[1]

IAEA Safety Standard Series No. SSR-2/1:2016, *Safety of Nuclear Power Plant: Design*

_____

1 To be published.

IAEA Safety Guide SSG-30, *Safety classification of structures, systems and components in Nuclear Power Plants*

IAEA Safety Guide SSG-34, *Design of electrical power systems in Nuclear Power Plants*

IAEA Safety Guide SSG-39:2016, *Design of instrumentation and control systems in Nuclear Power Plants*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
associated circuit
circuit of a lower safety class that is not physically separated or is not electrically isolated from the circuit(s) of the higher class by acceptable separation distances, safety class structures, barriers, or electrical isolation devices, but meets suitable criteria for safety. Circuits include the interconnecting cabling and the connected loads

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 or electrical system important to safety to an acceptable level

Note 1 to entry: The following definition is to be found in the IAEA Safety Glossary edition 2016: “A physical obstruction that prevents or inhibits the movement of people, radionuclides or some other phenomenon (e.g. fire), or provides shielding against radiation”. This IAEA definition is more general but consistent with the definition given in this document.

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

EXAMPLE For example, the single specific event or cause of failures (which may be failures of different types) could be a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a human induced event, saturation of signals, or an unintended cascading effect from any other operation or failure within the plant or from a change in ambient conditions.

[SOURCE: IAEA Safety Glossary, edition 2016]

3.5
defence in depth
hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers,

members of the public or the environment, in operational states and, for some barriers, in accident conditions

[SOURCE: IAEA Safety Glossary, edition 2016]

3.6
design extension condition
postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with melting of the reactor core

[SOURCE: IAEA Safety Glossary, edition 2016]

3.7
distance <separation by>
placement of the components being protected sufficiently far away from one another so as to ensure that they cannot be simultaneously damaged by the considered event

3.8
diversity
presence of two or more independent (redundant) systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure

[SOURCE: IAEA Safety Glossary, edition 2016]

3.9
division
collection of items, including their interconnections, that form one redundancy of a redundant system or safety group. Divisions may include multiple channels

Note 1 to entry: In the context of this document, “division” includes a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

[SOURCE: IAEA SSG-39, 2016]

3.10
electrical isolation
electrical isolation is used to prevent electrical failures in one system from affecting connected systems. Electrical isolation controls or prevents adverse interactions between equipment and components caused by factors such as electromagnetic interference, electrostatic pickup, short circuits, open circuits, grounding, or application of the maximum credible voltage (AC or DC)

[SOURCE: IAEA SSG-34 and SSG-39, 2016]

3.11
electromagnetic compatibility
EMC
ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment

[SOURCE: IEC 60050-161:1990, 161-01-07]

3.12
electromagnetic interference
EMI
degradation of the performance of an equipment, transmission channel or system caused by an electromagnetic disturbance

[SOURCE: IEC 60050-161:1990, 161-01-06]

3.13
independence
condition that exists when successful completion of a system's required functions is not dependent upon any behaviour including failures and normal operation of another system, or upon any signals, data, or information derived from the other system

Note 1 to entry: The following definition is to be found in the IAEA Safety Glossary, edition 2016 for "independent equipment": "Equipment that possesses both of the following characteristics: a) The ability to perform its required function is unaffected by the operation or failure of other equipment; b) The ability to perform its required function is unaffected by the occurrence of the effects resulting from the initiating event for which it is required to function". This IAEA definition is limited to equipment but is consistent with the definition given in this document.

3.14
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

[SOURCE: IEC 62808:2015, 3.4]

3.15
physical separation
separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof

[SOURCE: IAEA Safety Glossary, edition 2016]

3.16
postulated initiating event
PIE
postulated event identified in design as capable of leading to anticipated operational occurrences or accident conditions

[SOURCE: IAEA Safety Glossary, edition 2016]

3.17
redundancy
provision of alternative (identical or diverse) structures, systems and components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other

[SOURCE: IAEA Safety Glossary, edition 2016]]

3.18
safety group
assembly of equipment designated to perform all actions required for a particular initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

[SOURCE: IAEA Safety Glossary, edition 2016]

3.19
safety system
system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[SOURCE: IAEA Safety Glossary, edition 2016]

3.20
separation
set of measures that minimize the influence of one entity onto the other entity to improve the independence of the entities

3.21
structural separation
placement of the separated components in different buildings or compartments, or placement of protective structures between components located in the same room, in such a way that they cannot be simultaneously damaged by the considered threat

3.22
structures, systems and components
SSCs
general term encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human factors

[SOURCE: IAEA Safety Glossary, edition 2016]

4 Abbreviated terms

AC	alternating current
CCF	common cause failure
DC	direct current
DEC	design extension condition
DiD	defence in depth
EMC	electromagnetic compatibility
EMI	electromagnetic interference
HVAC	heating, ventilation and air-conditioning
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
LV	low voltage (<1 000 V)
MV	medium voltage
NC	non-classified
NPP	nuclear power plant
PIE	postulated initiating event
SSC	structures, systems and components
VDU	visual display unit

5 Principles and requirements for separation

5.1 Principles

5.1.1 General

According to IAEA SSR-2/1 Requirement 21, interference between safety systems or between redundant elements of a system shall be prevented by separation means, such as:

- physical separation;
- electrical isolation;
- functional independence;
- independence of communication.

A combination of one or more of these measures shall be implemented to achieve the required degree of separation based upon the potential hazards (threats) to the independence.

Note that as stated in Clause 1, functional independence and independence of communication are out of the scope of this document, including the threats to be considered which should be identified by the I&C cyber security programme. For details refer to IAEA SSG-39, IEC 61500 and IEC 61513:2011,5.4.2.4 and 5.4.3. Although out of scope of this document, measures already taken to address functional independence shall be considered when assessing the need for additional separation measures to meet the requirements of this document.

More details referring to functional independence, independence from control systems and independence of communication are given in Annex D.

The separation of safety class 1 from other classes, as used in this document, is only an example of the application of the requirements of the document.

5.1.2 Separation reasoning and boundaries

Separation is a principal means of preventing:

a) propagation of failures from system to system;

b) propagation of failures between redundant parts within safety systems;

c) common cause failures due to internal hazards and some external hazards;

d) propagation of failure between different DiD levels, when it is required by the safety principles of the project or national nuclear standards.

The types of possible failure-initiating events shall be taken into consideration (i.e. identified, documented and justified). Adequate provisions shall be made in I&C and electrical 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.

Failures and hazards to be considered as a basis for the elaboration of the separation principles shall be defined by every project individually. Hazards to be considered are given in 6.2. Design errors and I&C and electrical failure events are given in Annex C.

Dependencies between I&C and electrical systems could be on physical interfaces (e.g. power supply, signal exchange), layout design within a room or between buildings, support systems (e.g. HVAC) or the spreading of failures (e.g. fire, airplane crash).

During I&C and electrical architecture design, plant design constraints according to IEC 61513 and IEC 63046 shall be identified. Depending on the results appropriate design measures shall be specified.

The principle of physical separation by structure or distance is shown in Figure 1.

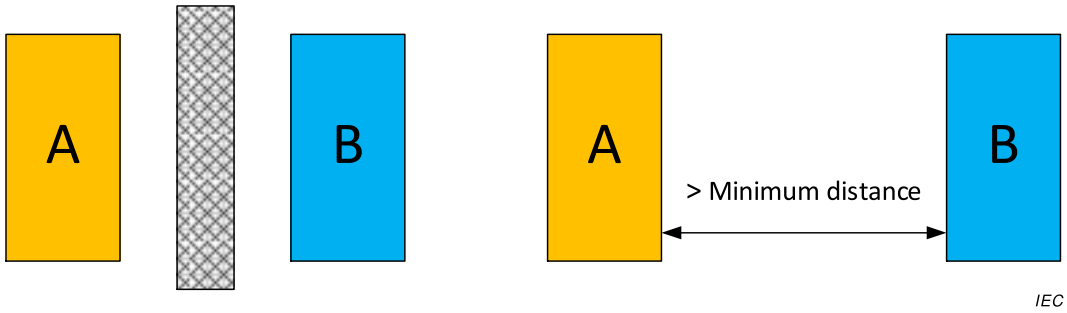


Figure 1 – Physical separation by structure or distance

The principle of separation by electrical isolation is shown in Figure 2.

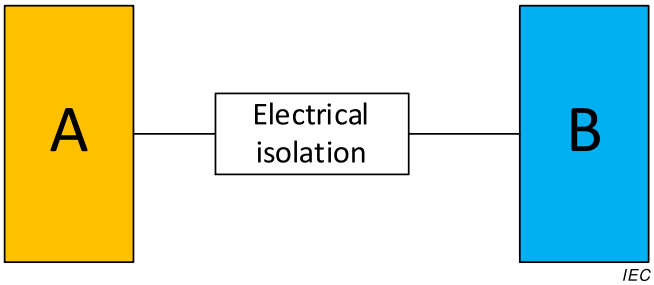


Figure 2 – Separation by electrical isolation

NOTE Common cause failure due to hazard may occur, combined hazard too.

5.1.3 Plant safety principles and requirements

The general principles for separation are mainly influenced by the specific requirements from nuclear facilities and general requirements. These principles are:

- independence requirements;
- hazard analyses and protection rules (including fire);
- deterministic safety rules;
- electrical fault propagation;
- requirements from non-nuclear industrial rules and standards (e.g. escape routes and layout constraints);
- requirements from EMC/EMI;
- requirements referring to cable laying distances due to heat dissipation.

In this document, mainly the specific requirements for nuclear facilities and some aspects of electrical fault propagation are treated; the other requirements are mentioned to cover the complete subject.

The separation principles and the means chosen to achieve them shall be described in a dedicated project document (separation concept). A verification activity shall be performed to ensure that separation requirements have been met (see Clause 9).

5.2 Safety class separation requirements

IEC 61226 defines how safety functions are categorized and SSCs 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.

As a design basis for I&C and electrical systems that fulfil and/or contribute or support systems 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. The grouping and separation criteria between the different safety classes shall be defined at the beginning of the project.

– Systems which are classified to safety class 1 shall be protected from consequential effects caused by faults and normal actions within:

  a) redundant parts of those systems;

  b) systems of a lower classification;

  c) in some cases, between different systems classified to safety class 1 where independence is required.

  The faults considered shall include those internal to the I&C or electrical systems as well as those that occur as a result of events external to the I&C or electrical systems.

– Systems classified to safety class 2 shall be protected from consequential effects caused by faults and normal actions within:

  d) redundant parts of those systems; and

  e) systems of a lower classification.

The faults considered shall include those internal to I&C or electrical systems, but may exclude those that occur as a result of events external to the I&C or electrical systems.

In cases where systems classified in safety class 2 are claimed to provide protection in the event of specific hazards, then those systems shall follow the principles of safety class 1. For example, in some countries, all systems required to achieve and maintain long-term shutdown shall be protected against fire hazard regardless of their classification.

Certain systems classified in safety class 3 may need to be protected from the influences of faults in other systems. This should be determined on a case-by-case basis. Class 3 systems used to control and monitor during DEC should be protected from the influence or faults in other systems.

Unclassified systems do not need to be protected from influences of faults in other systems.

For the electrical power supply circuit of lower classified components, the separation requirements of the power supply circuit unit (e.g. the unit in the switchboard) do not have to be fulfilled in the following cases:

1) where a power supply of lower classified systems or components is fed from a higher classified power source, due to power supply requirements, justifies the use of higher classified power supply circuits.
2) where dependence between a lower safety classified system (e.g. emergency lighting) and higher safety classified system (e.g. Emergency Power Supply System) justifies the use of a supply from the higher classified source.

In these cases the impact on the higher classified power supply system shall be justified including accounting for the power demand and electrical transient.

5.3 Associated circuits

5.3.1 General

When functions are categorized according to the requirements of IEC 61226 and systems are classified according to standards such as IAEA SSG-30, IEC 61513, or IEC 63046 it will often be the case that a given system or set of equipment will perform functions of different categories. Additionally, certain functions of a lower category may have a very close

relationship to category A function, for example process monitoring based on the same measurements as safety functions. The requirements stated earlier in this document generally indicate that circuits of lower safety class should be separated from those of safety class 1. However, as an alternative, the circuits of the lower safety class can be declared to be “associated circuits”, and the separation requirements are determined from this subclause. In the clauses of the document that follow only separation or association with safety class 1 will be considered. This principle may be extended to other classes depending on the project.

5.3.2 Criteria

Components and/or cables not classified in safety class 1 become associated circuits in one or more of the following ways:

a) electrical connection to a safety class 1 power supply without the use of an isolation device;

b) electrical connection to an associated power supply of safety class 1 systems without the use of an isolation device;

c) proximity to safety class 1 circuits and equipment without the required separation (physical distance or barriers);

d) proximity to associated circuits and equipment without the required separation (physical distance or barriers);

e) sharing a safety class 1 or associated signal without the use of an isolation device.

Associated circuits shall comply with one of the following requirements:

f) they shall be uniquely identified as such or as safety class 1 and shall remain (traceable to the associated safety class 1 division), or be physically separated to the same extent as, those safety class 1 circuits with which they are associated. They shall be subject to the requirements placed on safety class 1 circuits.

g) they shall be in accordance with f) above from the safety class 1 systems up to and including an isolation device. Beyond the isolation device, such a circuit does not belong to safety class 1 provided that it does not again become associated with a safety class 1 system.

h) they shall be analysed or tested to demonstrate that safety class 1 circuits are not degraded below an acceptable level.

Associated circuits and isolation devices shall be subject to appropriate qualification. This qualification shall show that the higher classified circuits will perform correctly when the associated circuit or isolation device and its cables are subjected to electrical conditions for which the higher classified circuit should function correctly. Where an associated circuit is connected to a device/system not belonging to safety class 1 without isolation, that device/system not belonging to safety class 1 shall also be subject to this appropriate qualification. Associated circuits need not be qualified for performance of function, since their function does not belong to category A/components do not belong to safety class 1. Isolation devices for I&C circuits shall be in accordance with IEC 62808.

Application of the associated circuit concept on a wide scale may lead to a broad combination of circuits of different safety classes provided that the general safety principles of physical separation are maintained. For example, cabling of differing safety classes need not be separated from each other within a safety group if the safety functions of the higher category can be performed by a redundant safety group that is separated from the safety group that contains the associated circuits.

Separation inside the electrical or I&C cabinets should not be necessary if the components belonging to the lower classified circuits are qualified following the rules for the qualification of the higher classified circuits.

5.4 Separation issues at existing plants

5.4.1 General

The separation of I&C and electrical systems important to safety in existing nuclear power plants is often incomplete because SSCs 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 document in all aspects due to practical considerations should be justified against the added safety gained through the upgrade taken as a whole.

5.4.2 Criteria

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

– separation in intermediate configurations when new I&C and/or electrical systems are installed through a phased programme;

– identification of subsystems, which can be separated without the need for intermediate interfaces;

– suitability of the existing separation to the new I&C and/or electrical technology (mainly sensitivity of digital I&C to EMI, power semiconductors, special temperature requirements and susceptibility to radiation);

– cable routing limits and an evaluation of the needs coming from new technologies for special cable trays, e.g. 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.

6 Separation design basis

6.1 Design inputs

The requirement to be considered for separation, as shown in the following, shall be summarized in a project document which should contain the requirements about separation induced from:

- the design constrains for divisional separation and defence in depth concept from the overall plant design;
- the consideration of the external and internal hazards (including fire) and combination of hazards;
- the EMC plan;
- the electrical faults;
- the other technical requirements.

Note that requirements induced by special operating conditions such as commissioning or maintenance and repair should also be considered.

- which hazards had to be mitigated by zone;
- the distance for protection against each hazard or ambient condition;
- the characteristics of the barriers by hazard;
- the separation requirement between safety classes or defence in depth levels.

The electrical fault types and boundaries have also to be considered in a project document.

6.2 Environmental conditions and hazards

6.2.1 General

I&C and electrical system equipment shall be designed, specified, qualified and installed in such a manner as to assure its functional capability under and following the expected environmental conditions and hazards.

6.2.2 Environmental conditions

Variation of environmental conditions such as radiation, temperature, pressure and humidity during normal operation and under accident conditions shall be considered.

6.2.3 External hazards

The construction of a NPP consists of several defence levels to withstand external hazards such as airplane crash, hurricanes, earthquakes or flooding. These constructional defence lines provide the prerequisite for I&C and electrical systems to manage operational states and accident conditions.

These external hazards, such as earthquake, could be without influence on the separation requirements, or with possible influence on the separation requirements, such as air plane crash.

Natural external hazards could be:

- meteorological;
- hydrological;
- geological;
- seismic.

Human induced external hazards could be:

- nearby industries;
- transportation routes (on air, water or land).

Natural and human induced external events that have been identified in the site evaluation process shall be considered.

The results of the external hazard analysis shall be considered in the project separation concept.

6.2.4 Internal hazards

Internal hazards have a significant influence on the separation requirements.

For the design of I&C and electrical architecture the impact of internal hazards shall be considered by means of physical separation of the different divisions in combination with electrical isolation.

Possible internal hazards include:

- fire;
- explosion;
- flooding;
- missile generation;

- collapse of structures and falling objects;
- high energy pipe breaks leading to pipe whip and jet impact;
- release of fluid from failed systems.

The results of the internal hazard analysis shall be considered in the separation concept.

Consequences of external hazards or events shall be considered when identifying possible internal hazard.

6.2.5 Fire protection

Fire protection requirements derived from applicable standards shall be followed.

Flame-retardant cables should be used, wherever practical. The IEC 60332 series provides guidance for the testing of electric cables to demonstrate their flame-retardant properties.

Cable tray and conduit penetrations of fire barriers (vertical and horizontal) shall be sealed with non-combustible materials to give protection at least equivalent to that required of the fire barrier.

Non-combustible materials shall be used for cable trays and conduits.

NOTE The separation of I&C and electrical systems important to safety and also the fire protection measures in existing nuclear power plants reflect the initial design. The SSCs safety classification, design standards and also fire protection requirements may have continuously evolved to more constraining requirements, therefore the existing design is often not compliant to modern standards.

6.3 EMI/EMC

EMC is a system engineering issue dealing with the balance of immunity and emissions at the interfaces between the various sub-systems.

Separation is one approach to guard against the potential CCF impact of EMI.

International EMC standards on industrial environments, IEC 61000 series and the dedicated standard for NPPs IEC 62003 should serve as the basis for the definition of the EMC requirements. These should be supplemented, where necessary, to cover the EMC environments of generating power plant components, which might be more demanding.

6.4 Electrical fault

The I&C or electrical system shall be either protected or be able to tolerate the faulty insertion of a systems own internal voltage and any credible external voltage, current (overvoltage barrier, short circuit / overcurrent barrier) and ensure the autonomy (electrical nonreactive, electrical insulation) of signal multiplication and transmission.

6.5 Requirements from non-nuclear technical standards

Requirements induced by other technical topics such as heat dissipation of components and cables (acceptable thermal loading) and escape route ways, etc., should also be considered in the project separation concept.

6.6 Requirements from special operating conditions

Requirements from special operating conditions such as commissioning, modification, maintenance and repair, design and administrative control procedures, shall be considered during design and construction.

7 Electrical isolation

7.1 Principles

7.1.1 General

Electrical isolation is described in IAEA SSG-34 and IAEA SSG-39.

The selection and combination of electrical isolation measures are illustrated in Figure 3.

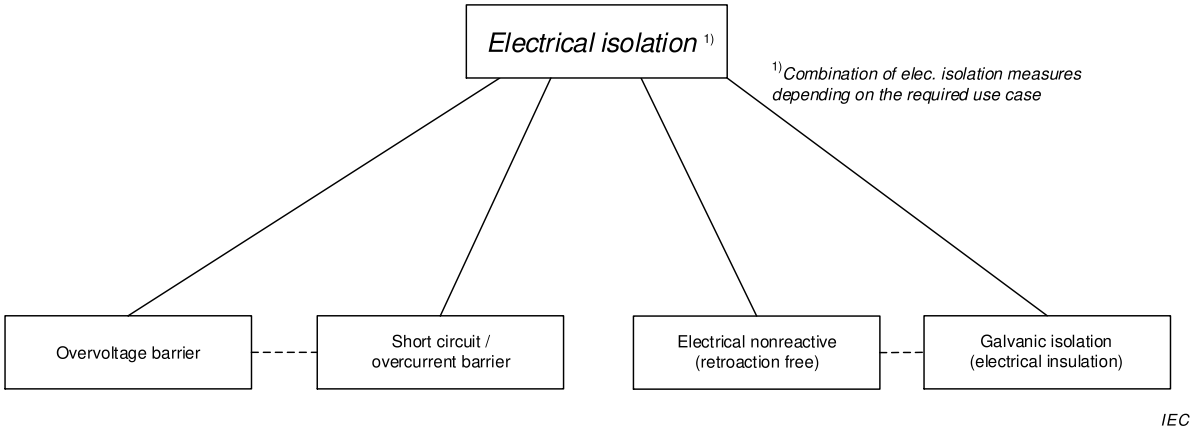


Figure 3 – Electrical Isolation measures and selection of components

Depending on the required use case a combination of measures shall be specified in the design. The omission of a single measure could lead to the consequence that the complete electrical isolation is ineffective.

7.1.2 Overvoltage barrier

An overvoltage barrier either physically separates or prevents the propagation of overvoltage or current transient in a given direction (depending on use case). Overvoltage is the existence of voltage (AC or DC), issued from a source, exceeding design voltage, between one electrical segment and any other electrical segment, including ground.

Generally infeed of overvoltage in a system has to be taken into account if it is a realistic failure mode from a physical point of view.

Foreign voltage shall be limited to a non-hazardous degree by implementation of dedicated electrical isolation devices for the system to be protected. Depending on the use case a combination of electrical devices shall be identified to consider the postulated maximum voltage transients and exposure time for the components to be protected.

Measures for overvoltage barrier could include deliberate destruction of a complete or limited part of the components. A physical destruction could be initiated by melting, combusting or bursting of components. The impacts of the triggered overvoltage barrier to further components of the signal chain shall be considered in the design of I&C and electrical systems by physical separation (see Clause 8).

7.1.3 Short circuit / Overcurrent protection

For short circuit protection, devices such as fuses or circuit breakers are used to interrupt the supply to the short circuit fault. Overcurrent is detected by dedicated devices, if installed, and interrupted by devices such as contactors or breakers.

The protection equipment in the emergency power system is generally designed such that defects or failures are reliably detected, the necessary disconnections are performed and

erroneous actuations from operational transients are prevented. Operational issues such as inrush current peaks or successive starting cycles of motors shall not actuate protection devices. Generally overcurrent protective features shall be selected and adjusted to such values that the minimum short-circuit currents are detected; however, no current transients from operating procedures shall cause any disconnections.

7.1.4 Electrical nonreactive (retroaction free)

Electrical retroaction is an effect that a source of an electrical signal may be falsified by a failure in the receiver of the signal. Retroaction free (or nonreactive) is a feature of an interface to ensure that failures in the target system will not degrade the source system.

For a nonreactive signal exchange (or signal multiplication) the output of a retroaction free component could be stressed by a low- or high signal level (system voltage) without any impact on the source of the signal. This signal level shall have no impact (retroaction free) on the input signal of the electrical isolation component.

Retroaction freeness is a characteristic of a component which ensures the following: When a source of an electrical signal supplies several components, in case of failure in one of the supplied components or interfaces, this failure will not degrade the source signal for the remaining components or the source itself.

7.1.5 Galvanic isolation (electrical insulation)

In addition to retroaction free signal transmission, high-impedance insulation devices shall protect (separate) signal interchange between I&C systems (including interfaces between different I&C systems).

