BRITISH STANDARD

BS EN
60709:2010

Nuclear power plants — Instrumentation and control systems important to safety — Separation

ICS 27.120.20

BSI
British Standards

National foreword

This British Standard is the UK implementation of EN 60709:2010. It is identical to IEC 60709:2004. It supersedes BS IEC 60709:2004, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee NCE/8, Reactor instrumentation.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 10 November 2004

ISBN 978 0 580 68113 4

Amendments/corrigenda issued since publication

Date	Comments
31 August 2010	This corrigendum renumbers BS IEC 60709:2004 as BS EN 60709:2010

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60709

May 2010

ICS 27.120.20

English version

Nuclear power plants - Instrumentation and control systems important to safety - Separation

(IEC 60709:2004)

Centrales nucléaires de puissance - Systèmes d'instrumentation et de contrôle commande importants pour la sûreté - Séparation
(CEI 60709:2004)

Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Physikalische und elektrische Trennung
(IEC 60709:2004)

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 60709:2010 E

Foreword

The text of the International Standard IEC 60709:2004, prepared by SC 45A, Instrumentation and control of nuclear facilities, of IEC TC 45, Nuclear instrumentation, was submitted to the CENELEC formal vote for acceptance as a European Standard and was approved by CENELEC as EN 60709 on 2010-05-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2011-05-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-05-01

Annex ZA has been added by CENELEC.

As stated in the nuclear safety Directive 2009/71/EURATOM, Chapter 1, Article 2, item 2, Member States are not prevented from taking more stringent safety measures in the subject-matter covered by the Directive, in compliance with Community law. In a similar manner, this European Standard does not prevent Member States from taking more stringent nuclear safety measures in the subject-matter covered by this European Standard.”

_____

Endorsement notice

The text of the International Standard IEC 60709:2004 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION 4
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 General principles for separation within I&C systems important to safety 9
4.1 General 9
4.2 Design errors 10
4.3 I&C system failure events 10
4.3.1 Single random failure 10
4.3.2 Multiple failures from a single common cause 10
4.4 Plant failure events 11
4.4.1 Environmental conditions 11
4.4.2 Electromagnetic interference 11
4.4.3 Failure of plant systems, equipment or structures 11
4.4.4 Operator error 11
4.5 External failure events 11
4.5.1 Natural events 11
4.5.2 External man-made causes 12
4.6 Special operating conditions 12
4.7 Separation issues at existing plants 12
5 Design basis 13
5.1 Fire protection 13
5.2 Environmental conditions during and after accidents 13
5.3 Isolation devices 13
5.3.1 General 13
5.3.2 Isolation characteristics 14
5.3.3 Actuation priority 14
5.4 Independence from control systems 14
6 Requirements for cabling separation 16
6.1 General requirement 16
6.2 Separation 16
6.2.1 Separation of redundant cables inside the I&C system important to safety 16
6.2.2 Lesser separation distances 16
6.2.3 Associated circuits 17
6.2.4 Separation of system cables of different safety categories 18
6.2.5 Separation of signal cables from power cables 18
6.2.6 Separation of cables from tubes or pipes 18
6.2.7 General routing considerations 18
6.2.8 Control room cabinets, desks, panels and related cables 18
6.3 Thermal and physical protection 20
6.4 Fire protection 20
6.5 Identification 20
Annex ZA (normative) Normative references to international publications with their corresponding European publications 21

INTRODUCTION

Background, main issues and organization of the standard

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

The object of this standard is as follows:

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

– in Clause 5, to establish design basis criteria for I&C systems important to safety that take the causes of failure identified in Clause 4 into consideration;

– in Clause 6, to give requirements to be fulfilled for cabling separation within an I&C system important to safety.

