

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

IECNORM.COM : Click to view the full PDF of IEC 62808:2015



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 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
Fax: +41 22 919 03 00
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 - www.iec.ch/searchpub

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 more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 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: csc@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 - www.iec.ch/searchpub

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 plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

Plus de 60 000 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: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-2665-0

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	3
INTRODUCTION	5
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Symbols and abbreviations	8
5 General principles for isolation devices	8
5.1 General	8
5.2 Isolation characteristics	9
5.3 Actuation priority	10
6 Isolation device design requirements	10
6.1 Requirements on isolation device application	10
6.1.1 Isolation device power	10
6.1.2 Maximum credible fault	10
6.1.3 Energy limiting devices	11
6.2 Requirements on isolation device design	11
6.2.1 Basic design requirements	11
6.2.2 Postulated faults	12
6.2.3 Physical component arrangement	12
6.3 Power isolation devices	13
6.3.1 General	13
6.3.2 Circuit breaker tripped by fault currents	13
6.3.3 Circuit breaker tripped by fault signals	13
6.3.4 Input current limiters	13
6.3.5 Fuses	13
7 Qualification test requirements	13
7.1 General	13
7.2 Requirements on the test method	14
7.2.1 Test specification	14
7.2.2 Testing energy limiting devices	14
7.2.3 Qualification test environment	14
7.3 Application specific testing	15
7.3.1 General	15
7.3.2 Isolation of safety circuits from lower class circuits	15
7.3.3 Isolation between redundant safety circuits	15
7.4 Documentation of test requirements and results	15
Bibliography	16
Figure 1 – Application of maximum credible fault	11
Figure 2 – Application of postulated fault	12

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY –
DESIGN AND QUALIFICATION OF ISOLATION DEVICES**

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 62808 has been prepared by subcommittee 45A: Instrumentation, control and electrical systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/1004/FDIS	45A/1019/RVD

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 62808:2015

INTRODUCTION

a) Technical background, main issues and organisation of the standard

I&C (instrumentation and control) systems important to safety in nuclear power plants need to tolerate the effects of plant / equipment faults as well as internal and external hazards. IEC 60709 provides requirements to establish independence between redundant portions of safety systems, and between safety systems and systems of a lower class. Among the techniques available to increase the level of tolerability of I&C systems to such effects is the provision of isolation devices where connections are made between redundant divisions of safety equipment, or between safety equipment and systems of a lower class. This standard provides technical requirements and recommendations for the design and qualification of isolation devices that are required by IEC 60709. This standard deals with the criteria and methods used to confirm that the design of isolation devices ensures that credible failures in the connected lower class system or redundant channels will not prevent the safety systems from meeting their required functions. Isolation devices may be required on power or signal interfaces within the system.

Guidance for other aspects of isolation device qualification (e.g. electromagnetic compatibility, environmental and seismic qualification) may be found in IEC 60780.

The object of this standard is:

- in Clause 5: to establish the basic criteria for acceptability of the design and application of isolation devices;
- in Clause 6: to establish design requirements on the selection and application of suitable isolation devices;
- in Clause 7: to establish requirements on qualification testing done to validate the adequacy of the isolation device design.

It is intended that the standard be used by operators of NPPs (utilities), designers of nuclear I&C system and equipment, systems evaluators and regulators.

b) Situation of the current standard in the structure of the IEC SC 45A standard series

IEC 62808 is the third level IEC SC 45A document tackling the issue of isolation devices.

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

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

IEC 62808 is intended to provide requirements and recommendations relating to the design and qualification of isolation devices which are identified in IEC 60709 as a means of achieving independence between systems when signals are extracted from a system for use in lower class systems, or between independent subsystems of the same classes.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of this standard

IEC 60709 applies to I&C systems and equipment important to safety. It establishes requirements for physical and electrical separation as one means to provide independence between the functions performed in those systems and equipment. IEC 60709 requires the use of isolation devices where connections between independent systems must be made. IEC 62808 provides criteria for the analysis and qualification of the the isolation device.

A fundamental criterion for isolation devices is that they be included in, and designed to, the standards of the higher class system for which they provide protection against hazards. Additional requirements relating to design and qualification of an isolation device as an element of a safety system are not given in this 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 document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

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

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

A fourth level extending the IEC SC 45A standard series, corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding nuclear safety. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements SSR-2/1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NOTE 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, that are based on the requirements of a standard such as IEC 61508.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – DESIGN AND QUALIFICATION OF ISOLATION DEVICES

1 Scope

This International Standard establishes requirements for the design, analysis and qualification of isolation devices used to ensure electrical independence of redundant safety system circuits, or between safety and lower class circuits, as specified in IEC 60709. This standard includes guidance on the determination of the maximum credible fault that is applied to the isolation devices. The maximum credible fault can be used as a basis for the test levels used in testing based on other standards (e.g. IEC TS 61000-6-5 or IEC 62003).

This standard does not address safety or CCF issues due to functional inter-dependencies and possible interferences or CCFs that may result from signal exchange or sharing between systems or sub-systems. It also does not address design or qualification issues related to digital or programmable logic in isolation devices. For isolation devices containing digital or programmable logic, additional design and qualification requirements must be considered; these requirements are outside the scope of this standard.

2 Normative references

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

IEC 60709, *Nuclear power plants – Instrumentation and control systems important to safety – Separation*

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

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

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

3 Terms and definitions

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

3.1

barrier

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

Note 1 to entry: The following definition is given in the IAEA Safety Glossary, edition 2007: “A physical obstruction that prevents or inhibits the movement of people, radionuclides or some other phenomenon (e.g. fire), or provides shielding against radiation”. The IAEA definition is more general and consistent with the definition given in this standard.

3.2

common mode electrical faults

voltage or current faults between both signal terminals and a common reference plane (ground)

Note 1 to entry: These faults should not be confused with common cause failures.

Note 2 to entry: This causes the potential of both signal terminals to be changed simultaneously and by the same amount relative to the common reference plane (ground).

3.3

differential mode electrical faults

voltage or current faults between signals

3.4

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

Note 1 to entry: As described in IEC 60709, malfunctions can be caused by faults and normal actions.

3.5

maximum credible fault

MCF

voltage or current transient that may exist in circuits, as determined by test or analysis, taking into consideration the circuit location, routing, and interconnections combined with failures that the circuit and adjacent circuits may credibly experience

Note 1 to entry: The evaluation shall consider the impact of seismic and flooding conditions.