Electrical insulation is in principle to prevent current flow between electric circuits even if power or signals are exchanged. Electrical insulation is needed to exchange information between I&C systems belonging to:

- different system voltage levels (e.g. 110 V (AC) ← → 24 V (DC)),
- different ground loops,
- different rooms (building constructions) if electrical interference is to be avoided, or
- long cable run distances (depending on voltage drop over cable distance).

The characteristic of the chosen electrical insulation measures has to be taken into account in I&C and electrical architecture design. An electrical insulated interface may be nonreactive and may protect against overvoltage on I&C side.

For electrical systems generally an inductive separation via transformers produces the galvanic isolation. A galvanic isolation on the electrical side is generally not a sufficient protection against overvoltage.

7.2 Isolation devices

7.2.1 General

Requirements referring the safety class of an isolation device depend on the safety class of the electrical circuit to be separated. The isolation device shall be such that failures or conditions at their output terminals (which are connected to the lower classified system) cannot prevent the safety action of the safety class 1 system or sub-system to which the isolation device is connected. As an example for I&C, a circuit at safety class 1 may be monitored for alarms by a relay in that circuit at that safety class whose contacts provide alarms at a lower safety class.

Temporary connections for maintenance to the safety class 1 systems 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.

Failures and mal-operations in the systems not belonging to safety class 1 shall cause no change in system performance, e.g. for the I&C topics such as response, drift, accuracy, sensitivity to noise, or other characteristics of the safety class 1 system which might impair the ability of the system to perform its safety functions.

7.2.2 Isolation characteristics

The properties of an isolation device shall include:

– tolerance and isolation for EMI defined in IEC 62003;
– 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;
– prevention of effects of short circuits;
– prevention of retroaction.

For electrical devices general rules are given in IEC 61439-1. If the I&C or electrical equipment does not have sufficient characteristics for electrical isolation, an isolation device shall be added.

The design and qualification of isolation devices for I&C systems important to safety are described in IEC 62808.

For the design of electrical protection, the time behaviour of possible failure also has to be considered.

In this context, an assessment should be done of the maximum voltage and current 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 for the I&C, that failure in a system not belonging to safety class 1 causes spurious or premature actuation of a safety class 1 system.

7.2.3 Actuation priority

Where plant equipment that is controlled by a safety class 1 system is also controlled by signals from a lower safety classified system, isolation devices shall be provided which ensure priority of the safety class 1 system actions over those of the lower safety classified system. Failures of, or normal actions by, the lower safety classified system shall not interfere with the safety class 1 system under plant conditions requiring success of those safety class 1 actions. The priority isolation devices shall be classified as part of the safety class 1 system.

Where signals are extracted from safety class 3 systems for use in non-safety classified systems, isolation devices may not be required; however, good engineering practices should be followed to prevent the propagation of faults. In cases where systems (e.g. safety class 2) performing category B functions need to take on the aspects of safety class 1 systems due to the functions performed, isolation shall be applied.

For a system of class 2, failures and mal-operations in the class 3 or unclassified systems shall cause no significant change in system performance, e.g. maximum response time, maximum usage of resources shall be respected, drift, accuracy, or other characteristics of

the safety class 2 systems which might impair the ability of the system to perform its safety functions.

For I&C systems fiber optic communications provide a very effective means of achieving electrical isolation/decoupling, and should be applied wherever practical.

8 Physical separation

8.1 Principles

8.1.1 General

Where physical separation is required, prevention of failure propagation shall be considered for failures which could occur:

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

Physical separation is a means to cope with mechanical or environmental impacts.

Physical separation may be achieved through separation by distance, structural separation or a combination of the two, and is a means to reduce the likelihood of dependent failures (common cause failures) resulting from failures as consequences of PIEs (such as fire, missile and flooding or high energy pipe break).

The choice depends on the postulated initiating events and may differ from location to location within the NPP. It will depend on the need to provide protection against all the PIEs considered in the design basis.

8.1.2 Separation by distance

Physical separation does not explicitly require installing structural barriers between two components but may be achieved by applying appropriately distance or geographical separation to cope with underlying PIEs (e.g. direct effect of airplane crash).

The measured distance is the space that has no interposing structures, equipment, or materials that could aid in the propagation of effects induced by hazards (e.g. fire, air plane crash, etc.) or that could otherwise disable I&C or electrical systems.

8.1.3 Structural separation

In the context for I&C and electrical systems, a physical structural barrier is a physical separation of two independent areas by means of constructional measures. These measures shall prevent the spreading of postulated initiating events and internal hazards. Depending on the relevant PIEs a structural barrier could be a wall as a fire barrier or dedicated shielding to protect against conditions imposed by accidents.

8.2 Separation of cables and cable support structures

8.2.1 General

The separation provision for cable should be defined based on tests performed to determine the flame retardant characteristics (IEC 60332) of the proposed cable installation considering features such as insulation and jacket materials, raceway fill, raceway types, and

arrangements. In hazardous areas, the severity of the hazards, such as the size of the fire or pipe break, and mitigating measures such as sprinklers should be considered.

Additionally, the minimum distance for power cable may consider industrial standards, such as e.g. IEC 60364-5-52.

8.2.2 Divisional separation of redundant cables and cable support structures

For redundant cables within an I&C or electrical system important to safety, generally a divisional separation shall be introduced. The following applies:

– each redundancy shall be provided with physically separate cable routes, trays, conduits, ducts, vertical ducts and penetrations;
– any given route, tray, conduit, duct, vertical duct or penetration shall carry or contain only cables of the same redundancy;
– for the I&C and electrical system failure-initiating events that have their cause in the cabling system, such as arcing or overheating due to short circuits, overloads, voltage transients, etc., a low degree of physical separation may be sufficient;
– for plant failure and external failure events (see 6.2), such as fire or structural collapse, adequate physical separation including barriers and/or safety structures shall be applied, as defined by the hazard analysis.

8.2.3 Separation of system cables and cable supporting structures of different safety classes

The separation of circuits not important to safety from circuits important to safety or associated circuits shall be achieved by complying with the following requirements.

a) circuits not belonging to safety class 1 shall be physically separated from safety class 1 circuits and associated circuits generally by distance, by metal divider or if applicable physical barriers except as permitted in item d), or the non- safety class 1 circuits shall be associated circuits; the minimum distances for horizontal and vertical separation of system cables of different safety classes should be established following all the defined criteria in the project separation concept.
b) circuits not belonging to safety class 1 shall be electrically isolated from safety class 1 circuits and associated circuits by the use of isolation devices, shielding, and wiring techniques or separation distance, except as permitted in item d), or the circuits not belonging to safety class 1 shall be associated circuits.
c) the effects of less than minimum separation or the absence of electrical isolation between the circuits not belonging to safety class 1 and the safety class 1 circuits or associated circuits shall be analysed to demonstrate that safety class 1 circuits are not degraded below an acceptable level or the non- safety class 1 circuits shall be associated circuits.
d) instrumentation signal and control circuits not belonging to safety class 1 are not required to be physically separated or electrically isolated from associated circuits provided that firstly the circuits not belonging to safety class 1 are not routed with associated cables of a redundant division and secondly the circuits not belonging to safety class 1 are analysed to demonstrate that safety class 1 circuits are not degraded below an acceptable level. As part of the analysis, consideration shall be given to potential energy and identification of the circuits involved.
e) fiber-optic circuits not belonging to safety class 1 are not required to be physically separated from safety class 1 and associated circuits. Electrical isolation is an inherent characteristic of fiber-optic circuits. Since fiber-optic circuits have no potential to degrade safety class 1 circuits, they can be considered safety class 1 associated circuits.

Note that cabinet internal separation criteria shall be derived from physical constrains, such as voltage levels/EMC requirements. Cabinet internal physical separation based on different safety classes is not required.

8.2.4 Separation of signal cables from power cables

Cables carrying analogue and other low-level electrical signals should be separated from power cables. Exceptions shall be justified. Depending on the technology, switchgear control cables may be low or high level and shall be subjected to this requirement accordingly. Fibre optic cables may be run together with power cables if their mechanical protection is ensured.

The separation of signal cables from power cables depends on EMC and on voltage isolation. The separation between signal cables and power cables shall be sufficient concerning both of these aspects.

8.2.5 Reduced separation distances

Separation distances reduced from those defined in the cabling concept at the beginning of a project may be established by analysis of the proposed cable installation.

8.2.6 Associated circuits

Regarding associated cable circuits the requirements of 5.3 shall be applied.

8.2.7 Separation of cables from tubes or pipes

Cables should not be placed adjacent to, or in, trays, trunks or conduits with tubes or pipes carrying fluids under pressure and/or temperature such as oil, steam, water, liquid metals or other fluids which may damage the cables in case of leakage or bursting, with justified exceptions, e.g. where the proximity of a sensor or actuator cable to the process piping is unavoidable due to the need to connect the sensor or actuator to the process.

8.2.8 General routing considerations

As far as possible all cables of the system important to safety should be routed along non-hazardous routes and in a manner to preserve their integrity.

8.2.9 Identification

I&C and electrical cables shall be identified and marked following the applicable identification code.

To facilitate commissioning and modification and to reduce the chance of errors, cables and cable routes which contain system cables important to safety shall be marked to identify their redundant safety group and safety classification. This marking should be:

a) at the beginning and at the end of the cables and at the penetrations of fire barriers;

b) on the cable trays, ducts and conduits.

8.3 Separation of components inside the I&C and electrical system important to safety

8.3.1 Divisional separation of redundant components inside the I&C and electrical system important to safety

For redundant components within an I&C or electrical system important to safety, in general a divisional separation shall be introduced.

Divisional separation is fulfilled in most cases by physical barriers. If separation by physical barriers is not possible, also separation by distance and/or additional fire protection measures should be implemented.

The minimum distances for horizontal and vertical separation should be established in a separate project document, e.g. layout concept, following the rules recommended in Clause 5 and Clause 6.

Where the minimum separation distance cannot be maintained, specific rules shall be defined. This could be that specific barriers are installed or a justification of lower distances shall be provided.

For plant failure and external failure events, such as fire or structure collapse, adequate physical separation including barriers and/or safety structures shall be applied.

8.3.2 Separation of components of different safety classes

The separation of components not important to safety from components important to safety or associated components should be achieved by complying with the following requirements.

a) components not belonging to safety class 1 shall be physically separated from safety class 1 components and associated circuits generally if the qualification of the non-safety-class-1-components is lower than the qualification of the safety-class-1-components. This shall be by distance or, if applicable, physical barriers.
b) circuits not belonging to safety class 1 shall be electrically isolated from safety class 1 circuits and associated circuits by the use of isolation devices, shielding, and wiring techniques or separation distance, or the circuits not belonging to safety class 1 shall be associated circuits.
c) the absence of electrical isolation between the circuits not belonging to safety class 1 and the safety class 1 circuits or associated circuits shall be analysed to demonstrate that safety class 1 circuits are not degraded below an acceptable level or the non- safety class 1 circuits shall be associated circuits.

In the case of the supply of an associated circuit the complete power supply unit of this associated circuit is considered as higher safety classified if the component, e.g. switchboard, is higher safety classified. The power supply unit shall fulfil in this case all safety and qualification requirements for the higher safety classified component.

Separation of associated circuits (electrical or signals) from the safety classified circuits inside the components or equipment, e.g. switchboards, is not required by this document.

8.3.3 Installation of equipment of different voltage levels

Equipment of different voltage levels shall be installed following industrial requirements, e.g. separation between medium voltage switchboards, low voltage switchboards, DC switchboards and I&C cabinets.

Referring to this topic, the EMC plan and normal industrial standard requirements should be followed.

Exceptions from this rule may be possible if:

- justified by technical reasons (for example for low energies);
- no product standard is available. In this case the applicable basic standard shall be applied in a reasonable way.

8.3.4 Reduced separation distances

Separation distances reduced from those specified in the separate project document required in Clause 5 may be established by analysis of the proposed installations. The analysis should be based on tests performed and calculations. For lesser separation distances in hazardous areas, the severity of hazards (such as size of the fire or pipe break) and mitigating measures should be considered.

8.3.5 Associated circuits

Regarding associated cable circuits the requirements of 5.3 shall be applied.

8.3.6 Separation of components from sources of hazards

I&C or electrical components important to safety should not be placed in areas were hazards could arise due to existing tubes or pipes carrying media under pressure and/or temperature such as oil, steam, water, liquid metals or other media which may damage the components in case of leakage or bursting. There may be some cases where proximity between process piping and I&C and electrical component is unavoidable; in this case protection measures shall be provided.

8.4 Control room cabinets, desks, panels and related cables

Although the probability of fire in the control room and its immediate area is low, its consequences could be very severe. There are major problems in maintaining physical separation or barriers in the control room areas and its panels and desks, where many cables are brought together. Therefore, plants are designed so that fire is not likely in the control room area, and so that any fire which might start is restricted, will spread slowly and will not cause loss of safety control before other control can be established. The methods for this can be complex and they interact strongly with the station cable design, and the layout of the control panels, which are governed by human factors considerations.

The control panel layout should allow for human factors consideration (see IEC 60964), such that information and controls of redundant safety plant are grouped suitably for minimisation of the possibility of human errors. The expected frequency of human errors may be high, whereas that of fire in the control room will be low. This requirement can therefore conflict with the requirement for separation by space, barriers or isolation devices given elsewhere in this document, since the human factors requirement for the front-of-panel layout may be required to take priority over convenience or simplicity of cable and connecting wiring design.

Methods to control the potential for fire, for detection of fire and for fire suppression shall be identified and applied in the control room and its cabinets, desks and panels, and the relevant cables to and within those items. Methods of retaining physical separation or providing resistance to the spread of fire which may be used include:

– full separation of the safety plant controls and indications of different safety groups, which is preferred;
– internal metal trunking for the connections to the front of panel devices controlling redundant safety plant;
– the provision of heat detectors or automatic fire suppression within control room cabinets;
– the fire tolerance of the cabinet structure and any fire barriers between sections of the cabinets.

Factors which may be considered include the following:

– the control room is always staffed and fire will therefore be rapidly detected and extinguished;
– the control room is a controlled access area, in which accumulation of flammable material will be prevented and sabotage is unlikely;
– the detection of fire within any compartment of the control room cabinets, panels and desks will be rapid, and the potential rate of spread of fire from one compartment to another is slow enough to allow fires to be extinguished before control is lost;
– the availability of redundant controls over safety plant, where one panel section provides individual control of safety plant items and another and separated section provides an alternative and possible grouped control over the safety plant;

– the ignition of fire within a panel section is of very low frequency, within the design basis of the plant, by control of the use of flammable material and heat sources within the panel sections;
– provision of an alternate, supplementary control room from which the necessary safety control actions can be taken. Suitable means shall be provided to isolate the effects of fires in either control room.

Means of ensuring that a fire does not cause short circuits, open circuits or hot shorts such that control is degraded should be included in the I&C system designs. These include physical separation of power and control or indication wires in different cables, application of fibre optic cables and optical isolators, the use of multiplexed systems of control, and VDU soft control.

9 Verification

The project organization shall specify the verification of the implemented separation based on the project separation concept. The project separation concept shall be verified referring to the fulfilment of the requirements mentioned in this document and additional applicable standards, specific national nuclear standard and specific project requirements.

Two main topics shall be considered:

- electrical isolation;
- physical separation.

Referring to electrical isolation:

Design verification shall be undertaken referring to:

– overvoltage protection (Insulation coordination study) following e.g. IEC 60071;
– short circuit/overcurrent protection – following e.g. IEC 60909 for AC and IEC 61660 for DC;
– electrical non-reactive (retroaction-free) following e.g. IEC 60364-5-56;
– galvanic isolation following e.g. IEC 60364-4-41.

Implementation verification shall be performed based on a project specific verification plan. Implementation verification referring to electrical isolation should be completed in the frame of the commissioning tests.

Referring to physical separation:

Design verifications shall be undertaken referring to the implementation of the following requirements:

– divisional separation;
– hazard analysis;
– personnel protection;
– safety class separation;
– DiD level separation;
– additional technical requirements.

Implementation verification referring to physical separation should be completed in the frame of the installation tests.

In Annex C possible design errors and electrical failure events are listed.

Annex A
(normative)

Relation to IAEA guidelines and IEC 61226

A.1 Object of this Annex

This Annex presents the explanation with IAEA guidelines and IEC 61226 for the safety categorization of I&C and electrical functions and the safety classification of I&C and electrical systems and also the definitions of the Defence in Depth levels.

A.2 Applicability of this document

The general rules given in this document for separation of safety classes can be applied for the separation following other design constraints, such as defence in depth concept.

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

Furthermore separation distances are not defined in this document. The distance requirements shall be assessed following the installation rules, fire protection requirements, cable heating, escape routes, etc.

A.3 IAEA Guidelines, applicable for this document

The IAEA guidelines which contain requirements to be applied for safety categorization of I&C and electrical functions and safety classification of I&C and electrical systems and/or definitions of the Defence in Depth levels are:

– IAEA SSR-2/1, *Safety of Nuclear Power Plants: Design;*

– IAEA SSG-30, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants;*

– IAEA SSG-34, *Design of Electrical Power Systems for Nuclear Power Plants;*

– IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants.*

A.4 IEC standards, applicable for the safety categorization and classification

The IEC standards which contain requirements to be applied for safety categorization of I&C and electrical functions and safety classification of I&C and electrical systems are:

– 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*

Note that in this document IEC 60709 the categorization of IEC 61226 with the categories A, B and C and the corresponding classes 1, 2 and 3 are used.

A.5 Defence in Depth levels, simplified definitions

Referring to the DiD levels, the basis of the definitions is the IAEA documents.

Simplified definitions of the five levels of defence in depth are as follows:

– Level 1: Prevents deviations from normal operation;
– Level 2: Detects failures and controls abnormal operations;
– Level 3: Controls accidents that are within the plant design basis;
– Level 4: Controls the consequences of design extension conditions;
– Level 5: Mitigates the radiological consequences of significant releases of radiation.

Annex B
(informative)

Examples of separation realizations

B.1 Object of this Annex

This Annex presents practical examples for the implementation of separation requirements in the design of an NPP.

B.2 Example of physical separation

B.2.1 General

The principles of physical separation are described in Clause 5.

Physical separation is defined as: “Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof”.

B.2.2 Examples of physical separation by distance

Figure B.1 shows the separation of safety-class-1-cables and the other (non-safety-class 1) cables by distance on separate cable supporting structures in cable galleries, assigned to one division, as an example.

Furthermore the cables of different voltage levels in safety class 1 are also separated due to EMC-reasons.

The distance of 300 mm for the separation of the voltage levels for power cables follows the recommendation of IEC 60364-5-52. This standard refers to the reduction factors for cable loading, if the cables are installed on cable trays. Following this standard the 300 mm distance can be reduced, but the reduction factors for the power cable dimensioning has also to be adapted.

The width shown in Figure B.1 is influenced by different parameters, e.g. the fire load of the cables and the requirement for minimum width of escape routes.

Figure B.2 shows the separation of safety-class-1-cables and the other (non-safety-class 1) cables by distance where the cable trays are installed on the same cable supporting structure. The applicable distance has to be defined at the beginning of the project.

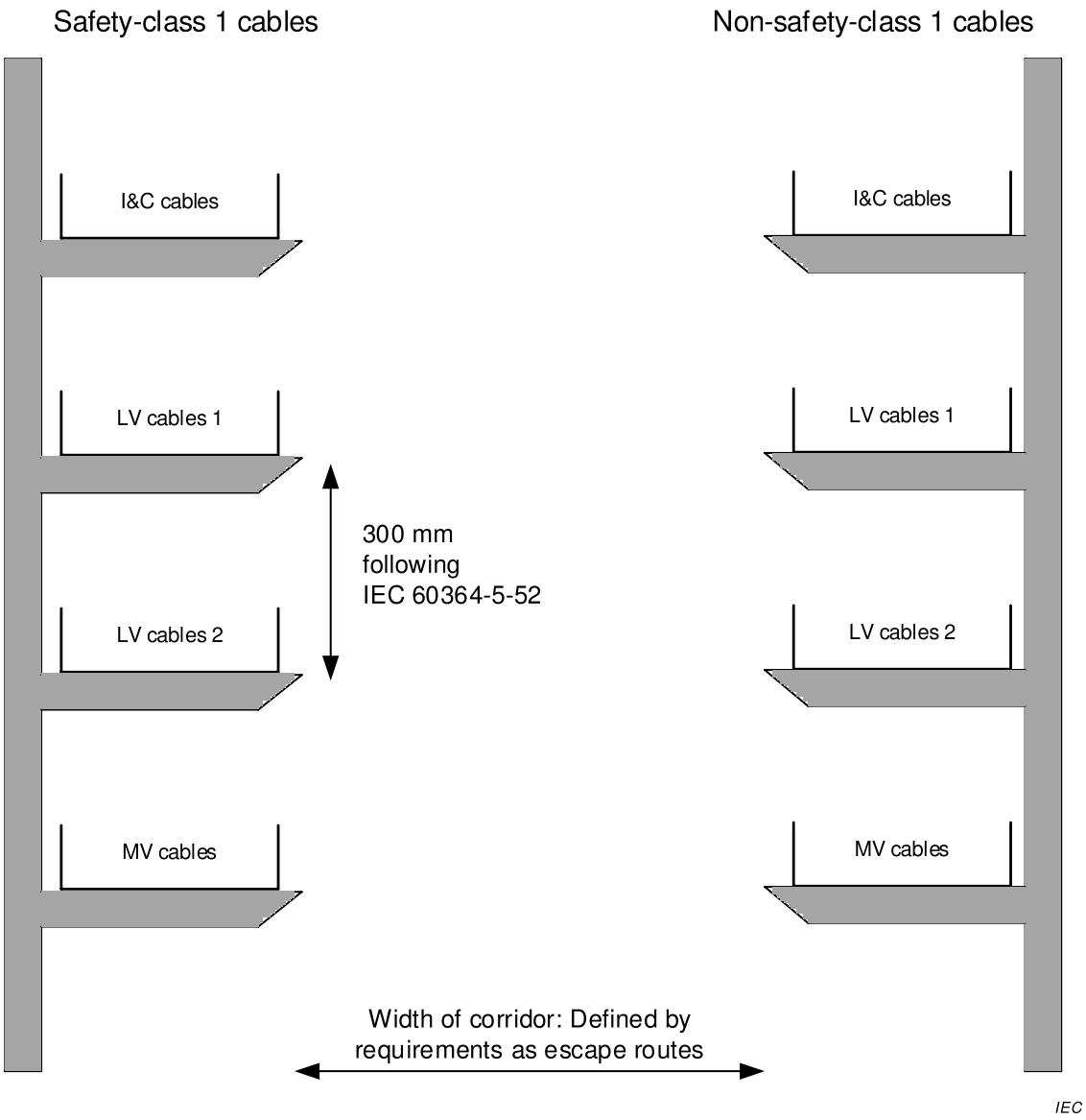


Figure B.1 – Separation of cable supporting structures by distance

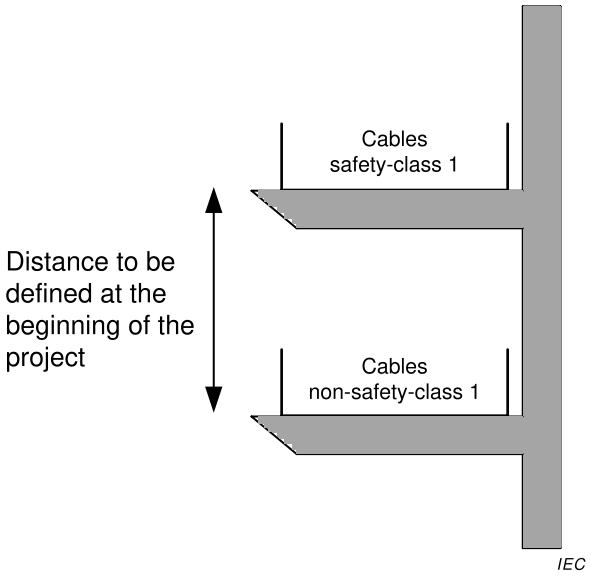


Figure B.2 – Separation of cable trays by distance

B.2.3 Examples of physical separation by structure

Figure B.3 shows the separation of cables by structures, as usually done in the case of separation of two divisions.

