BRITISH STANDARD

BS EN
62340:2010

Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure (CCF)

ICS 27.120.20

BSI
British Standards

National foreword

This British Standard is the UK implementation of EN 62340:2010. It is identical to IEC 62340:2007. It supersedes BS IEC 62340:2007 which is withdrawn.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 31 March 2008

ISBN 978 0 580 68114 1

Amendments/corrigenda issued since publication

Date	Comments
31 July 2010	This corrigendum renumbers BS IEC 62340:2007 as BS EN 62340:2010

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62340

May 2010

ICS 27.120.20

English version

Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with Common Cause Failure (CCF)

(IEC 62340:2007)

Centrales nucléaires de puissance - Systèmes d'instrumentation et de contrôle commande importants pour la sûreté - Exigences permettant de faire face aux Défaillances de Cause Commune (DCC)
(CEI 62340:2007)

Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache
(IEC 62340:2007)

This European Standard was approved by CENELEC on 2010-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

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 62340:2010 E

Foreword

The text of the International Standard IEC 62340:2007, 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 62340 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 62340:2007 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION 4

1 Scope 7
2 Normative references 8
3 Terms and definitions 8
4 Abbreviations 12
5 Conditions and strategy to cope with CCF 13
5.1 General 13
5.2 Characteristics of CCF 13
5.3 Principal mechanisms for CCF of digital I&C systems 13
5.4 Conditions to defend against CCF of individual I&C systems 14
5.5 Design strategy to overcome CCF 15
6 Requirements to overcome faults in the requirements specification 15
6.1 Deriving the requirements specification for the I&C from the plant safety design base 15
6.2 Application of the defence-in-depth principle and functional diversity 16
6.3 CCF related issues at existing plants 17
7 Design measures to prevent coincidental failure of I&C systems 17
7.1 The principle of independence 17
7.2 Design of independent I&C systems 18
7.3 Application of functional diversity 18
7.4 Avoidance of failure propagation via communications paths 19
7.5 Design measures against system failure due to maintenance activities 19
7.6 Integrity of I&C system hardware 19
7.7 Precaution against dependencies from external dates or messages 20
7.8 Assurance of physical separation and environmental robustness 20
8 Tolerance against postulated latent software faults 20
9 Requirements to avoid system failure due to maintenance during operation 21

Annex A (informative) Relation between IEC 60880 and this standard 22
Annex ZA (normative) Normative references to international publications with their corresponding European publications 23

INTRODUCTION

a) Background, main issues and organisation of this Standard

In order to achieve a high safety level, redundancy is applied as one of the key features for designing instrumentation and control systems (I&C systems) important to safety. Since a Common Cause Failure (CCF) could compromise the effectiveness of redundancy, it is essential to take adequate measures against it. The nuclear industry has pioneered systems design and engineering to address CCF. Over the last thirty years it has implemented and reached consensus on a number of practices to handle and overcome CCF.

The intention of this standard is to address the whole scope of aspects to overcome Common Cause Failures (CCFs) and to provide an overview of the relevant requirements for I&C systems that are used to perform functions important to safety (according to IEC 61226) in nuclear power plants.

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

IEC 62340 is a second level IEC SC 45A document tackling the issue of CCF.

This international standard supplements IEC 61513 and related standards with requirements to reduce and overcome the possibility of CCF of I&C functions of category A. The requirements given by this standard are applicable to category A (IEC 61226) functions if their failure would be unacceptable with respect to the plant safety design.

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

This standard applies to I&C systems important to safety of new NPPs as well as to the replacement of I&C systems of existing plants. The I&C functions may need to be kept or upgraded if an I&C system is replaced. The requirements of this standard also consider the replacement of I&C which entails changes in the structure of I&C systems.

For existing plants, only a subset of the requirements from this standard may be applicable and this subset should be identified at the beginning of any project. The requirements and recommendations which are not to be implemented in an I&C upgrading or replacement project should be justified on a case by case basis by an overall safety assessment. The potential consequences of not following this standard in some aspects due to plant constrains should be considered in comparison to the added safety gained through the upgrade as a whole.

To avoid overlapping requirements, this standard takes advantage of other existing standards by referring to the relevant (sub)clauses, especially to the nuclear sector standards IEC 61513, IEC 60709, IEC 60780 and IEC 60880. New requirements are given where not covered by these standards.

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 and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 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 (now replaced by IAEA GS-R-3) 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 NS-R-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.

This page deliberately set blank

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – REQUIREMENTS FOR COPING WITH COMMON CAUSE FAILURE (CCF)

1 Scope

I&C systems important to safety may be designed using conventional hard-wired equipment, computer-based equipment or by using a combination of both types of equipment. This International Standard provides requirements and recommendations[1] for the overall architecture of I&C systems, which may contain either or both technologies.