4 Symbols and abbreviations

AC	alternating current
CCF	common cause failure
DC	direct current
EMI	electromagnetic interference
I&C	instrumentation and control
MCF	maximum credible fault
NPP	nuclear power plant

5 General principles for isolation devices

5.1 General

The requirements for the application of isolation devices are in IEC 60709. Clause 5 is included as a summary and provides additional requirements for the isolation devices. The word "shall" identifies the additional requirements.

Isolation devices used in interfaces between I&C systems important to safety or between channels within a system important to safety may have an impact on the integrity of the overall design and in particular, on defence in depth. When used, they may be relied upon to provide electrical isolation between redundant safety functions or safety functions in different layers of defence in the overall architecture. In general, the introduction of such interfaces between systems should be considered carefully based on the principles and approaches outlined in IEC 61513. A systematic analysis of failures at system and overall I&C architecture level is required. Functional inter-dependencies are introduced between systems due to signal interfaces and their associated failure modes shall be considered carefully.

Where signals are transmitted between a Class 1 system or equipment (performing Category A functions) and systems of a lower class, the transmission of these signals are through isolation devices that are included within the higher class system. When failures or conditions are present at the output terminals of the isolation devices (which are connected to the lower class system) the safety action of the Class 1 system or sub-system to which the isolation device is connected cannot be affected. As an example, a circuit performing a Category A function may be monitored by a lower class circuit utilizing a relay coil in the Class 1 system and the relay contact in a lower class system.

Isolation devices are to be used where signals are transmitted between independent Class 1 systems and between redundant equipment channels of Class 1 systems.

Where signals are transmitted from Class 2 or 3 systems for use in lower class systems, or between independent subsystems in these classes, isolation devices may not be required; however, good engineering practices are followed to prevent the propagation of faults. In cases where Class 2 systems need to take on the aspects of Class 1 systems due to the functions performed, isolation is applied. An example of this is a Class 2 system performing a Category B function in support of a Class 1 system performing a Category A function to protect against the same fault.

Temporary connections for maintenance to systems performing Category A functions without isolation devices are only 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.

NOTE This standard discusses isolation devices as stand-alone devices which are separate from the equipment performing safety functions. The isolation device may be part of a module or equipment that performs a safety function. In other designs, the isolation device may be contained in several modules (e.g. one part handling rapid transient overvoltages and the other static voltages). This standard is also applicable to these design variations.

5.2 Isolation characteristics

The isolation device shall be capable of providing isolation against the following failure conditions:

- a) short-circuits between terminals or to ground;
- b) open circuits;
- c) application of the maximum AC or DC potential that could reasonably occur, considering potentials and sources available in both the Class 1 and non-Class 1 systems; and
- d) electromagnetic and electrostatic interference.

If the equipment can generate other signal types in fault conditions, such as a square wave or other form of oscillating signal in fault conditions, the isolation device shall be capable of providing isolation against such signals.

The properties of an isolation device shall include:

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

In this context, an assessment shall be done of the maximum credible fault 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 safety class.

Precautions are also taken to minimise the possibility that failure in a non-Class 1 system causes spurious or premature actuation of a Category A function.

5.3 Actuation priority

Where plant equipment that is controlled by a Class 1 system is also controlled by a lower class system, devices are provided which ensure priority of the Class 1 system actions over those of the lower class systems. Failures of, or normal actions by, the lower class system cannot interfere with the Category A functions under plant conditions requiring success of those Category A functions. The equipment performing the priority function is classified as Class 1. The circuit that provides the required isolation could be within the same system, or may be in other systems.

Failures and mal-operations in the non-Class 1 systems cannot cause a change in response, drift, accuracy, sensitivity to noise, or other characteristics of the Class 1 system which might impair the ability of the system to perform its safety functions.

Where plant equipment that is controlled by a Class 2 or 3 system is also controlled by signals from a lower class system, failures, or normal actions by the lower class system cannot prevent the higher class system from performing its function.

Where signals are extracted from Class 2 or 3 systems for use in lower class systems, isolation may not be required; however, good engineering practices are followed to prevent the propagation of faults. In cases where Class 2 systems need to take on the aspects of Class 1 systems due to the functions performed (i.e. Category A functions), isolation is used.

6 Isolation device design requirements

6.1 Requirements on isolation device application

6.1.1 Isolation device power

Isolation devices are classified as part of the safety system and are powered in accordance with the criteria of IEC 61513 if a power supply is necessary for the function. The power supply of the isolation device shall not be required for the device to perform its isolation function.

6.1.2 Maximum credible fault

Maximum credible fault (MCF) requirements shall be established by analysis of neighbouring circuits that are credible sources of the fault, either through inadvertent application from human error or through a fault or failure postulated to occur that involves proximate circuits, cabling, or terminations (e.g., a "hot short" from an adjacent conductor). The circuits that shall be analyzed depend on how the isolation device is used. The circuits could be within the same system, or may be in other systems.

The highest voltage to which the faulted side of the isolation device maybe exposed to shall determine the minimum voltage level that the device shall withstand. This voltage shall be applied across the faulted side terminals, and between the faulted side terminals and ground (see Figure 1). Transient voltages that may appear in the faulted side shall also be considered. Surge waveforms and characteristics shall be defined for the worst-case conditions expected at the installation.