The fire resistance of the separation structure and also other data have to be defined by the project, following the requirements for internal hazards.

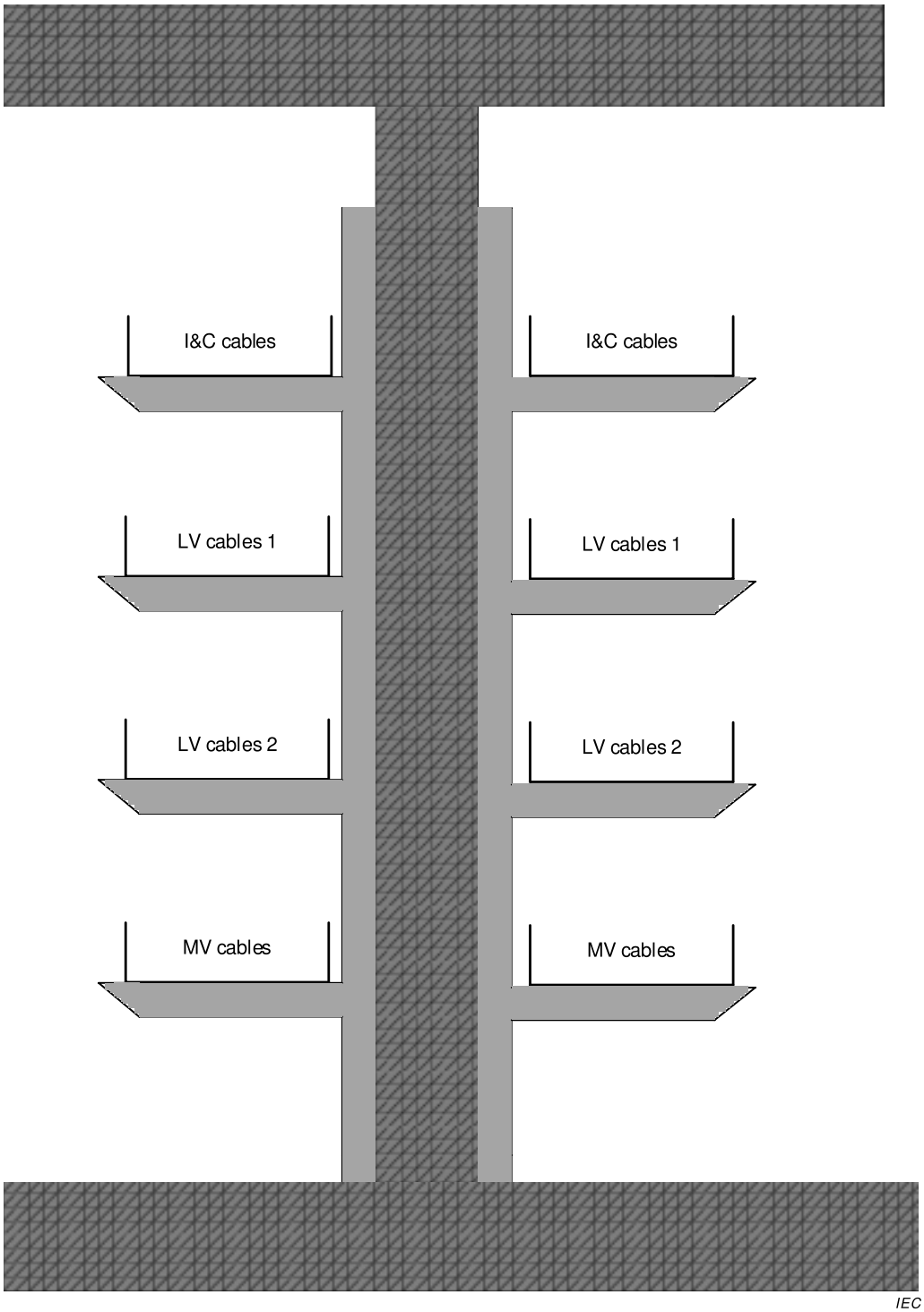


Figure B.3 – Separation by structures

B.3 Example of electrical isolation

B.3.1 General

Electrical isolation is defined in IAEA SSG-34 and IAEA SSG-39.

Electrical isolation is used to prevent electrical failures in one system from affecting connected systems. Electrical isolation controls or prevents adverse interactions between equipment and components caused by factors such as electromagnetic interference, electrostatic pickup, short circuits, open circuits, grounding, or application of the maximum credible voltage (AC or DC).

The principles of electrical isolation are described in Clause 6.

B.3.2 Examples of overvoltage barriers

Generally the components in electrical circuits are designed to operate at and withstand at a maximum supply voltage. If this voltage is higher than that for which the devices of the electrical circuit are rated, this could cause damage.

One of the main sources of overvoltage is lightning. Protection measures against lightning are taken on a general plant level, e.g. considering IEC 62305.

In order to limit overvoltage in I&C and electrical circuits overvoltage barriers are used. Standards to be considered in the specification of these overvoltage barriers are defined in IEC 61643, IEC 61647 and IEC 60364-5-53.

Figure B.4 gives an example of the installation of an overvoltage barrier in an I&C circuit.

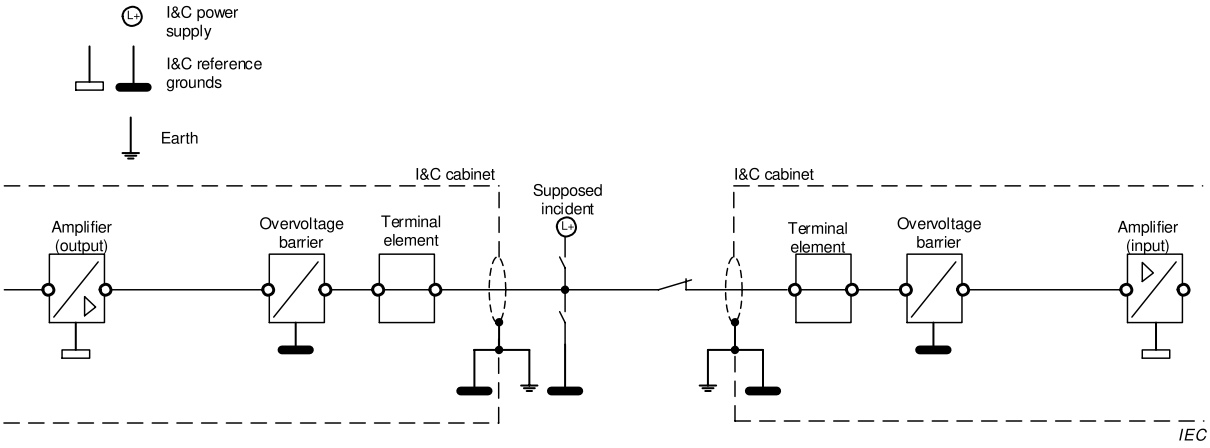


Figure B.4 – Overvoltage barriers in I&C systems

For electrical systems overvoltage protections are also installed, generally in different defence levels.

Figure B.5 shows the installation of a surge arrester in the power supply of an MV motor.

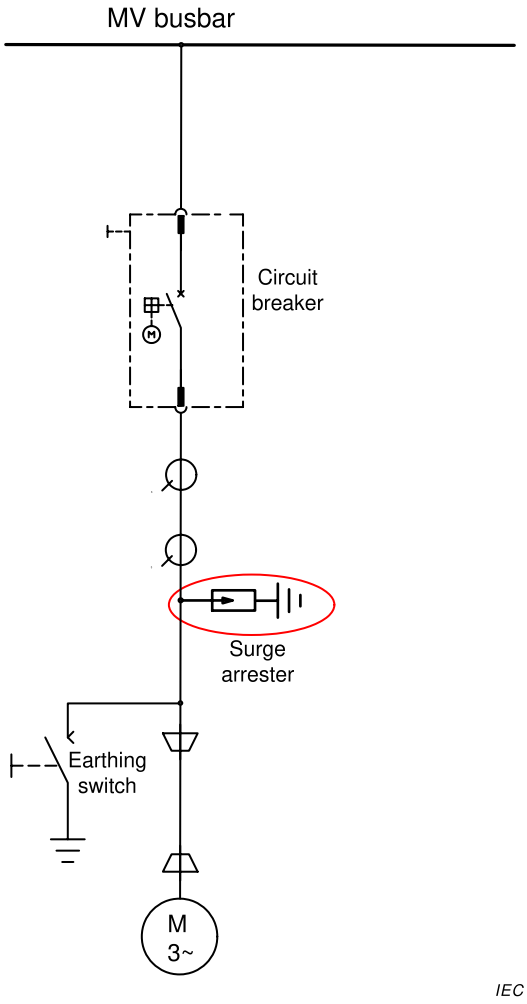


Figure B.5 – Overvoltage protection in electrical systems

B.3.3 Examples of short circuit / overcurrent protection

Overcurrent is generally caused by overload conditions in current-using equipment or by faults such as short circuits or earth faults. An overcurrent may or may not have harmful effects, depending on its magnitude and duration.

A short circuit is an abnormal connection of nodes of an electrical circuit intended to be at different voltages. The nodes will be at the same voltage during the short circuit. The result of a short circuit is generally an excessive current, which could cause damage.

Details also referring to protection measures are given in IEC 60364.

Figure B.6 shows the short-circuit protection in the case of an electrical cross-connection between two divisions. Generally this type of cross-connection is used during outages and maintenance of one division, to ensure power supply of loads such as lighting circuits.

As the power supply can be from both directions, the protection devices (fuses) are installed at both ends of the cables.

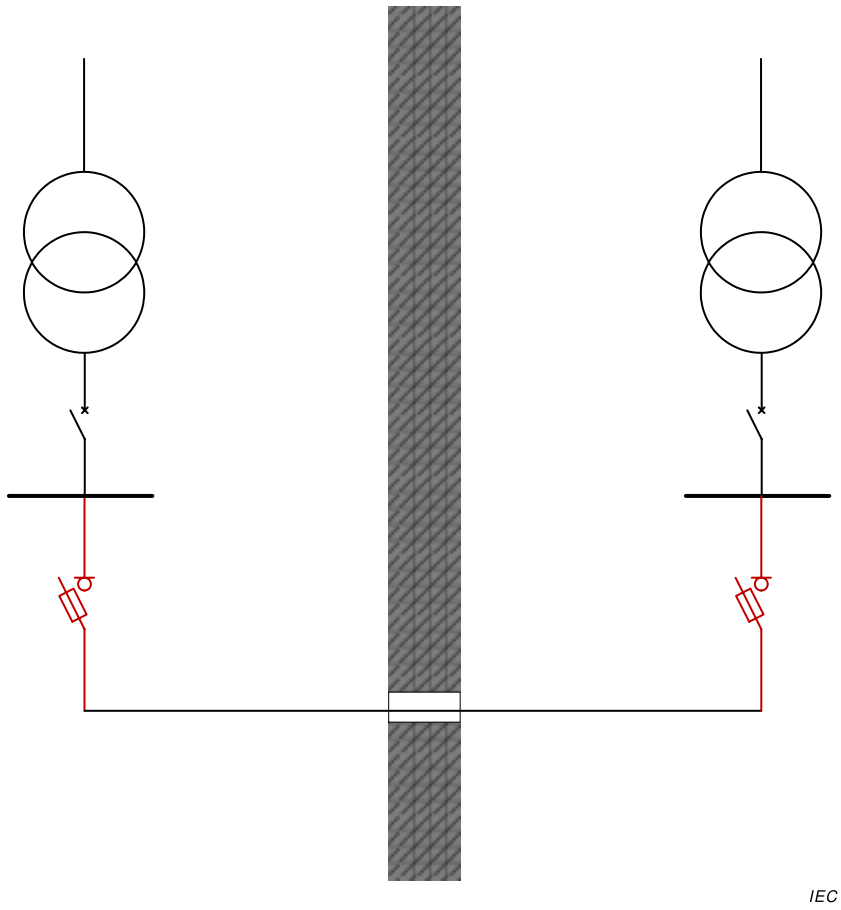


Figure B.6 – Short circuit protection in case of a cross-connection

B.3.4 Examples of galvanic isolation

Galvanic isolation is done in order to prevent direct current flow between different electrical systems. Energy or information exchange can be done by other means only, such as capacitance, induction, electromagnetic waves, optical or acoustical. In general galvanic isolation is required in cases when e.g. the grounding concept is not fully consistent, that means the grounds could have different potentials.

Figure B.7 gives an example of the installation of a galvanic isolation in an I&C circuit.

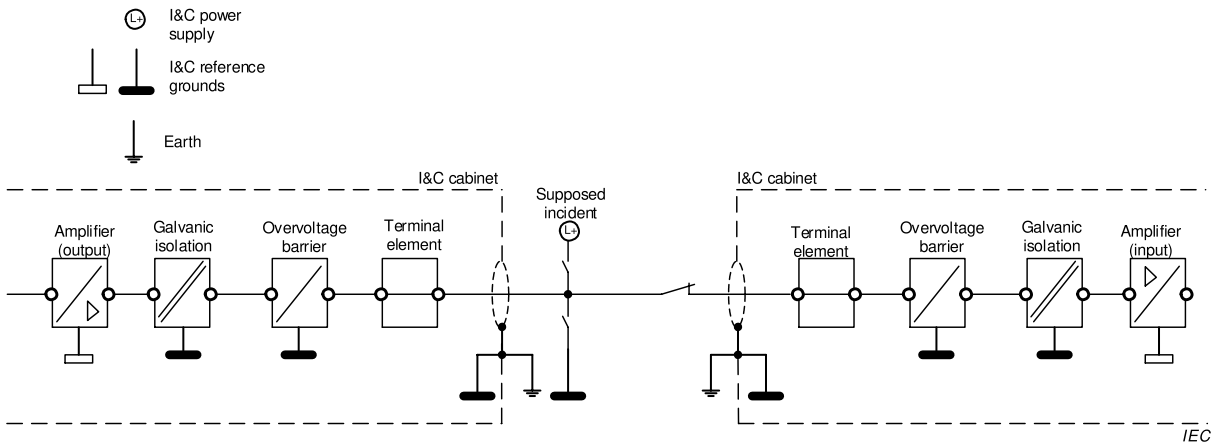


Figure B.7 – Galvanic isolation in I&C systems

In electrical systems galvanic isolation can be used for personnel safety, preventing accidental currents from reaching ground through a person's body.

An example of galvanic separation in electrical systems, usually done by transformers, is shown in Figure B.8.

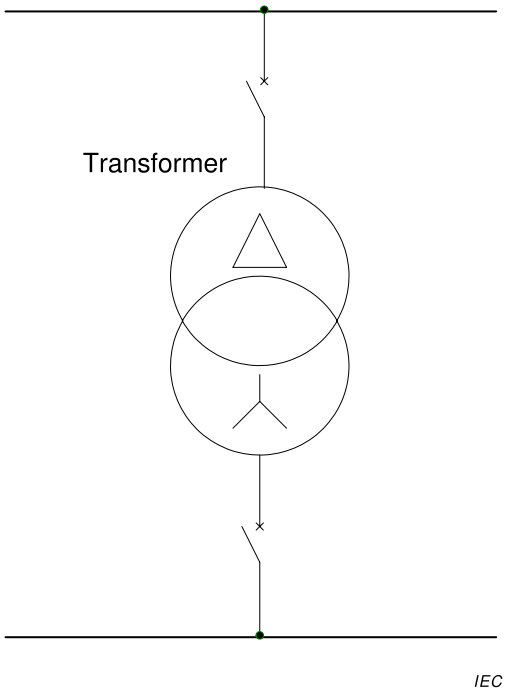


Figure B.8 – Galvanic isolation in electrical systems

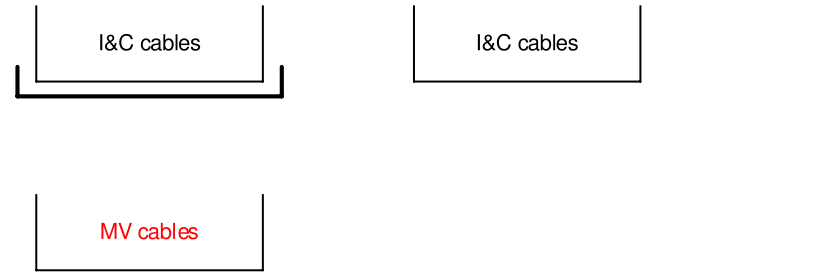
B.4 Example of EMC protection

Electromagnetic Compatibility (EMC) is the ability of a device, component, system or facility to function as intended without degradation or malfunction in their intended operational electromagnetic environment.

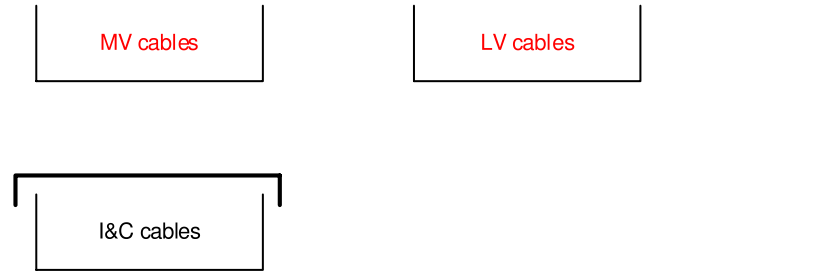
Details referring to EMC are given in the IEC 61000 series and in the dedicated IEC 62003.

The EMC requirements applicable for a plant are generally described in an EMC plan/report.

An example of one specific EMC protection of I&C cables in cable supporting structures is shown in Figure B.9.



EMC protection for I&C cables – plate or cover at the bottom



EMC protection for I&C cables – cover on ladder

EMC protection for I&C cables – totally enclosed

IEC

Figure B.9 – EMC protection of I&C cables

B.5 Associated circuits

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

The principles for associated circuits are described in 5.3.

Examples of associated circuits are shown in Figure B.10.

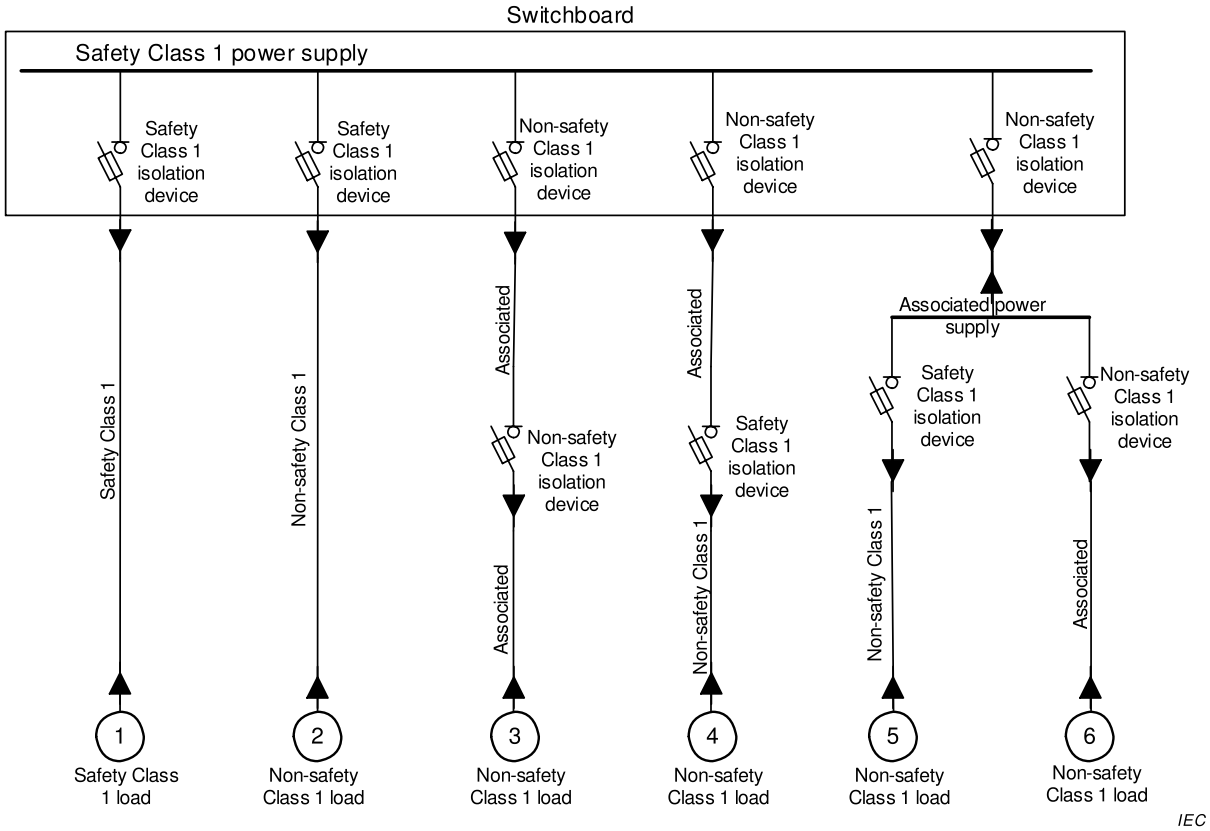


Figure B.10 – Examples of associated circuits

Annex C
(informative)

Examples of design errors and I&C and electrical failure events

C.1 Object of this Annex

This Annex shows examples of design errors and I&C and electrical failure events.

C.2 Design errors

The potential for errors in the specifications of the requirements for I&C and electrical 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 components or conductors, etc. Means to address this type of fault generally should include conservative design of physical separation and electrical isolation.

C.3 I&C and electrical system failure events

C.3.1 General

Failure initiating events having their cause within each I&C or electrical system important to safety should 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 and electrical failure events can be subdivided as follows.

C.3.2 Single random failure

A single random failure of an I&C or electrical system component, 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 should 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.

C.3.3 Multiple failures from a single common cause

Consideration should 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 should be taken into consideration.

Annex D
(informative)

Functional independence and independence of communication

D.1 Object of this Annex

This Annex presents the description of the above mentioned topics.

D.2 Functional independence

D.2.1 General

Two functions, systems or components are functionally independent if they do not need to exchange information to perform their function. Functional independence may be bilateral, if there is no exchange of information, or unilateral, if a one-way exchange of information is authorized.

The execution of safety and process functions by means of I&C and electrical systems could be interrupted by:

- blocking of safety and process functions (e.g. belonging to different levels of defence);
- faulty support systems (with direct or delayed impact to system operation);
- interlocking of automatic safety actuations (e.g. to prevent progression to more severe plant conditions);
- interference by service functions (e.g. during maintenance and periodic testing).

According to IAEA SSG-39:2016, “6.46. Functional independence is supported by the architectural design and careful treatment of data that are shared between functions (…).”

Measures regarding functional independence should be taken as input data for the separation measures.

For electrical systems this could be the actuation of a power source without impact on other power sources.

NOTE The requirements regarding functional diversity is a further method to consider independence between process and safety functions but cannot be assigned as a separation measure.

D.2.2 Independence from control system

The use of safety class 1 system signals in control systems (regardless of classification) requires precautions beyond those required when safety class 1 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 should 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 safety class 1 system.