The scope of this standard is:

a) to give requirements related to the avoidance of CCF of I&C systems that perform category A functions;

b) to additionally require the implementation of independent I&C systems to overcome CCF, while the likelihood of CCF is reduced by strictly applying the overall safety principles of IEC SC 45A (notably IEC 61226, IEC 61513, IEC 60880 and IEC 60709);

c) to give an overview of the complete scope of requirements relevant to CCF, but not to overlap with fields already addressed in other standards. These are referenced.

This standard emphasises the need for the complete and precise specification of the safety functions, based on the analysis of design basis accidents and consideration of the main plant safety goals. This specification is the pre-requisite for generating a comprehensive set of detailed requirements for the design of I&C systems to overcome CCF.

This standard provides principles and requirements to overcome CCF by means which ensure independence[2]:

a) between I&C systems performing diverse safety functions within category A which contribute to the same safety target;

b) between I&C systems performing different functions from different categories if e.g. a category B function is claimed as back-up of a category A function and;

c) between redundant channels of the same I&C system.

The implementation of these requirements leads to various types of defence against initiating CCF events.

Means to achieve protection against CCF are discussed in this standard in relation to:

a) susceptibility to internal plant hazards and external hazards;

b) propagation of physical effects in the hardware (e.g. high voltages); and

c) avoidance of specific faults and vulnerabilities within the I&C systems notably:

   1) propagation of functional failure in I&C systems or between different I&C systems (e.g. by means of communication, fault or error on shared resources),

---

1 To support a clear addressing of all requirements and recommendations these are introduced by a clause number.

2 Independence between I&C systems or between redundant channels of the same I&C system is the capability that in case of a postulated failure of one system or one channel the other systems or channels perform their functions as intended.

2) existence of common faults introduced during design or during system operation (e.g. maintenance induced faults),
3) insufficient system validation so that the system behaviour in response to input signal transients does not adequately correspond to the intended safety functions,
4) insufficient qualification of the required properties of hardware, insufficient verification of software components, or insufficient verification of compatibility between replaced and existing system components.

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 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

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

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 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 61000-4 (all parts), *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques*

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

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

IAEA Safety Guide NS-G-1.3, *Instrumentation and control systems important to safety in Nuclear Power Plants*

IAEA Safety Guide SG-D11, *General design safety principles for nuclear power plants*

IAEA Safety Glossary Ed.2.0, 2006

3 Terms and definitions

For the purposes of this document, the terms and definitions of IEC 61513 and IEC 61226 apply as well as the following.

3.1
Common Cause Failure (CCF)
failure of two or more structures, systems or components due to a single specific event or cause

[IAEA Safety Glossary, Ed. 2.0, 2006]

NOTE 1 The coincidental failure of two or more structures, systems or components is caused by any latent deficiency from design or manufacturing, from operation or maintenance errors, and which is triggered by any event induced by natural phenomenon, plant process operation or an action caused by man or by any internal event in the I&C system.

NOTE 2 Coincidental failure is interpreted in a way which covers also a sequence of system or component failures when the time interval between the failures is too short to set up repair measures.

3.2
defence-in-depth
the application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails

[IAEA Safety Glossary, Ed. 2.0, 2006]

NOTE The protective measures are assumed to be independent.

3.3
diversity
existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against CCF. It may be achieved by providing systems that are physically different from each other, or by functional diversity, where similar systems achieve the specified objective in different ways

[IEC 60880, 3.14]

NOTE See also ”functional diversity”.

3.4
fail-safe design
design of system functions so that they respond to specified faults in a predefined, safe way

3.5
failure
inability of a structure, system or component to function within acceptance criteria

[IAEA Safety Glossary, Ed. 2.0, 2006]

NOTE 1 A failure is the result of a hardware fault, software fault, system fault, or human error, and the associated signal trajectory which triggers the failure.

NOTE 2 See also “fault”, “software failure”.

3.6
fault
defect in a hardware, software or system component

[IEC 61513, 3.22]

NOTE 1 Faults may be subdivided into random faults, that result e.g. from hardware degradation due to ageing, and systematic faults, e.g. software faults, which result from design errors.

NOTE 2 A fault (notably a design fault) may remain undetected in a system until specific conditions are such that the result produced does not conform to the intended function, i.e. a failure occurs.

NOTE 3 See also ”software fault” and “random fault”.

3.7
fault avoidance
use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety life cycle

[IEC 61508-4, 3.6.2, modified]

3.8
fault tolerance
the built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware and software faults

[IEC 60880, 3.18]

3.9
functional diversity
application of diversity at the functional level (for example, to have trip activation on both pressure and temperature limit)

[IEC 60880, 3.19]

NOTE See also ”diversity”.

