

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2018 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

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

About the IEC

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

About IEC publications

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

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.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**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

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	10
1.1 General.....	10
1.2 Application: new and pre-existing plants	10
2 Normative references	11
3 Terms and definitions	12
4 Abbreviated terms	15
5 Principles and requirements for separation	16
5.1 Principles.....	16
5.1.1 General	16
5.1.2 Separation reasoning and boundaries.....	16
5.1.3 Plant safety principles and requirements	17
5.2 Safety class separation requirements.....	17
5.3 Associated circuits	18
5.3.1 General	18
5.3.2 Criteria	19
5.4 Separation issues at existing plants	20
5.4.1 General	20
5.4.2 Criteria	20
6 Separation design basis	20
6.1 Design inputs.....	20
6.2 Environmental conditions and hazards	21
6.2.1 General	21
6.2.2 Environmental conditions.....	21
6.2.3 External hazards.....	21
6.2.4 Internal hazards.....	21
6.2.5 Fire protection	22
6.3 EMI/EMC	22
6.4 Electrical fault.....	22
6.5 Requirements from non-nuclear technical standards	22
6.6 Requirements from special operating conditions	22
7 Electrical isolation	23
7.1 Principles.....	23
7.1.1 General	23
7.1.2 Overvoltage barrier.....	23
7.1.3 Short circuit / Overcurrent protection	23
7.1.4 Electrical nonreactive (retroaction free)	24
7.1.5 Galvanic isolation (electrical insulation)	24
7.2 Isolation devices	24
7.2.1 General	24
7.2.2 Isolation characteristics	25
7.2.3 Actuation priority	25
8 Physical separation	26
8.1 Principles.....	26

8.1.1	General	26
8.1.2	Separation by distance	26
8.1.3	Structural separation	26
8.2	Separation of cables and cable support structures	26
8.2.1	General	26
8.2.2	Divisional separation of redundant cables and cable support structures	27
8.2.3	Separation of system cables and cable supporting structures of different safety classes	27
8.2.4	Separation of signal cables from power cables	28
8.2.5	Reduced separation distances	28
8.2.6	Associated circuits	28
8.2.7	Separation of cables from tubes or pipes	28
8.2.8	General routing considerations	28
8.2.9	Identification	28
8.3	Separation of components inside the I&C and electrical system important to safety	28
8.3.1	Divisional separation of redundant components inside the I&C and electrical system important to safety	28
8.3.2	Separation of components of different safety classes	29
8.3.3	Installation of equipment of different voltage levels	29
8.3.4	Reduced separation distances	29
8.3.5	Associated circuits	30
8.3.6	Separation of components from sources of hazards	30
8.4	Control room cabinets, desks, panels and related cables	30
9	Verification	31
Annex A (normative)	Relation to IAEA guidelines and IEC 61226	32
A.1	Object of this Annex	32
A.2	Applicability of this document	32
A.3	IAEA Guidelines, applicable for this document	32
A.4	IEC standards, applicable for the safety categorization and classification	32
A.5	Defence in Depth levels, simplified definitions	33
Annex B (informative)	Examples of separation realizations	34
B.1	Object of this Annex	34
B.2	Example of physical separation	34
B.2.1	General	34
B.2.2	Examples of physical separation by distance	34
B.2.3	Examples of physical separation by structure	36
B.3	Example of electrical isolation	37
B.3.1	General	37
B.3.2	Examples of overvoltage barriers	37
B.3.3	Examples of short circuit / overcurrent protection	38
B.3.4	Examples of galvanic isolation	39
B.4	Example of EMC protection	40
B.5	Associated circuits	41
Annex C (informative)	Examples of design errors and I&C and electrical failure events	43
C.1	Object of this Annex	43
C.2	Design errors	43
C.3	I&C and electrical system failure events	43
C.3.1	General	43

C.3.2	Single random failure.....	43
C.3.3	Multiple failures from a single common cause	43
Annex D (informative)	Functional independence and independence of communication.....	44
D.1	Object of this Annex.....	44
D.2	Functional independence	44
D.2.1	General	44
D.2.2	Independence from control system	44
D.3	Independence of communication	45
Bibliography.....		46
Figure 1 – Physical separation by structure or distance		17
Figure 2 – Separation by electrical isolation.....		17
Figure 3 – Electrical Isolation measures and selection of components		23
Figure B.1 – Separation of cable supporting structures by distance		35
Figure B.2 – Separation of cable trays by distance.....		35
Figure B.3 – Separation by structures		36
Figure B.4 – Overvoltage barriers in I&C systems		37
Figure B.5 – Overvoltage protection in electrical systems		38
Figure B.6 – Short circuit protection in case of a cross-connection.....		39
Figure B.7 – Galvanic isolation in I&C systems		39
Figure B.8 – Galvanic isolation in electrical systems		40
Figure B.9 – EMC protection of I&C cables		41
Figure B.10 – Examples of associated circuits		42

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 upgrading 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.

