IEC 62340

Edition 1.0 2007-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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)

IEC 62340:2007

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 62340

Edition 1.0 2007-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

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)

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX T

ICS 27.120.20

ISBN 2-8318-9452-2

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62340 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/668/FDIS	45A/676/RVD

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

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

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

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

INTRODUCTION

a) 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.

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.