For the case where a single random failure, and any consequential failures, within the safety class 1 system could cause a control system action that results in a condition requiring safety action, then the safety class 1 system should be capable of providing this action even when degraded by a second random failure. Provisions should 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, 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 should 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 should 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.

D.3 Independence of communication

The intention of communication is to distribute information from system A to system B or vice versa. The methods for communication in NPPs require a physical connection by which information is distributed based on electrical values (binary / analog) or on data communication protocol (excluding wireless connections).

For each type of communication it should be considered that either the transmitter or the receiver could influence / destroy its counterpart (bidirectional). Depending on the communication method different factors could impact the communication.

The measures to ensure independence of data communication are out of scope of this document, including the threats to be considered which should be identified by the I&C cyber security programme. For details refer to IEC 62645.

Bibliography

IEC 60364 (all parts), *Low-voltage electrical installations*

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61643 (all parts), *Low-voltage surge protective devices*

IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62305 (all parts), *Protection against lightning*

IEC 62645, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

IAEA GS-R-3:2006, *The management system for facilities and activities*

IAEA Safety Guide No, GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA Safety Guide No, GS-G-3.5:2009, *Management system for nuclear installations*

IAEA 50-C-Q, *Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations*

IAEA Safety Glossary:2016, *Terminology used in nuclear safety and radiation protection*

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60709 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette troisième édition annule et remplace la deuxième édition parue en 2004. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) intégration d'exigences relatives au principe de séparation dans les systèmes électriques importants pour la sûreté;

b) définition de critères de séparation pour les systèmes d'I&C et électriques de manière générale;

c) restructuration de la norme selon les critères;

d) prise en considération des interférences entre les équipements d'I&C et électriques de différentes classes de sûreté;

e) mise en cohérence de la norme avec les nouvelles révisions des documents de l'AIEA et extension du domaine d'application pour inclure de nouveaux aspects de séparation;

f) couverture de nouvelles technologies qui soit présentent des questions particulières de séparation, soit fournissent un moyen nouveau pour l'assurer;

g) amélioration des exigences et des préconisations relatives aux zones de câblage congestionnées, par exemple salle de commande, passages des chemins de câbles, etc.;

h) introduction du concept de «circuits associés» (issu de la pratique américaine) pour prendre en compte les équipements non importants pour la sûreté et les câbles qui ne sont pas séparés des équipements et des câbles classés de sûreté;

i) traitement des implications des circuits basse énergie, telles que l'utilisation possible de l'analyse pour réduire les distances minimales de séparation;

j) revue des exigences existantes, mise à jour de la terminologie et des définitions;

k) préconisations pour l'application de la présente norme aux centrales existantes.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1185/FDIS	45A/1195/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.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

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

Il est nécessaire que les systèmes d'I&C (instrumentation et contrôle-commande) et électriques importants pour la sûreté des centrales nucléaires de puissance tolèrent les effets liés aux pannes des équipements/de la centrale comme ceux liés aux événements dangereux internes et externes. Différentes techniques sont disponibles pour augmenter le niveau de tolérance des systèmes d'I&C et électriques à de tels effets, comprenant les dispositions d'indépendance prises au niveau des systèmes, des sous-systèmes et des équipements. Pour prétendre à l'indépendance de systèmes ou d'équipements, il convient de prévoir et de maintenir une séparation appropriée. La présente norme fournit des exigences techniques et des recommandations générales pour la mise en œuvre de la séparation lors de la conception des systèmes d'I&C et électriques.

L'objet de la présente norme est le suivant:

– l'Article 5 présente les principes de séparation des systèmes d'I&C et/ou électriques. Le paragraphe 5.4 porte sur la modernisation des centrales nucléaires de puissance existantes;
– l'Article 6 définit la base de conception de la séparation, y compris les entrées, et identifie un certain nombre de causes possibles d'événements dangereux internes et externes;
– l'Article 7 établit des mesures d'isolement électrique pour les systèmes d'I&C et électriques importants pour la sûreté ainsi que des exigences relatives aux appareils d'isolement;
– l'Article 8 fournit des exigences à satisfaire pour la séparation du câblage et des composants dans un système d'I&C et électrique important pour la sûreté.

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

L'IEC 60709 est un document du deuxième niveau qui est directement référencé par l'IEC 61513 et l'IEC 63046 pour ce qui concerne la séparation physique et l'isolement électrique exigées entre les sous-systèmes des différents trains de sûreté des systèmes d'I&C et électriques importants pour la sûreté et entre les systèmes d'I&C et électriques importants pour la sûreté et ceux qui ne sont pas importants pour la sûreté et entre les différents niveaux de défense en profondeur.

L'IEC 61226 qui est cohérente avec le guide de sûreté SSG-30 de l'AIEA établit les principes de catégorisation des fonctions d'I&C et électriques et le classement des structures, des systèmes et des composants (SSC) suivant leur niveau d'importance pour la sûreté. L'IEC 61226 fait référence à l'IEC 60709 comme la norme traitant des exigences de séparation.

Pour plus de détails sur la relation de la présente norme avec les lignes directrices de l'AIEA et l'IEC 61226, voir l'Annexe A de la présente norme.

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

L'IEC 60709 est applicable aux équipements et systèmes d'I&C et électriques importants pour la sûreté. Elle donne les exigences de séparation physique et électrique qui constituent un moyen permettant d'assurer l'indépendance entre les fonctions implantées dans ces équipements et ces systèmes. Les autres aspects relatifs à l'indépendance qui peuvent être exigés pour répondre aux préoccupations concernant les défaillances de cause commune ne sont pas couverts par la présente norme. En outre, les critères de séparation dus aux exigences de sûreté ne sont pas non plus pris en considération.

Les exigences énoncées dans la présente norme concernant la séparation des classes de sûreté peuvent être appliquées à la séparation pour d'autres contraintes de conception, telles

que le concept de défense en profondeur. Ces règles doivent être définies au début d'un projet par un concept de séparation.

La séparation entre la classe de sûreté 1 et les autres classes, telle qu'utilisée dans la présente norme, ne constitue qu'un exemple de l'application des exigences de la norme.

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

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. La norme IEC 61513 traite des exigences générales relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires. La norme IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être considérées ensemble et au même niveau. Les normes IEC 61513 et IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre complet, cohérent et consistant établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

Les normes IEC 61513 et IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC 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, la conception des salles de commande, compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes programmés numériques, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec les normes IEC 61513 et IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par les normes IEC 61513 ou IEC 63046, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

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

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires, avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en œuvre NSS17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes

ISO ainsi qu'aux documents AIEA GS-R partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, la norme IEC 62645 est le document chapeau des normes du SC 45A de l'IEC portant sur la cybersécurité. Elle est élaborée sur les principes pertinents de haut niveau des normes ISO/IEC 27001 et ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec la norme IEC 62443. Au second niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et la norme IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales.

NOTE 2 Le domaine de l'IEC SC 45A a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein de l'IEC SC 45A pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts de l'IEC SC 45A ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée la présente NOTE 2 de l'introduction sera supprimée.

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

1 Domaine d'application

1.1 Généralités

Le présent document est applicable aux systèmes d'instrumentation et de contrôle-commande (I&C) des centrales nucléaires de puissance ainsi qu'aux systèmes et équipements électriques, dont il est exigé que les fonctions soient indépendantes en raison de leur contribution à:

- un groupe de sûreté redondant ou varié;
- différents niveaux de défense en profondeur;
- différentes classes de sûreté et avec les systèmes non classés (NC).

Il est aussi applicable aux installations temporaires qui font partie de ces systèmes d'I&C et électriques importants pour la sûreté (par exemple, les équipements auxiliaires pour les essais de mise en service et l'expérimentation ou pour les systèmes mobiles d'alimentation électrique). L'Article 7 traite plus particulièrement de l'isolement électrique et l'Article 8 du câblage et de la disposition des équipements des systèmes d'I&C et électriques importants pour la sûreté.

Le présent document s'applique aux systèmes d'I&C et électriques des nouvelles centrales nucléaires de puissance et aux systèmes d'I&C et électriques améliorés ou rénovés de centrales existantes. Pour les centrales existantes, voir 1.2 et 5.4.

Lorsque l'indépendance est exigée par une norme générale de sûreté telle que les guides sûreté AIEA, l'IEC 61513 (pour les systèmes d'I&C), l'IEC 63046 (pour les systèmes électriques) ou par d'autres contraintes de projets, un des moyens pour atteindre cette indépendance est la séparation physique et l'isolement électrique des systèmes et des équipements qui réalisent des fonctions de sûreté. Le présent document définit les évaluations nécessaires et les exigences techniques qui doivent être satisfaites par les systèmes d'I&C et électriques, les équipements ou les câbles pour lesquels la séparation est exigée. Ces moyens permettent d'obtenir une séparation physique et un isolement électrique appropriés entre les parties redondantes d'un système ou entre un système de classe supérieure et un système de classe inférieure. Cette séparation est nécessaire pour prévenir ou réduire le plus possible l'impact sur la sûreté qui pourrait résulter de pannes ou de défaillances qui pourraient être propagées ou qui pourraient affecter plusieurs parties d'un système ou de plusieurs systèmes.

Les exigences relatives aux fonctions à rendre indépendantes sont normalement définies en détail dans la documentation relative au projet, ainsi que leurs systèmes et équipements associés. La méthode de détermination et de définition de ces exigences ne relève pas du présent document.

Selon la Prescription 21 du SSR-2/1 de l'AIEA, les moyens de séparation tels que la séparation physique, l'isolement électrique, l'indépendance fonctionnelle et l'indépendance en matière de communication sont normalement pris en considération. Le présent document traite de la séparation physique et de l'isolement électrique tandis que l'indépendance fonctionnelle et l'indépendance en matière de communication ne sont pas traitées dans le présent document. Des informations plus détaillées concernant l'indépendance fonctionnelle,

l'indépendance des systèmes de contrôle-commande et l'indépendance en matière de communication sont fournies à l'Annexe D.

1.2 Application: nouvelles centrales et centrales préexistantes

Le présent document s'applique aux systèmes d'I&C et électriques des nouvelles centrales nucléaires de puissance ainsi qu'à l'amélioration et à la rénovation des centrales existantes.

Pour les centrales existantes, seul un sous-ensemble des exigences est applicable. Ce sous-ensemble est normalement spécifié et discuté au début de chaque projet.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences 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).

IEC 60071 (toutes les parties), *Coordination de l'isolement*

IEC 60332 (toutes les parties), *Essais des câbles électriques et à fibres optiques soumis au feu*

IEC 60364-4-41, *Installations électriques à basse tension – Partie 4-41: Protection pour assurer la sécurité – Protection contre les chocs électriques*

IEC 60364-5-52, *Installations électriques à basse-tension – Partie 5-52: Choix et mise en oeuvre des matériels électriques – Canalisations*

IEC 60364-5-56, *Installations électriques des bâtiments – Partie 5-56: Choix et mise en oeuvre des matériels électriques – Services de sécurité*

IEC 60909 (toutes les parties), *Courants de court-circuit dans les réseaux triphasés à courant alternatif*

IEC 60964, *Centrales nucléaires de puissance – Salles de commande – Conception*

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

IEC 61226, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

IEC 61439-1, *Ensembles d'appareillage à basse tension – Partie 1: Règles générales*

IEC 61500, *Centrales nucléaires de puissance – Système d'instrumentation et de contrôle-commande importants pour la sûreté – Communication de données dans les systèmes réalisant des fonctions de catégorie A*

IEC 61513:2011, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 61660 (toutes les parties), *Courants de court-circuit dans les installations auxiliaires alimentées en courant continu dans les centrales et les postes*

IEC 62003, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences relatives aux essais de compatibilité électromagnétique*

IEC TR 62096, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Guide pour décider d'une modernisation*

IEC 62808, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Conception et qualification des appareils d'isolement*

IEC 63046, *Nuclear power plants – Electrical systems – General requirements* (disponible en anglais seulement)[1]

Normes de sûreté de l'AIEA N° SSR-2/1:2016, *Sûreté des centrales nucléaires: Conception*

IAEA Safety Guide SSG-30, *Safety classification of structures, systems and components in Nuclear Power Plants* (disponible en anglais seulement)

IAEA Safety Guide SSG-34, *Design of electrical power systems for Nuclear Power Plants* (disponible en anglais seulement)

IAEA Safety Guide SSG-39:2016, *Design of instrumentation and control systems for Nuclear Power Plants* (disponible en anglais seulement)

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
circuit associé
circuit de classe de sûreté inférieure qui n'est pas physiquement séparé ou électriquement isolé du ou des circuits de classe supérieure par des distances de séparation acceptables, par des structures de classe de sûreté, des barrières ou des appareils d'isolement électrique, mais qui satisfait aux critères de sûreté approprié. Les circuits comprennent les câblages d'interconnexion et les charges connectées

3.2
barrière
dispositif ou structure interposé entre deux équipements ou structures importants pour la sûreté redondants ou entre des équipements ou des structures importants pour la sûreté et une source potentielle d'endommagement pour limiter à un niveau acceptable les dommages sur le système d'I&C important pour la sûreté

Note 1 à l'article: La définition suivante du terme existe dans le Glossaire de sûreté de l'AIEA édition 2016: "Obstacle physique qui empêche ou entrave le passage de personnes, radionucléides ou certains autres phénomènes (le feu par exemple), ou protège contre les rayonnements." La définition de l'AIEA est plus générale et cohérente avec la définition donnée dans le présent document.

[1] À publier.

3.3
chemin de câble
chemin physique sur l'installation, dans lequel de nombreux câbles peuvent être installés, traversant un local ou dans une goulotte dans un bâtiment de l'installation, ou dans une goulotte métallique ou sur une trémie ou dans une gaine ou une conduite en-dessous ou un pont au-dessus d'une route

3.4
défaillance de cause commune
DCC
défaillance de plusieurs structures, systèmes ou composants due à un événement ou à une cause spécifique unique

EXEMPLE: Par exemple, un événement ou une cause spécifique commune (qui peut correspondre à des défaillances de différents types) pourrait être un défaut de conception, un défaut de fabrication, des erreurs de maintenance ou d'exploitation, un phénomène naturel, un événement d'origine humaine, saturation de signal, ou des effets en cascade imprévus suite à des fonctionnements ou à des défaillances se produisant sur l'installation ou des changements au niveau des conditions d'ambiance.

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.5
défense en profondeur
mise en place hiérarchisée de différents niveaux d'équipements et de procédures variés pour prévenir la multiplication des incidents de fonctionnement prévus et maintenir l'efficacité des barrières physiques placées entre une source de rayonnements ou des matières radioactives et les travailleurs, les personnes du public ou l'environnement, dans différentes conditions de fonctionnement et, pour certaines barrières, dans des conditions accidentelles

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.6
conditions hors dimensionnement
conditions accidentelles hypothétiques qui ne sont pas prises en compte dans les accidents de dimensionnement mais qui le sont dans le processus de conception de l'installation conformément aux méthodes de type «meilleure estimation», et dans lesquelles les rejets de matières radioactives sont maintenus dans des limites acceptables. Les conditions hors dimensionnement comprennent les conditions correspondant aux événements sans dégradation significative du combustible et les conditions avec fusion du cœur

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.7
distance <de séparation>
installation du composant à protéger suffisamment loin d'un autre de façon à assurer qu'ils ne peuvent être endommagés en même temps par un événement considéré

3.8
diversité
présence de plusieurs systèmes ou composants redondants pour l'accomplissement d'une fonction déterminée, lorsque ces différents systèmes ou composants possèdent des attributs différents afin de réduire le risque de défaillance de cause commune, y compris de défaillance de mode commun

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.9
division
ensemble de composants, y compris leurs interconnexions, qui forment une redondance d'un système redondant ou d'un groupe de sûreté. Des divisions peuvent comprendre des canaux multiples

Note 1 à l'article: Dans le cadre ce document, la «division» comprend un système donné ou un ensemble de composants qui permet l'établissement, le maintien de l'indépendance physique, électrique et fonctionnel par rapport à d'autres ensembles de composants redondants.

[SOURCE: IAEA SSG-39, 2016]

3.10
isolement électrique
l'isolement électrique est utilisé pour empêcher les défaillances électriques d'un système d'affecter des systèmes connectés. L'isolement électrique limite ou empêche les interactions dommageables entre équipements et composants conséquences de facteurs tels que les interférences électromagnétiques, les piques électrostatiques, les courts-circuits, les ouvertures de circuits, les mises à la terre ou l'application de la tension maximale crédible (en CC ou en CA)

[SOURCE: IAEA SSG-34 et SSG-39, 2016]

3.11
compatibilité électromagnétique
CEM
aptitude d'un appareil ou d'un système à fonctionner dans son environnement électromagnétique de façon satisfaisante et sans produire lui-même des perturbations électromagnétiques intolérables pour tout ce qui se trouve dans cet environnement

[SOURCE: IEC 60050-161:1990, 161-01-07]

3.12
brouillage électromagnétique
trouble apporté au fonctionnement d'un appareil, d'une voie de transmission ou d'un système par une perturbation électromagnétique

[SOURCE: IEC 60050-161:1990, 161-01-06]

3.13
indépendance
condition qui existe lorsque la réalisation avec succès de fonctions nécessaires d'un système ne dépend d'aucun comportement, y compris les défaillances et le fonctionnement normal, d'un autre système, ou d'aucun autre signal, ou donnée ou information provenant d'un autre système

Note 1 à l'article La définition suivante pour "système indépendant" se trouve dans le glossaire de sûreté de l'AIEA, édition 2016: "Équipement qui possède les deux caractéristiques suivantes: a) La capacité d'exécuter la fonction demandée n'est pas affectée par le fonctionnement ou la défaillance d'un autre équipement; b) La capacité d'exécuter la fonction demandée n'est pas affectée par les effets de l'événement initiateur postulé pour lequel il doit fonctionner". Cette définition AIEA est limitée aux équipements, mais est cohérente avec la présente définition fournie dans ce document.

3.14
appareil d'isolement
dispositif d'un circuit qui empêche que les dysfonctionnements dans une partie du circuit aient une influence non acceptable sur les autres parties du circuit ou sur d'autres circuits

[SOURCE: IEC 62808:2015, 3.4]

3.15
séparation physique
séparation par la géométrie (distance, orientation, etc.), par des barrières appropriées ou par ces deux moyens à la fois

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.16
événement initiateur postulé
EIP
événement postulé dont on détermine au stade de la conception qu'il peut entraîner des incidents de fonctionnement prévus ou des conditions accidentelles

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.17
redondance
mise en place de structures, systèmes ou composants (identiques ou différents) supplémentaires, afin qu'une structure, qu'un système ou qu'un composant quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.18
groupe de sûreté
ensemble d'équipements prévus pour accomplir toutes les actions requises si un événement initiateur postulé particulier se produit afin que les limites spécifiées dans la base de conception pour les incidents de fonctionnement prévus et les accidents de dimensionnement ne soient pas dépassées

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

3.19
système de sûreté
système important pour la sûreté destiné à garantir la mise à l'arrêt sûre du réacteur ou l'évacuation de la chaleur résiduelle du cœur, ou à limiter les conséquences des incidents de fonctionnement prévus et des accidents de dimensionnement

[SOURCE: Glossaire de sûreté de l'AIEA, Edition 2016]

3.20
séparation
ensemble de dispositions qui minimise l'influence d'une entité sur une autre entité pour améliorer l'indépendance des entités

3.21
séparation structurelle
installation des composants séparés dans différents bâtiments ou locaux ou installation de structures protectrices entre les composants situés dans une même pièce, de telle façon qu'ils ne puissent pas être endommagés simultanément par une menace considérée

3.22
structures, systèmes et composants
SSC
expression générale englobant tous les éléments, à l'exception des facteurs humains, d'une installation ou activité qui contribuent à la protection et à la sûreté

[SOURCE: Glossaire de sûreté de l'AIEA, Édition 2016]

4 Termes abrégés

CA	courant alternatif
DCC	défaillance de cause commune
CC	courant continu
DEC	design extension condition (conditions hors dimensionnement)
DiD	defence in depth (défense en profondeur)
CEM	compatibilité électromagnétique
IME	brouillage électromagnétique
HVAC	heating, ventilation and air-conditioning (chauffage, ventilation et air conditionné)
I&C	instrumentation et contrôle-commande
AIEA	Agence Internationale de l'Energie Atomique
IEC	International Electrotechnical Commission (Commission électrotechnique internationale)
BT	basse tension (<1 000 V)
MT	moyenne tension
NC	non classé
CNP	centrale nucléaire de puissance
EIP	événement initiateur postulé
SSC	structures, systèmes et composants
VDU	Unité d'affichage

5 Principes et exigences relatifs à la séparation

5.1 Principes

5.1.1 Généralités

Conformément à la Prescription 21 du SSR-2/1 de l'AIEA, toute interférence entre les systèmes de sûreté ou entre les éléments redondants d'un système doit être exclue grâce à des moyens de séparation, tels que:

- la séparation physique;
- l'isolement électrique;
- l'indépendance fonctionnelle;
- l'indépendance en matière de communication.

Une combinaison de plusieurs de ces mesures doit être mise en œuvre afin d'atteindre le degré exigé de séparation correspondant aux événements dangereux (menaces) potentiels pour l'indépendance.

Notons, comme indiqué dans l'Article 1, l'indépendance fonctionnelle et l'indépendance en matière de communication ne relèvent pas du domaine d'application du présent document, y compris les menaces à prendre en considération qu'il convient d'identifier par le biais du programme de cybersécurité d'I&C. Pour plus de détails, voir le SSG-39 de l'AIEA, l'IEC 61500, et l'IEC 61513:2011,5.4.2.4 et 5.4.3. Bien que l'indépendance fonctionnelle ne relève pas du domaine d'application du présent document, les mesures déjà prises afin de la traiter doivent être prises en considération lors de l'évaluation du besoin de mesures supplémentaires de séparation afin de satisfaire aux exigences du présent document.

Des informations plus détaillées concernant l'indépendance fonctionnelle, l'indépendance des systèmes de contrôle-commande et l'indépendance en matière de communication sont fournies dans l'Annexe D.

La séparation de la classe de sûreté 1 des autres classes, telle qu'utilisée dans le présent document, n'est qu'un exemple de l'application des exigences du présent document.

5.1.2 Raisonnement et limites de la séparation

La séparation est le moyen principal de prévention contre:

a) la propagation de défaillances de système à système;

b) la propagation de défaillances entre les parties redondantes à l'intérieur des systèmes de sûreté;

c) les défaillances de cause commune dues aux événements dangereux internes et à certains événements dangereux externes;

d) la propagation de défaillances entre différents niveaux de DiD, lorsque cela est exigé par les principes de sûreté du projet ou des normes nationales dans le domaine nucléaire.

Les types possibles d'événements initiateurs de défaillances doivent être pris en considération (c'est-à-dire, identifiés, documentés et justifiés). Des dispositions appropriées doivent être prises dans les systèmes d'I&C et électriques importants pour la sûreté pour limiter les effets possibles de ces événements à un niveau acceptable. Il convient de prendre en considération les effets des combinaisons d'événements de défaillances.

Les défaillances et les événements dangereux à prendre en considération lors de l'élaboration des principes de séparation doivent être définis individuellement dans chaque projet. Les événements dangereux à prendre en considération sont décrits en 6.2. Les erreurs de conception et les défaillances d'I&C et électriques sont décrites dans l'Annexe C.

Les dépendances entre les systèmes d'I&C et électriques peuvent survenir sur des interfaces physiques (par exemple, alimentation électrique, échange de signaux), le schéma de configuration d'une salle ou entre des bâtiments, les systèmes support (par exemple, HVAC) ou la propagation des défaillances (par exemple, incendie, accident d'avion).