3.10
functional validation
verification of the correctness of the application functions specifications versus the first plant functional and performance requirements. It is complementary to the system validation that verifies the compliance of the system with the functions specification

[IEC 61513, 3.24]

3.11
human error (or mistake)
human action that produces an unintended result

[IEC 60880, 3.21]

3.12
independent I&C systems
systems that are independent possess the following characteristics:

a) the ability of one system to perform its required functions is unaffected by the operation or failure of the other system;
b) the ability of the systems to perform their functions is unaffected by the presence of the effects resulting from the postulated initiating event for which they are required to function;
c) adequate robustness against common external influences (e.g. from earthquake and EMI) is assured by the design of the systems

[modified definition of “independent equipment” from IAEA Safety Glossary, Ed. 2.0, 2006]

NOTE Means to achieve independence by the design are electrical isolation, physical separation, communications independence and freedom of interference from the process to be controlled.

3.13
input signal transient
time behaviour of all process signals which are fed into the I&C system

NOTE The behaviour of an I&C system is actually determined by the signal trajectory which includes the internal states of the I&C equipment. The requirements specification, however, defines the safety related reactions of the I&C system in response to “input signal transients”.

3.14
latent fault
undetected faults in an I&C system

NOTE Latent faults may result from errors during specification or design or from manufacturing defects and may be of any physical or technical type which it is reasonable to be assumed. In the case of specification or design faults it should be assumed that latent faults may be implemented in all redundant sub-systems in the same way so that a specific signal trajectory could trigger CCF of the concerned I&C system.

3.15
random fault
non-systematic fault of hardware components

NOTE Faults of hardware components are a consequence of physical or chemical effects, which may occur at any time. A good description of the probability of the occurrence of random faults can be given using statistics (fault rate). Increased fault rates may be the consequence of systematic faults in hardware design or manufacture, if these occur without temporal correlation, for example as a consequence of premature ageing.

3.16
signal trajectory
time histories of all equipment conditions, internal states, input signals and operator inputs which determine the outputs of a system

[IEC 60880, 3.33]

3.17
single failure
a failure which results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) which result from it

[IAEA Safety Glossary, Ed. 2.0, 2006]

3.18
single-failure criterion
a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure

[IAEA Safety Glossary, Ed. 2.0, 2006]

NOTE See also ”single failure”, “software failure”.

3.19
software failure
system failure due to the activation of a design fault in a software component

[IEC 61513, 3.57]

NOTE 1 All software failures are due to design faults, since software does not wear out or suffer from physical failure. Since the triggers which activate software faults are encountered at random during system operation, software failures also occur randomly.

NOTE 2 See also ”failure, fault, software fault”.

3.20
software fault
design fault located in a software component

[IEC 61513, 3.58]

NOTE See also ”fault”.

3.21
specification
document that specifies, in a complete, precise, verifiable manner, the requirements, design, behaviour, or other characteristics of a system or component, and, often, the procedures for determining whether these provisions have been satisfied

[IEC 60880, 3.39]

3.22
system validation
confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness)

[IEC 60880, 3.42]

3.23
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

[IEC 61513, 3.62]

NOTE The common cause failure is a sub-type of systematic failure such that the failures of separate systems, redundancies or components can be triggered coincidentally.

3.24
systematic fault
fault in the hardware or software which concerns systematically some or all components of a specific type

NOTE 1 Systematic faults may result from errors in the specification or design, from manufacturing defects or from errors which are introduced during maintenance activities.

NOTE 2 Components containing a systematic latent fault may fail randomly or coincidentally, depending on the kind of fault and the related mechanisms that trigger the fault.

3.25
validation
process of determining whether a product or service is adequate to perform its intended function satisfactorily

[IAEA Safety Glossary, Ed.2.0, 2006]

NOTE See also “functional validation and “system validation”.

3.26
verification
the process of determining whether the quality or performance of a product or service is as stated, as intended or as required

[IAEA Safety Glossary, Ed.2.0, 2006]

4 Abbreviations

CCF Common Cause Failure
DBA Design Basis Accident[3]
DBE Design Basis Event
EMI Electro-Magnetic Interference
FAT Factory Acceptance Test
IAEA International Atomic Energy Agency
I&C Instrumentation and Control
NPP Nuclear Power Plant

[3] The terms DBA and DBE are used in accordance with their definition in IEC 61226.

PIE Postulated Initiating Event

SAT Site Acceptance Test

5 Conditions and strategy to cope with CCF

5.1 General

This clause explains the strategy to cope with CCF and makes plausible the requirements given by Clauses 6 through 9.