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

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

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

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

Recommendations and limitations regarding the application of the Standard

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

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

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

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

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

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

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

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508-1, -2 and -4, for the nuclear application sector. Compliance with this standard will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

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

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

This page deliberately set blank

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

1 Scope

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

3.2
barrier
device or structure interposed between redundant equipment or circuits important to safety, or between equipment or circuits important to safety and a potential source of damage to limit damage to the I&C system important to safety to an acceptable level

3.3
cable route
physical pathway through the plant along which multiple cables can be laid, such as through a room or duct in the plant building, or a metal duct, tray, or tube, or a duct below or gantry over roads

3.4
common cause failure (CCF)
failure of two or more structures, systems or components due to a single specific event or cause

[IAEA NS-G-1.3]

3.5
isolation device
device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits

3.6
postulated initiating event (PIE)
event identified during design as capable of leading to anticipated operational occurrences or accident conditions

[IAEA NS-G-1.3]

3.7
redundancy
provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other

[IAEA NS-G-1.3]

3.8
safety group
assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

[IAEA NS-G-1.3]

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

4.1 General

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

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

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

– Systems performing category A functions shall be protected from consequential physical effects caused by faults and normal actions within

  a) redundant parts of those systems, and

  b) systems of a lower category.

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

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

– Systems performing category B functions shall be protected from consequential physical effects caused by faults and normal actions within

  a) redundant parts of those systems, and

  b) systems of a lower category.

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

– Certain systems performing category C functions may need to be protected from the influences of faults in other systems. This shall be determined on a case-by-case basis.

– Un-categorised systems need not be protected from influences of faults in other systems.

Separation prevents

a) propagation of failures from system to system,

b) propagation of failures between redundant parts within systems,

c) common cause failures due to common internal plant hazards.

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

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

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

4.2 Design errors

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

4.3 I&C system failure events

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

4.3.1 Single random failure

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

4.3.2 Multiple failures from a single common cause

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

4.4 Plant failure events

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

4.4.1 Environmental conditions

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

4.4.2 Electromagnetic interference

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

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

4.4.3 Failure of plant systems, equipment or structures

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

4.4.4 Operator error

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

4.5 External failure events

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

4.5.1 Natural events

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

4.5.2 External man-made causes

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

4.6 Special operating conditions

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

4.7 Separation issues at existing plants

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

– the civil structures or physical space available at the plant may not allow the required separation. Physical constraints should be reviewed in locating the upgraded I&C systems;

– the major weaknesses of existing I&C shall be identified with respect to both existing separation and safety improvements possible through upgrading;

– the existing separation, or feasible improvements of separation, shall be evaluated through a systematic methodology, recognising particular strengths or alternatives to the requirements of this standard;

– an alternative set of separation rules may be established, recognising and justifying existing conditions proven through records of plant operation;

– alternative technologies shall be presented and evaluated in the case of special plant situations; e.g. through use of barriers, optical cabling, distribution of the I&C systems.

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

– separation in intermediate configurations when new I&C is installed through a phased programme;

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

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

– cable routing limits and an evaluation of the needs coming from new technologies for special cable trays for fibre optic cables, bus cables and requirements for separation.

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

5 Design basis

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

5.1 Fire protection

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

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

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

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

a) space between redundant systems or cables shall not contain interposing structures, equipment or materials that could assist in the propagation of the fire;

b) barriers when used between redundant systems or cables shall have a fire rating commensurate with the fire hazard protection requirements.

5.2 Environmental conditions during and after accidents

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

5.3 Isolation devices

5.3.1 General

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

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

5.3.2 Isolation characteristics

Failures and conditions that shall be protected against include

a) short-circuits between terminals or to ground;

b) open circuits;

c) application of the maximum a.c. or d.c. potential that could reasonably occur, considering potentials and sources available in both the category A and non-category A systems;

d) electromagnetic and electrostatic interference.

The properties of an isolation device shall include

– tolerance of and isolation for the electrical surges and spikes defined in IEC 61000-6-5;

– tolerance and isolation for EMI to IEC 61000-6-5;

– simple barriers between close or adjacent terminals or contact groups on relay equipment used for electrical isolation;

– prevention of transmission of excessively high or damaging voltages.