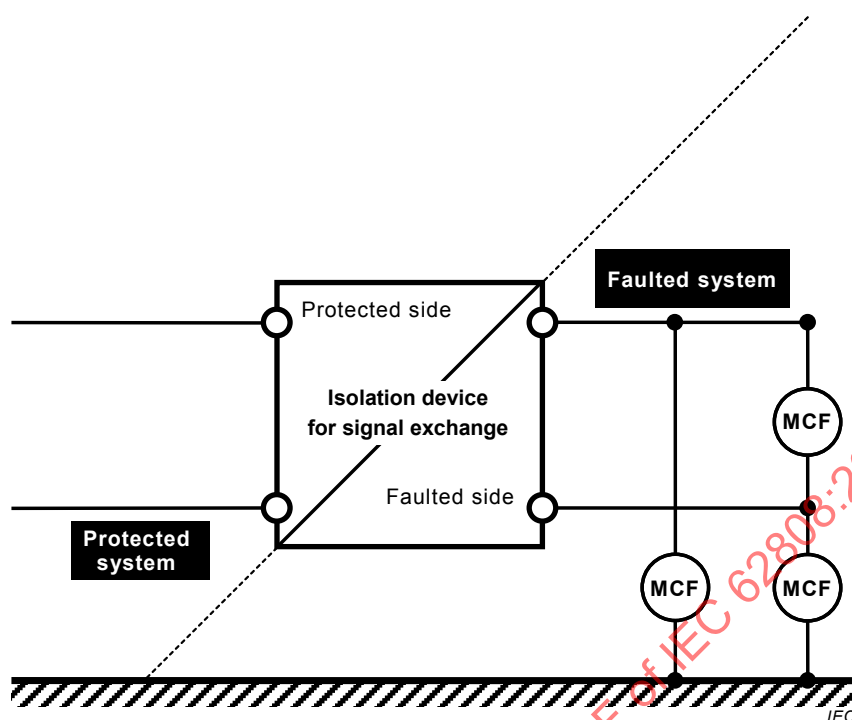


Figure 1 – Application of maximum credible fault

The MCF voltage shall be the highest AC or DC voltage present in an enclosure containing the conductors of the faulted side circuit of the isolation device, or in any proximate cable raceway which may collapse on to the raceway containing the lower class circuit of the isolation device. Where grounded metallic barriers separate the isolated circuit from higher voltages, those voltages may be excluded from consideration of the MCF provided that the barriers and grounding measures are designed to withstand the design basis hazards (induced vibrations due to design basis earthquakes or air plane crash, fire, etc.) for the plant.

In establishing the MCF voltage and current, the analysis shall include the consequences of flooding or fire causing a fault voltage to be introduced on a signal line from a proximate circuit or cable.

The available fault current for a direct short to ground shall be determined for each MCF source.

6.1.3 Energy limiting devices

Energy limiting devices (e.g. fuses for current or suppressors for voltage) may be used to limit the fault energy that must be dissipated in the isolation device or which may be available to be transferred to the protected circuits. In such cases, the energy limiting devices shall be considered to be part of the isolation device, even if they are separately packaged. Effective surveillance procedures shall be implemented to verify during plant operation that the energy limiting devices are properly in place and capable of performing their claimed role.

6.2 Requirements on isolation device design

6.2.1 Basic design requirements

The design of isolation devices conforms to IEC 61513 for:

- a) independence of redundant safety divisions, and
- b) independence between protection and control systems.

The isolation device shall include design features for which credit is taken (e.g., surge protectors or barriers) and shall identify the application limits of the device.

6.2.2 Postulated faults

The device shall be designed for postulated electrical faults or failures. The impact on the protected side for each fault shall be determined. As a minimum, the following faults shall be defined on the faulted side of the isolation device (see Figure 2):

- (a) short circuit to supply voltage if the isolation device is powered from the faulted side;
- (b1) short circuit between the faulted side terminals;
- (b2) short circuit between each faulted side terminal and ground;
- (c) open circuit of faulted side;
- (MCF) MCF between each faulted side terminal and ground;
- (MCF) MCF between faulted side terminals.

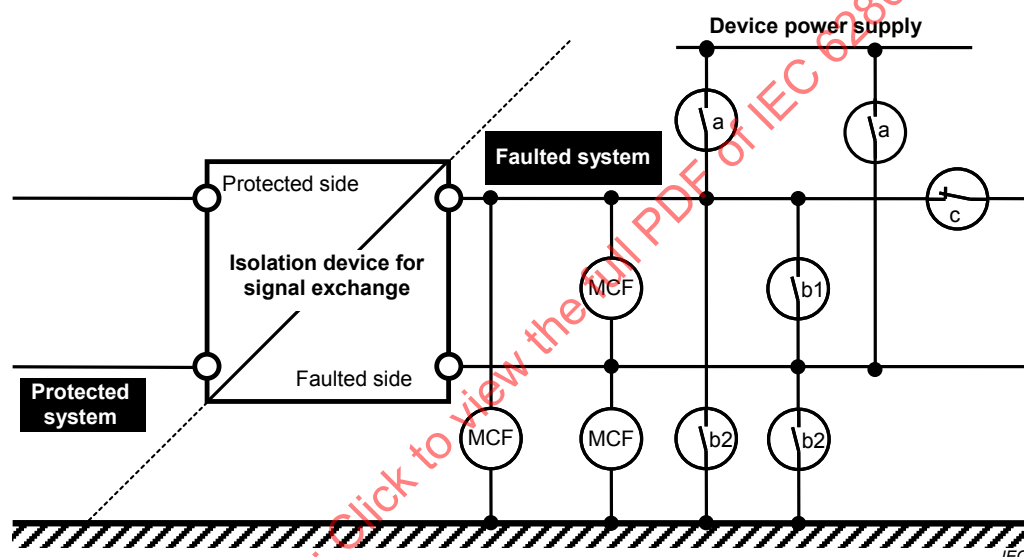


Figure 2 – Application of postulated fault

The specified MCF shall equal or exceed the application requirements. The device design shall accommodate the fault voltage and current waveforms and characteristics defined for the application. Appropriate industry standards shall be used as a basis for establishing the fault-transient exposure level (e.g. IEC TS 61000-6-5 or IEC 62003). The testing shall use the MCF as a basis for the test levels.

6.2.3 Physical component arrangement

The physical arrangement of components in the isolation device shall be configured to prevent, in the event of failure, the effects of shattered parts or material (e.g., solder spatter), fire, and smoke from breaching the isolation barrier.

Circuit terminals shall be arranged to permit the IEC 60709 specified separation distance between conductors associated with functions of different categories to be established as soon as practical. Minimum separation requirements do not apply for wiring and components within the isolation device; however, separation should be provided wherever practicable.

6.3 Power isolation devices

6.3.1 General

When the maximum credible voltage or current transient are applied to the faulted side of the power isolation device, the operation of the circuit on the protected side of that device will not be affected.

6.3.2 Circuit breaker tripped by fault currents

A circuit breaker automatically tripped by fault current is considered an isolation device, provided the following criteria are met:

- a) The breaker time-overcurrent trip characteristic for all circuit faults shall cause the breaker to interrupt the fault current prior to initiation of a trip of any upstream breaker. Periodic testing shall demonstrate that the overall coordination scheme remains within the limits specified in the design criteria. This testing may be performed as a series of overlapping tests.
- b) The power source shall supply the necessary fault current for sufficient time to ensure the proper coordination without loss of function of safety class loads. (For example, diesel generator excitation systems should be capable of providing the required transient current during faults.)
- c) The voltage on the protected side shall not degrade below an acceptable level.