5.2 Characteristics of CCF

For I&C systems that perform category A functions the appropriate application of redundancy combined with voting mechanisms has been proven to meet the single failure criterion. This design ensures that the likelihood of a failure of such I&C systems is very low.

I&C systems with this design can fail if two or more redundant channels fail concurrently (CCF). The CCF can occur if a latent fault is systematically incorporated in some or all redundant channels and if by a specific event this fault is triggered to cause the coincidental failure of some or all channels. A redundant I&C system fails if the number of faulted channels exceeds its design limit.

Latent faults which are systematically incorporated in some or all redundant channels may originate from any phase of the life cycle of an I&C system. Latent faults may result from human errors which do not depend on the I&C technology or may result from the manufacturing process dependent on the I&C technology. At a comparatively high probability latent systematic faults are related to the design basis of an I&C system as e.g.:

- errors in the requirements specification of the safety functions, or
- an inadequate specification of the hardware design limits against environmental loadings (e.g. seismic loads or EMI), or
- technical design faults which could cause system failure by internally induced mechanisms.

Triggering events for CCF may be caused from outside of the I&C system by a common loading to all redundant channels such as from an input signal transient, from environmental stress or from specific real time or calendar dates. Additionally the existence of latent propagation mechanisms may be assumed such that corrupted data which are transferred from one faulty system to corresponding systems of the other redundancies may cause consequential failure of other redundant channels. Such a mode of failure propagation is relevant for computer-based I&C systems only.

5.3 Principal mechanisms for CCF of digital I&C systems

In hard-wired technology, the functions important to safety within each redundant channel are generally implemented by chains of separate electronic components, while the hardware components of computer based systems typically process a group of assigned functions. Therefore the following considerations apply mainly to digital I&C systems.

Under normal operation conditions (without changes due to maintenance activities and without physical influence of the environment as listed in 7.8), processing of the input signal transients by the digital I&C system forms the main contribution to their signal trajectories. Specific signal trajectories which can cause a system failure may occur during safety demands from untested combinations of input signals or may result from specific system internal states. Such specific system internal states may be related to stored data from earlier input signal transients or to latent faults from earlier maintenance activities or could be caused by hardware faults.

CCF could be caused if hardware components of some or all redundancies are faulted by environmental effects which exceed the hardware design limits. The cause for this failure mechanism can be for example:

- an insufficient design of the physical separation so that a single failure of one supply system can influence two or more redundancies, or
- inadequately specified hardware design limits e.g. with respect to seismic events.

The likelihood that a CCF could be caused by random faults of hardware components is very low. Such a CCF mechanism would presuppose that a specific fault can stay latent for a longer time so that components of other redundancies could also be affected by this type of fault. Staying latent requires that the fault is not identified by self-supervision or periodic testing and that the concerned components do not fail spontaneously but fail when being activated by a common trigger in some or all redundancies.

The consequences of a system CCF may be that, in the case of a demand, system responses such as the following occur:

– no response or an erroneous response is given compared to the required response although the I&C system keeps processing;
– the system is caused to stop its processing, so no response can be given.

5.4 Conditions to defend against CCF of individual I&C systems

The CCF characteristics as given in 5.2 indicate the following possibilities for reducing the likelihood of CCF:

a) to reduce the probability of latent systematic faults incorporated in the redundant channels of an individual I&C system, and
b) to reduce the probability that mechanisms exist which could trigger coincidentally latent systematic faults or which could cause a single failure in one channel to propagate to other channels (failure propagation).

The difficulty for an effective defence against CCF is caused by the fact that faults and triggering mechanisms of an I&C system are latent. The avoidance of latent systematic faults and triggering mechanisms requires therefore designing and analysing I&C systems under postulates which are related to the experience of CCF occurrences in NPPs and to the potential weaknesses of the selected I&C technology.

The experienced frequency of CCF occurrences is very low for I&C systems which perform category A functions. The reasons for this experience is partly based on the high quality level of design, manufacturing and maintenance which is applied to such I&C systems, however this is also based on the nature of CCF which can only occur at the combined probability of the existence of a latent systematic fault and the activation of a corresponding triggering mechanism by a signal trajectory. Therefore an effective defence against CCF has to assign the same importance to the avoidance of potential triggering mechanisms and to the avoidance of latent faults.

The experience of CCF occurrences in NPPs shows that the following types of causes are dominant:

a) latent faults which are related to faults in the requirements specification. The identification of errors in the requirements specification of I&C functions is difficult and such errors may propagate through subsequent design phases including the verification and system validation activities. Latent faults from this potential source can be detected by functional validation activities only (see 3.25);
b) latent faults which are introduced during maintenance because the possibility for analysing and testing modifications may be limited under plant constraints (e.g. modification of set-points, use of revised versions of spare-parts or the up-grading of I&C system components); and

c) the triggering of latent faults during maintenance activities by causing partly specific system states or partly invalid data which do not represent the actual plant status.