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

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

5.3.3 Actuation priority

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

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

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

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

5.4 Independence from control systems

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

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

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

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

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

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

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

6 Requirements for cabling separation

6.1 General requirement

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

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

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

6.2 Separation

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

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

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

– each redundant group shall be provided with physically separate cable routes, trays, conduits, ducts and penetrations;

– any given route, tray, conduit, duct, vertical duct or penetration shall carry or contain only cables of the same redundant group;

– for the I&C system failure-initiating events that have their cause in the cabling system, such as arcing or overheating due to shorts, overloads, voltage transients, etc. (see 4.3), a low degree of physical separation may be sufficient. A horizontal distance of 30 cm and a vertical distance of 80 cm shall be maintained as a minimum. Where the minimum separation distance is not maintained, the redundant cables shall be run in enclosed raceways that qualify as barriers or a justification of lower distances shall be provided;

– for plant failure and external failure events (see 4.4 and 4.5), such as fire or structure collapse, greater physical separation including barriers and/or safety structures shall be applied.

6.2.2 Lesser separation distances

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

6.2.3 Associated circuits

When functions are classified according to the requirements of IEC 61226, it will often be the case that a given system or set of equipment will perform functions of different categories. Also, certain functions of a lower category may have a very close relationship to category A functions, for example process monitoring based on the same measurements as safety functions. The requirements stated earlier in this document generally indicate that circuits of lower category functions should be separated from those of category A. However, as an alternative, the circuits of the lower category function can be declared to be “associated circuits”, and the separation requirements are determined from this subclause. While in principle it is possible to have circuits performing category C or lower functions associated with category B, in practice this provide little benefit since the separation requirements between functions of these categories are minimal. This subclause describes the situation for circuits associated with category A circuits.

Cables for non-category A functions become associated circuits in one or more of the following ways:

a) electrical connection to a category A power supply without the use of an isolation device;

b) electrical connection to the power supply of category A systems without the use of an isolation device;

c) proximity to category A circuits and equipment without the required separation (physical distance or barriers);

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

e) sharing a category A or associated signal without the use of an isolation device.

Associated circuits shall comply with one of the following requirements:

1) they shall be uniquely identified as such or as category A and shall remain with (traceable to the associated category A division), or be physically separated to the same extent as, those category A circuits with which they are associated. They shall be subject to the requirements placed on category A circuits, unless it can be demonstrated by analysis or testing that the absence of such requirements cannot degrade the category A circuits below an acceptable level;

2) they shall be in accordance with (1) above from the category A systems to and including an isolation device. Beyond the isolation device, such a circuit is non-category A provided that it does not again become associated with a category A system;

3) they shall be analysed or tested to demonstrate that category A circuits are not degraded below an acceptable level.

Associated circuits and isolation devices shall be subjected to appropriate qualification. This qualification shall show that the higher category circuits will perform correctly when the associated circuit or isolation device and its cables are subjected to electrical conditions for which the higher category circuit should function correctly. Where an associated circuit is connected to a non-category A device without isolation, that non-category A device shall also be subject to this appropriate qualification. Associated circuits need not be qualified for performance of function, since their function is non-category A.

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

6.2.4 Separation of system cables of different safety categories

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

a) Non-category A circuits shall be physically separated from category A circuits and associated circuits by the minimum separation requirements specified in 6.2.1, except as permitted in item d), or the non-category A circuits shall be associated circuits.

b) Non-category A circuits shall be electrically isolated from category A circuits and associated circuits by the use of isolation devices, shielding, and wiring techniques or separation distance, except as permitted in item d), or the non-category A circuits shall be associated circuits.

c) The effects of less than minimum separation or the absence of electrical isolation between the non-category A circuits and the category A circuits or associated circuits shall be analysed to demonstrate that category A circuits are not degraded below an acceptable level or the non-category A circuits shall be associated circuits.

d) Non-category A instrumentation signal and control circuits are not required to be physically separated or electrically isolated from associated circuits provided that firstly the non-category A circuits are not routed with associated cables of a redundant division and secondly the non-category A circuits are analysed to demonstrate that category A circuits are not degraded below an acceptable level. As part of the analysis, consideration shall be given to potential energy and identification of the circuits involved.