6.3.3 Circuit breaker tripped by fault signals

A circuit breaker can be considered an isolation device provided it shall be automatically tripped by a signal generated within the same division as that to which the isolation device is applied. The time delay involved in generating the fault signal and tripping the breaker shall not cause unacceptable degradation of the safety power system.

6.3.4 Input current limiters

Devices that will limit the input current to an acceptable value under faulted conditions of the output are considered isolation devices. Periodic testing shall verify that the current-limiting characteristic has not been compromised or lost. Devices in this category may include inverters, regulating transformers, and battery chargers with current limiting characteristics.

6.3.5 Fuses

A fuse may be used as a power isolation device if the following criteria are met:

- a) Fuses shall provide the design overcurrent protection capability for the life of the fuse.
- b) The fuse time-overcurrent trip characteristic for all circuit faults shall cause the fuse to open prior to the initiation of an opening of any upstream interrupting device.
- c) The power source shall supply the necessary fault current to ensure the proper coordination without loss of function of safety loads.

The effects of single-phasing shall be considered for three-phase AC circuits.

7 Qualification test requirements

7.1 General

Qualification of isolation devices shall be based on a combination of design analysis and qualification testing. Clause 7 addresses the testing portion of the qualification. The objective of the testing is to validate the results of the analysis at the extremes of fault conditions.

7.2 Requirements on the test method

7.2.1 Test specification

A specification shall be prepared for the specific testing that is to be performed for each type of isolation device. The test specification should include elementary or schematic diagrams as necessary to describe the test configuration and how the MCF and surges shall be applied to the devices during the test. The basis for the set of postulated electrical faults and failures shall be documented or referenced in the test program.

A specific definition of pass/fail acceptance criteria for each type of device shall be provided. This shall include justification that the pass/fail acceptance criterion is sufficient to evaluate the safety system performance, and to demonstrate that the tested device meets the requirements of IEC 61513 and IEC 60709 when used in the system. In particular, the following points shall be included:

- The maximum credible voltage or current transient applied to the faulted side of the device shall not degrade below an acceptable level (i.e. to prevent the safety function) the operation of the circuit connected to the protected side of the device.
- Shorts, grounds, or open circuits occurring in the faulted side shall not degrade below an acceptable level the circuit connected to the protected side of the device.
- Transient voltages that may appear in the faulted side circuit (e.g., surges) should also be considered.
- The qualification shall consider the levels and duration of the fault current on the faulted side of the device.

For isolation between systems of different classes, during and following the application of the MCF or surge test, there shall be no degradation or distortion of the isolation device input that would have a detrimental effect on the performance of the safety system. For isolation of redundant safety circuits, there shall be no degradation or distortion of the redundant channel that would have a detrimental effect on the performance of the safety system.

Applicable industry standards shall be used as the basis for performing the qualification testing (e.g. IEC TS 61000-6-5 or IEC 62003). The testing shall use the MCF as a basis for the test levels.

7.2.2 Testing energy limiting devices

When the isolation device contains devices that limit the energy (e.g. fuses or suppressors), the qualification testing shall include cases where the applied voltage and current is less than that necessary to activate the limiting devices in addition to testing at worst case conditions where the limiting devices will become active.

7.2.3 Qualification test environment

Qualification of isolation devices shall be carried out on samples prior to installation. Testing entails applying the postulated faults to the faulted side terminals and recording the electrical signals and observing the physical integrity at the protected side terminals. Any disturbance that is seen shall be evaluated to determine if there would be an effect on the safety system. If an evaluation cannot demonstrate that the safety system would not be affected, testing shall be repeated with the device connected to the safety system equipment for all the configurations where the device is intended to be used. The performance of the system shall be monitored to demonstrate operability throughout the test. Requirements for testing the device in the system are provided in 7.3.

7.3 Application specific testing

7.3.1 General

Devices might be used either for isolation of safety circuits from lower class circuits or for isolation of redundant safety divisions. For qualification testing, the detailed device configuration depends on the objective of the isolation and the specific type and configuration of the isolation.

The MCF represents the application of the maximum credible AC and DC voltages and currents that are applied to the device in common and differential modes that exist based on the installation of the device. Common mode refers to faults between both signal terminals and a common reference plane (ground) and causes the potential of both sides of the transmission path to be changed simultaneously and by the same amount relative to the common reference plane (ground). Differential mode refers to faults between the signal terminals that cause the potential of one side of the signal transmission path to be changed relative to the other side. The mode of application shall satisfy the following guidelines for test configurations.

7.3.2 Isolation of safety circuits from lower class circuits

MCFs and surges shall be applied between the faulted side terminals of the (lower class) circuits (differential mode) and between any faulted side terminal and ground (common mode).

MCFs and surges shall be applied to any power terminals that provide power to the faulted side of the isolation device.

The protected side terminals shall be monitored to ensure that no unacceptable interactions (degradations or distortions) between lower class and safety circuits would occur.

7.3.3 Isolation between redundant safety circuits

MCFs shall be applied between the faulted side terminals (differential mode) and between any faulted side terminal and ground (common mode); the other side shall be monitored to ensure that no unacceptable interactions (degradations or distortions) between redundant safety circuits will occur.

If the isolation device performs its protective function in two directions, the MCF shall be applied separately on both sides.

MCFs shall be applied to the isolation device for a sufficient duration to allow any measurable effects to occur on the isolation device and to allow monitored values or effects to reach steady-state.

7.4 Documentation of test requirements and results

The test specification and acceptance criteria shall be documented in advance of the test.

Test data and results shall be documented to verify that the design basis faults, including short circuits, open circuits, grounds, MCF, and surge were applied to the device in all of the applicable connection modes (i.e. applicable input, output, power, and ground connection modes).

Test data and results shall verify that the test acceptance criteria are met.