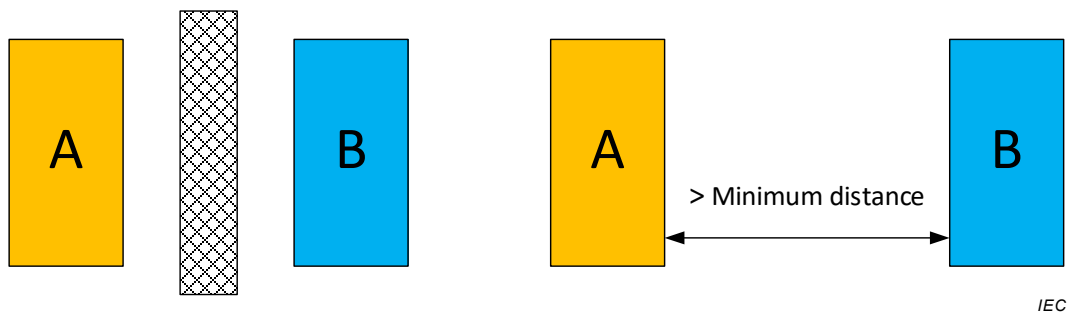


Figure 1 – Physical separation by structure or distance

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

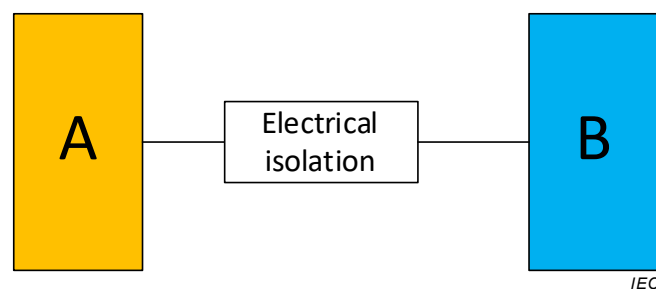


Figure 2 – Separation by electrical isolation

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 constraints 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.

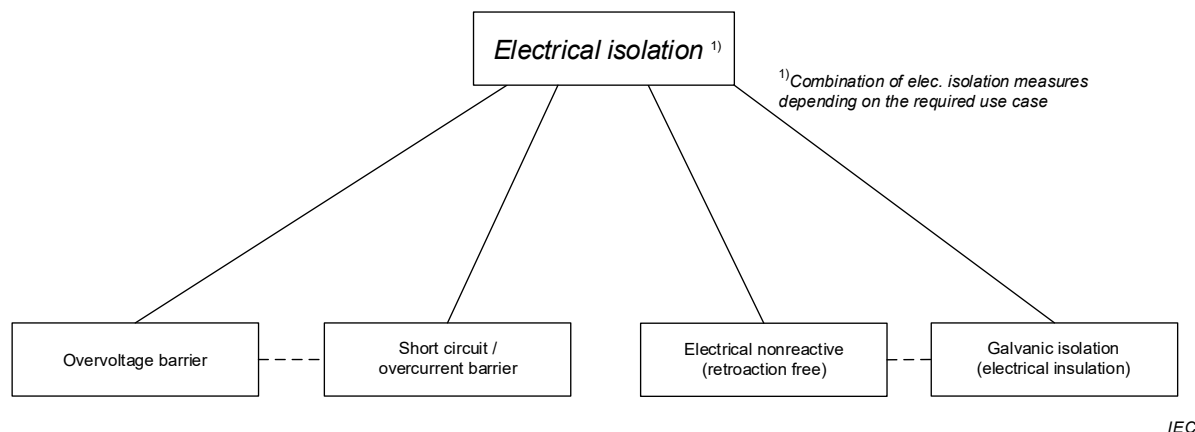


Figure 3 – Electrical Isolation measures and selection of components

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) $\leftrightarrow$ 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 constraints, 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.