6.2.5 Separation of signal cables from power cables

Analogue and other low-level electrical signals shall not be run in the same cable trays, trunks or conduits as power cables. Depending on the technology, switchgear control cables may be low or high level and shall be submitted to this requirement accordingly. Fibre optic cables may be run together with power cables if their mechanical protection is assured.

6.2.6 Separation of cables from tubes or pipes

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

6.2.7 General routing considerations

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

6.2.8 Control room cabinets, desks, panels and related cables

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

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

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

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

Factors which may be considered include the following:

– the control room is always staffed and fire will therefore be rapidly detected and extinguished;
– the control room is a controlled access area, in which accumulation of flammable material will be prevented and sabotage is unlikely;
– the detection of fire within any compartment of the control room cabinets, panels and desks will be rapid, and the potential rate of spread of fire from one compartment to another is slow enough to allow fires to be extinguished before control is lost;
– the availability of redundant controls over safety plant, where one panel section provides individual control of safety plant items and another and separated section provides an alternative and possible grouped control over the safety plant;
– the ignition of fire within a panel section is of very low frequency, within the design basis of the plant, by control of the use of flammable material and heat sources within the panel sections;
– provision of an alternate, emergency control room from which the necessary safety control actions can be taken. Suitable means shall be provided to isolate the effects of fires in either control room.

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

6.3 Thermal and physical protection

Attention shall be given to acceptable thermal loading and de-rating factors for cable routing in cable trays to ensure that physical separation provisions remain effective.

To minimise the possibility of damage to cable sheats and insulation, due to the weight of upper cables pressing on lower ones in trays, the maximum depth of cables in a tray shall be limited to the no-damage weight carrying capability of the lower cables.

6.4 Fire protection

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

As an additional precaution when system or equipment cables important to safety are in close proximity to power cables, barriers of fire-resistant material shall be provided, separating category A system cables from all other cables.

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

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

Where category A cables are demonstrated to retain circuit integrity when exposed to fire, and where the insulation withstand voltage of the cable is greater than the postulated fault voltage of the lower category circuits in proximity to the cable, then such cables provide sufficient barriers to electrically induced fires. In such cases, physical separation of the category A cables from those of lower category may be less than the minimum distances specified in 6.2.1.

6.5 Identification

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

a) on the cables;

b) on the cable trays, ducts and conduits;

c) at all terminal points.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

NOTE Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 60332	Series	Tests on electric and optical fibre cables under fire conditions	EN 60332	Series
IEC 60964	-	Design for control rooms of nuclear power plants	-	-
IEC 61000	Series	Electromagnetic compatibility (EMC)	EN 61000	Series
IEC/TS 61000-6-5	-	Electromagnetic compatibilty (EMC) - Part 6-5: Generic standards - Immunity for power station and substation environments	-	-
IEC 61226	-	Nuclear power plants - Instrumentation and control systems important to safety - Classification	-	-
IEC 61513	-	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-
IEC/TR 62096	-	Nuclear power plants - Instrumentation and control - Guidance for the decision on modernization	-	-
IAEA safety guide NS-G-1.3	-	Instrumentation and control systems important to safety in nuclear power plants	-	-

BSI - British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001 Email: orders@bsigroup.com You may also buy directly using a debit/credit card from the BSI Shop on the Website http://www.bsigroup.com/shop

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact Information Centre. Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001 Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsigroup.com/BSOL

Further information about BSI is available on the BSI website at http://www.bsigroup.com

Copyright

BSI Group
Headquarters 389
Chiswick High Road,
London, W4 4AL, UK
Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/
standards