Bibliography

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

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

IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

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

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

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

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

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

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 Safety Standard Series No. SSR-2/1:2012, *Safety of Nuclear Power Plant: Design*

IAEA Safety Guide NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

IAEA Safety Glossary:2007, *Terminology used in nuclear safety and radiation protection*

IECNORM.COM : Click to view the full PDF of IEC 62808:2015

SOMMAIRE

AVANT-PROPOS	19
INTRODUCTION	21
1 Domaine d'application	24
2 Références normatives	24
3 Termes et définitions	24
4 Symboles et abréviations	25
5 Principes généraux portant sur les appareils d'isolement	25
5.1 Généralités	25
5.2 Caractéristiques d'isolement	26
5.3 Mise en service prioritaire	27
6 Exigences de conception pour les appareils d'isolement	28
6.1 Exigences portant sur l'utilisation des appareils d'isolement	28
6.1.1 Appareils d'isolement de puissance	28
6.1.2 Défaut maximal prévisible	28
6.1.3 Appareils de limitation d'énergie	29
6.2 Exigences portant sur la conception des appareils d'isolement	29
6.2.1 Exigences de dimensionnement	29
6.2.2 Défauts hypothétiques	29
6.2.3 Disposition physique des composants	30
6.3 Appareils d'isolement de puissance	30
6.3.1 Généralités	30
6.3.2 Disjoncteur déclenché par courant de défaut	30
6.3.3 Disjoncteur déclenché par signal de commande d'ouverture	31
6.3.4 Limiteurs de courant d'entrée	31
6.3.5 Fusibles	31
7 Exigences d'essais de qualification	31
7.1 Généralités	31
7.2 Exigences portant sur les méthodes d'essai	31
7.2.1 Spécification des essais	31
7.2.2 Essais des appareils de limitation d'énergie	32
7.2.3 Essais de qualification environnementale	32
7.3 Réalisation d'essais particuliers	33
7.3.1 Généralités	33
7.3.2 Isolement entre les circuits de sûreté et les circuits de classe de sûreté inférieure	33
7.3.3 Isolement entre circuits de sûreté redondants	33
7.4 Documentation des exigences et des résultats d'essai	33
Bibliographie	35
Figure 1 – Application du principe de DMP	28
Figure 2 – Application du défaut hypothétique	30

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES
D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE
IMPORTANTS POUR LA SÛRETÉ –
CONCEPTION ET QUALIFICATION DES APPAREILS D'ISOLEMENT**

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 62808 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et électriques des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/1004/FDIS	45A/1019/RVD

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

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

Le comité a décidé que le contenu de cette publication 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 à la publication recherchée. A cette date, la publication sera

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

IECNORM.COM : Click to view the full PDF of IEC 62808:2015

INTRODUCTION

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

Il est nécessaire que les systèmes d'I&C (instrumentation et contrôle-commande) importants pour la sûreté nucléaire tolèrent les effets induits par les défauts des matériels ou de l'installation, comme ceux liés aux risques internes ou externes. L'IEC 60709 fournit des exigences pour assurer l'indépendance entre les parties redondantes des systèmes de sûreté, et entre les systèmes de sûreté et les systèmes de classes de sûreté inférieures. Parmi les techniques disponibles pour améliorer le niveau de tolérance des systèmes d'I&C se trouve la mise en œuvre d'appareils d'isolement au niveau des connexions faites entre les divisions redondantes des matériels de sûreté ou entre les matériels de sûreté et les systèmes de classe de sûreté inférieures. La présente norme fournit des exigences et des recommandations portant sur la conception et la qualification des appareils d'isolement qui sont requis par l'IEC 60709. La présente norme traite des critères et des méthodes utilisés pour assurer que la conception des appareils d'isolement garantit que des défaillances crédibles dans les canaux connectés et appartenant à des classes de sûreté inférieures, ou dans des canaux redondants n'empêcheront pas les systèmes de sûreté de remplir les fonctions exigées. L'emploi d'appareil d'isolement peut être nécessaire à l'intérieur des systèmes au niveau des interfaces signal ou puissance.

Des recommandations pour d'autres aspects pertinents pour la qualification des appareils d'isolement (par exemple la compatibilité électromagnétique, la qualification environnementale ou aux séismes) peuvent être trouvées dans l'IEC 60780.

L'objet de la présente norme est:

- à l'Article 5: d'établir les critères de base pour la recette de la qualification et pour l'utilisation des appareils;
- à l'Article 6: d'établir les exigences de conception pour choisir et pour utiliser les appareils d'isolement adaptés;
- à l'Article 7: d'établir les exigences portant sur les essais de qualification à réaliser pour valider la pertinence de la conception des appareils d'isolement.

L'objectif de la présente norme est d'être utilisée par les exploitants de centrales nucléaires, les concepteurs d'équipement et de système d'I&C nucléaires, les évaluateurs de système et par les régulateurs.

b) Position de la présente norme dans la collection de normes du SC 45A de l'IEC

L'IEC 62808 est le document du SC 45A de l'IEC de troisième niveau qui traite des appareils d'isolement.

L'IEC 60709 est directement référencée par l'IEC 61513 pour ce qui est de la séparation physique et électrique exigée entre les sous systèmes des différents trains de sûreté des systèmes d'I&C importants pour la sûreté, et entre les systèmes d'I&C importants pour la sûreté et ceux qui ne sont pas importants pour la sûreté.

L'IEC 61226 établit les principes de catégorisation des fonctions, des systèmes et des matériels d'I&C suivant leurs niveaux d'importance pour la sûreté. Elle demande qu'une séparation adaptée soit mise en place entre les fonctions des différentes catégories. L'IEC 61226 fait référence à l'IEC 60709 en tant que norme traitant des exigences de séparation.

L'IEC 62808 a pour objectif de fournir des exigences et des recommandations pour la conception et la qualification des appareils d'isolement qui sont identifiés dans l'IEC 60709 comme étant des moyens permettant de garantir l'indépendance entre les systèmes lorsque des signaux produits par un système doivent être utilisés par des systèmes

de classes de sûreté inférieures, ou entre des sous systèmes indépendants de même classe de sûreté.

Pour plus de détails sur la collection de normes du SC 45A de l'IEC, voir le point d) de cette introduction.

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

L'IEC 60709 est applicable pour les systèmes et matériels d'I&C importants pour la sûreté. Elle établit des exigences portant sur la séparation physique et électrique qui est un moyen pour assurer l'indépendance entre les fonctions réalisées par ces systèmes et ces matériels. L'IEC 60709 demande à ce que des appareils d'isolement soient utilisés lorsque des connexions doivent être établies entre des systèmes indépendants. L'IEC 62808 fournit les critères pour l'analyse et la qualification d'aptitude de l'appareil d'isolement.

Un critère fondamental concernant les appareils d'isolement est qu'ils soient couverts par et conçus suivant les normes pertinentes pour les systèmes de la classe de sûreté la plus élevée pour lesquels ils assurent une protection contre des risques. Les exigences supplémentaires portant sur la conception et la qualification des appareils d'isolement considérés comme composant d'un système de sûreté ne sont pas couvertes par cette 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)

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

L'IEC 61513 fait 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, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la norme IEC 61513, un ensemble documentaire cohérent.

