IEC 62808

Edition 1.0 2015-05

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

IEC 62808:2015-05(en-fr)

About the IEC

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

About IEC publications

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

IEC Catalogue - webstore.iec.ch/catalogue

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

IEC publications search - 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 It also gives information on projects, replaced and withdrawn publications.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.

IEC 62808

Edition 1.0 2015-05

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

CONTENTS

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.

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.

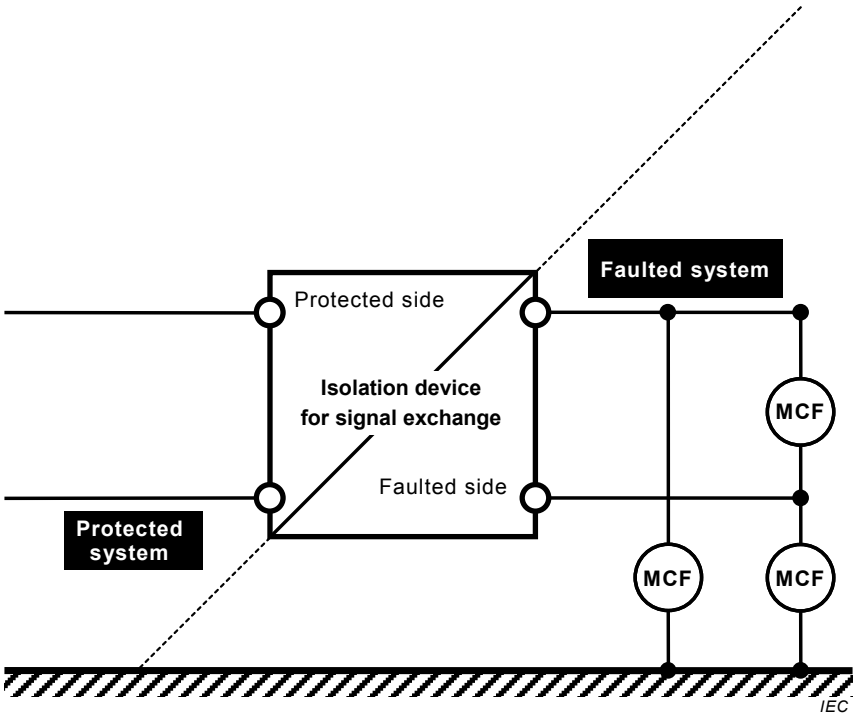

Figure 1 – Application of maximum credible fault

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.