Depending on the I&C technology different types of failure propagation are relevant:

d) analogue I&C systems might be endangered by high voltages if one channel could be affected by a single failure and neighbouring channels could be affected by consequential failures if design limits for channel separation are exceeded;

e) for digital technology the failure propagation via high voltages can be excluded if fibre optics are applied but specific means are required to reduce susceptibilities to failure propagation from erroneous or missing data.

This standard gives guidance for reducing the possibility of the existence of mechanisms that could support the triggering of postulated types of latent design faults to cause CCF during transients (see Clauses 7, 8 and 9).

To reduce the likelihood that latent design faults may remain in the final I&C system to the minimum possible level, reference is made to the design requirements of the standards of SC 45A (see Clause 2).

5.5 Design strategy to overcome CCF

Design measures to overcome CCF are related to the I&C architecture which includes at least two or more I&C systems to perform the category A functions. The demonstration that any individual I&C system is completely fault free is not possible and therefore the existence of latent faults and related triggering mechanisms cannot be excluded in principle. Consequently an occurrence of CCF cannot be excluded for any of the individual I&C systems although the expected frequency should be lower than once during the intended plant life.

If one I&C system is postulated to fail according to a CCF it is necessary that main category A functions are performed by another I&C system to avoid unacceptable consequences and to ensure the main plant safety targets. This other I&C system is required to perform its assigned safety functions independently (see 3.12) so that the likelihood of a coincident failure of both I&C systems is reduced to an extent that this is not relevant during the intended plant life.

Reducing the likelihood of a coincident failure for independent I&C systems to a negligible level requires that the systems are operated at different signal trajectories and that the systems are adequately protected against physical hazards (see 5.3). Different signal trajectories can be ensured by the application of diversity (e. g. by equipment diversity or functional diversity).

The application of functional diversity forms the only possibility to provide protection against a postulated latent functional fault in the requirements specification. Assigning the diverse functions to independent I&C systems can at the same time be used as a means of ensuring operation of the I&C systems with different signal trajectories.

This standard gives guidance on the design and implementation of independent I&C systems that operate with different signal trajectories (see definition 3.16), so the likelihood of coincident failure of these independent systems is not relevant with regard to the intended plant life even if latent common design faults may exist (see clauses 6, 7 and 9).

6 Requirements to overcome faults in the requirements specification

6.1 Deriving the requirements specification for the I&C from the plant safety design base

Functional diversity serves to ensure that the main plant safety targets are met, in spite of the possible existence of latent faults related to errors from the requirements specification.

The analysis of the DBAs and of the relevant DBEs which can be caused by failures of the I&C or related subsystems provides the requirements specification from which any need for the application of functional diversity will arise. This may depend on the estimated consequences in case of failure, and the estimated frequencies of these DBEs.[4]

6.1.1 Within this analysis, the following steps shall be taken:

a) The DBEs shall be identified which could cause unacceptable consequences if CCF is postulated for the relevant I&C system. A design to tolerate CCF is needed for that subset of DBEs which are to be expected at a frequency that is higher than a specified limit.

b) For this subset of DBEs, at least one second plant safety parameter shall be identified, and evaluated for the specification of diverse safety functions. [5]

6.1.2 The implementation of the safety functions which are identified with respect to CCF (according to 6.1.1) can be performed according to different design strategies[6]. For the selected design it shall be demonstrated that the essential plant safety targets are met in the presence of a postulated CCF.

6.2 Application of the defence-in-depth principle and functional diversity

The application of the defence-in-depth principle and functional diversity requires the identification of those specific I&C functions of category A that can ensure independently that the main plant safety targets are met. These functions are called diverse functions with respect to a specific safety target.

6.2.1 Diverse I&C functions of category A shall be assigned to independent I&C systems and implemented in a way that in the case of the postulated failure of one of these independent I&C systems, the main safety targets of the plant are still met by the functions performed by the other independent I&C system(s).

The following design steps shall be taken.

6.2.2 The demonstration of the independent performance of diverse functions shall be documented in the safety case.

6.2.3 If I&C functions of category B are claimed for independent effectiveness e.g. as back-up of category A functions, the independence between the system performing the category A functions and the system performing the category B functions shall be demonstrated according to the requirements of this standard.

---

4 The availability of diverse protective functions and in particular, the availability of diverse or independent measurement signals, is a result of the design of the plant process systems. In general, the requirements and recommendations of this standard aim at utilising the safety potential of the plant process systems when designing I&C systems important to safety (e.g. the existence of diverse actuators).