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

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

L'IEC 61513 a adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est 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, pour ce qui concerne le domaine de la sûreté nucléaire. Dans ce domaine, l'IEC 60880 et l'IEC 62138 correspondent à l'IEC 61508-3 pour le secteur nucléaire. L'IEC 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires.

et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle-commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

NOTE Il est fait l'hypothèse que pour la conception des systèmes d'I&C des centrales nucléaires 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, dont les exigences sont comparables à des normes telles que l'IEC 61508.

IECNORM.COM : Click to view the full PDF of IEC 62808:2015

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈMES D'INSTRUMENTATION ET DE CONTRÔLE-COMMANDE IMPORTANTES POUR LA SÛRETÉ – CONCEPTION ET QUALIFICATION DES APPAREILS D'ISOLEMENT

1 Domaine d'application

La présente Norme internationale établit des exigences pour la conception, les analyses et la qualification des appareils d'isolement utilisés pour garantir l'indépendance électriques entre les circuits des systèmes de sûreté redondants ou entre les circuits des systèmes de sûreté et des systèmes dont la classe de sûreté est inférieure, comme spécifié dans l'IEC 60709. La présente norme comprend des recommandations portant sur la détermination du défaut maximal prévisible qui est pris en compte pour les appareils d'isolement. Le défaut maximal prévisible peut être utilisé comme une base pour le niveau des essais définis à partir d'autres normes (par exemple l'IEC TS 61000-6-5 ou l'IEC 62003).

La présente norme ne couvre pas les questions de sûreté ou de DCC relatives aux interdépendances fonctionnelles et aux interférences ou DCC potentielles fonctionnelles qui pourraient survenir du fait d'échange ou de partage de signaux entre systèmes ou sous systèmes. Elle ne couvre pas non plus les questions de conception et de qualification propres à la logique programmable ou programmée embarquée dans les appareils d'isolement. Pour les appareils d'isolement embarquant de la logique programmable ou programmée, des exigences supplémentaires de conception et de qualification doivent être prises en compte; ces exigences sont hors du domaine de la présente norme.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation*

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

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

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

3 Termes et définitions

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

3.1 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 2007: "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 la présente norme.

3.2

défauts électriques de mode commun

défauts de tension ou de courant survenant entre des bornes de raccordement du signal et une référence de masse commune (terre)

Note 1 à l'article: Il convient de ne pas confondre ces défauts avec les DCC (défaillance de cause commune).

Note 2 à l'article: Cela entraîne une modification simultanée de même niveau de la tension des bornes en fonction de la référence de tension commune (terre).

3.3

défauts électriques de mode différentiel

défauts de tension ou de courant survenant entre signaux

3.4

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

Note 1 à l'article: Comme il est indiqué dans l'IEC 60709, ces dysfonctionnements peuvent être produits par des défauts ou des actions normales.

3.5

défaut maximal prévisible

DMP

tension ou courant transitoire qui peut être atteint au niveau des circuits, définis par essai ou par analyse, prenant en compte la localisation du circuit, les cheminements et les interconnexions combinées avec les défaillances prévisibles du fait du retour d'expérience qui peuvent survenir sur le circuit et les circuits adjacents

Note 1 à l'article: L'évaluation doit prendre en compte les conséquences d'inondations et de phénomènes sismiques.

4 Symboles et abréviations

CA	courant alternatif
DCC	défaillance de cause commune
CC	courant continu
IME	interférence électromagnétique
I&C	instrumentation et contrôle-commande
DMP	défaut maximal prévisible
CNP	centrale nucléaire de puissance

5 Principes généraux portant sur les appareils d'isolement

5.1 Généralités

L'IEC 60709 fournit des exigences relatives à l'utilisation des appareils d'isolement. L'Article 5 en fait un résumé et introduit des exigences supplémentaires pour les appareils d'isolement. Le mot «doit» identifie les exigences supplémentaires.

Les appareils d'isolement utilisés au niveau des interfaces entre les systèmes d'I&C importants pour la sûreté ou entre les circuits à l'intérieur de système important pour la sûreté peuvent avoir un impact au niveau de l'intégrité de la conception d'ensemble et en particulier au niveau de la défense en profondeur. Lorsqu'on utilise des appareils d'isolement, on peut s'appuyer sur ceux-ci pour assurer un isolement électrique entre des fonctions de sûreté redondantes ou entre des fonctions de sûreté situées dans différents niveaux de défense de l'architecture d'ensemble. En général, il convient de considérer l'introduction de telles interfaces entre des systèmes avec précaution et en prenant en compte les principes et approches mis en avant dans l'IEC 61513. Une analyse systématique des défaillances au niveau système et au niveau de l'architecture d'ensemble d'I&C est nécessaire. Du fait des interfaces au niveau signal des interdépendances fonctionnelles sont introduites entre les systèmes et leurs modes de défaillance associés doivent être pris en compte avec précaution.

Lorsque des signaux sont transmis entre un système ou un matériel de Classe 1 (réalisant des fonctions de Catégorie A) et des systèmes d'une classe de sûreté inférieure, la transmission de ces signaux se fait par le truchement d'appareils d'isolement qui sont intégrés dans le système de classe de sûreté plus élevée. Si des défaillances surviennent ou des conditions apparaissent au niveau des bornes de raccordement de sortie des appareils d'isolement (qui sont connectées au système de classe de sûreté inférieure) les actions de sûreté lancées par le système ou le sous système de Classe 1 auquel l'appareil d'isolement est connecté ne peuvent pas être impactées. Un exemple de cela est un circuit qui réalise une fonction de Catégorie A qui peut être surveillé à l'aide d'un circuit appartenant à une classe de sûreté inférieure, utilisant une bobine de relaying du système de Classe 1 et le contact d'un relai du système de classe de sûreté inférieure.

Les appareils d'isolement doivent aussi être utilisés lorsque des signaux sont transmis entre systèmes de Classe 1 indépendants et entre des canaux d'équipements redondants de systèmes de Classe 1.

Lorsque des signaux sont transmis à partir de systèmes de Classe 2 ou 3 pour être utilisés dans des systèmes de classe de sûreté inférieure, ou bien entre des sous systèmes indépendants dans ces classes, l'utilisation d'appareils d'isolement peut ne plus être exigée; cependant, de bonnes pratiques d'ingénierie sont suivies pour empêcher la propagation des défauts. Lorsque des systèmes de Classe 2 ont besoin de prendre en compte des aspects propres aux systèmes de Classe 1 du fait des fonctions réalisées, le principe d'isolement est appliqué. Par exemple, un système de Classe 2 réalise une fonction de Catégorie B en support d'un système de Classe 1 réalisant une fonction de Catégorie A pour protéger d'un même défaut.