Au cours de la conception architecturale d'I&C et électrique, les contraintes imposées par la conception des centrales conformément à l'IEC 61513 et à l'IEC 63046 doivent être identifiées. En fonction des résultats, des mesures de conception appropriées doivent être spécifiées.

Le principe de séparation physique par le biais d'une structure ou d'une distance est représenté à la Figure 1.

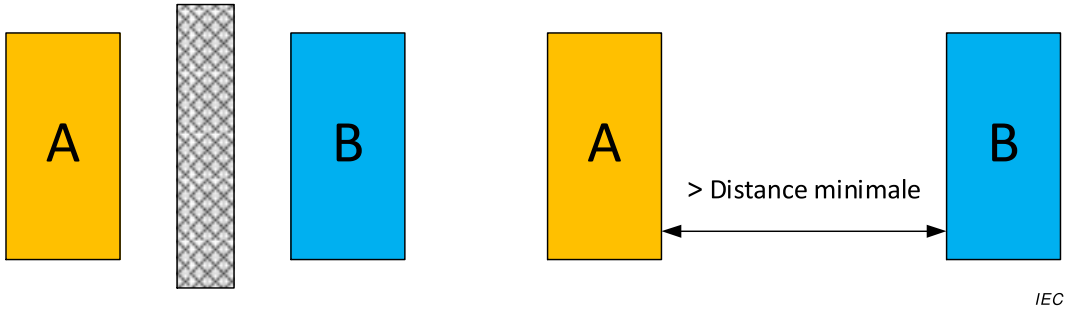


Figure 1 – Séparation physique par structure ou par distance

Le principe de séparation par isolement électrique est représenté à la Figure 2.

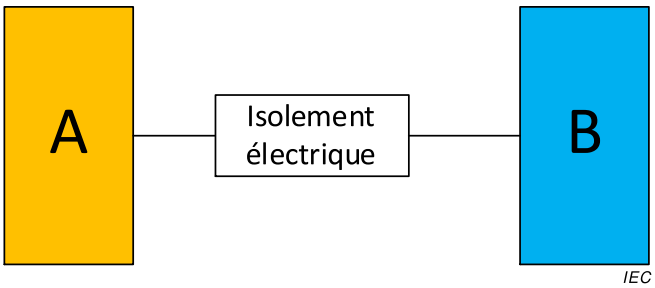


Figure 2 – Séparation par isolement électrique

NOTE Les défaillances de cause commune dues liées aux évènements dangereux peuvent survenir, ainsi que des évènements dangereux.

5.1.3 Principes et exigences de sûreté des centrales

Les principes généraux concernant la séparation sont principalement influencés par les exigences particulières relatives aux installations nucléaires et aux exigences générales. Ces principes sont les suivants:

- exigences d'indépendance;
- analyses des événements dangereux et règles de protection (y compris les incendies);
- règles déterministes de sûreté;
- propagation de défauts électriques;
- exigences provenant de règles et de normes industrielles non relatives à l'énergie nucléaire (par exemple, chemins d'évacuation et contraintes de disposition);
- exigences relatives à la CEM/au brouillage électromagnétique;
- exigences relatives aux distances de tirage des câbles dues à la dissipation de chaleur.

Les exigences particulières relatives aux installations nucléaires et à certains aspects de la propagation de défauts électriques sont principalement traitées dans le présent document; les autres exigences sont mentionnées afin de couvrir le sujet dans son ensemble.

Les principes de séparation et les moyens choisis pour les respecter doivent être décrits dans un document dédié au projet (concept de séparation). Une activité de vérification doit être effectuée afin de garantir que les exigences de séparation ont été respectées (voir l'Article 9).

5.2 Exigences relatives à la séparation des classes de sûreté

L'IEC 61226 définit comment les fonctions de sûreté sont catégorisées et comment les SSC sont classés selon leur importance pour la sûreté. Elle exige également une séparation physique assurant une protection contre la propagation de défaillances dues à des effets physiques et contre la mise en péril de systèmes redondants de manière simultanée.

Les principes suivants doivent être appliqués comme base de conception des systèmes d'I&C et électriques qui constituent des systèmes importants pour la sûreté et/ou y contribuent ou les supportent afin de maintenir l'indépendance des systèmes redondants et entre différents systèmes, et afin d'assurer l'efficacité de la redondance et de la diversité (prévues pour atteindre un haut niveau de fiabilité des systèmes importants pour la sûreté). Les critères de groupement et de séparation entre les différentes classes de sûreté doivent être définis au début du projet.

– Les systèmes de classe de sûreté 1 doivent être protégés contre les effets indirects provoqués par des pannes et des actions normales dans:
  a) les parties redondantes de ces systèmes;
  b) les systèmes de classe inférieure;

c) dans certains cas, entre différents systèmes de classe de sûreté 1 lorsque l'indépendance est exigée.

Les pannes prises en considération doivent comprendre les pannes internes aux systèmes d'I&C ou électriques ainsi que celles qui se produisent par suite d'événements externes aux systèmes d'I&C ou électriques.

– Les systèmes de classe de sûreté 2 doivent être protégés contre les effets indirects provoqués par des pannes et des actions normales dans:

d) les parties redondantes de ces systèmes; et

e) les systèmes de classe inférieure.

Les pannes prises en considération doivent comprendre les pannes internes aux systèmes d'I&C ou électriques, mais peuvent ne pas comprendre celles qui se produisent par suite d'événements externes aux systèmes d'I&C ou électriques.

Lorsque les systèmes de classe de sûreté 2 sont réputés pour fournir une protection en cas d'événements dangereux spécifiques, ces systèmes doivent suivre les principes applicables à la classe de sûreté 1. Par exemple, dans certains pays, tous les systèmes exigés afin d'obtenir et de maintenir un arrêt de longue durée doivent être protégés contre les dangers d'incendie, quelle que soit leur classe.

Certains systèmes de classe de sûreté 3 peuvent nécessiter une protection contre les influences des pannes des autres systèmes. Il convient de déterminer ladite protection au cas par cas. Il convient de protéger les systèmes de classe 3 utilisés pour le contrôle-commande et la surveillance au cours d'une DEC contre les influences des pannes des autres systèmes.

Les systèmes non classés ne nécessitent pas de protection contre les influences des pannes des autres systèmes.

Pour les circuits d'alimentation électrique des composants de classe inférieure, les exigences de séparation des unités de circuits d'alimentation électrique (par exemple, l'unité du tableau de distribution) ne doivent pas être satisfaites dans les cas suivants:

1) lorsqu'une alimentation électrique de systèmes ou de composants de classe inférieure provenant d'une source d'alimentation de classe supérieure, en raison des exigences relatives à l'alimentation électrique, justifie l'utilisation de circuits d'alimentation électrique de classe supérieure.
2) lorsqu'une dépendance entre un système de classe de sûreté inférieure (par exemple, l'éclairage de secours) et un système de classe de sûreté supérieure (par exemple, le système d'alimentation de secours) justifie l'utilisation d'une alimentation provenant d'une source de classe supérieure.

Dans les cas susmentionnés, l'impact sur le système d'alimentation électrique de classe supérieure doit être justifié en tenant compte de la puissance appelée et des transitoires électriques.

5.3 Circuits associés

5.3.1 Généralités

Lorsque des fonctions sont catégorisées conformément aux exigences de l'IEC 61226 et que des systèmes sont classés conformément à des normes telles que le SSG-30 de l'AIEA, l'IEC 61513 ou l'IEC 63046, il est fréquent qu'un système ou un ensemble d'équipements donné réalise des fonctions de différentes catégories. En outre, certaines fonctions de catégorie inférieure peuvent avoir des relations étroites avec une fonction de catégorie A, par exemple la surveillance du procédé réalisée à partir des mêmes mesurages que les fonctions de sûreté. Les exigences établies précédemment dans le document indiquent généralement qu'il convient de séparer les circuits de classe de sûreté inférieure des circuits de classe de sûreté 1. Cependant, en variante, les circuits de classe de sûreté inférieure peuvent être déclarés «circuits associés», et les exigences de séparation à satisfaire sont établies par le

présent paragraphe. Les articles suivants du présent document ne tiennent compte que de la séparation ou de l'association avec la classe de sûreté 1. Ce principe peut être étendu à d'autres classes en fonction du projet.

5.3.2 Critères

Les composants et/ou les câbles qui n'appartiennent pas à la classe de sûreté 1 deviennent des circuits associés s'ils satisfont à un ou plusieurs des points suivants:

a) connexion électrique à une source d'alimentation électrique de classe de sûreté 1 sans utilisation d'un appareil d'isolement;

b) connexion électrique à une source d'alimentation électrique associée d'un système de classe de sûreté 1 sans utilisation d'un appareil d'isolement;

c) proximité par rapport aux circuits et équipements de classe de sûreté 1 sans observer les règles de séparation exigées (distance physique ou barrière);

d) proximité par rapport aux circuits et équipements associés sans observer les règles de séparation exigées (distance physique ou barrière);

e) partage de signaux associés ou de classe de sûreté 1 sans utilisation d'un appareil d'isolement.

Les circuits associés doivent être conformes à l'une des exigences suivantes:

f) ils doivent être identifiés de façon unique en tant que tels ou en classe de sûreté 1 et ils doivent le rester (traçabilité jusqu'à la division associée de classe de sûreté 1), ou bien observer les mêmes règles de séparation physique que les circuits de classe de sûreté 1 auxquels ils sont associés. Ils doivent répondre aux exigences imposées aux circuits de classe de sûreté 1;

g) ils doivent être en conformité avec le point f) ci-dessus concernant les systèmes de classe de sûreté 1 et inclure un appareil d'isolement. Au-delà de l'appareil d'isolement, un tel circuit n'appartient pas à la classe de sûreté 1 tant qu'il n'est pas de nouveau associé à un système de classe de sûreté 1;

h) ils doivent être analysés ou soumis à l'essai pour démontrer qu'ils ne peuvent dégrader les circuits de classe de sûreté 1 au-delà d'un certain niveau acceptable.

Les circuits associés et les appareils d'isolement doivent être qualifiés de façon adéquate. Cette qualification doit indiquer que les circuits de classe supérieure se comportent correctement lorsque le circuit associé ou l'appareil d'isolement et ses câbles sont en présence de conditions électriques pour lesquelles il convient que le circuit de classe supérieure fonctionne correctement. Lorsqu'un circuit associé est connecté à un appareil/système n'appartenant pas à la classe de sûreté 1 sans isolation, cet appareil ou système doit aussi être qualifié de façon adéquate. Il n'est pas nécessaire de qualifier les circuits associés en fonction des performances de leurs fonctions, car leurs fonctions n'appartiennent pas à la catégorie A/leurs composants n'appartiennent pas à la classe de sûreté 1. Les appareils d'isolement pour les circuits d'I&C doivent être conformes à l'IEC 62808.

L'application du concept de circuit associé à grande échelle peut amener à combiner de nombreux circuits de différentes classes de sûreté dans la mesure où les principes généraux de sûreté pour la séparation physique sont respectés. Par exemple, il n'est pas nécessaire de séparer le câblage de différentes classes de sûreté pour chacune de celles-ci dans un groupe de sûreté si les fonctions de sûreté de catégorie supérieure peuvent être réalisées par un groupe de sûreté redondant séparé du groupe de sûreté qui contient les circuits associés.

Il convient que la séparation à l'intérieur des armoires électriques ou d'I&C ne soit pas nécessaire lorsque les composants appartenant aux circuits de classe inférieure sont qualifiés selon les règles de qualification des circuits de classe supérieure.

5.4 Problème de la séparation dans les installations existantes

5.4.1 Généralités

La séparation des systèmes d'I&C et électriques importants pour la sûreté dans les centrales nucléaires de puissance existantes est souvent incomplète car les SSC n'ayant initialement pas de classe de sûreté assignée peuvent nécessiter d'être classés comme étant importants pour la sûreté et car les normes de conception ont changé entre-temps. Lors de l'amélioration de centrales existantes, il convient de justifier les conséquences éventuelles résultant du non-respect du présent document pour des raisons pratiques par rapport à la sûreté supplémentaire obtenue grâce à l'amélioration dans son ensemble.

5.4.2 Critères

Les problèmes de séparation doivent être traités de manière particulière dans la stratégie de mise en œuvre des améliorations de centrales. Les problèmes qui doivent être pris en compte comprennent:

– la séparation dans les configurations intermédiaires lorsque de nouveaux systèmes d'I&C et/ou électriques sont installés en plusieurs étapes;
– l'identification de sous-systèmes qui peuvent être séparés sans interface intermédiaire;
– la pertinence de la séparation existante des nouvelles technologies d'I&C et/ou électriques (principalement concernant le caractère sensible des systèmes numériques d'I&C au brouillage électromagnétique, semiconducteurs de puissance, les exigences particulières concernant la température ou la susceptibilité aux rayonnements);
– les limitations liées au câblage et l'évaluation des besoins propres aux nouvelles technologies pour des chemins de câbles spéciaux, par exemple pour fibres optiques ou pour bus, et les exigences de séparation.

Des préconisations sur le choix de l'amélioration et de la modernisation d'I&C peuvent être consultées dans l'IEC 62096.

6 Base de conception de la séparation

6.1 Entrées de conception

L'exigence à prendre en compte pour la séparation, comme indiqué ci-dessous, doit être résumée dans un document de projet. Il convient que ledit document de projet comporte les exigences de séparation induites par:

- des contraintes de conception relatives à la séparation par division et au concept de défense en profondeur provenant de la conception globale de la centrale;
- la prise en considération d'événements dangereux externes et internes (y compris les incendies) et la combinaison d'événements dangereux;
- le plan de CEM;
- les défauts électriques;
- les autres exigences techniques.

Noter qu'il convient de prendre également en considération les exigences induites par des conditions particulières de fonctionnement, telles que la mise en service ou la maintenance et les réparations.

- les événements dangereux qui ont dû être atténués par zone;
- la distance suffisante pour la protection contre chaque événement dangereux ou condition ambiante;
- les caractéristiques des barrières par événement dangereux;

- l'exigence de séparation entre les classes de sûreté ou les niveaux de défense en profondeur.

Les types de défauts électriques ainsi que leurs limites doivent également être pris en considération dans un document de projet.

6.2 Conditions environnementales et événements dangereux

6.2.1 Généralités

Les équipements de systèmes d'I&C et électriques doivent être conçus, spécifiés, qualifiés et installés de manière à assurer leurs capacités fonctionnelles dans les conditions environnementales et événements dangereux prévus.

6.2.2 Conditions environnementales

La variation des conditions environnementales, telle que les rayonnements, la température, la pression et l'humidité en fonctionnement normal et en conditions accidentelles, doit être prise en compte.

6.2.3 Événements dangereux externes

La construction d'une CNP comprend plusieurs niveaux de défense permettant de résister aux événements dangereux externes tels que les accidents d'avion, les ouragans, les tremblements de terre ou les inondations. Ces lignes de défense structurelles assurent les conditions préalables permettant aux systèmes d'I&C et électriques de gérer les états de fonctionnement et les conditions accidentelles.

Ces événements dangereux externes peuvent survenir sans l'influence des exigences de séparation, comme c'est le cas pour les tremblements de terre, ou avec l'influence éventuelle des exigences de séparation, comme c'est le cas pour les accidents d'avion.

Les événements dangereux externes d'origine naturelle peuvent être d'ordre:

- météorologique;
- hydrologique;
- géologique;
- sismique.

Les événements dangereux externes d'origine humaine peuvent être:

- les industries proches;
- les voies de transport (aériennes, maritimes et fluviales ou terrestres).

Les événements dangereux externes d'origine humaine et naturelle ayant été identifiés lors du processus d'évaluation du site doivent être pris en considération.

Les résultats de l'analyse des événements dangereux externes doivent être pris en considération par le concept de séparation retenu pour le projet.

6.2.4 Événements dangereux internes

Les événements dangereux internes ont une influence importante sur les exigences de séparation.

Pour la conception de l'architecture des systèmes d'I&C et électriques, l'impact des événements dangereux internes doit être pris en considération par des moyens de séparation physique en différentes divisions en combinaison avec l'isolement électrique.

Les événements dangereux internes possibles comprennent:

- les incendies;
- les explosions;
- les inondations;
- l'émission de projectiles;
- l'effondrement des structures et la chute d'objets;
- les ruptures de tuyauterie vapeur vive causant l'effet de fouet des tuyaux;
- le rejet de fluide provenant des systèmes défaillants.

Les résultats de l'analyse des événements dangereux internes doivent être pris en considération dans le concept de séparation.

Les conséquences des évènements dangereux externes ou autres évènements doivent être pris en compte pour identifier les évènements dangereux internes.

6.2.5 Protection contre les incendies

On doit satisfaire les exigences de protection contre les incendies déduites des normes applicables.

Il convient d'utiliser des câbles retardateurs de flammes. La série IEC 60332 fournit des préconisations pour les essais sur des câbles électriques afin de démontrer leurs propriétés retardatrices de flammes.

Les traversées de chemins de câbles et de buses de coupe-feux (verticaux et horizontaux) doivent être rendues étanches par des matériaux non combustibles afin d'assurer une protection au moins équivalente à la protection exigée des coupe-feux.

Des matériaux non combustibles doivent être utilisés pour les chemins de câbles et les buses.

NOTE La séparation des systèmes d'I&C et électriques importants pour la sûreté ainsi que les mesures de protection contre les incendies dans les centrales nucléaires de puissance existantes sont le reflet de la conception d'origine. Le classement de sûreté des SSC, les normes de conception ainsi que les exigences de protection contre les incendies, sont susceptible d'avoir évolué de manière continue vers des exigences plus strictes. Par conséquent, il est fréquent que la conception existante ne soit pas conforme aux normes modernes.

6.3 Brouillage électromagnétique/CEM

La CEM constitue un problème technique du système concernant l'équilibre entre l'immunité et les émissions aux interfaces entre les différents sous-systèmes.

La séparation constitue une approche permettant d'assurer une protection contre le risque éventuel de DCC du brouillage électromagnétique.

Il convient d'utiliser les normes CEM internationales relatives aux environnements industriels, la série IEC 61000, ainsi que la norme dédiée aux CNP, l'IEC 62003, comme base pour la définition des exigences de CEM. Il convient de compléter ces normes, le cas échéant, afin de couvrir les environnements de CEM des composants des centrales de puissance, qui peuvent être plus contraignants.

6.4 Défaut électrique

Le système d'I&C ou électrique doit être protégé ou en mesure de tolérer l'insertion incorrecte de la tension interne d'un système et de toute tension ou tout courant externe prévisible (barrière contre les surtensions, barrière contre les courts-circuits/surintensités) et assurer l'autonomie (isolation électrique non réactive, isolation électrique) de la multiplication et de la transmission de signaux.

6.5 Exigences issues de normes techniques non nucléaires

Concernant le concept de séparation retenu pour le projet, il convient de prendre également en compte les exigences issues d'autres sujets techniques, telles que la dissipation de la chaleur des composants et des câbles (charge thermique acceptable) et les voies des chemins d'évacuation, etc.

6.6 Exigences issues de conditions particulières de fonctionnement

Les exigences issues de conditions particulières de fonctionnement, telles que la mise en service, les modifications, la maintenance et les réparations, les procédures de conception et de contrôle-commande administratif, doivent être prises en considération lors de la conception et de la construction.

7 Isolement électrique

7.1 Principes

7.1.1 Généralités

L'isolement électrique est décrit dans les guides de sûreté SSG-34 et SSG-39 de l'AIEA.

La sélection et la combinaison de mesures d'isolement électrique sont représentées à la Figure 3.

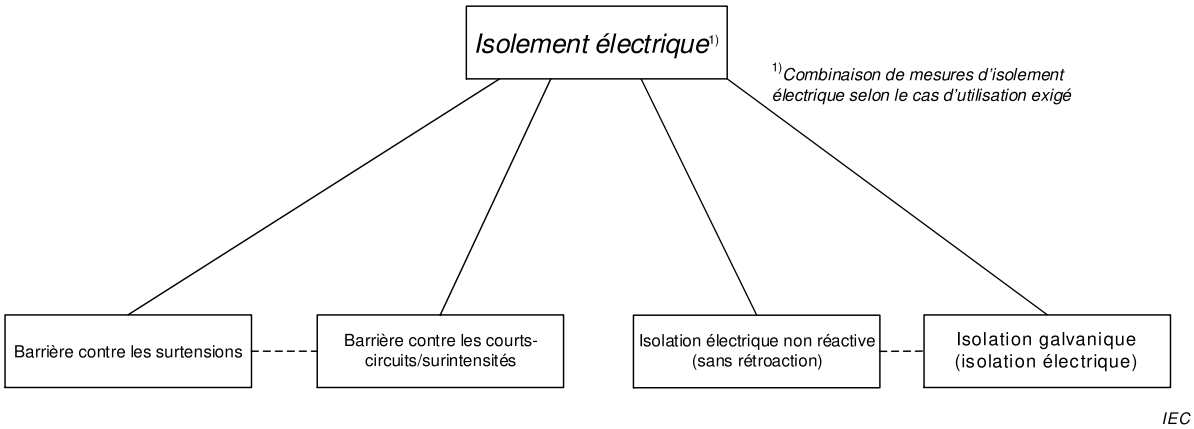


Figure 3 – Mesures d'isolement électrique et sélection des composants

Selon le cas d'utilisation exigé, une combinaison de mesures doit être spécifiée lors de la conception. L'omission d'une seule mesure peut conduire à l'inefficacité de l'isolement électrique complète.

7.1.2 Barrière contre les surtensions

Une barrière contre les surtensions sépare physiquement ou empêche la propagation de surtension ou de courant transitoire dans une direction donnée (selon le cas d'utilisation). La surtension est l'existence de tension (alternative ou continue), provenant d'une source, qui dépasse la tension de conception, entre un segment électrique et tout autre segment électrique, y compris la terre.

En général, l'alimentation de la surtension dans un système doit être prise en compte si, d'un point de vue physique, il s'agit d'un mode réaliste de défaillance.

Les tensions étrangères doivent être limitées à un degré non dangereux par la mise en œuvre d'appareils d'isolement électrique dédiés pour le système à protéger. En fonction du cas d'utilisation, une combinaison d'appareils électriques doit être identifiée afin de prendre en

compte les tensions transitoires maximales hypothétiques et le temps d'exposition pour les composants à protéger.

Les mesures en termes de barrière contre les surtensions peuvent comprendre la destruction délibérée de la totalité ou d'une partie des composants. Une destruction physique peut être initiée par la fusion, la combustion ou l'éclatement des composants. Les impacts du déclenchement de la barrière contre les surtensions sur d'autres composants de la chaîne de signaux doivent être pris en considération lors de la conception des systèmes d'I&C et électriques par la séparation physique (voir l'Article 8).

7.1.3 Protection contre les courts-circuits/surintensités

Des appareils, tels que des fusibles ou des disjoncteurs, sont utilisés pour la protection contre les courts-circuits afin de couper l'alimentation vers le défaut de court-circuit. Les surintensités sont détectées par des appareils dédiés, le cas échéant, et coupées par des appareils tels que des contacteurs ou des disjoncteurs.

L'équipement de protection du système d'alimentation de secours est généralement conçu de sorte à détecter de manière fiable les défauts ou les défaillances. Les déconnexions nécessaires sont effectuées et les fausses manœuvres des transitoires de fonctionnement sont empêchées. Les problèmes de fonctionnement, tels que les courants d'appel de crête ou les cycles successifs de démarrage de moteurs, ne doivent pas actionner les appareils de protection. En général, les caractéristiques de protection contre les surintensités doivent être sélectionnées et ajustées pour atteindre les valeurs auxquelles les courants minimaux de court-circuit sont détectés. Cependant, aucun courant transitoire provenant des procédures de fonctionnement ne doit provoquer de déconnexion.