5 The majority of the large transients influence nearly all safety parameters in parallel, so the application of functional diversity requires as a precondition a more detailed analysis of design basis accidents, but generally no additional safety parameters are required.

6 Examples of design strategies that may be acceptable or have been found to be acceptable in certain (but not necessarily all) national contexts:

- The identified diverse safety functions are grouped in a way that each of the relevant DBEs is handled by both sets of safety functions. Each set is assigned to an independent I&C system. The remainder of the category A functions are assigned to either of these I&C systems. This assignment procedure ensures adequately differentiated signal trajectories to be processed by the independent I&C systems so that these may be based on the same I&C system platform.
- The complete scope of functions of category A (including the pairs of diverse functions) is assigned to one I&C system (primary I&C protection system). Then the processing of one group of the identified diverse safety functions is duplicated in an independent secondary protection system which may be from a lower equipment class. To ensure adequately differentiated signal trajectories between the independent I&C systems equipment diversity is necessary.

6.2.4 The functional validation of the I&C functions important to safety shall be performed to demonstrate by suitable means (e.g. by process simulation) the correctness of the application functions specification versus the plant functional and performance requirements. The validation shall be performed according to the relevant clauses of IEC 61513.

6.2.5 During the validation it shall be demonstrated that the main plant safety targets are met even if any one of the two independent I&C systems and its assigned group of the diverse functions is postulated to be ineffective:

a) System validation shall be performed according to the relevant clauses of IEC 61513 and IEC 60880.

b) For overall validation of the implemented functions of category A, all validation related activities should be assessed in an integrated way by joint consideration of:
   – the functional validation (e.g. the application software processed in a suitable hardware environment which may be different from the target system),
   – checks of the integrated target system in a representative test configuration and for the FAT,
   – final commissioning tests after integration into the plant (SAT).

6.3 CCF related issues at existing plants

6.3.1 Where this standard is applied to plant I&C upgrades, exceptions to the requirements of this standard shall be justified.

The following justification arguments may apply:

- comparison of major weaknesses and advantages of the existing I&C to the upgrade,
- physical constraints imposed by the existing plant,
- consideration of experience regarding CCF occurrences in NPPs,
- a re-analysis of the design basis which should consider the state-of-the-art in design requirements.

7 Design measures to prevent coincidental failure of I&C systems

7.1 The principle of independence

I&C systems perform their safety functions independently if a postulated failure of one of these I&C systems does not prevent the other systems from performing their functions as intended (see 3.12).

The following design principles shall be used for effective defence against CCF.

7.1.1 The required reliability target imposes requirements on design, implementation and operation of the related I&C systems which perform category A functions. It is necessary to fulfil the relevant requirements to individual systems for system design (IEC 61513), software design (IEC 60880) physical separation (IEC 60709) and component qualification (general aspects: IEC 60780 and seismic robustness: IEC 60980). Additionally, the requirements of this standard shall be met to ensure the independent performance of the diverse safety functions.

7.1.2 The principle of independent I&C systems aims at limiting the influence of CCF to one I&C system only. An analysis shall be performed to identify common mechanisms which could jeopardize the independence of such I&C systems. The identified common mechanisms should be eliminated or shall be shown to have adequate mitigation.

7.1.3 The design of the architecture of I&C systems which are claimed to be independent I&C systems shall provide:

a) system specific processing paths from sensing the plant status to the actuation of the plant safety systems without using shared components, and

b) support systems (e.g. power supply or air conditioning systems), which consist of sufficiently redundant and separated sub-systems (IEC 60709),

c) means for self-supervision which operate independently for each processing unit.

7.1.4 In order to exclude a coincident failure of I&C systems which are claimed to be independent, their operating conditions shall be analysed to identify common triggers.

7.1.5 Functional diversity shall be used in accordance with 6.1 where practicable in the implementation of I&C systems, to overcome potential faults in the requirements specification of category A functions. This measure is effective irrespective of the I&C technology used.

7.2 Design of independent I&C systems

7.2.1 Independent I&C systems which perform category A functions shall be designed so the likelihood of triggering a coincident failure of these systems from the same input signal transient is reduced to a level that is not relevant during the intended plant life. This requirement can be met by measures to ensure different signal trajectories (see 6.1.2 and 7.3).

7.2.2 Independent I&C systems shall not use shared components or services if the postulated failure of these shared components or services can cause a coincident failure of the independent I&C systems (e.g. a common power supply).

7.2.3 The use of identical hardware or software components for the realization of independent I&C systems shall be analyzed to demonstrate that the potential for CCF is negligible. Otherwise it shall be restricted:

– to operation at different conditions and loadings (mainly relevant e.g. for digital units, which process different input signals), and/or

– to operation independent from the demand profile and from influencing factors of the plant process (e.g. hardware components which are not exposed to accident conditions or software components which perform their intended functions without sensitivity to the processed data).

7.2.4 If it is necessary to operate specific components dependent on the demand profile (e.g. sensors inside containment or relays which are to be energised or de-energised during a demand) these components shall be qualified for the operating conditions during the demand (IEC 60780) and shall be subject to periodic testing (IEC 60671). The application of diverse hardware components may result in advantages, but the need for diversity should be analysed.

7.3 Application of functional diversity

7.3.1 For software based I&C systems, the sensitivity to CCF shall be analysed by assessing the potential application and the signal trajectories for the individual software modules:

– the application of functional diversity shall be used to diversify the “input signal” component of signal trajectories. Diversification of the other components of the trajectories shall be considered (for example internal states);

– the exclusion of latent faults may be possible for very small and simple software modules so that a fault analysis and adequate testing can be performed.

7.3.2 Independent I&C systems shall not perform identical application functions, to reduce the possibility of conditions in which a coincidental, quasi-synchronised failure of these systems may be triggered from the same input signal transient. If the implementation of identical sub-functions cannot be avoided due to the plant design, these identical sub-functions shall be fed at least with input signals from separate sensors.

7.4 Avoidance of failure propagation via communications paths

7.4.1 In order to handle CCF, there shall be no communication between independent I&C systems which are provided to overcome CCF in the sense of 6.1.2.

7.4.2 The design of I&C systems performing category A functions shall ensure the highest possible protection against propagation of failure inside the I&C system. The implementation of this design target requires the application of the following design measures in parallel:

a) I&C systems shall be designed so that system operation cannot be jeopardised by central subsystems which e.g. may provide information to the main control room for display or may support modifications of parameters derived from the plant process and which, for such functions, require communication to all redundancies of an I&C system performing a category A function.
b) Faulty data shall be excluded from further processing within the application software.
c) All functions provided by the system software for the transfer of messages shall be implemented in such a way that the correct execution of these software transfer functions cannot be disturbed by any values of the process dependent data which are the objects to be transferred (see also 8.1).
d) Correctness of the received data shall be checked prior to further processing.
e) Physical separation of redundant sub-systems shall be designed according to IEC 60709.

7.4.3 Exchanging input data between redundant units can introduce dependencies between channels and shall therefore be analysed regarding CCF possibilities. On-line validation of input data (e.g. by means of voting on them) should be used as a means to limit the propagation of faulty data. Those input signals which are already known to be faulty (e.g. by range overflow) should be labelled and excluded from further processing.

7.5 Design measures against system failure due to maintenance activities

In addition to the requirements given by IEC 61513 the following specific requirements are relevant with respect to CCF:

7.5.1 I&C systems performing category A functions shall be analysed during design to demonstrate tolerable system behaviour during maintenance and test activities.

Key items of this demonstration are:

a) If process components may cause a DBE in case of spurious actuation by the controlling I&C system, means shall be provided to avoid the possibility of spurious actuation due to maintenance activities.
b) The amount of category A functions which may be affected simultaneously by maintenance activities shall be compatible with the safety design principles of the plant.

7.5.2 To reduce the risk of disabling several redundancies caused by maintenance and online testing activities, means should be provided to detect these faults (e.g. by online monitoring of the system status) during maintenance and means to terminate maintenance activities in a controlled way leaving the system in an acceptable state.

7.6 Integrity of I&C system hardware

Self-supervision is necessary to improve the availability of the systems important to safety. Although not directly relevant to CCF, the following clauses are included for completeness.

7.6.1 Means for self-supervision during operation shall be used (see IEC 60880):

a) A pre-determined and specifically defined state shall be adopted when self-supervision detects a fault.

b) The state shall be chosen on 'fail safe' principles, by analysis of the preferred action to be taken at faults. This may often be to cause a safety actuation, but may be also to prevent a spurious actuation if it could lead to a DBE.

c) To reduce the possibility that system failure can be caused by accumulation of unidentified hardware faults.

7.6.2 For safety actuations that are prevented or automatically initiated if a fault is identified by the self-supervision, alarms shall be provided for information to the main control room.

7.6.3 From the experience gained in operating analogue I&C systems in mild environments, hardware modules with systematic minor manufacturing defects which behave as expected during system commissioning show an increased fault rate at a later time. For early detection of systematic faults, all failures of hardware components shall be analysed and logged so the maintenance staff will be warned early enough to take countermeasures before a CCF would be triggered. (Hardware modules with manufacturing defects which already prevent successful commissioning are not relevant for CCF.)

7.6.4 Components of the applied I&C technology can show an essentially decreasing fault rate at the beginning of their life time. Therefore a burn-in on component or system level should be performed before starting its safety relevant operation.

7.7 Precaution against dependencies from external dates or messages

7.7.1 I&C systems performing category A functions shall be designed so their operational behaviour is free of unintended dependencies from any external influences such as specific calendar dates.

7.7.2 For prevention of access to, and manipulations of the I&C system by unauthorised personnel, and the avoidance of unintended maloperation by authorised personnel, the requirements given in IEC 60880 shall be applied.

7.8 Assurance of physical separation and environmental robustness

Ensuring sufficient robustness of I&C systems performing category A functions is essential. All known failure mechanisms caused by environmental effects jeopardise the hardware components of I&C systems. To handle CCF there is no need for additional requirements to those of established standards. Therefore this group of failure mechanisms is mentioned only from the viewpoint of completeness.

To handle CCF due to environmental effects, for systems performing category A functions, the relevant requirements are given in the following standards:

– IEC 60780 for equipment qualification (general),

– IEC 60980 for seismic qualification,

– IEC 61000-4 for electromagnetic compatibility,

– IEC 60709 for separation and isolation requirements.

8 Tolerance against postulated latent software faults

8.1 Digital I&C systems performing category A functions should be designed according to IEC 61513 to operate internally without dependence on the demand profile. The following software requirements are in addition to the requirements of IEC 60880 and consistent with it. They reduce the possibility that assumed latent software faults may be triggered from data which depend on transients of the plant process:

a) Application and system software should be separated in such a way that the algorithmic processing of plant process data is entirely performed by the application software.

b) The operation of system software functions should not be influenced by any data which directly or indirectly depends on the plant status (e.g. transfer of process data as bit-strings). This general requirement is to be met additionally to those given by Clause B.2 of IEC 60880 and includes:

   – invariant cyclic processing of the application functions;

   – invariance of processing load and communication load;

   – avoidance of interrupts triggered by process data (for the generally restricted use of interrupts, see Clause B.2 of IEC 60880).

8.2 The (application) software shall be designed to be tolerant of invalid input signals, singly or in groups or due to spurious short-term transients on the input signals, such that safe action is ensured but spurious actuations are avoided.

8.3 Invalid or faulty input signals shall be identified on-line. If faulty signals are identified and processed by comparison of redundant information, then the dependencies thus introduced between redundant sub-systems shall be analysed for CCF possibilities.

8.4 If an I&C system performs different functions and if one or some signals used by one function are invalid, all other functions with undisturbed input signals shall not be affected.

8.5 The software shall be designed to take safe action even in response to multiple coincident failures or apparent failures of input signals. This safe action should avoid DBE caused by spurious actuations and may be to trip or alarm as specified in the system functional requirements.

9 Requirements to avoid system failure due to maintenance during operation

9.1 For I&C systems performing category A functions, simultaneous activities shall be restricted to a single redundancy to avoid a resulting failure of more than one of the redundant trains, channels or sub-systems (e.g. by means of interlocks or administrative procedures).

9.2 The effects of maintenance activity during power operation shall be analysed to prevent other I&C systems, which perform category A functions and which are not subject to this maintenance activity, from failing.

9.3 In cases where a hardware component needs to be replaced by a substitute, it shall be ensured by adequate qualification of hardware and software features and by verification of compatibility between replaced and existing components that the reliability of the I&C safety systems is not reduced and new failure modes are not introduced. The adequacy of the qualification shall be justified taking into account the complexity of the components.

9.4 To limit the effect of a degradation of component robustness due to ageing the useful lifetime of the I&C components should be analysed.

Annex A
(informative)

Relation between IEC 60880 and this standard

During the FDIS stage of IEC 60880 (edition 2 of 2006) working group A3 of subcommittee 45A decided to integrate Clause 13 on CCF from IEC 60880-2:2000 without changes with respect to the development of this standard. Consequently, the proposal to integrate the CCF specific software requirements from Clause 8 of this standard into annex B of IEC 60880 was rejected.

_____

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 60671	-	Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing	-	-
IEC 60709	-	Nuclear power plants - Instrumentation and control systems important to safety - Separation	EN 60709	-
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	EN 60880	-
IEC 60980	-	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations	-	-
IEC 61000-4	Series	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques	EN 61000-4	Series
IEC 61226	-	Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions	-	-
IEC 61513	-	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-
IAEA Safety Guide NS-G-1.3	-	Instrumentation and control systems important to safety in nuclear power plants	-	-
IAEA Safety Guide SG-D11	-	General design safety principles for nuclear power plants; a safety guide	-	-
IAEA Safety Glossary	2007	Terminology used in nuclear safety and radiation protection	-	-

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