Des branchements temporaires à des fins de maintenance des systèmes réalisant des fonctions de Catégorie A sans utilisation d'appareils d'isolement sont autorisés à condition qu'ils soient connectés uniquement sur une redondance à un instant donné, qu'ils soient débranchés après utilisation et que le système soit capable de résister à un défaut introduit du fait d'une défaillance ou de l'utilisation de la connexion.

NOTE La présente norme traite les appareils d'isolement comme des appareils autonomes, séparés des équipements réalisant les fonctions de sûreté. L'appareil d'isolement peut être une partie d'un module ou d'un équipement réalisant une fonction de sûreté. Au niveau d'autres conceptions, l'appareil d'isolement peut appartenir à plusieurs modules (par exemple une partie prenant en charge des transitoires de surtension rapides et une autre des tensions statiques). La présente norme est aussi applicable pour ces différences de conception,

5.2 Caractéristiques d'isolement

L'appareil d'isolement doit être capable d'isoler par rapport aux conditions de défaillance suivantes:

- a) courts-circuits entre bornes de raccordement ou avec la terre;
- b) ouverture de circuit;
- c) application de la tension maximale de CA ou de CC qui peut être raisonnablement prévue, en prenant en compte les sources et tensions présentes dans les systèmes de Classe 1 et ceux n'appartenant pas à la Classe 1; et

d) interférences électromagnétiques et électrostatiques.

Si l'équipement peut produire d'autres signaux en condition de défaillance, tels que des échelons ou d'autres formes de signaux oscillatoires, l'appareil d'isolement doit être capable de fournir un niveau d'isolement acceptable par rapport à de tels signaux.

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

- la tolérance et l'isolement aux transitoires électriques tels que définis dans l'IEC TS 61000-6-5;
- la tolérance et l'isolement pour les IME conformément à l'IEC TS 61000-6-5;
- celles de barrières physiques simples entre les bornes de raccordement voisines ou proches ou les groupes de contacts sur les équipements de relayage utilisés pour l'isolement électrique; et
- la prévention de la transmission des tensions et/ou des courant excessivement élevés ou pouvant provoquer des dommages.

Dans ce contexte, une évaluation du défaut maximal prévisible qui pourrait être pris en compte doit être réalisée pour des conditions normales et en présence de défaillances et des effets possibles sur les équipements importants pour la sûreté, s'il est appliqué aux bornes de l'appareil d'isolement du circuit appartenant à une classe de sûreté inférieure.

Des précautions sont aussi à prendre pour minimiser la possibilité qu'une défaillance d'un système qui n'est pas de Classe 1 n'entraîne le déclenchement intempestif ou prématuré d'une fonction de Catégorie A.

5.3 Mise en service prioritaire

Lorsque la mise en service d'équipements qui est commandée par un système de Classe 1 est aussi commandée par un système de classe de sûreté inférieure, des appareils sont mis en œuvre pour garantir la priorité des commandes du système de Classe 1 sur celle des systèmes de classe de sûreté inférieure. Le fonctionnement normal ou les défaillances des systèmes de catégories inférieures ne peuvent pas interférer avec fonctions de Catégorie A, lorsque les conditions de l'installation nécessitent la réalisation de ces fonctions de Catégorie A. L'équipement réalisant la fonction de gestion des priorités est de Classe 1. Le circuit qui assure l'isolement nécessaire peut être dans le même système ou peut être dans d'autres systèmes.

Les défaillances et les dysfonctionnements des systèmes n'appartenant pas à la Classe 1 ne peuvent pas altérer les réponses du système de Classe 1 au niveau décalage, précision, sensibilité au bruit ou d'autres caractéristiques du système de Classe 1 qui pourraient dégrader l'aptitude du système à réaliser ses fonctions de sûreté.

Lorsque des équipements de tranche sont commandés par des systèmes de Classe 2 ou 3 et qu'ils sont aussi commandés par des signaux provenant de systèmes de classes de sûreté inférieures, le fonctionnement normal ou les défaillances des systèmes de classe inférieure ne peuvent pas empêcher les systèmes de classe supérieure de réaliser leurs fonctions.

Lorsque des signaux sont pris sur des systèmes de Classe 2 ou 3 pour être utilisés dans les systèmes de classe de sûreté inférieure, l'isolement peut ne pas être requis; cependant, de bonnes pratiques d'ingénierie sont suivies pour empêcher la propagation des défauts. Si des systèmes de Classe 2 prennent en compte des aspects propres aux systèmes de Classe 1 du fait des fonctions à réaliser (par exemple des fonctions de catégorie A), le principe d'isolement est appliqué.

6 Exigences de conception pour les appareils d'isolement

6.1 Exigences portant sur l'utilisation des appareils d'isolement

6.1.1 Appareils d'isolement de puissance

Les appareils d'isolement sont classés en les considérant comme faisant partie du système de sûreté et ils sont alimentés en respectant les critères de l'IEC 61513 si une alimentation de puissance est nécessaire pour la fonction. L'alimentation de puissance de l'appareil d'isolement ne doit pas être nécessaire pour que l'appareil s'acquitte de sa fonction d'isolement.

6.1.2 Défaut maximal prévisible

Les exigences portant sur le défaut maximal prévisible (DMP) doivent être établies à partir de l'analyse des circuits environnants qui peuvent être des origines prévisibles du défaut, ou bien du fait d'utilisation par inadvertance due à l'erreur humaine ou du fait de défauts ou de défaillances hypothétiques qui impliquent les circuits, câblage ou borniers proches (par exemple court-circuit avec une borne de raccordement voisine). Les circuits qui doivent faire l'objet de l'analyse dépendent du mode d'utilisation de l'appareil d'isolement. Les circuits peuvent être dans les mêmes systèmes ou dans des systèmes différents.

La tension la plus haute à laquelle le côté en défaut peut être exposé doit déterminer la tension minimale à laquelle l'appareil doit résister. Cette tension doit être appliquée au niveau des bornes de raccordement du côté en défaut, et entre les bornes de raccordement du côté en défaut et la terre (voir la Figure 1). Les transitoires affectant la tension qui peuvent apparaître au niveau du côté en défaut doivent aussi être pris en compte. Les ondes sinusoïdales et leurs caractéristiques doivent être définies pour les pires des conditions prévues à l'installation.

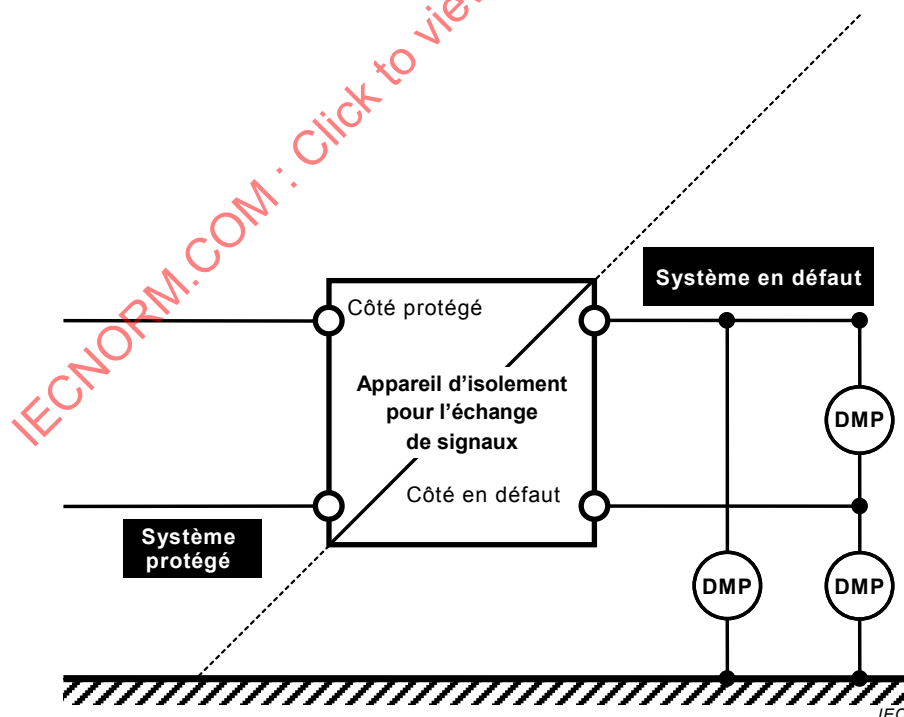


Figure 1 – Application du principe de DMP

La tension de DMP doit être la plus élevée des tensions en CA ou en CC présentes au niveau du volume clos contenant les conducteurs appartenant au circuit du côté en défaut de l'appareil d'isolement, ou situés dans n'importe quel chemin de câbles proche qui peut s'effondrer sur le chemin de câbles contenant les circuits de l'appareil d'isolement appartenant

à une classe de sûreté inférieure. Si des barrières métalliques mises à la terre séparent le circuit isolé de tensions plus élevées, ces tensions peuvent ne pas être prises en compte au niveau du DMP si ces barrières et ces mesures de mise à la terre sont conçues pour résister aux événements de dimensionnement de l'installation (induits par les vibrations produites par les séismes ou les accidents d'avion, les incendie, etc., pris en compte pour le dimensionnement).

Pour déterminer la tension et le courant de DMP, l'analyse doit prendre en compte les conséquences des inondations et des incendies qui entraînent l'apparition de défauts de tension sur les câbles signal provenant de circuits ou de câbles proches.

Le courant de défaut disponible pour une mise en court-circuit avec la terre doit être déterminé pour chaque source de DMP.

6.1.3 Appareils de limitation d'énergie

Des appareils de limitation d'énergie (par exemple fusibles pour les courants ou surtenseurs) peuvent être utilisés pour limiter les défauts énergétiques qui doivent être dissipés au niveau de l'appareil d'isolement ou qui peuvent être disponibles pour être transmis aux circuits protégés. Dans ces cas là, les dispositifs de limitation d'énergie doivent être considérés comme faisant partie de l'appareil d'isolement, même s'ils sont conditionnés à l'écart. Des procédures de surveillance efficaces doivent être mises en place pour vérifier au cours de l'exploitation de l'installation que les dispositifs de limitation d'énergie sont correctement en place et capables de tenir le rôle prévu.

6.2 Exigences portant sur la conception des appareils d'isolement

6.2.1 Exigences de dimensionnement

La conception des appareils d'isolement est conforme à l'IEC 61513 en ce qui concerne:

- a) l'indépendance des divisions de sûreté, et
- b) l'indépendance entre les systèmes de protection et de commande.

Les appareils d'isolement doivent comprendre des caractéristiques de conception qui leur permettent de garantir qu'ils assureront leurs fonctions (par exemple protecteurs contre les ondes de chocs ou des barrières) et les limites de l'utilisation des appareils d'isolement doivent avoir été identifiées.

6.2.2 Défauts hypothétiques

Les appareils doivent être conçus en fonction des défauts et des défaillances électriques hypothétiques. L'impact sur le côté protégé doit être déterminé pour chaque défaut. Au minimum, les défauts suivant doivent être définis au niveau du côté en défaut de l'appareil d'isolement (voir la Figure 2):

- (a) court-circuit sur la tension d'alimentation si l'appareil d'isolement est alimenté du côté en défaut;
- (b1) court-circuit entre bornes de raccordement du côté en défaut;
- (b2) court-circuit entre borne de raccordement du côté en défaut et la terre;
- (c) ouverture du circuit côté en défaut;
- (DMP) DMP entre chaque borne de raccordement côté en défaut et la terre;
- (DMP) DMP entre bornes de raccordement côté en défaut.



6.2.3 Disposition physique des composants

Les bornes des circuits doivent être disposées pour permettre la définition aussitôt que pratiquement possible des distances de séparation des conducteurs associés à des fonctions de différentes catégories telles que spécifiées dans l'IEC 60709. Les exigences de séparation minimale pour le câblage et la disposition interne des composants dans l'appareil d'isolement ne s'appliquent pas; cependant, il convient d'assurer la séparation partout où cela est pratiquement possible.

6.3.1 Généralités

6.3.2 Disjoncteur déclenché par courant de défaut

a) Les caractéristiques temporelles d'ouverture du dispositif de protection en surcharge de courant doivent pour tous les défauts du circuit être telles que le disjoncteur coupe le courant en défaut avant que l'ouverture des disjoncteurs en amont ne se déclenche. Des essais périodiques doivent démontrer que le schéma de coordination d'ensemble s'inscrit