7.1.4 Isolation électrique non réactive (sans rétroaction)

La rétroaction électrique est un effet survenant lorsqu'une source de signal électrique peut être biaisée par une défaillance dans le récepteur du signal. L'isolation sans rétroaction (ou non réactive) est une caractéristique d'interface permettant d'assurer que les défaillances du système cible ne dégradent pas le système source.

Pour un échange de signaux (ou une multiplication de signaux) non réactif, la sortie d'un composant sans rétroaction peut être soumise à des contraintes par un niveau de signal (tension système) faible ou élevé sans que cela ait d'impact sur la source du signal. Ce niveau de signal ne doit pas avoir d'impact (sans rétroaction) sur le signal d'entrée du composant de l'isolement électrique.

L'absence de rétroaction est une caractéristique d'un composant qui assure la protection suivante: Lorsqu'une source de signal électrique alimente plusieurs composants, en cas de défaillance dans l'un(e) des composants ou interfaces alimenté(e)s, ladite défaillance ne dégrade pas le signal source pour les composants restants ou la source proprement dite.

7.1.5 Isolation galvanique (isolation électrique)

En plus de la transmission de signaux sans rétroaction, des appareils d'isolement à haute impédance doivent protéger (séparer) l'échange de signaux entre les systèmes d'I&C (y compris les interfaces entre les différents systèmes d'I&C).

L'isolation électrique sert, en principe, à éviter tout flux de courant entre les circuits électriques, même en cas d'échange de puissance ou de signaux. L'isolation électrique est nécessaire afin d'échanger des informations entre les systèmes d'I&C appartenant à:

- différents niveaux de tension système (par exemple, 110 V (courant alternatif) ← → 24 V (courant continu)),
- différentes boucles de terre,

- différentes salles (constructions de bâtiments) si l'interférence électrique doit être évitée, ou
- de longues distances de parcours de câbles (en fonction de la chute de tension sur la longueur des câbles).

Les caractéristiques des mesures d'isolation électrique choisies doivent être prises en compte lors de la conception de l'architecture d'I&C et électrique. Une interface électrique isolée peut être non réactive et peut protéger contre les surtensions du côté I&C.

Généralement, dans les systèmes électriques, l'isolation galvanique est assurée par une séparation inductive (par le biais de transformateurs). Une isolation galvanique du côté électrique n'assure généralement pas une protection suffisante contre les surtensions.

7.2 Appareils d'isolement

7.2.1 Généralités

Les exigences se référant à la classe de sûreté d'un appareil d'isolement dépendent de la classe de sûreté du circuit électrique à séparer. L'appareil d'isolement doit être tel que les défaillances ou les conditions aux bornes de sortie (qui sont raccordées au système de classe inférieure) ne peuvent pas prévenir l'action de sûreté du système ou du sous-système de classe de sûreté 1 auquel l'appareil d'isolement est raccordé. Par exemple, pour l'I&C, les alarmes d'un circuit de classe de sûreté 1 peuvent être surveillées par un relais situé dans ledit circuit avec la classe de sûreté dont les contacts produisent des alarmes avec une classe de sûreté inférieure.

Les connexions temporaires des systèmes de classe de sûreté 1 sans appareil d'isolement à des fins de maintenance doivent être autorisées dans la mesure où elles raccordent ces systèmes uniquement à une redondance simple à la fois, où ils sont déconnectés après utilisation et où le système est capable de supporter une panne introduite lors d'une défaillance ou de l'utilisation de la connexion.

Les défaillances et les dysfonctionnements dans les systèmes appartenant à des classes de sûreté autres que la classe de sûreté 1 ne doivent provoquer aucune modification des performances du système, par exemple, pour les éléments relatifs à l'I&C, tels que les réponses, les dérives, l'exactitude, la sensibilité au bruit ou les autres caractéristiques des systèmes de classe de sûreté 1 pouvant compromettre la capacité du système à réaliser ses fonctions de sûreté.

7.2.2 Caractéristiques d'isolement

Les propriétés d'un appareil d'isolement doivent comprendre:

– la tolérance et l'isolation relatives au brouillage électromagnétique définies dans l'IEC 62003;
– des barrières simples entre les bornes de proximité ou adjacentes ou les groupes de contacts sur les équipements relais utilisés pour l'isolement électrique;
– la prévention de la transmission de tensions excessivement hautes ou nuisibles;
– la prévention des effets des courts-circuits;
– la prévention de la rétroaction.

Les règles générales relatives aux appareils électriques sont fournies dans l'IEC 61439-1. Si les caractéristiques d'isolement électrique des équipements d'I&C ou électriques ne sont pas suffisantes, un appareil d'isolement doit être ajouté.

La conception et la qualification des appareils d'isolement pour les systèmes d'I&C importants pour la sûreté sont décrites dans l'IEC 62808.

Concernant la conception de la protection électrique, le comportement en fonction du temps d'une défaillance possible doit également être pris en considération.

Dans ce contexte, il convient d'effectuer une évaluation de la tension maximale et du courant maximal pouvant être envisagés dans des conditions normales et de défaillance, ainsi que de leurs effets potentiels sur les équipements importants pour la sûreté lorsque ceux-ci sont appliqués aux bornes de l'appareil d'isolement du circuit de moindre importance pour la sûreté.

Il convient de prendre des précautions afin de réduire le plus possible la possibilité pour l'I&C qu'une défaillance dans un système de classe de sûreté autre que la classe de sûreté 1 ne provoque de manœuvre intempestive ou prématurée d'un système de classe de sûreté 1.

7.2.3 Priorité actionneur

Lorsque l'équipement de la centrale qui est commandé par un système de classe de sûreté 1 est également commandé par des signaux provenant d'un système de classe de sûreté inférieure, des appareils d'isolement doivent être fournis afin d'assurer la priorité des actions du système de classe de sûreté 1 sur celles du système de classe de sûreté inférieure. Les défaillances ou les actions normales du système de classe de sûreté inférieure ne doivent pas interférer avec le système de classe de sûreté 1 lorsque les conditions de la centrale exigent la réussite des actions de la classe de sûreté 1. Les appareils d'isolement prioritaires doivent être classés comme faisant partie du système de classe de sûreté 1.

Lorsque les signaux sont issus des systèmes de classe de sûreté 3 pour l'utilisation dans les systèmes n'appartenant à aucune classe de sûreté, les appareils d'isolement peuvent ne pas être exigés. Cependant, il convient de suivre des principes techniques bien établis afin d'empêcher la propagation de défauts. Lorsque les systèmes (par exemple, de classe de sûreté 2) réalisant des fonctions de catégorie B nécessitent de prendre en charge les aspects des systèmes de classe de sûreté 1 en raison des fonctions réalisées, l'isolement doit être appliqué.

Pour un système de classe 2, les défaillances et les dysfonctionnements des systèmes de classe 3 ou des systèmes n'appartenant à aucune classe de sûreté ne doivent provoquer aucune modification significative des performances du système (par exemple, le temps maximal de réponse, l'usage maximal des ressources qui doivent être respectés), de la dérive, de l'exactitude ou des autres caractéristiques des systèmes de classe de sûreté 2 pouvant compromettre la capacité du système à réaliser ses fonctions de sûreté.

Pour les systèmes d'I&C, les communications par fibres optiques constituent un moyen très efficace d'obtenir l'isolement électrique/le découplage, et il convient de les appliquer dans toute la mesure du possible.

8 Séparation physique

8.1 Principes

8.1.1 Généralités

Lorsqu'une séparation physique est exigée, la prévention de la propagation de défaillance doit être prise en considération pour les défaillances pouvant se produire:

– de manière simultanée sur plusieurs composants du système par suite d'EIP;

– entre des systèmes de même classe de sûreté;

– entre des groupes redondants de sûreté du même système d'I&C important pour la sûreté, et;

– entre des systèmes de classe de sûreté inférieure et des systèmes de classe de sûreté supérieure et, dans certains cas spécifiques, des systèmes de classe de sûreté supérieure et des systèmes de classe de sûreté inférieure.

La séparation physique est un moyen de traiter les impacts mécaniques ou environnementaux.

La séparation physique peut être obtenue par l'application d'une distance, d'une séparation structurelle ou d'une combinaison des deux, et constitue un moyen de réduire la probabilité de survenue de défaillances dépendantes (défaillances de cause commune) résultant de défaillances par suite d'EIP (tels que les incendies, les projectiles et les inondations ou les ruptures tuyauteries vapeur vive).

Le choix dépend des événements initiateurs postulés et peut varier selon l'emplacement au sein de la CNP. Cela dépend du besoin de protection contre tous les EIP pris en considération lors de la base de conception.

8.1.2 Séparation par la distance

La séparation physique n'exige pas explicitement l'installation de barrières structurelles entre deux composants, mais peut être obtenue de manière appropriée par la distance ou la séparation géographique afin de traiter les EIP sous-jacents (par exemple, l'effet direct d'un accident d'avion).

La distance mesurée est l'espace n'ayant pas de structures, d'équipements ou de matériaux s'interposant et pouvant contribuer à la propagation d'effets résultant d'événements dangereux (par exemple, des incendies, des accidents d'avion, etc.) ou pouvant désactiver les systèmes d'I&C ou électriques d'une autre manière.

8.1.3 Séparation structurelle

Dans le contexte de systèmes d'I&C et électriques, une barrière physique structurelle constitue une séparation physique entre deux zones indépendantes au moyen de mesures constructives. Ces mesures doivent empêcher le développement d'événements initiateurs postulés et d'événements dangereux internes. En fonction des EIP pertinents, la barrière structurelle peut être constituée d'un mur, comme un coupe-feu, ou d'un blindage dédié à la protection contre les conditions imposées par suite d'accidents.

8.2 Séparation des câbles et des structures supports de câbles

8.2.1 Généralités

Il convient de baser la disposition de séparation sur des essais effectués afin de déterminer les caractéristiques retardatrices de flammes (IEC 60332) de l'installation proposée des câbles en tenant compte des caractéristiques telles que l'isolation et les matériaux de la gaine, le remplissage des canalisations, les types de canalisations et les dispositions. Dans les zones dangereuses, il convient de prendre en considération le sévérité des événements dangereux, tel que l'ampleur des incendies ou des ruptures de tuyauteries, ainsi que les mesures d'atténuation, telles que les extincteurs automatiques.

En outre, la distance minimale du câble de puissance peut prendre en considération une norme industrielle telle que, par exemple, l'IEC 60364-5-52.

8.2.2 Séparation par division des câbles redondants et des structures supports de câbles

Pour les câbles redondants dans un système d'I&C ou électrique important pour la sûreté, une séparation par division doit généralement être introduite. Les points suivants s'appliquent:

– chaque groupe redondant doit comporter des chemins de câbles, des tablettes, des buses, des gaines, des gaines verticales 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 et électrique 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 tensions transitoires, etc., un degré faible de séparation physique peut être suffisant;
– concernant les événements dangereux dus à des défaillances de la centrale ou à des défaillances externes (voir 6.2), tels que l'incendie ou l'effondrement de structure, des règles de séparation physique appropriées faisant intervenir des barrières et/ou des structures de sûreté doivent être appliquées, tel que défini dans l'analyse des événements dangereux.

8.2.3 Séparation des câbles des systèmes et des structures supports de câbles de différentes classes de sûreté

La séparation des circuits classés non importants pour la sûreté de ceux classés importants pour la sûreté ou des circuits associés doit être réalisée en étant conforme aux exigences suivantes.

a) les circuits de classe de sûreté autre que la classe 1 doivent être physiquement séparés des circuits de classe de sûreté 1 et des circuits associés par une distance, un séparateur métallique ou, le cas échéant, des barrières physiques, aux exceptions près autorisées au point d), ou bien les circuits de classe de sûreté autre que la classe 1 doivent être des circuits associés; il convient d'établir les distances minimales de séparation horizontale et verticale des câbles de système de différentes classes de sûreté en respectant tous les critères définis au niveau du concept de séparation retenu pour le projet.
b) les circuits de classe de sûreté autre que la classe 1 doivent être électriquement isolés des circuits de classe de sûreté 1 et des circuits associés par l'utilisation d'appareils d'isolement, de blindage et de techniques de câblage ou d'une distance de séparation, aux exceptions près autorisées au point d), ou bien les circuits de classe de sûreté autre que la classe 1 doivent être des circuits associés.
c) les conséquences du non-respect du minimum de séparation ou de l'absence d'isolement électrique entre les circuits de classe de sûreté autre que la classe 1 et les circuits de classe de sûreté 1 ou les circuits associés doivent être analysées afin de démontrer que les circuits de classe de sûreté 1 ne sont pas endommagés au-delà d'un niveau acceptable ou bien les circuits de classe de sûreté autre que la classe 1 doivent être des circuits associés.
d) il n'est pas exigé d'établir une séparation physique ou une isolation électrique entre l'instrumentation de signalisation et les circuits de commande de classe de sûreté autre que la classe 1 et les circuits associés étant donné que, premièrement, les circuits de classe de sûreté autre que la classe 1 ne cheminent pas avec des câbles associés d'une division redondante et que, deuxièmement, les circuits de classe de sûreté autre que la classe 1 sont analysés afin de démontrer que les circuits de classe de sûreté 1 ne sont pas endommagés au-delà d'un niveau acceptable. Dans le cadre de l'analyse, une attention particulière doit être portée à l'énergie potentielle et à l'identification des circuits impliqués.
e) il n'est pas exigé d'établir une séparation physique entre les circuits à fibre optique de classe de sûreté autre que la classe 1 et les circuits de classe de sûreté 1 ou les circuits associés. L'isolement électrique est une caractéristique intrinsèque des circuits à fibre optique. Étant donné que les circuits à fibre optique n'ont pas suffisamment de potentiel pour endommager les circuits de classe de sûreté 1, ils peuvent être considérés comme des circuits associés de classe de sûreté 1.

Remarque: Les critères de séparation interne des armoires doivent être déduits des contraintes physiques, telles que les exigences relatives aux niveaux de tension/à la CEM. La séparation physique interne des armoires selon différentes classes de sûreté n'est pas exigée.

8.2.4 Séparation entre les câbles de signalisation et les câbles de puissance

Il convient que les câbles porteurs de signaux analogiques et autres courants faibles soient séparés des câbles de puissance. Les exceptions doivent être justifiées. Suivant la technologie employée, les câbles de contrôle-commande de l'appareillage de connexion peuvent être classés dans une catégorie élevée ou basse, et ils doivent satisfaire aux exigences correspondantes. Les câbles à fibre optique peuvent cheminer avec les câbles de puissance si leur protection mécanique est assurée.

La séparation entre les câbles de signalisation et les câbles de puissance dépend de la CEM et de l'isolation de la tension. La séparation entre les câbles de signalisation et les câbles de puissance doit être suffisante par rapport à ces deux aspects.

8.2.5 Distances de séparation réduites

Des distances de séparation réduites par rapport à celles définies dans le concept de câblage au début d'un projet peuvent être établies en analysant l'installation proposée de câbles.

8.2.6 Circuits associés

Concernant les circuits en câble associés, les exigences de 5.3 doivent être appliquées.

8.2.7 Séparation entre le câblage et les canalisations ou la tuyauterie

Il convient de ne pas placer le câblage de sorte qu'il soit contigu à, ou contenu dans, des tablettes, des goulottes ou des buses avec des tuyaux ou des canalisations véhiculant des fluides sous pression et/ou température tels que l'huile, la vapeur, l'eau, du métal sous forme liquide ou d'autres fluides qui pourraient endommager les câbles en cas de fuite ou d'éclatement, sauf aux endroits justifiés, par exemple dans lesquels la proximité de câblage de capteur ou d'actionneur rend cela inévitable du fait de la nécessité de connecter le capteur ou l'actionneur au procédé.

8.2.8 Généralités sur le cheminement des câbles

Il convient, dans la mesure du possible, que le câblage des systèmes importants pour la sûreté chemine dans des zones ne présentant pas de danger, de façon à préserver son intégrité.

8.2.9 Identification

Les câbles d'I&C et électriques doivent être identifiés et porter un marquage selon le code d'identification applicable.

Afin de faciliter la mise en service et les modifications et afin de réduire les probabilités d'apparition d'erreurs, les câbles et les chemins de câbles qui comportent des câbles de systèmes importants pour la sûreté doivent porter un marquage permettant d'identifier leur groupe redondant de sûreté et leur classe de sûreté. Il convient que ce marquage soit situé:

a) aux extrémités des câbles et au niveau des traversées des coupe-feux;

b) sur les tablettes, les gaines et les buses.

8.3 Séparation des composants à l'intérieur du système d'I&C et électrique important pour la sûreté

8.3.1 Séparation par division des composants redondants à l'intérieur du système d'I&C et électrique important pour la sûreté

En général, pour les composants redondants au sein d'un système d'I&C ou électrique important pour la sûreté, une séparation par division doit être introduite.

Dans la plupart des cas, la séparation par division s'effectue par le biais de barrières physiques. Si la séparation par le biais de barrières physiques n'est pas possible, il convient également de mettre en œuvre une séparation établie par une distance et/ou des mesures de protection supplémentaires contre les incendies.

Il convient d'établir les distances minimales de séparation horizontale et verticale dans un document de projet séparé, par exemple un concept de disposition, selon les règles énoncées dans l'Article 5 et l'Article 6.

Lorsque la distance minimale de séparation ne peut pas être maintenue, des règles spécifiques doivent être définies. Ces règles peuvent comprendre l'installation de barrières spécifiques ou la justification des raisons pour lesquelles des distances inférieures doivent être employées.

Concernant les événements dangereux dus à des défaillances de la centrale ou à des défaillances externes, tels que l'incendie ou l'effondrement de structure, des règles de séparation physique appropriées faisant intervenir des barrières et/ou des structures de sûreté doivent être appliquées.

8.3.2 Séparation des composants de différentes classes de sûreté

Il convient d'établir la séparation entre les composants non importants pour la sûreté et les composants importants pour la sûreté ou les composants associés conformément aux exigences suivantes.

a) les composants de classe de sûreté autre que la classe 1 doivent généralement être physiquement séparés des composants de classe de sûreté 1 et des circuits associés si la qualification des composants de classe de sûreté autre que la classe 1 est inférieure à la qualification des composants de classe de sûreté 1. Cette séparation doit être effectuée par une distance ou, le cas échéant, des barrières physiques.
b) les circuits de classe de sûreté autre que la classe 1 doivent être électriquement isolés des circuits de classe de sûreté 1 et des circuits associés par l'utilisation d'appareils d'isolement, de blindage et de techniques de câblage ou d'une distance de séparation, ou les circuits de classe de sûreté autre que la classe 1 doivent être des circuits associés.
c) l'absence d'isolement électrique entre les circuits de classe de sûreté autre que la classe 1 et les circuits de classe de sûreté 1 ou les circuits associés doit être analysée afin de démontrer que les circuits de classe de sûreté 1 ne sont pas endommagés au-delà d'un niveau acceptable ou bien les circuits de classe de sûreté autre que la classe 1 doivent être des circuits associés.

Lorsqu'un circuit associé est alimenté, le bloc complet d'alimentation dudit circuit associé est considéré comme étant de classe de sûreté supérieure si le composant, par exemple, le tableau de distribution, est de classe de sûreté supérieure. Le bloc d'alimentation doit, dans ce cas, satisfaire à toutes les exigences de sûreté et de qualification relatives au composant de classe de sûreté supérieure.

La séparation entre les circuits associés (électriques ou de signalisation) et les circuits appartenant à une classe de sécurité dans les composants ou les équipements, par exemple, les tableaux de distribution, n'est pas exigée par le présent document.

8.3.3 Installation d'équipements de différents niveaux de tension

Les équipements de différents niveaux de tension doivent être installés conformément aux exigences industrielles, par exemple, la séparation entre les tableaux de distribution de tension moyenne, les tableaux de distribution basse tension, les tableaux de distribution à courant continu et les armoires d'I&C.

À cet effet, il convient d'appliquer les exigences relatives au plan de CEM et les exigences normales de normes industrielles.

Des exceptions à cette règle peuvent être possibles si:

- elles sont justifiées par des motifs techniques (par exemple, énergie faible);
- aucune norme de produit n'est disponible. Dans ce cas, la norme fondamentale applicable doit être appliquée de manière raisonnable.

8.3.4 Distances de séparation réduites

Des distances de séparation réduites par rapport à celles spécifiées dans le document de projet séparé exigé dans l'Article 5 peuvent être établies en analysant les installations proposées. Il convient de baser cette analyse sur des essais et des calculs. Pour des distances de séparation moindres dans les zones dangereuses, il convient de prendre en considération la sévérité des événements dangereux (tel que l'ampleur des incendies ou des ruptures de tuyauteries) ainsi que les mesures d'atténuation.

8.3.5 Circuits associés

Concernant les circuits en câble associés, les exigences de 5.3 doivent être appliquées.

8.3.6 Séparation entre les composants et les sources d'événements dangereux

Il convient de ne pas placer les composants d'I&C et électriques dans des zones dans lesquelles des événements dangereux peuvent survenir en raison de tuyaux ou de canalisations véhiculant des fluides sous pression et/ou température tels que l'huile, la vapeur, l'eau, du métal sous forme liquide ou d'autres fluides qui pourraient endommager les composants en cas de fuite ou d'éclatement. Il peut y avoir des cas dans lesquels la proximité par rapport à la tuyauterie industrielle ou à l'I&C ou aux alimentations électriques liés les besoins du procédé est inévitable. Dans ce cas, des mesures de protection doivent être prévues.

8.4 Armoires de commande, pupitres, panneaux et câbles attachés

Bien que la probabilité d'incendie en salle de commande et dans les zones proches soit faible, les conséquences pourraient être graves. Le maintien de la séparation physique ou des barrières dans la zone de la salle de commande, ses panneaux et ses pupitres, est très problématique du fait du rassemblement des câbles en ces endroits. Ainsi, les centrales sont conçues de façon que l'incendie soit improbable dans la zone de la salle de commande, et aussi de façon que tout incendie pouvant avoir lieu soit circonscrit, se propage lentement et n'entraîne aucune perte de moyens de commande de sûreté avant que d'autres moyens de commande puissent être rendus opérationnels. Les méthodes à employer pour cela peuvent être complexes et fortement influer sur la conception du câblage de l'installation et la disposition des panneaux de commande, qui sont régies par des considérations liées aux facteurs humains.

Il convient que la disposition des panneaux de commande prenne en compte des considérations liées aux facteurs humains (voir l'IEC 60964), telles que le regroupement approprié des informations et des commandes de sûreté redondantes de la centrale, afin de réduire le plus possible les possibilités d'erreurs humaines. La fréquence attendue des erreurs humaines peut être haute, tandis que celle d'un incendie en salle de commande sera basse. Cette exigence peut donc être contradictoire avec les exigences relatives à la séparation par espacement, barrière ou appareil d'isolement énoncées ailleurs dans le présent document, puisque la prévalence des exigences liées aux facteurs humains concernant la disposition de la façade des pupitres par rapport à la commodité ou à la simplicité liées à la conception du câblage et de ses branchements peut être exigée.

Les méthodes de contrôle-commande des incendies potentiels, de leur détection ou de leur extinction doivent être identifiées et appliquées dans la salle de commande, dans ses armoires, pupitres et panneaux, et pour le câblage interne et externe de ces éléments. Les méthodes basées sur la séparation physique ou résistant à la propagation de l'incendie qui peuvent être utilisées comprennent:

– la séparation complète des commandes de sûreté de la centrale et l'indication des différents groupes de sûreté; qui est une solution préférentielle;
– l'utilisation de goulottes métalliques internes pour la connexion de la façade du panneau à des appareils de commande de sûreté redondante de la centrale;
– les dispositions concernant les détecteurs de chaleur ou les extincteurs automatiques dans les armoires de la salle de commande;
– la résistance au feu des structures des armoires et de tous les coupe-feux entre les secteurs d'armoires.

Les éléments suivants peuvent, entre autres, être pris en considération:

– du personnel est toujours présent en salle de commande; ainsi, l'incendie sera rapidement détecté et éteint;
– la salle de commande est une zone à accès contrôlé, dans laquelle l'accumulation de matériaux inflammables est évitée et dans laquelle le sabotage est improbable;
– la détection d'un incendie dans n'importe quel secteur d'armoires de salle de commande, de panneaux et de pupitres est rapide et la vitesse de propagation de l'incendie d'un secteur à un autre est suffisamment lente pour permettre l'extinction de celui-ci avant que le contrôle de la situation ne soit perdu;
– la disponibilité de commandes redondantes pour l'ensemble de la sûreté de la centrale, telle que, lorsqu'une commande individuelle de sûreté d'éléments de la centrale se trouve sur un secteur de panneau, d'autres commandes de sûreté de la centrale groupées équivalentes soient accessibles à partir d'un autre secteur séparé;
– la fréquence de départ d'un incendie dans un secteur de panneau, considérée lors de la base de conception de la centrale, est très basse du fait que l'utilisation de matériaux inflammables et de sources de chaleur dans les secteurs de panneau est contrôlée;
– la mise en place d'une salle de commande supplémentaire à partir de laquelle les actions de commande de sûreté nécessaires peuvent être initiées. Des moyens adaptés doivent être fournis afin d'isoler les conséquences des incendies dans chaque salle de commande.

Il convient de considérer, lors de la conception des systèmes d'I&C, les moyens permettant de garantir qu'un incendie ne cause pas de courts-circuits, d'ouvertures de circuit ou d'échauffements, tels que la commande de la centrale soit dégradée. Cela comprend la séparation physique des fils de puissance et de commande ou de mesure dans les différents câbles, l'application de câbles à fibre optique et d'optocoupleurs, l'utilisation de systèmes de commande multiplexés et de commandes numériques VDU.

9 Vérification

L'organisation d'un projet doit spécifier la vérification de la séparation mise en œuvre d'après le concept de séparation retenu pour le projet. Le concept de séparation retenu pour le projet doit être vérifié par rapport à la conformité aux exigences mentionnées dans le présent document et dans les normes supplémentaires applicables, la norme particulière nationale en matière de sûreté nucléaire et les exigences spécifiques au projet.

Deux thèmes principaux doivent être pris en considération:

- l'isolement électrique;
- la séparation physique.

Concernant l'isolement électrique:

La vérification de la conception doit porter sur:

– la protection contre les surtensions (étude sur la coordination de l'isolement),conformément, par exemple, à l'IEC 60071;

- la protection contre les courts-circuits/surintensités,conformément, par exemple, à l'IEC 60909 pour le courant alternatif, et à l'IEC 61660 pour le courant continu;
- l'isolation électrique non réactive (sans rétroaction),conformément, par exemple, à l'IEC 60364-5-56;
- l'isolation galvanique,conformément, par exemple, à l'IEC 60364-4-41.

La vérification de la mise en œuvre doit être effectuée d'après un plan de vérification spécifique au projet. Il convient de compléter la vérification de la mise en œuvre concernant l'isolement électrique dans le cadre d'essais de mise en service.

Concernant la séparation physique:

Les vérifications de conception doivent porter sur la mise en œuvre des exigences suivantes:

- la séparation par division;
- l'analyse des événements dangereux;
- la protection du personnel;
- la séparation des classes de sûreté;
- la séparation des niveaux de DiD;
- les exigences techniques supplémentaires.

Il convient de compléter la vérification de la mise en œuvre concernant la séparation physique dans le cadre d'essais d'installation.

L'Annexe C énumère des erreurs possibles de conception et des cas de défaillances électriques.

Annexe A
(normative)

Relation avec les lignes directrices de l'AIEA et l'IEC 61226

A.1 Objet de la présente Annexe

La présente Annexe donne des explications des lignes directrices de l'AIEA et de l'IEC 61226 concernant la catégorisation de sûreté des fonctions d'I&C et électriques et le classement de sûreté des systèmes d'I&C et électriques ainsi que les définitions des niveaux de défense en profondeur.

A.2 Applicabilité du présent document

Les règles générales fournies dans le présent document pour la séparation des classes de sûreté peuvent s'appliquer pour la séparation selon d'autres contraintes de conception, telles que le concept de défense en profondeur.

Le présent document ne fournit pas d'exigences supplémentaires concernant la disponibilité, ni d'exigences détaillées relatives à l'élimination des interférences électriques au sein des équipements.

En outre, le présent document ne définit pas de distances de séparation. Les exigences relatives à la distance doivent faire l'objet d'une évaluation suivant les règles d'installation, les exigences de protection contre les incendies, le chauffage des câbles, les chemins d'évacuation, etc.

A.3 Lignes directrices de l'AIEA applicables au présent document

Les lignes directrices de l'AIEA qui comportent des exigences à appliquer relatives à la catégorisation de sûreté des fonctions d'I&C et électriques ainsi que le classement de sûreté des systèmes d'I&C et électriques et/ou les définitions des niveaux de défense en profondeur sont comprises dans les documents suivants:

– SSR-2/1 de l'AIEA, *Sûreté des centrales nucléaires: Conception;*
– SSG-30 de l'AIEA, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants;*
– SSG-34 de l'AIEA, *Design of Electrical Power Systems for Nuclear Power Plants;*
– SSG-39 de l'AIEA, *Design of Instrumentation and Control Systems for Nuclear Power Plants.*

A.4 Normes IEC applicables à la catégorisation et au classement de sûreté

Les normes IEC qui comportent des exigences à appliquer relatives à la catégorisation de sûreté des fonctions d'I&C et électriques ainsi que le classement de sûreté des systèmes d'I&C et électriques sont les suivantes:

– IEC 61226, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*
– IEC 61513, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

Remarque: Dans le présent document IEC 60709, la catégorisation de l'IEC 61226 en catégories A, B et C ainsi que les classes 1, 2 et 3 correspondantes sont utilisées.

A.5 Niveaux de défense en profondeur, définitions simplifiées

Concernant les niveaux de DiD, les documents de l'AIEA servent de référence pour les définitions.

Les définitions simplifiées des cinq niveaux de défense en profondeur sont les suivantes:

– Niveau 1: Empêche les écarts par rapport au fonctionnement normal;
– Niveau 2: Détecte les pannes et contrôle les conditions anormales de fonctionnement;
– Niveau 3: Contrôle les accidents compris dans la base de conception de la centrale;
– Niveau 4: Contrôle les conséquences des conditions hors dimensionnement;
– Niveau 5: Atténue les conséquences radiologiques des rejets significatifs de rayonnements.

Annexe B
(informative)

Exemples de séparations

B.1 Objet de la présente Annexe

La présente Annexe donne des exemples pratiques de mise en œuvre d'exigences de séparation lors de la conception d'une CNP.

B.2 Exemple de séparation physique

B.2.1 Généralités

Les principes de la séparation physique sont décrits dans l'Article 5.

La séparation physique est définie de la manière suivante: «Séparation par la géométrie (distance, orientation, etc.), par des barrières appropriées ou par ces deux moyens à la fois».

B.2.2 Exemples de séparations physiques par une distance

La Figure B.1 représente la séparation relative aux câbles de classe de sûreté 1 et aux autres câbles (classe de sûreté autre que la classe 1) par une distance sur des structures de support de câbles dans les galeries de câbles, affectées à une même division, par exemple.

En outre, les câbles de différents niveaux de tension dans la classe de sûreté 1 sont également séparés pour des raisons de CEM.

L'IEC 60364-5-52 recommande une distance de 300 mm pour la séparation des niveaux de tension des câbles de puissance. Cette norme prend pour référence les facteurs de réduction de la charge de câble, si les câbles sont installés sur des tablettes. Conformément à cette norme, la distance de 300 mm peut être réduite, mais les facteurs de réduction pour le dimensionnement des câbles de puissance doivent également être adaptés.

La largeur représentée à la Figure B.1 est influencée par différents paramètres, par exemple, la charge calorifique des câbles et l'exigence d'une largeur minimale des chemins d'évacuation.

La Figure B.2 représente la séparation relative aux câbles de classe de sûreté 1 et aux autres câbles (classe de sûreté autre que la classe 1) par une distance lorsque les tablettes sont installées sur la même structure de support de câbles. La distance applicable doit être définie au début du projet.

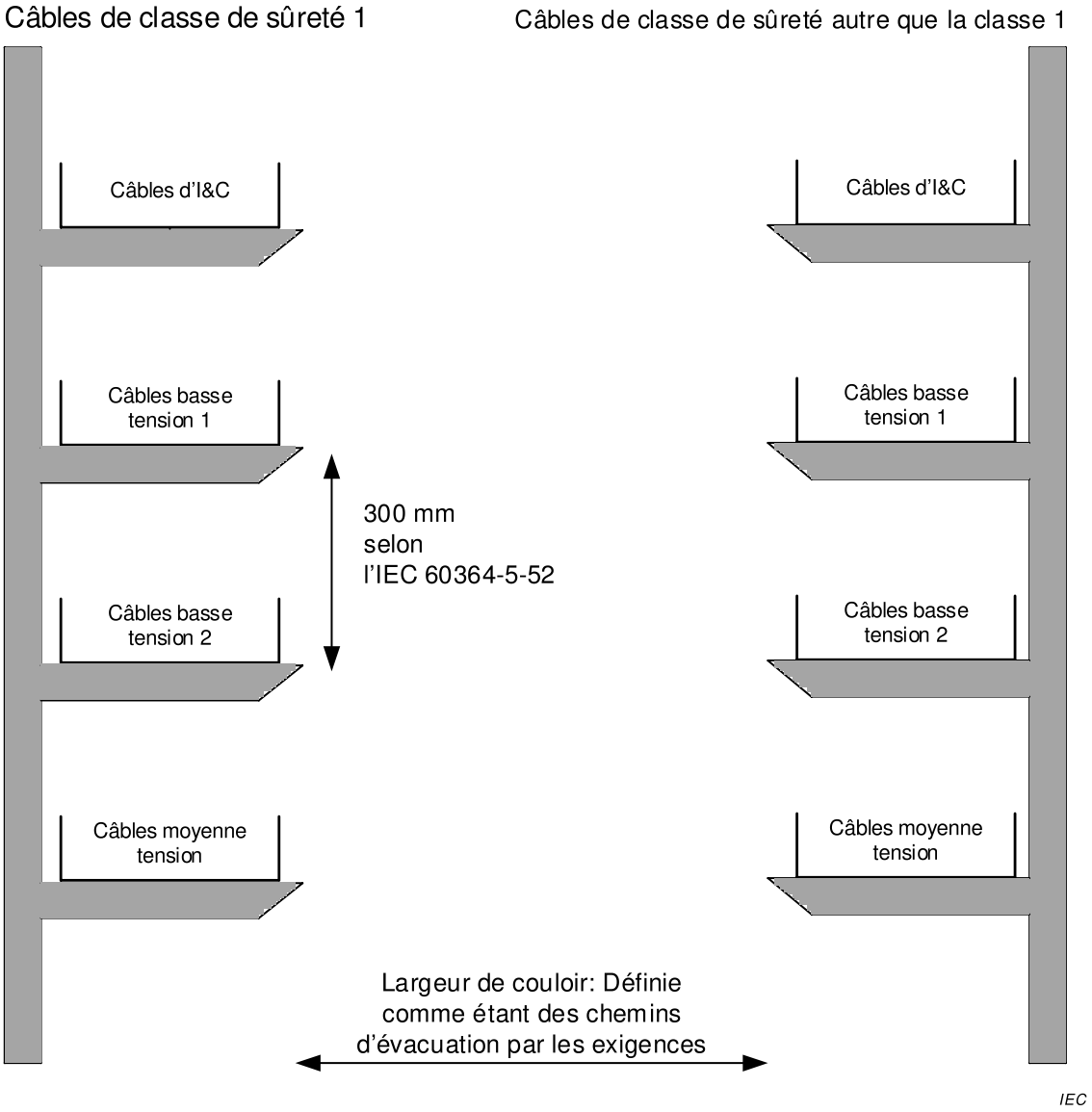


Figure B.1 – Séparation des structures de support de câbles par une distance

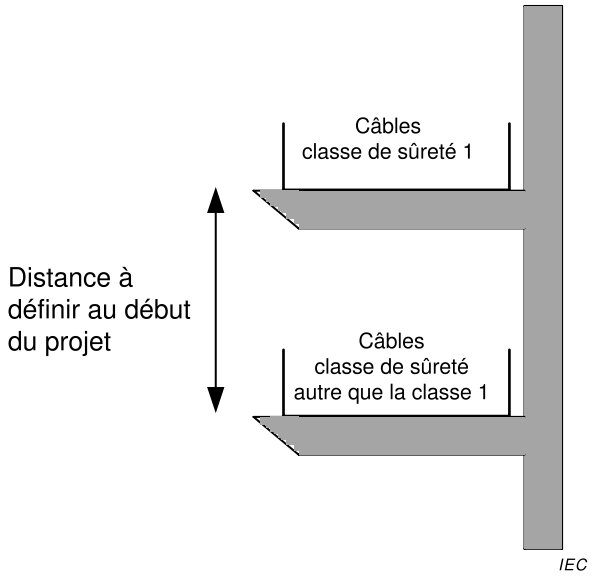


Figure B.2 – Séparation des tablettes par une distance

B.2.3 Exemples de séparations physiques par une structure

La Figure B.3 représente la séparation des câbles par des structures, comme cela est généralement effectué lorsque deux divisions sont séparées.

La résistance au feu de la structure de séparation ainsi que d'autres données doivent être définies par le projet, selon les exigences relatives aux événements dangereux internes.

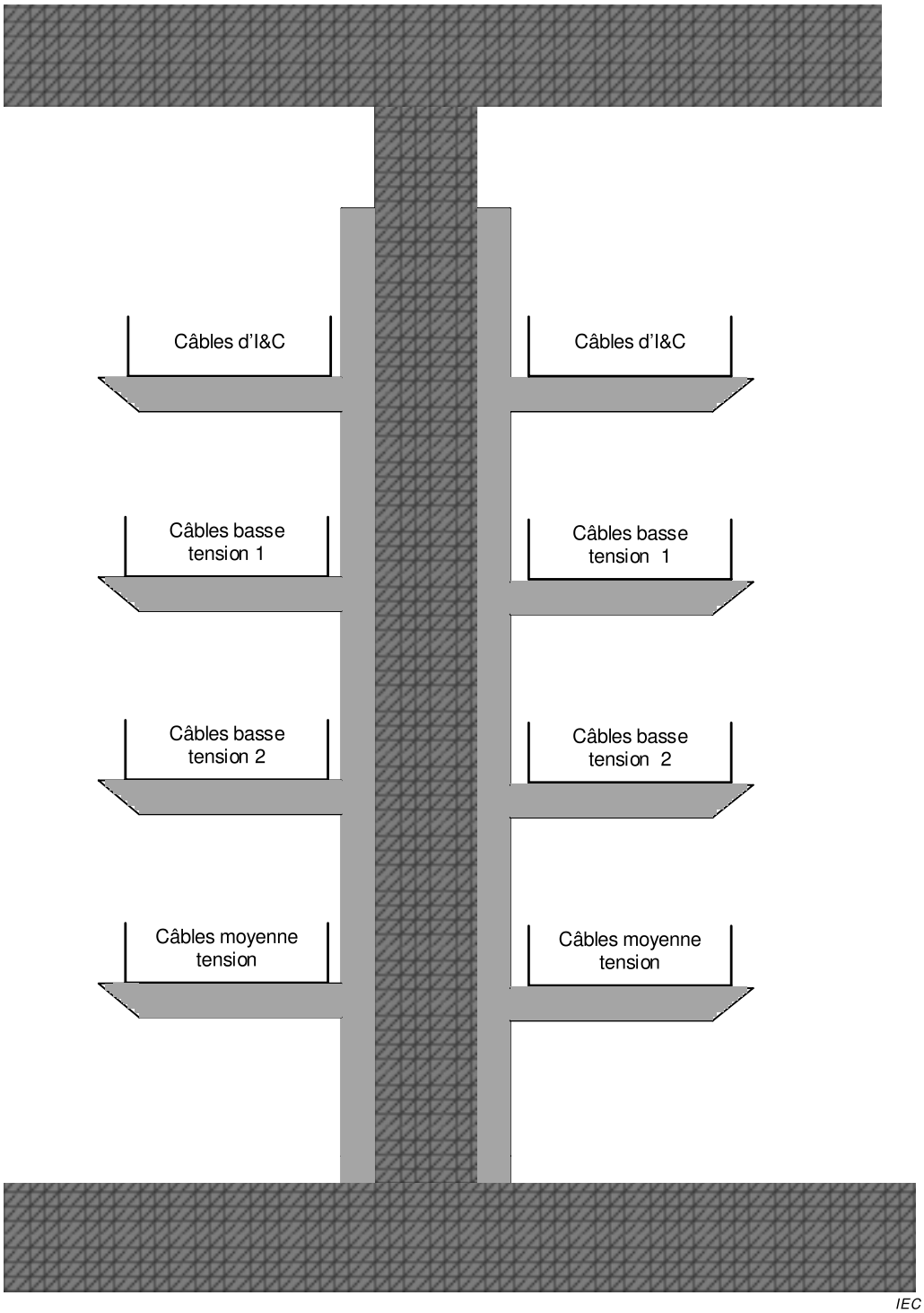


Figure B.3 – Séparation par des structures

B.3 Exemple d'isolement électrique

B.3.1 Généralités

L'isolement électrique est défini dans les guides SSG-34 et SSG-39 de l'AIEA.

L'isolement électrique est utilisé pour empêcher les défaillances électriques d'un système d'affecter des systèmes connectés. L'isolement électrique limite ou empêche les interactions dommageables entre équipements et composants conséquences de facteurs tels que les interférences électromagnétiques, les piques électrostatiques, les courts-circuits, les ouvertures de circuits, les mises à la terre ou l'application de la tension maximale crédible (en CC ou en CA).

Les principes d'isolement électrique sont décrits dans l'Article 6.

B.3.2 Exemples de barrières contre les surtensions

En général, les composants dans les circuits électriques sont conçus pour fonctionner et supporter une tension d'alimentation maximale. Une tension d'alimentation maximale supérieure à la tension assignée des appareils pourrait donner lieu à des dommages.

La foudre constitue l'une des principales sources de surtension. Des mesures de protection contre la foudre sont prises pour l'ensemble de la centrale, par exemple celles de l'IEC 62305.

Afin de limiter la surtension dans les circuits d'I&C et électriques, des barrières contre les surtensions sont utilisées. Les normes à prendre en considération pour la spécification de ces barrières contre les surtensions sont l'IEC 61643, l'IEC 61647 et l'IEC 60364-5-53.

La Figure B.4 donne un exemple d'installation de barrière contre les surtensions d'un circuit d'I&C.

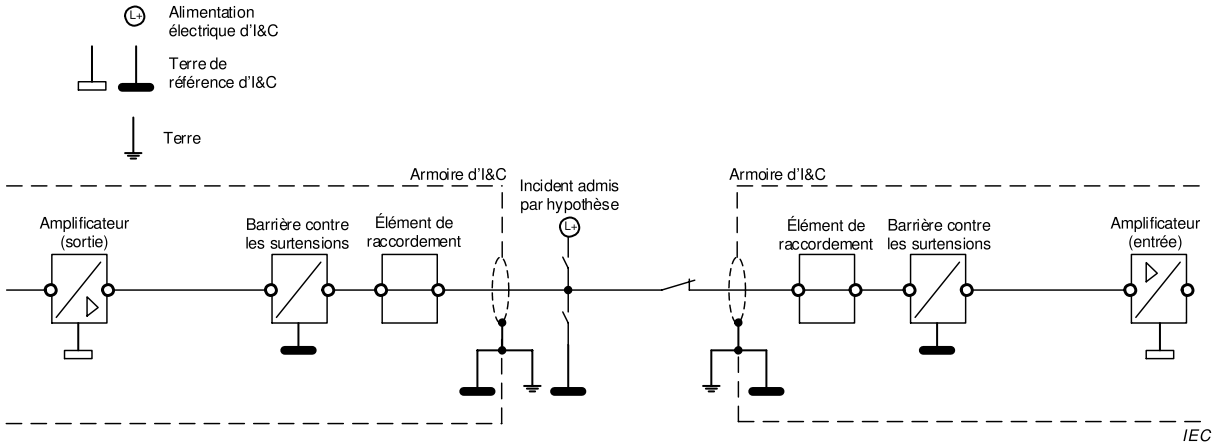


Figure B.4 – Barrières contre les surtensions dans les systèmes d'I&C

Pour les systèmes électriques, des protections contre les surtensions sont également installées. Elles se trouvent généralement à différents niveaux de défense.

La Figure B.5 représente l'installation d'un parafoudre dans l'alimentation électrique d'un moteur MT.

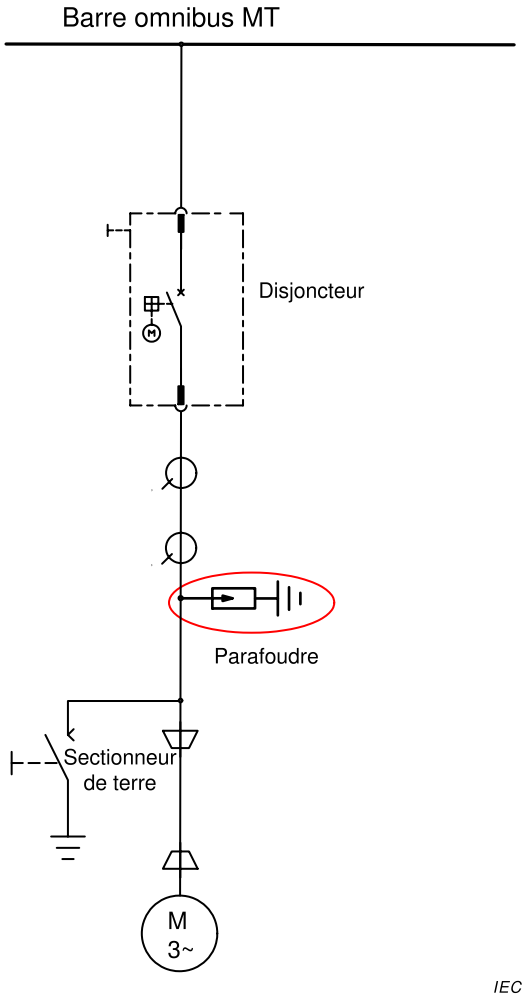


Figure B.5 – Protection contre les surtensions dans les systèmes électriques

B.3.3 Exemples de protections contre les courts-circuits/surintensités

Les surintensités sont généralement provoquées par des conditions de surcharge dans des matériels d'utilisation ou par des défauts tels que des courts-circuits ou des défauts à la terre. Une surintensité peut avoir ou ne pas avoir d'effets préjudiciables. Cela dépend de son amplitude et de sa durée.

Un court-circuit est une connexion anormale de nœuds d'un circuit électrique destiné à être alimenté à différentes tensions. Les nœuds sont à la même tension pendant le court-circuit. Un court-circuit engendre généralement un courant excessif, lequel peut provoquer des dommages.

Des détails supplémentaires concernant les mesures de protection sont donnés dans l'IEC 60364.

La Figure B.6 représente la protection contre les courts-circuits en cas d'interconnexion électrique entre deux divisions. En général, ce type d'interconnexion est utilisé pendant les indisponibilités et les travaux de maintenance d'une division afin d'assurer l'alimentation des charges telles que les circuits d'éclairage.

Étant donné que l'alimentation peut aller dans les deux directions, des dispositifs de protection (fusibles) sont installés aux deux extrémités des câbles.

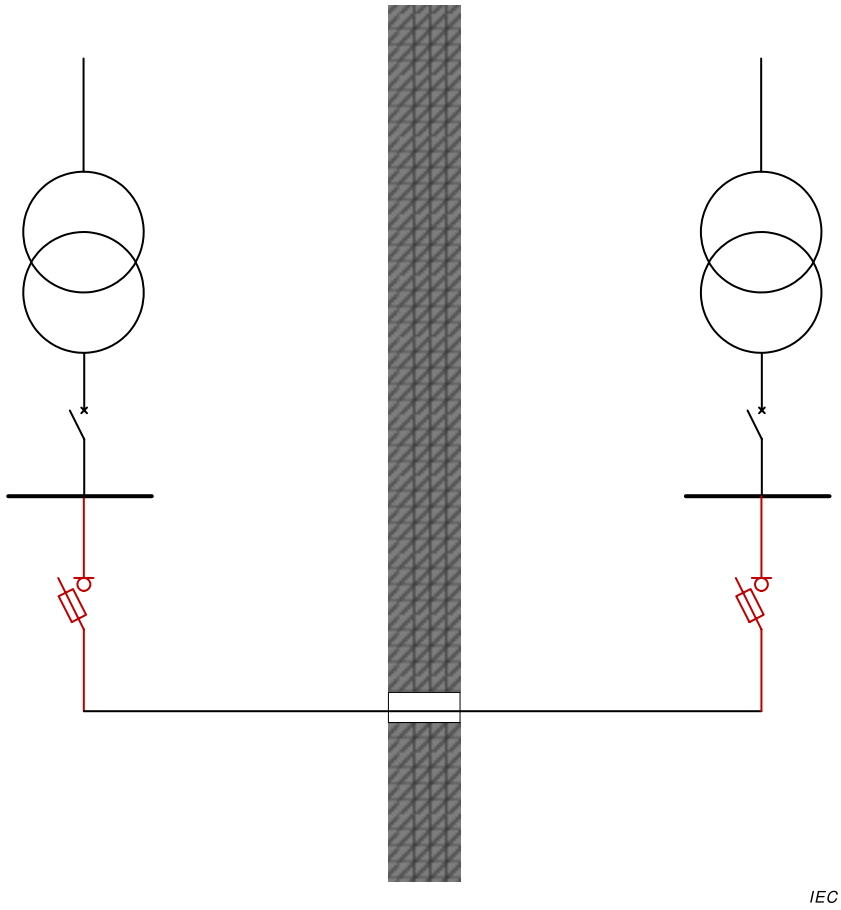


Figure B.6 – Protection contre les courts-circuits en cas d'interconnexion

B.3.4 Exemples d'isolations galvaniques

L'isolation galvanique est effectuée afin d'empêcher du courant continu de circuler entre différents systèmes électriques. L'échange d'énergie ou d'informations peut uniquement être effectué par d'autres moyens, tels que la capacité, l'induction, les ondes électromagnétiques, optiques ou acoustiques. En général, l'isolation galvanique est exigée lorsque, par exemple, le concept de mise à la terre n'est pas complètement cohérent, c'est-à-dire que les terres peuvent avoir différents potentiels.

La Figure B.7 donne un exemple d'installation d'isolation galvanique dans un circuit d'I&C.

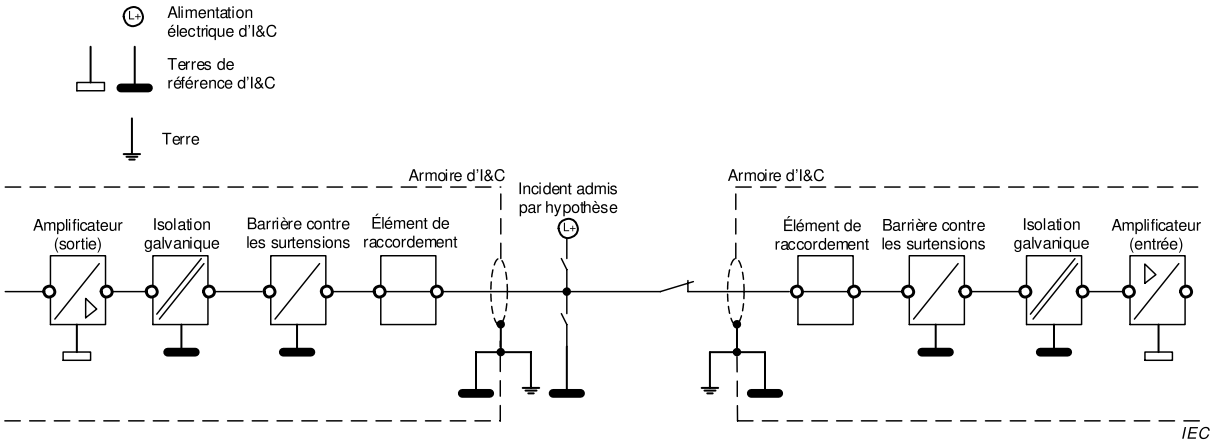


Figure B.7 – Isolation galvanique dans les systèmes d'I&C

Dans les systèmes électriques, l'isolation galvanique peut être utilisée pour la sûreté du personnel ou pour empêcher les courants accidentels d'atteindre la terre par le biais d'un corps humain.

La Figure B.8 donne un exemple de séparation galvanique dans les systèmes électriques, généralement fournie par des transformateurs.

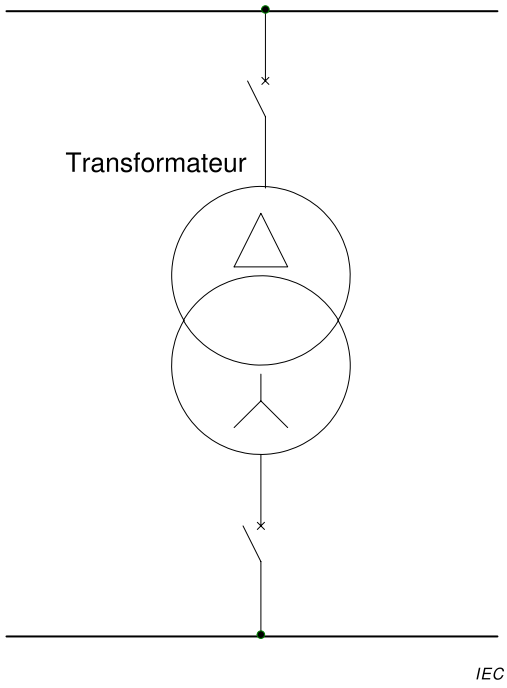


Figure B.8 – Isolation galvanique dans les systèmes électriques

B.4 Exemple de protection CEM

La compatibilité électromagnétique (CEM) est l'aptitude d'un appareil, d'un composant, d'un système ou d'une installation à fonctionner comme prévu sans dégradation ou dysfonctionnement dans leur environnement électromagnétique d'exploitation prévu.

Des détails supplémentaires concernant la CEM sont fournis dans la série IEC 61000 et la norme dédiée: l'IEC 62003.

Les exigences de CEM applicables à une centrale sont généralement décrites dans un plan/rapport de CEM.

La Figure B.9 donne un exemple de protection CEM spécifique de câbles d'I&C dans des structures de support de câbles.

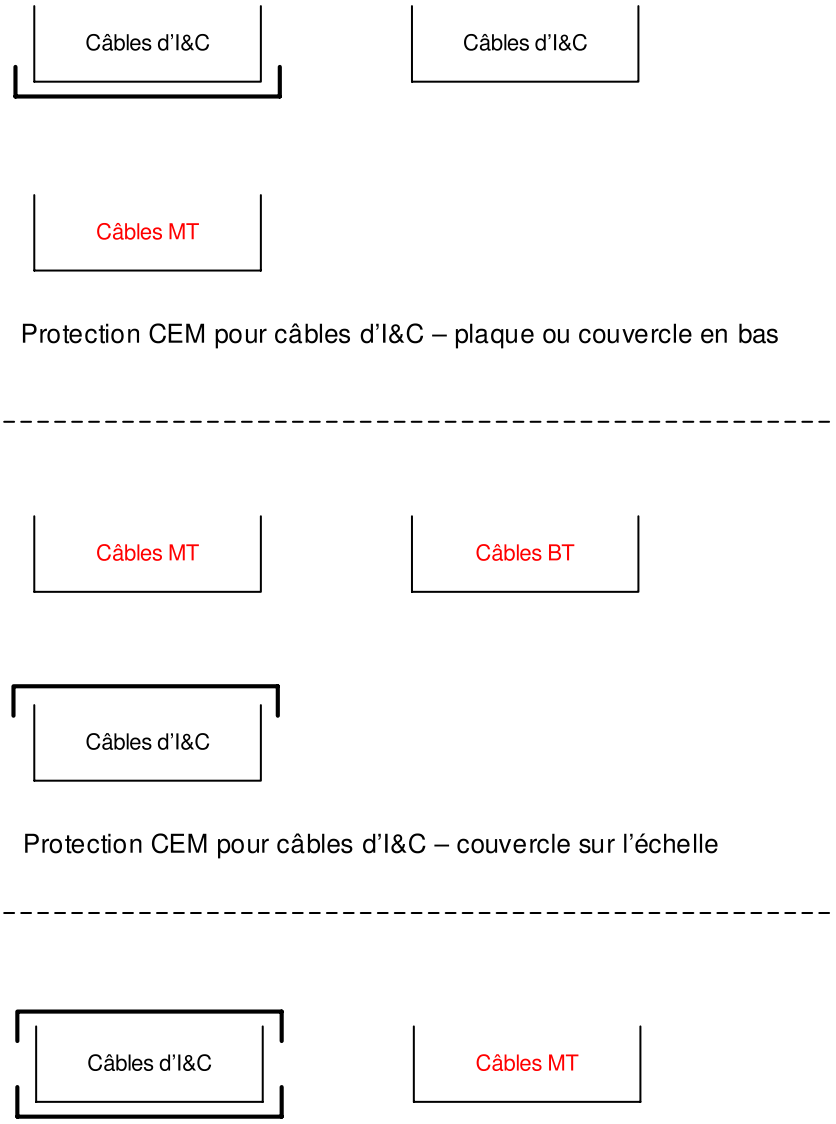


Figure B.9 – Protection CEM des câbles d'I&C

B.5 Circuits associés

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

Les principes des circuits associés sont décrits en 5.3.

La Figure B.10 donne des exemples de circuits associés.

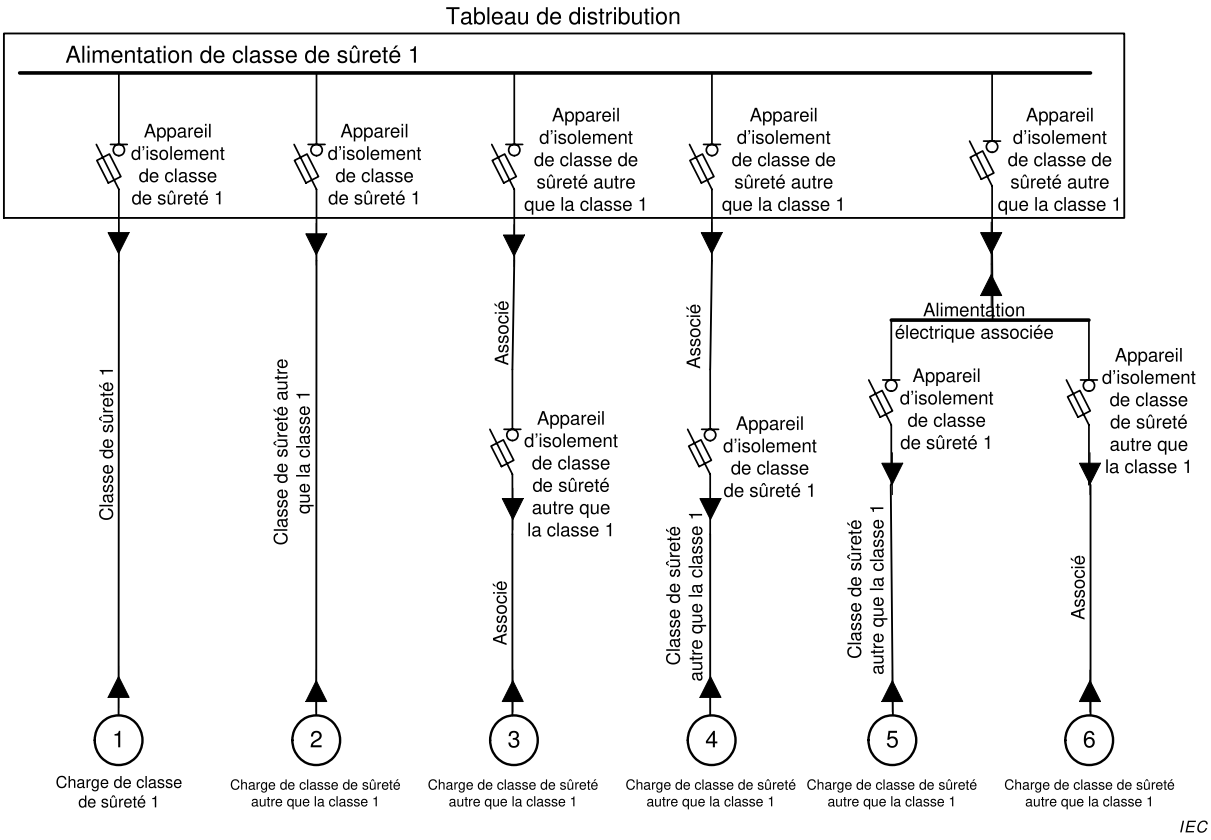


Figure B.10 – Exemples de circuits associés

Annexe C
(informative)

Exemples d'erreurs de conception et de défaillances de systèmes d'I&C et électriques

C.1 Objet de la présente Annexe

La présente Annexe donne des exemples d'erreurs de conception et de défaillances électriques ou de l'I&C.

C.2 Erreurs de conception

La survenue éventuelle d'erreurs dans les spécifications des exigences des systèmes d'I&C et électriques importants pour la sûreté ne peut pas être ignorée. De telles erreurs de conception peuvent se traduire par la propagation de défauts entre les systèmes, par exemple, une isolation insuffisante du câblage, le dimensionnement inadéquat des composants ou des conducteurs, etc. Il convient que les moyens permettant de traiter ce type de défaut comprennent généralement une conception conservative de la séparation physique et de l'isolement électrique.

C.3 Défaillances de systèmes d'I&C et électriques

C.3.1 Généralités

Il convient de prendre en considération les événements initiateurs de défaillances provoqués au sein de chaque système d'I&C ou électrique important pour la sûreté. Ces événements sont généralement caractérisés par des effets mécaniques et électriques localement limités pouvant avoir différentes conséquences fonctionnelles. Les défaillances uniques au sein des unités centrales d'I&C et sur des interfaces de communication multiplexées peuvent également être susceptibles de générer plusieurs défaillances. Les cas de défaillances de systèmes d'I&C et électriques peuvent être répartis comme suit.

C.3.2 Défaillance aléatoire unique

Il convient de prendre en considération les défaillances aléatoires uniques de composants de systèmes d'I&C ou électriques pouvant se traduire par des dysfonctionnements de composants, des courts-circuits, des coupures de la continuité du circuit, le contact avec la terre, des variations de tension ou de fréquence, la défaillance mécanique des composants ou un incendie local. Un tel événement peut provenir d'une surcharge, d'une perte ou d'une insuffisance de refroidissement, d'un dommage mécanique, d'erreurs au cours de travaux de maintenance ou de réparation, de dommages chimiques, d'une défaillance aléatoire causée par une déficience matérielle ou d'autres événements.

C.3.3 Défaillances multiples issues d'une cause unique commune

Il convient de porter une attention particulière aux conséquences des défaillances de deux composants ou plus, lesquelles affectent les groupes redondants de sûreté, en raison d'une cause unique commune telle qu'une erreur de maintenance, un dommage mécanique ou une interférence électrique. Il convient de prendre en considération les effets environnementaux, les dommages dus à des rayonnements et les autres facteurs physiques communs éventuels.

Annexe D
(informative)

Indépendance fonctionnelle et indépendance en matière de communication

D.1 Objet de la présente Annexe

La présente Annexe fournit une description de l'indépendance fonctionnelle et de l'indépendance en matière de communication.

D.2 Indépendance fonctionnelle

D.2.1 Généralités

Deux fonctions, systèmes ou composants sont fonctionnellement indépendants s'ils ne nécessitent pas d'échanger des informations afin de réaliser leur fonction. L'indépendance fonctionnelle peut être bilatérale, lorsqu'il n'y a pas d'échange d'informations, ou unilatérale, lorsqu'un échange d'informations unidirectionnel est autorisé.

L'exécution de fonctions de sûreté et de procédé au moyen de systèmes d'I&C et électriques peut être interrompue par:

- le blocage des fonctions de sûreté et de procédé (par exemple, appartenant à différents niveaux de défense);
- des systèmes support défaillants (avec un impact direct ou différé sur le fonctionnement du système);
- le verrouillage d'actionneurs automatiques de sûreté (par exemple, afin d'éviter la progression vers des conditions plus graves pour la centrale);
- l'interférence par des fonctions de service (par exemple, pendant la maintenance et les essais périodiques).

Conformément au guide de sûreté SSG-39 de l'AIEA:2016: «6.46. L'indépendance fonctionnelle est favorisée par la conception architecturale et le traitement soigneux des données qui sont partagées entre des fonctions (...)».

Il convient de considérer les mesures relatives à l'indépendance fonctionnelle comme des données d'entrée pour les mesures de séparation.

Pour les systèmes électriques, il peut s'agir de l'actionnement d'une source d'alimentation sans impact sur les autres sources d'alimentation.

NOTE Les exigences relatives à la diversité fonctionnelle constituent une autre méthode permettant de prendre en considération l'indépendance entre les fonctions de procédé et les fonctions de sûreté. Cependant, ces exigences ne peuvent pas être assignées en tant que mesures de séparation.

D.2.2 Indépendance du système de contrôle-commande

L'utilisation de signaux de systèmes de classe de sûreté 1 dans les systèmes de contrôle-commande (de classe quelconque) exige de prendre des précautions plus strictes que celles exigées lorsque des signaux de systèmes de classe de sûreté 1 sont utilisés uniquement à des fins de surveillance ou de protection. Une défaillance du capteur peut se traduire par une valeur de mesure du système de contrôle-commande hors des tolérances demandées, ainsi qu'une action de contrôle-commande dangereuse, tout en empêchant le système de protection de détecter la condition dangereuse.

Il convient de concevoir le système de protection et le système de contrôle-commande de sorte que les défaillances uniques hypothétiques, y compris les défaillances consécutives relatives aux signaux transférés entre ces deux systèmes, ne puissent pas provoquer d'accident ou de transitoire exigeant une action de sûreté ni provoquer en même temps de dégradation inacceptable du système de classe de sûreté 1.

Lorsqu'une défaillance unique aléatoire, et toute défaillance consécutive, au sein du système de classe de sûreté 1, peuvent provoquer une action du système de contrôle-commande qui donne lieu à une condition exigeant une action de sûreté, il convient que le système de classe de sûreté 1 soit capable d'effectuer cette action même lorsqu'il est dégradé par une deuxième défaillance aléatoire. Il convient d'inclure des dispositions de sorte que cette exigence puisse être satisfaite lorsqu'un composant ou un ensemble est mis hors service ou supprimé du service pour une raison quelconque, y compris à des fins d'essai ou de maintenance.

Les dispositions acceptables dépendent du type de réacteur et des défaillances possibles. Elles comprennent:

– la dégradation de la logique de vote majoritaire lorsqu'une défaillance du capteur ou des pannes d'équipements sont détectées;
– le retrait des signaux de contrôle-commande des composants ou des ensembles redondants lorsque ces signaux sont déterminés comme ne représentant pas la condition réelle du procédé;
– le lancement d'une action de sûreté depuis un ensemble logique de sûreté, mettant ainsi la centrale dans un état qui ne soit plus impacté de manière préjudiciable par l'action du système de contrôle-commande;
– une protection assurée par le biais de différents paramètres physiques.

Un système de protection à logique de vote 1 sur 2 fournissant des signaux de contrôle-commande exige d'être justifié par des arguments de compromis même si les mises hors service efficaces, la détection de haut niveau et la fiabilité des équipements, sont prouvées par le biais d'essais périodiques. Un système à logique de vote 2 sur 3 peut satisfaire aux exigences avec un équipement de sécurité intrinsèque et la détection automatique de capteurs défaillants si des installations de mise hors service sont utilisées pendant la maintenance.

Lorsqu'il peut être démontré, en raison de l'événement d'origine, que la défaillance simultanée des ensembles redondants de surveillance de sûreté est peu probable, des ensembles de surveillance de sûreté qui comparent les signaux peuvent être fournis. Il convient que ces ensembles de surveillance de sûreté fournissent une indication ou émettent une alarme ou un signal d'action de sûreté, ou rendent la logique plus restrictive lorsqu'un signal s'écarte de manière excessive des autres signaux redondants de condition ou paramètre de centrale similaire. Il convient d'assurer une isolation appropriée aux ensembles de surveillance de sûreté qui effectuent des comparaisons afin d'empêcher l'interaction entre les voies redondantes. L'envoi de toutes les valeurs de détection à chaque voie redondante du système de sûreté en est un exemple. Chaque voie compare ensuite les valeurs afin de détecter des valeurs inadéquates ou anormales. Chaque voie peut ensuite utiliser pour le vote toutes les valeurs des capteurs, ou retenir le capteur le plus défavorable dans chaque voie pour l'action de vote. Il convient que les capteurs qui sont détectés comme étant défectueux soient signalés par une alarme et que les valeurs puissent être affichées.

D.3 Indépendance en matière de communication

L'objet de la communication est de diffuser des informations d'un système A à un système B ou inversement. Les méthodes de communication dans les CNP exigent une connexion physique par laquelle les informations sont diffusées selon des valeurs électriques (binaires/analogiques) ou un protocole de communication de données (à l'exception des connexions sans fil).

Pour chaque type de communication, il convient de considérer que, soit l'émetteur, soit le récepteur, peut influencer/détruire son homologue (dans les deux sens). En fonction de la méthode de communication, différents facteurs peuvent agir sur la communication.

Les mesures permettant d'assurer l'indépendance de la communication de données ne relèvent pas du domaine d'application du présent document, y compris les menaces à prendre en considération, qu'il convient d'identifier par le programme d'I&C de cybersécurité. Pour de plus amples informations, voir l'IEC 62645.

Bibliographie

IEC 60364 (toutes les parties), *Installations électriques à basse tension*

IEC 60880, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

IEC 61643 (toutes les parties), *Parafoudres basse tension*

IEC 62138, *Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C*

IEC 62305 (toutes les parties), *Protection contre la foudre*

IEC 62645, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés*

AIEA GS-R-3:2006, *Système de gestion des installations et des activités*

Guide de sûreté de l'AIEA n° GS-G-3.1:2006, *Application of the management System for facilities and activities* (disponible en anglais seulement)

Guide de sûreté de l'AIEA n° GS-G-3.5:2009, *Management system for nuclear installations* (disponible en anglais seulement)

Collection sécurité n° 50-C-Q de l'AIEA, *L'assurance de la qualité pour la sûreté des centrales nucléaires et autres installations nucléaires*

IAEA Safety Glossary:2016, *Terminology used in nuclear safety and radiation protection* (disponible en anglais seulement)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch