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 It also gives information on projects, withdrawn and replaced publications.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

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.

_____

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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)

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62340 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/668/FDIS	45A/676/RVD

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

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

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

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

INTRODUCTION

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

L'application du principe de redondance est un des points clef de la conception des systèmes d'instrumentation et de contrôle-commande (systèmes d'I&C) importants pour la sûreté qui permet d'atteindre un haut niveau de sûreté. Les Défaillances de Cause Commune (DCC) pouvant remettre en cause l'efficacité de la redondance, il est essentiel de prendre des mesures palliatives appropriées contre celles-ci. L'industrie nucléaire a été pionnière dans le domaine du traitement des DCC au niveau de la conception et de l'ingénierie des systèmes. Au cours des trois dernières décades un consensus a pu être atteint et mis en œuvre au niveau d'un certain nombre de pratiques permettant de traiter et de surmonter les DCC.

L'intention de cette norme est de couvrir complètement le domaine des aspects permettant de surmonter les DCC et de fournir une vue générale des exigences pertinentes applicables aux systèmes d'I&C utilisés pour réaliser les fonctions importantes pour la sûreté (conformément à la CEI 61226) dans les centrales nucléaires.

b) Position de la présente norme dans la collection de normes du SC 45A de la CEI

La CEI 62340 est un document de deuxième niveau du SC 45A de la CEI traitant des DCC.

Cette norme internationale complète la CEI 61513 et ses normes fille par des exigences permettant de réduire la probabilité d'occurrence des DCC de fonctions d'I&C de catégorie A et de les surmonter. Les exigences fournies par cette norme s'appliquent aux fonctions de catégorie A (CEI 61226) dont la défaillance n'est pas acceptable par rapport à la conception de sûreté de la centrale.

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

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

Cette norme est applicable aux systèmes d'I&C importants pour la sûreté des nouvelles centrales nucléaires comme aux systèmes d'I&C de remplacement dans les centrales existantes. Lors du remplacement d'un système d'I&C, il peut être nécessaire de maintenir en l'état ou de mettre à niveau les fonctions d'I&C. Les exigences de cette norme prennent aussi en compte les remplacements d'I&C qui entraînent des modifications de la structure de l'I&C.

Pour les centrales existantes, seul un sous-ensemble des exigences de cette norme peut être applicable et il convient d'identifier ce sous-ensemble au début de chaque projet. Il convient de justifier au cas par cas, lors de l'évaluation de sûreté d'ensemble, les exigences et les recommandations qui ne sont pas mises en œuvre dans le cadre d'une mise à niveau ou d'un remplacement. Il convient de comparer dans un tout, les conséquences potentielles du non-respect de certains points de cette norme du fait de contraintes liées à la centrale, aux gains de sûreté obtenus lors de la mise à niveau.

Pour éviter d'empiéter sur des exigences existantes, cette norme tire avantage d'autres normes publiées en faisant référence aux paragraphes pertinents de celles-ci, et plus particulièrement à ceux des normes du secteur nucléaire: à savoir la CEI 61513, la CEI 60709, la CEI 60780 et la CEI 60880. Les nouvelles exigences sont fournies lorsqu'elles ne relèvent pas des domaines de ces normes.

d) Description de la structure de la collection des normes du SC 45A de la CEI et relations avec d'autres documents de la CEI et d'autres organisations (AIEA, ISO)

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la norme CEI 61513. Cette norme traite des exigences relatives aux systèmes et

équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la norme CEI 61513, un ensemble documentaire cohérent.

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

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

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie et de sûreté global, un cycle de vie et de sûreté des systèmes, et une interprétation des exigences générales de la CEI 61508-1, de la CEI 61508-2 et de la CEI 61508-4 pour le secteur nucléaire. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire. Dans ce cadre, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur nucléaire.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA (remplacé depuis par le document AIEA GS-R-3) pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle-commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

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)

1 Domaine d'application

Les systèmes d'I&C importants pour la sûreté peuvent être conçus en utilisant des matériels câblés conventionnels, des matériels informatiques ou en utilisant une combinaison des deux types de matériel. Cette norme fournit des exigences et des recommandations[1] pour l'ensemble de l'architecture des systèmes d'I&C qui peuvent contenir l'une, l'autre ou les deux technologies.

L'objectif de cette norme est de:

a) fournir des exigences relatives à l'évitement des DCC dans les systèmes d'I&C réalisant des fonctions de catégorie A;

b) exiger de façon complémentaire la mise en œuvre de systèmes d'I&C indépendants pour surmonter les DCC, lorsque la probabilité d'occurrence des DCC est déjà réduite en appliquant strictement les principes de sûreté prévalant au SC 45A de la CEI (en particulier ceux énoncés dans les CEI 61226, CEI 61513, CEI 60880 et CEI 60709);

c) donner une vue générale du domaine complet des exigences applicables aux DCC sans empiéter sur les domaines d'autres normes, celles-ci étant référencées.

Cette norme met l'accent sur la nécessité d'avoir un ensemble complet et précis de spécifications des fonctions de sûreté, reposant sur l'analyse des accidents de dimensionnement et sur la prise en compte des principaux objectifs de sûreté de la centrale. Ces spécifications sont un prérequis pour la production d'un ensemble exhaustif d'exigences qui est à la base de la conception permettant de surmonter les DCC.

Elle fournit les principes et les exigences pour surmonter les DCC par des moyens qui assurent l'indépendance[2]:

a) entre systèmes d'I&C réalisant diverses fonctions de sûreté de la catégorie A qui contribuent au même objectif de sûreté;

b) entre systèmes réalisant différentes fonctions dans différentes catégories, par exemple lorsqu'une fonction de catégorie B est déclarée comme assurant le secours d'une fonction de catégorie A et;

c) entre les canaux redondants au sein d'un même système d'I&C.

Différents types de défense contre les évènements initiateurs de DCC découlent de la mise en place de ces exigences.

Dans cette norme, les moyens permettant de se protéger contre les DCC sont traités en termes de:

a) sensibilité aux risques internes et externes à l'installation;

---

1 Afin de pouvoir identifier sans ambiguïté toutes les exigences et toutes les recommandations celles-ci sont numérotées dans le texte.

2 L'indépendance entre systèmes d'I&C ou entre chaînes redondantes du même système d'I&C est la capacité que les autres systèmes ou chaînes ont de réaliser leurs fonctions telles que prévues, en cas de défaillance hypothétique d'un système ou d'une chaîne d'autres systèmes.

b) propagation des effets physiques dans le matériel (par exemple surtensions); et

c) évitement d'erreurs ou de vulnérabilités propres aux systèmes d'I&C, en particulier:

   1) propagation des défaillances fonctionnelles au sein des systèmes d'I&C ou entre les différents systèmes d'I&C (par exemple par le biais des communications, de défauts ou d'erreurs affectant des ressources partagées),

   2) existence de défauts communs introduits lors de la conception ou durant l'exploitation du système (par exemple induits par des défauts de maintenance),

   3) validation système insuffisante telle que le comportement du système en réponse à des transitoires de données d'entrée ne pas correspond bien aux fonctions de sûreté prévues,

   4) qualification insuffisante des propriétés nécessaires des composants matériels, vérification insuffisante des composants logiciels, ou vérification insuffisante de la compatibilité des composants du système existants et de ceux qui ont été remplacés.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60671, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

CEI 60709, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Séparation*

CEI 60780, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 60880, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

CEI 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 61000-4 (toutes les parties), *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure*

CEI 61226, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle commande*

CEI 61513, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

AIEA Guide de Sûreté NS-G-1.3, *Instrumentation and control systems important to safety in Nuclear Power Plants*

AIEA Guide de Sûreté SG-D11, *General design safety principles for nuclear power plants*

AIEA Glossaire de sûreté, Ed. 2.0, 2006

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de la CEI 61513 et la CEI 61226 s'appliquent, ainsi que les suivants.

3.1
Défaillance de Cause Commune (DCC)
défaillance de deux ou de plusieurs structures, systèmes ou composants due à une cause ou à un événement spécifique unique

[AIEA Glossaire de sûreté, Ed. 2.0, 2006]

NOTE 1 La défaillance concomitante d'au moins deux structures, systèmes ou composants, produite par tous défauts cachés dus aux erreurs de conception, de fabrication, d'exploitation ou de maintenance, est dévoilée par un événement conséquence de phénomènes naturels, du fonctionnement de la centrale ou d'une action humaine ou par un événement interne au système d'I&C.

NOTE 2 L'expression défaillance concomitante est interprétée pour couvrir une séquence de défaillances de systèmes ou de composants, si l'intervalle de temps entre les défaillances est trop court pour mettre en place des mesures pour réparer.

3.2
défense en profondeur
mise en œuvre de plusieurs mesures de protection en vue d'un même objectif de sûreté, de façon à atteindre l'objectif même en cas d'échec d'une des mesures

[AIEA Glossaire de sûreté, Ed. 2.0, 2006]

NOTE Les mesures de protection sont supposées indépendantes.

3.3
diversité
existence de deux ou de plusieurs manières différentes d'atteindre un objectif donné. La diversité est en particulier utilisée comme moyen de défense contre une défaillance de cause commune. Elle peut être réalisée par la mise en oeuvre de systèmes physiquement différents les uns des autres ou par une diversité fonctionnelle, dans laquelle des systèmes similaires réalisent l'objectif spécifié de manière différente

[CEI 60880, 3.14]

NOTE Voir aussi «diversité fonctionnelle».

3.4
conception orientée vers la sûreté
conception de fonctions d'un système, telle qu'elles répondent en cas de défauts spécifiés de façon prédéfinie et sûre

3.5
défaillance
incapacité d'une structure, d'un système ou d'un composant à fonctionner conformément aux critères de recette

[AIEA Glossaire de sûreté, Ed. 2.0, 2006]

NOTE 1 Une défaillance est le résultat d'un défaut matériel, d'un défaut logiciel, d'un défaut système, ou d'une erreur humaine, et la trajectoire de signal associée qui provoque la défaillance.

NOTE 2 Voir aussi «défaut» et «défaillance logicielle».

3.6
défaut
imperfection dans un composant matériel, logiciel ou système

[CEI 61513, 3.22]

NOTE 1 L'ensemble des défauts peut être subdivisé en défauts aléatoires, qui par exemple résultent de dégradations matérielles entraînées par le vieillissement, et en défauts systématiques, par exemple les défauts logiciels qui résultent d'erreurs de conception.

NOTE 2 Un défaut (en particulier un défaut de conception) peut rester non détecté dans un système jusqu'à ce que les conditions particulières soient réunies pour que le résultat produit ne soit pas conforme à la fonction voulue, à savoir une défaillance apparaît.

NOTE 3 Voir aussi «défaut logiciel» et «défaut aléatoire».

3.7
évitement des défauts
utilisation de techniques et de procédures destinées à éviter l'introduction de défaut durant chacune des phases du cycle de vie de sûreté

[CEI 61508-4, 3.6.2, modifiée]

3.8
tolérance aux fautes
capacité intrinsèque d'un système de fonctionner correctement de manière continue en présence d'un nombre limité de défauts matériels ou logiciels

[CEI 60880, 3.18]

3.9
diversité fonctionnelle
application de la diversité au niveau fonctionnel (par exemple le déclenchement d'une action de protection sur seuil de pression ou sur seuil de température)

[CEI 60880, 3.19]

NOTE Voir aussi «diversité».

3.10
validation fonctionnelle
vérification de la conformité des spécifications des fonctions d'application aux exigences des fonctions et des performances primaires de la centrale. Elle est complémentaire de la validation du système, qui vérifie la conformité du système à la spécification des fonctions

[CEI 61513, 3.24]

3.11
erreur (ou faute) humaine
action humaine conduisant à un résultat indésirable

[CEI 60880, 3.21]

3.12
systèmes d'I&C indépendants
les systèmes indépendants possèdent les caractéristiques suivantes:

a) l'aptitude d'un système à réaliser sa fonction n'est pas affectée par le fonctionnement ou la défaillance de l'autre système;

b) l'aptitude des systèmes à réaliser leurs fonctions n'est pas affectée par les effets résultant de l'événement initiateur hypothétique pour lequel leur fonctionnement est requis;

c) une robustesse appropriée contre les influences externes communes (par exemple les tremblements de terre ou les IEM).

[définition modifiée d'«équipement indépendant» de l' AIEA Glossaire de sûreté, Ed. 2.0, 2006]

NOTE L'isolement électrique, la séparation physique, l'indépendance des communications et la non-interférence avec le procédé contrôlé sont les moyens qui lors de la conception permettent d'atteindre l'indépendance.

3.13
transitoire du signal d'entrée
comportement dans le temps de tous les signaux d'entrée qui alimentent le système d'I&C

NOTE Le comportement d'un système d'I&C est en fait déterminé par la trajectoire de signal qui couvre les états internes des matériels d'I&C. Cependant, les spécifications d'exigence définissent les réactions liées à la sûreté du système d'I&C répondant à des «transitoires de signaux d'entrée».

3.14
défaut caché
défaut non détecté dans un système d'I&C

NOTE Les défauts cachés peuvent être le résultat d'erreurs de spécification, de conception ou de défauts de réalisation et ils peuvent être de tous les types physiques ou techniques que l'on peut raisonnablement envisager. Dans le cas de défaut issu des spécifications ou de la conception, il convient de supposer que le défaut caché peut avoir été implanté dans tous les sous systèmes redondants de la même façon et qu'ainsi une trajectoire de signal puisse provoquer une DCC dans le système d'I&C en question.

3.15
défaut aléatoire
défaut non systématique d'un composant matériel

NOTE Les défauts matériels sont les conséquences d'effets chimiques ou physiques, qui peuvent survenir à tout instant. Une bonne description de la probabilité d'apparition des défauts aléatoires peut être assurée en utilisant les statistiques (taux de défauts). Un taux de défauts en augmentation peut être la conséquence de défauts systématiques dans la conception ou la fabrication du matériel, si cela survient sans corrélation temporelle, par exemple comme conséquence d'un vieillissement prématuré.

3.16
trajectoire de signal
historique de toutes les conditions des équipements, des états internes, des signaux d'entrée, et des entrées opérateur qui déterminent les valeurs de sortie d'un système

[CEI 60880, 3.33]

3.17
défaillance unique
défaillance qui rend un système ou un composant impropre à remplir sa ou ses fonctions de sûreté prévues et toute(s) défaillance(s) consécutive(s) à celle-ci

[AIEA Glossaire de sûreté, Ed. 2.0, 2006]

3.18

Critère de Défaillance Unique (CDU)
critère (ou exigence) appliqué à un système pour qu'il soit capable de réaliser sa tâche de sûreté en présence de toute défaillance unique

[AIEA Glossaire de sûreté, Ed. 2.0, 2006]

NOTE Voir également «défaillance unique», «défaillance logicielle».

3.19
défaillance logicielle
défaillance du système due à l'activation d'un défaut de conception d'un composant logiciel

[CEI 61513, 3.57]

NOTE 1 Toutes les défaillances logicielles sont dues à des défauts de conception, dans la mesure où un logiciel ne fait l'objet d'aucune usure ni ne souffre d'aucune défaillance physique. Les commandes qui activent les défauts du logiciel se présentant d'une manière aléatoire pendant le fonctionnement du système, les défaillances du logiciel se produisent également de manière aléatoire.

NOTE 2 Voir aussi «défaillance», «défaut», «défaut logiciel».

3.20
défaut logiciel
défaut de conception situé dans un composant logiciel

[CEI 61513, 3.58]

NOTE Voir aussi «défaut».

3.21
spécification
document qui spécifie de manière complète, précise et vérifiable les exigences, le comportement de la conception ou autres caractéristiques d'un système ou composant et, souvent, les procédures permettant de déterminer si ces dispositions ont été satisfaites

[CEI 60880, 3.39]

3.22
validation système
confirmation par examen et apport d'autres éléments justificatifs qu'un système satisfait à la totalité des exigences spécifiées (fonctionnalités, temps de réponse, tolérance aux fautes, robustesse)

[CEI 60880, 3.42]

3.23
défaillance systématique
défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

[CEI 61513, 3.62]

NOTE La défaillance de cause commune est un sous type des défaillances systématiques tel que les défaillances de systèmes séparés, d'éléments redondants ou de composants peuvent être déclenchées.

3.24
défaut systématique
défaut du matériel ou du logiciel qui concerne systématiquement certains ou tous les composants d'un type particulier

NOTE 1 Les défauts systématiques peuvent être le résultat d'erreurs de spécification ou de conception, de défauts de fabrication ou d'erreurs introduites durant les activités de maintenance.

NOTE 2 Les composants contenant des défauts systématiques cachés peuvent avoir des défaillances aléatoires ou de façon coïncidente, suivant le type de défaut et les mécanismes associés qui sollicitent le défaut.

3.25
validation
processus permettant de déterminer si un produit ou un service est apte à réaliser de façon satisfaisante sa fonction attendue

[AIEA Glossaire de sûreté, Ed. 2.0, 2006]

NOTE Voir aussi «validation fonctionnelle» et «validation système».

3.26
vérification
processus permettant de déterminer si la qualité ou les performances d'un produit ou d'un service sont telles que déclarées, prévues et exigées

[AIEA Glossaire de sûreté, Ed. 2.0, 2006]

4 Abréviations

DCC Défaillance de Cause Commune

ADD Accident De Dimensionnement[3]

EDD Evénement De Dimensionnement

IME Interférences Electro-Magnétiques

RU Recette Usine

AIEA Agence Internationale de l'Energie Atomique

I&C Instrumentation et Contrôle-commande

CNP Centrale Nucléaire de Puissance

EIH Evénement Initiateur Hypothétique

RS Recette Site

5 Conditions et stratégie permettant de faire face aux DCC

5.1 Généralités

Cet article explique la stratégie permettant de faire face aux DCC et justifie les exigences qui sont fournies dans les Articles 6 à 9.

5.2 Caractéristiques des DCC

Dans le cas des systèmes d'I&C réalisant des fonctions de catégories A, il a été prouvé que l'application appropriée de redondances, combinée à l'utilisation de mécanismes de vote permettent de satisfaire au critère de défaillance unique. Une telle conception garantit que la probabilité de défaillance des systèmes d'I&C est très basse.

Des systèmes d'I&C ainsi conçus peuvent défaillir si deux ou plus de leurs chaînes redondantes font défaut ensemble (DCC). La DCC peut survenir si un défaut caché est présent systématiquement dans certaines ou dans toutes les chaînes redondantes et si un événement particulier sollicite ce défaut entraînant la défaillance concomitante de certaines ou de toutes les chaînes. Un système d'I&C redondant peut faire défaut si le nombre de chaînes défaillantes dépasse sa limite de conception.

Les défauts cachés qui sont systématiquement présents dans certaines ou dans toutes les chaînes redondantes peuvent avoir leur origine dans n'importe laquelle des phases du cycle de vie du système d'I&C. Les défauts cachés peuvent résulter d'erreurs humaines indépendantes de la technologie d'I&C ou bien du processus de fabrication dépendant de la technologie d'I&C. Comparativement, les défauts systématiques cachés ont une forte probabilité d'être liés à la conception de base du système d'I&C comme par exemple:

– des erreurs de spécification d'exigences des fonctions de sûreté, ou
– une spécification inappropriée des limites de conception du matériel par rapport aux contraintes environnementales (par exemple les contraintes sismiques ou les IEM), ou
– des défauts de conception techniques qui peuvent entraîner la défaillance du système du fait de mécanismes internes induits.

Pour les DCC, les événements déclenchants peuvent avoir leur origine à l'extérieur du système d'I&C du fait de conditions communes à toutes les chaînes redondantes telles que des transitoires de signaux d'entrée, des contraintes environnementales ou des dates calendaires ou temps réel particulières. En plus, on peut faire l'hypothèse de l'existence de mécanismes de propagation cachés, tels que des données corrompues qui sont transférées d'un système en défaut aux systèmes correspondants en redondance, puissent entraîner la

[3] Les termes ADD et EDD sont utilisés conformément à leurs définitions fournies dans la CEI 61226.

défaillance des autres chaînes redondantes. Un tel mode de propagation de défaillances est seulement pertinent pour les systèmes d'I&C informatisés.

5.3 Principaux mécanismes des DCC des systèmes informatisés d'I&C

En technologie câblée, les fonctions importantes pour la sûreté sont généralement mises en oeuvre dans chaque chaîne redondante, par des ensembles de composants électroniques séparés alors que les composants matériel d'un système informatisé assurent généralement le traitement d'un groupe de fonctions affectées. Ainsi les considérations qui suivent s'appliquent principalement aux systèmes informatisés.

En condition de fonctionnement normal (sans modification due aux activités de maintenance et sans influence physique liée à l'environnement, telles que celles dont la liste est fournie en 7.8), le traitement des transitoires de signaux d'entrée par le système informatisé représente la contribution principale à leurs trajectoires de signal. Des trajectoires de signal particulières qui peuvent entraîner une défaillance du système peuvent survenir à l'occasion de demandes de sûreté résultant de combinaisons de signaux d'entrée non testées ou peuvent résulter d'états internes du système. De tels états internes particuliers du système peuvent être liés à des données mémorisées lors de transitoires de signaux d'entrée apparus précédemment, ou à des défauts cachés introduits par des activités de maintenance anciennes ou à des défauts matériel.

Des DCC peuvent apparaître si des composants matériel de certaines ou de toutes les redondances sont mis en défaut par des conditions environnementale dépassant les limites de conception du matériel. Les causes de ces mécanismes de défaillance peuvent par exemple être:

– une conception négligeant les principes de séparation physique, telle qu'une défaillance unique d'un système d'alimentation ait un impact sur deux redondances ou plus; ou
– des limites de conception du matériel spécifiées de façon inappropriée par exemple en ce qui concerne les évènements sismiques.

La probabilité qu'une DCC puisse être la conséquence de défauts aléatoires des composants matériel est très faible. Cette DCC présupposerait qu'un défaut particulier puisse rester caché pour une période suffisamment longue pour que les composants des autres redondances puissent être affectés par ce type de défaut. Pour rester caché, il faut que le défaut ne soit pas identifié par les moyens de surveillance ou par les essais périodiques et que les composants incriminés ne soient pas l'objet de défaillance spontanée mais se mettent en défaut lorsqu'ils sont sollicités par un événement déclencheur commun dans certaines ou dans toutes les redondances.

Les conséquences d'une DCC système peuvent faire qu'en cas de sollicitation la réponse du système soit telle que les évènements suivants surviennent:

– aucune réponse n'est donnée ou bien une réponse erronée par rapport à la réponse attendue est donnée par le système d'I&C qui poursuit ses traitements;
– l'arrêt du système provoque l'interruption des traitements, ainsi aucune réponse ne peut être fournie.

5.4 Conditions permettant de lutter contre les DCC des systèmes d'I&C individuels

On déduit des caractéristiques des DCC dont la liste est fournie en 5.2, les moyens suivants pour réduire les probabilités de DCC:

a) réduire la probabilité de défauts systématiques cachés présents dans les chaînes redondantes du système d'I&C individuel, et
b) réduire la probabilité de présence de mécanismes pouvant solliciter de façon concomitante les défauts systématiques cachés ou pouvant entraîner la propagation d'une défaillance unique d'une chaîne aux autres chaînes.

La difficulté pour assurer une défense efficace contre les DCC réside dans le fait que les défauts et les mécanismes déclencheurs du système d'I&C sont cachés. L'évitement des défauts systématiques cachés et des mécanismes déclencheurs nécessite une analyse et une conception des systèmes postulants, d'après expérience, l'occurrence de DCC en centrale nucléaire et la faiblesse potentielle de la technologie d'I&C choisie.

D'après l'expérience, la fréquence d'occurrence des DCC est très faible pour les systèmes d'I&C réalisant des fonctions de catégorie A. Ceci repose en partie sur le haut niveau de qualité de conception, de fabrication et de maintenance observé pour de tels systèmes, néanmoins cela repose aussi sur la nature des DCC qui ne peuvent survenir que par la probabilité combinée de l'existence de défauts systématiques cachés et de l'activation des mécanismes déclencheurs correspondant par une trajectoire de signal. Ainsi une défense efficace contre les DCC doit considérer avec la même importance l'évitement des mécanismes déclencheurs potentiels et l'évitement des défauts cachés.

L'expérience montre que dans l'apparition de DCC en centrale nucléaire les types de causes suivants dominent:

a) des défauts cachés liés à des défauts de spécification d'exigences. L'identification des erreurs dans la spécification d'exigences des fonctions d'I&C est difficile et de telles erreurs peuvent se propager au cours des phases de conception successives y compris lors des activités de vérification et de validation système. Les défauts cachés de cette origine potentielle ne peuvent être détectés que lors d'activités de validation fonctionnelle (voir 3.25);
b) des défauts cachés introduits lors de maintenance peuvent être limités du fait des contraintes imposées par la centrale en termes d'analyse et d'essai des modifications (par exemple modification des points de consigne, utilisation de modèle révisé de pièce de rechange ou mise à niveau des composants de système d'I&C); et
c) le déclenchement des défauts cachés durant les activités de maintenance, dû en partie à des états de système particuliers ou en partie à des données invalides qui ne représentent pas l'état réel de la centrale.

Suivant la technologie d'I&C, différents types de propagation de défaillance sont pertinents:

d) les systèmes d'I&C analogique peuvent être menacés par les surtensions, si une chaîne peut être endommagée par une défaillance unique et que les chaînes voisines peuvent être endommagées par les défaillances consécutives et si les limites de conception relatives à la séparation des chaînes sont dépassées;
e) pour la technologie numérique la propagation des défaillances par surtension peut être exclue si des fibres optiques sont employées, néanmoins des moyens particuliers sont nécessairement mis en œuvre pour réduire la sensibilité à la propagation de défaillance liée à des données manquantes ou erronées.

Cette norme donne des recommandations pour réduire la probabilité d'existence de mécanismes qui peuvent faciliter la sollicitation de types potentiels de défauts de conception cachés entraînant l'apparition de DCC durant les transitoires (voir Articles 7, 8 et 9).

Pour réduire au niveau minimum possible la probabilité que des défauts de conception cachés subsistent dans la version finale du système d'I&C, on doit faire référence aux exigences de conception contenues dans les normes du SC 45A (voir Article 2).

5.5 Stratégie de conception permettant de surmonter les DCC

Les mesures de conception permettant de surmonter les DCC sont liées à une architecture d'I&C qui comprend au moins deux systèmes d'I&C ou plus pour réaliser les fonctions de catégories A. La démonstration prouvant que chaque système individuel d'I&C est sans défaut est impossible et donc l'existence de défauts cachés et de mécanismes de déclenchement associés ne peut en principe être exclue. En conséquence l'occurrence de DCC ne peut être exclue pour aucun des systèmes d'I&C individuels bien que la fréquence d'occurrence attendue puisse être inférieure à une pour la durée de vie prévue de la centrale.

Si on suppose qu'un système d'I&C est en défaut suite à une DCC, il est nécessaire que la fonction principale de catégorie A soit réalisée par un autre système d'I&C pour éviter les conséquences inacceptables et pour préserver les principaux objectifs de sûreté de la centrale. Cet autre système d'I&C doit réaliser indépendamment sa fonction de sûreté qui lui est affectée (voir 3.12) pour que la probabilité d'une défaillance concomitante des deux systèmes soit réduite à un niveau négligeable pour la durée de vie prévue de la centrale.

La réduction de la probabilité d'une défaillance concomitante de systèmes d'I&C indépendants à un niveau négligeable implique que les systèmes fonctionnent avec des trajectoires de signal différentes et que les systèmes soient protégés de façon correcte contre les risques physiques (voir 5.3). On peut garantir la différence des trajectoires de signal en appliquant le principe de diversité (par exemple diversité matériel ou diversité fonctionnelle).

L'application de la diversité fonctionnelle est la seule possibilité pour assurer une protection contre les défauts fonctionnels cachés potentiels présents dans la spécification d'exigences. L'affectation des fonctions diversifiées à des systèmes d'I&C indépendants peut en même temps servir de moyen pour garantir que les systèmes fonctionnent avec des trajectoires de signal différentes.

Cette norme fournit des recommandations pour la conception et la mise en oeuvre de systèmes indépendants fonctionnant avec des trajectoires de signal différentes (voir 3.16), pour que la probabilité de défaillance concomitante de ces systèmes indépendants soit négligeable au regard de la durée de vie prévue de la centrale même si des défauts de conception communs cachés peuvent exister (voir Articles 6, 7 et 9).

6 Exigences permettant de surmonter les défauts de spécification d'exigences

6.1 Elaboration des spécifications d'I&C à partir des bases de conception de sûreté de la tranche

La diversité fonctionnelle permet de garantir que les principaux objectifs de sûreté de la centrale sont atteints, malgré l'existence possible de défauts cachés liés à des erreurs de spécification d'exigences.

L'analyse des ADD et des EDD pertinents qui peuvent être conséquence de défaillances de l'I&C fournit les spécifications d'exigence à partir desquelles découlent tous les besoins de diversité fonctionnelle de l'application. Ceci peut dépendre de l'estimation des conséquences de défaillance, et de l'estimation de la fréquence des EDD.[4]

6.1.1 Cette analyse doit comprendre les étapes suivantes:

a) Les EDD qui pourraient avoir des conséquences inacceptables en cas de DCC hypothétiques, doivent être identifiés si une DCC est postulée pour le système d'I&C pertinent. Une conception tolérant les DCC est nécessaire pour ce sous-ensemble d'EDD dont la fréquence est plus élevée que les limites spécifiées.

b) Pour ce sous-ensemble d'EDD on doit identifier au moins un second paramètre de sûreté et l'évaluer au niveau de la spécification des fonctions de sûreté diversifiées.[5]

---

[4] La disponibilité des fonctions de protection diversifiées, et en particulier la disponibilité de signaux de mesure diversifiés ou indépendants, est un résultat de conception des systèmes procédé de la centrale. En général, lors de la conception des systèmes d'I&C importants pour la sûreté (par exemple existence d'actionneurs diversifiés), l'application des exigences et les recommandations de cette norme visent à utiliser le potentiel de sûreté des systèmes de procédé de la centrale.

[5] La majorité des grands transitoires ont une influence sur pratiquement tous les paramètres de sûreté en même temps, si bien que l'application du principe de diversité fonctionnelle est préconditionnée par une analyse plus détaillée des accidents de référence, mais généralement aucun paramètre de sûreté supplémentaire n'est nécessaire.

6.1.2 La mise en œuvre des fonctions de sûreté qui sont identifiées par rapport aux DCC, conformément à 6.1.1, peut être réalisée en suivant différentes stratégies de conception[6]. On doit démontrer que pour les conceptions retenues, les objectifs de sûreté principaux de la centrale sont satisfaits en présence de DCC hypothétiques.

6.2 Application des principes de défense en profondeur et de diversité fonctionnelle

L'application des principes de défense en profondeur et de diversité fonctionnelle nécessite d'identifier les fonctions de catégorie A particulières qui peuvent assurer indépendamment qu'on atteint les principaux objectifs de sûreté de la tranche. Ces fonctions sont appelées fonctions diversifiées par rapport à rapport à un objectif de sûreté particulier.

6.2.1 Les fonctions d'I&C de catégorie A diversifiées doivent être affectées à des systèmes d'I&C indépendants et doivent être mises en œuvre de telle façon qu'en cas de défaillance hypothétique d'un de ces systèmes indépendants, les principaux objectifs de sûreté de la centrale sont encore atteints par les fonctions réalisées par le ou les autres systèmes d'I&C indépendants.

Les étapes de conception suivantes doivent être réalisées.

6.2.2 La démonstration de l'indépendance de l'exécution des fonctions diversifiées doit être documentée dans les études de sûreté.

6.2.3 Si des fonctions de catégorie B sont utilisées au titre d'une action efficace indépendante par exemple comme secours de fonctions de catégorie A, alors l'indépendance entre le système réalisant des fonctions de catégorie A et le système réalisant des fonctions de catégorie B doit être démontrée conformément aux exigences de cette norme.

6.2.4 La validation fonctionnelle des fonctions importantes pour la sûreté doit être réalisée à l'aide de moyens adaptés pour démontrer (par exemple par simulation du procédé) que les spécifications d'exigence sont correctes par rapport aux exigences relatives aux performances et aux fonctionnalités de l'installation. La validation doit être réalisée conformément aux articles applicables de la CEI 61513.

6.2.5 Lors de la validation on doit démontrer que les principaux objectifs de sûreté de la centrale sont satisfaits, même si l'un des deux systèmes d'I&C indépendants et son groupe de fonctions diversifiées est supposé non opérationnel.

a) La validation système doit être réalisée conformément aux articles applicables de la CEI 61513 et de la CEI 60880.
b) Dans le cadre de la validation d'ensemble des fonctions de catégorie A mises en oeuvre, il convient que toutes activités associées à la validation soient évaluées d'une façon globale en considérant en même temps:
   – la validation fonctionnelle (par exemple le traitement du logiciel d'application s'exécutant dans un environnement matériel approprié bien que différent du système cible),

---

6 Des exemples de stratégies de conception qui peuvent être acceptables ou avoir été reconnues acceptables dans certains (mas pas forcément tous les) contextes nationaux:

- Les fonctions de sûreté diversifiées identifiées sont groupées de telle façon que chacun des EDD considérés soit géré par l'ensemble des groupes de fonctions de sûreté. Chacun de ces groupes est affecté à un système d'I&C indépendant. Le reste des fonctions de catégorie A est affecté à n'importe lequel de ces systèmes d'I&C. L'affectation garantit suffisamment la différentiation des trajectoires de signal qui seront traitées par les systèmes d'I&C indépendants pour que ceux ci puissent reposer sur la même plate-forme matériel de système d'I&C.

- Le domaine complet des fonctions de catégorie A (y compris les paires de fonctions diversifiées) est assigné à un système d'I&C (système d'I&C de protection primaire). Puis le traitement d'un groupe de fonctions de sûreté diversifiées identifiées est dupliqué dans un système de protection secondaire indépendant qui peut être de classe matériel inférieure. La diversité matériel est nécessaire pour suffisamment garantir la différentiation des trajectoires de signal entre les systèmes d'I&C indépendants.

– les vérifications du système intégré cible dans une configuration d'essai représentative et pour les RU,

– les essais de mise en service définitive après intégration dans la centrale (RS).

6.3 Questions relatives aux DCC pour les centrales existantes

6.3.1 Lorsque cette norme est appliquée dans le cadre de mise à niveau d'I&C de centrale, les dérogations aux exigences de la norme doivent être justifiées.

Les arguments de justification suivant peuvent être retenus:

– comparaison des avantages et inconvénients de l'I&C existant avant et après mise à niveau,

– contraintes physiques imposées par la centrale existante,

– prise en compte du retour d'expérience relatif à l'apparition de DCC dans les centrales,

– nouvelle analyse de la conception de base pour laquelle il convient de considérer les exigences de conception conformes à l'état de l'art courant.

7 Mesures de conception pour lutter contre les défaillances concomitantes des systèmes d'I&C

7.1 Principe d'indépendance

Les systèmes d'I&C réalisent leurs fonctions de sûreté indépendamment, si une défaillance hypothétique d'un de ces systèmes d'I&C n'empêche pas les autres systèmes de réaliser leurs fonctions comme prévu (voir 3.12).

Les principes de conception suivants doivent être utilisés pour assurer une défense efficace contre les DCC.

7.1.1 L'atteinte de l'objectif de fiabilité cible impose de satisfaire aux exigences portant sur la conception, la mise en œuvre et l'exploitation des systèmes d'I&C associés qui réalisent des fonctions de catégorie A. Il est nécessaire de satisfaire aux exigences pertinentes au niveau des systèmes individuels pour la conception système (CEI 61513), pour la conception du logiciel (CEI 60880), pour la séparation physique (CEI 60709) et pour la qualification des composants (aspect généraux: CEI 60780 et tenue aux séismes: CEI 60980). En plus de cela, les exigences de cette norme doivent être satisfaites pour garantir une exécution indépendante des diverses fonctions de sûreté.

7.1.2 Le principe de l'indépendance des systèmes d'I&C vise à limiter l'influence de la DCC à un seul système. Une analyse doit être réalisée pour identifier les mécanismes communs qui pourraient mettre en péril l'indépendance de tels systèmes. Il convient d'éliminer les mécanismes communs identifiés qui pourraient mettre en péril l'indépendance de tels systèmes d'I&C ou bien on doit montrer que l'on peut limiter les conséquences de ceux-ci de façon satisfaisante.

7.1.3 La conception de l'architecture des systèmes d'I&C réputés indépendants doit assurer que:

a) les chemins de traitement particuliers du système, de l'acquisition des données d'état de la centrale jusqu'aux actionneurs des systèmes de sûreté de la centrale, n'utilisent aucun composant commun; et

b) les systèmes support (par exemple systèmes d'alimentation électrique ou de conditionnement de l'air) soient constitués de sous-systèmes suffisamment séparés et redondants (CEI 60709);

c) les moyens d'auto-surveillance fonctionnent de façon indépendante par rapport aux unités de traitement.

7.1.4 Pour exclure la défaillance concomitante de systèmes d'I&C déclarés indépendants, on doit analyser leurs conditions de fonctionnement pour identifier les événements déclencheurs communs.

7.1.5 La diversité fonctionnelle doit être appliquée conformément à 6.1 lorsque cela est applicable à la mise en œuvre des systèmes d'I&C, pour surmonter les défauts potentiels de spécification des fonctions de catégorie A. Cette mesure est efficace indépendamment de la technologie d'I&C utilisée.

7.2 Conception des systèmes d'I&C indépendants

7.2.1 Les systèmes d'I&C indépendants réalisant des fonctions de catégorie A doivent être conçus de telle façon que la probabilité d'occurrence d'une défaillance concomitante de ces systèmes due à un même transitoire de signaux d'entrée soit réduite à un niveau non significatif pour la durée de vie prévue de la centrale. Cette exigence peut être satisfaite par des mesures garantissant la différence des trajectoires de signal (voir 6.1.2 et 7.3).

7.2.2 Les systèmes indépendants ne doivent pas utiliser de composants ou des services partagés si la défaillance hypothétique de ces composants ou services partagés peut entraîner une défaillance concomitante des systèmes indépendants (par exemple alimentation électrique commune).

7.2.3 L'utilisation de matériels ou de logiciels identiques pour la réalisation de systèmes d'I&C indépendants doit être analysée pour démontrer que l'apparition de DCC hypothétiques peut être négligée. Sinon elle doit être restreinte:

– à des tâches réalisées dans des conditions et avec des charges différentes (principalement applicables aux unités numériques réalisant des traitements de trajectoires de signal différentes), ou/et
– à des tâches indépendantes du profil de sollicitation et des facteurs d'influence du procédé de tranche (par exemple composant matériel non soumis aux ambiances accidentelles ou composants logiciel dont le comportement n'est pas influencé par les données traitées par les fonctions prévues qu'ils réalisent).

7.2.4 Si l'utilisation de composants particuliers dont le comportement dépend de leur profil de sollicitation est nécessaire (par exemple des capteurs dans l'enceinte de confinement ou des relais qui doivent être mis sous ou hors tension lors de leur sollicitation), alors ces composants doivent être qualifiés pour les conditions opérationnelles prévalant lors de leur sollicitation (voir la CEI 60780) et ils doivent faire l'objet de tests périodiques (voir la CEI 60671). L'utilisation de composants matériels différents peut présenter des avantages, mais il convient d'analyser le besoin de diversité.

7.3 Application de la diversité fonctionnelle

7.3.1 La sensibilité des systèmes d'I&C programmés aux DCC doit être analysée en évaluant les applications et les trajectoires de signal possibles pour les modules logiciels élémentaires:

– la diversité fonctionnelle doit être appliquée pour diversifier la partie « signaux d'entrée » des trajectoires de signal. La diversification des autres parties des trajectoires de signal doit être prise en compte (par exemple les états internes);
– l'absence de défaut caché peut être garantie pour des modules logiciels très petits et très simples pour lesquels une analyse de défaut et des essais appropriés peuvent être réalisés.

7.3.2 Les systèmes d'I&C indépendants ne doivent pas réaliser des fonctions d'application identiques, afin de réduire la probabilité d'occurrence de conditions dans lesquelles une défaillance fortuite quasi synchronisée de ces systèmes puisse être provoquée par le même transitoire de signaux d'entrée. Si la mise en œuvre de sous-fonctions identiques ne peut être évitée pour des raisons de conception de la centrale, ces sous-fonctions identiques doivent au moins être alimentées par des signaux d'entrée provenant de capteurs différents.

7.4 Evitement de la propagation des défaillances par les canaux de communication

7.4.1 Dans le cadre de la prise en compte des DCC, il ne doit pas y avoir de communications entre systèmes d'I&C indépendants mis en œuvre pour lutter contre les DCC au sens de 6.1.2.

7.4.2 La conception des systèmes d'I&C réalisant des fonctions de catégorie A doit garantir que l'on assure une protection maximale contre la propagation de défaillance à l'intérieur du système d'I&C. L'implémentation de cet objectif de conception nécessite la mise en œuvre en parallèle des mesures de conception suivantes:

a) Les systèmes d'I&C doivent être conçus pour que le fonctionnement système ne puisse pas être menacé par des sous-systèmes centralisés, qui par exemple peuvent fournir de l'information pour affichage en salle de commande principale ou qui peuvent être à l'origine de modifications de paramètres provenant du procédé et qui doivent être transmis à toutes les redondances du système d'I&C pour des fonctions de catégorie A.

b) Les données corrompues identifiées doivent être exclues des traitements ultérieurs au niveau du logiciel d'application.

c) Toutes les fonctions assurées par le logiciel système pour le transfert des messages doivent être mises en oeuvre de telle façon que l'exécution correcte de ces fonctions de transfert logiciel ne puisse être perturbée par aucune valeur dépendant du procédé et objet du transfert, voir aussi 8.1.

d) La correction des données reçues doit être vérifiée avant de réaliser les traitements ultérieurs.

e) La séparation physique des sous-systèmes redondants doit être conçue conformément à la CEI 60709.

7.4.3 L'échange de données d'entrée entre les unités redondantes peut introduire des dépendances entre les voies et doit donc être analysé du point de vue des DCC possibles. Il convient d'utiliser la validation en ligne des données d'entrée (par exemple au moyen d'un vote) comme moyen adapté pour limiter la propagation de données corrompues. Il convient de marquer et d'exclure des futurs traitements ces données d'entrée que l'on sait déjà être corrompues (par exemple les sorties de gamme).

7.5 Mesures à prendre contre les défaillances système provoquées par les activités de maintenance

Les exigences particulières suivantes applicables aux DCC doivent être satisfaites en plus de celles fournies par la CEI 61513:

7.5.1 Les systèmes d'I&C réalisant des fonctions de catégorie A doivent être analysés au cours de la conception pour démontrer leur aptitude système à tolérer au niveau de leur comportement les activités de maintenance et d'essai.

Les points clef de cette démonstration sont les suivants:

a) Si un EDD peut être la conséquence de la mise en service intempestive de composants procédé contrôlés par un système d'I&C, alors les moyens pour éviter cette mise en service intempestive par des actions de maintenance doivent être fournis.

b) Le volume des fonctions de catégorie A qui peuvent être affectées simultanément par des activités de maintenance doit être compatible avec les principes de conception de sûreté de la centrale.

7.5.2 Afin de réduire le risque d'inhibition des redondances multiples au cours d'activités de maintenance et d'essais en ligne, il convient de mettre en place les moyens de détecter ces erreurs (par exemple surveillance en ligne de l'état des systèmes) durant la maintenance ainsi que les moyens permettant de terminer sous contrôle les activités de maintenance pour laisser le système dans un état acceptable.

7.6 Intégrité du matériel du système d'I&C

L'auto-surveillance est nécessaire pour améliorer la disponibilité des systèmes importants pour la sûreté. Bien que non directement liées aux DCC, les exigences suivantes sont fournies dans un souci de complétude:

7.6.1 Des moyens d'auto-surveillance en fonctionnement doivent être mis en œuvre (voir la IEC 60880):

a) Lorsque les fonctions d'auto-surveillance détectent un défaut le système doit se mettre dans un état particulier prédéterminé.

b) Cet état doit être choisi en fonction des principes associés aux positions de repli orientées vers la sûreté, en analysant l'action privilégiée qui est prise lors de l'apparition du défaut. Ceci peut souvent entraîner une mise en service de moyens pour raison de sûreté, mais cela peut aussi prévenir une mise en service intempestive lorsque celle-ci pourrait être à l'origine d'un EDD.

c) Pour réduire la probabilité que l'accumulation de défauts matériels non identifiés ne produise une défaillance système.

7.6.2 Une alarme doit être à disposition en salle de commande lorsque des actions de sûreté sont bloquées ou initiées automatiquement par les fonctions d'auto-surveillance lorsqu'un défaut est détecté.

7.6.3 Le retour d'expérience concernant le fonctionnement des systèmes d'I&C analogiques en ambiance contrôlée prouve que les modules matériels présentant des défauts de fabrication mineurs et dont le comportement est conforme à ce qui était attendu, ont un taux de défaillance qui augmente sur le tard. Concernant la détection précoce des défauts systématiques, toutes les défaillances doivent être analysées et enregistrées pour que le personnel de maintenance puisse être prévenu suffisamment tôt pour prendre les contre-mesures nécessaires avant qu'une DCC ne survienne. (Les modules matériels présentant des défauts de fabrication qui compromettent déjà le succès de la mise en service ne relèvent pas des DCC.)

7.6.4 Les composants de technologie d'I&C choisie peuvent présenter essentiellement en début de leur vie une baisse du taux de défaillance. Ainsi, il convient de réaliser un premier vieillissement au niveau composant ou système avant de débuter le fonctionnement relatif à la sûreté.

7.7 Précautions contre les dépendances liées à des dates ou à des messages externes

7.7.1 Les systèmes d'I&C réalisant des fonctions de catégorie A doivent être conçus pour que leur comportement en exploitation ne soit influencé de l'extérieur par aucune dépendance non prévue liée aux informations contextuelles telle que des dates calendaires particulières.

7.7.2 Concernant la prévention des accès et des manipulations des systèmes d'I&C par des personnels non autorisés, ainsi que le fait d'éviter les erreurs de manipulation du personnel d'exploitation, on doit appliquer les exigences fournies par la CEI 60880.

7.8 Assurance de la séparation physique et de la robustesse aux conditions d'ambiance

L'assurance de la robustesse des systèmes d'I&C réalisant des fonctions de catégorie A est essentielle. Tous les mécanismes connus de défaillance liés aux conditions d'ambiance menacent les composants matériels des systèmes d'I&C. Il n'est pas nécessaire d'ajouter d'exigences à celles établies par les normes déjà publiées. Ainsi ce groupe de mécanismes de défaillance n'est évoqué que d'un point de vue de la complétude du document.

Pour maîtriser les DCC liées aux conditions d'ambiance et concernant les systèmes réalisant des fonctions de catégorie A, on doit satisfaire aux exigences pertinentes des normes suivantes:

– CEI 60780 pour la qualification du matériel (en général),
– CEI 60980 pour la qualification du matériel aux séismes,
– CEI 61000-4 pour la compatibilité électromagnétique,
– CEI 60709 pour les exigences de séparation et d'isolement.

8 Tolérance aux défauts logiciels cachés hypothétiques

8.1 Il convient que les systèmes informatisés d'I&C réalisant des fonctions de catégorie A soient conçus conformément à la CEI 61513, pour que le fonctionnement interne soit indépendant du profil de sollicitation. Les exigences suivantes s'ajoutent à celles fournies par la CEI 60880 et sont cohérentes avec ces dernières. Elles réduisent les possibilités que des défauts logiciels cachés puissent être sollicités par des données associées à des transitoires du procédé de la centrale.

a) Il convient que les logiciels système et application soient séparés de façon que le traitement algorithmique des données liées au procédé de la centrale soit entièrement réalisé par le logiciel d'application.
b) Il convient que la mise en œuvre des fonctions logiciel système ne puisse être influencée par des données qui dépendent directement ou indirectement de l'état de la centrale (par exemple transfert des données procédé comme des chaînes de bits). Cette exigence générale doit être satisfaite en plus de celles fournies à l'Article B.2 de la CEI 60880 et ceci comprend:
   – Le traitement cyclique des fonctions d'application est invariant.
   – Les charges de traitement et de communication sont invariantes.
   – L'évitement des interruptions déclenchées par des données procédé (pour la restriction générale de l'usage des interruptions, voir l'Article B.2 de la CEI 60880).

8.2 Le logiciel (d'application) doit être conçu pour être tolérant aux signaux d'entrée invalides, lorsqu'ils se présentent de façon isolée ou en groupe ou lorsqu'ils sont dus à des transitoires courts intempestifs de signaux d'entrée, et ceci pour que l'exécution des actions de sûreté soit garantie et que les actions intempestives soient évitées.

8.3 Les signaux d'entrée invalides ou en défaut doivent être identifiés en ligne. Si des signaux en défaut identifiés sont traités par comparaison avec des informations redondantes, alors les dépendances introduites entre les sous-systèmes redondants doivent être analysées du point de vue des DCC.

8.4 Lorsqu'un système d'I&C réalise différentes fonctions et qu'un ou plusieurs signaux utilisés par une fonction se révèlent invalides, aucune des autres fonctions dont les signaux d'entrée n'ont pas été perturbés ne doit être affectée.

8.5 Le logiciel doit être conçu pour agir de façon sûre même lors de sa réponse à plusieurs défaillances concomitantes ou à des défaillances apparentes affectant les signaux d'entrée. Il convient que cette action orientée sûreté évite les mises en marche intempestives

et puisse envoyer les ordres d'arrêt ou les alarmes comme cela est spécifié dans les exigences fonctionnelles du système.

9 Exigences permettant d'éviter les défaillances système dues à la maintenance en exploitation

9.1 Pour éviter de produire des défaillances au niveau de plus d'un des trains, des chaînes ou des sous-systèmes redondants des systèmes d'I&C réalisant des fonctions de catégorie A, les activités simultanées doivent être restreintes à une seule redondance (par exemple par des verrouillages croisés ou des procédures administratives).

9.2 Les effets de l'activité de maintenance devant se dérouler tranche fonctionnant en puissance doivent être analysés pour empêcher la défaillance de tout autre système d'I&C réalisant des fonctions de catégorie A et qui n'est pas l'objet de cette activité de maintenance.

9.3 Lorsqu'il est nécessaire de remplacer des composants matériel par des pièces de rechange différentes, on doit s'assurer par une qualification appropriée logiciel comme matériel et par une vérification de la compatibilité des composants remplacés avec les composants existants que la fiabilité des systèmes d'I&C de sûreté n'a pas été dégradée et que de nouveaux modes de défaillance n'ont pas été introduits. On doit justifier du caractère adapté de la qualification en prenant en compte la complexité des composants.

9.4 Afin de limiter les effets de dégradation de la robustesse des composants liés au vieillissement, il convient d'analyser la durée de vie utile de ceux-ci.

Annexe A
(informative)

Relation entre la CEI 60880 et cette norme

Au niveau du FDIS de la CEI 60880 (édition 2 de 2006), le groupe de travail A3 du sous-comité 45A a décidé d'intégrer l'Article 13 de la CEI 60880-2: 2000, traitant des DCC sans modifications conformément aux principes de développement de cette norme. De la même façon, la proposition d'intégrer l'Article 8 de cette norme relatif aux DCC particulières au logiciel dans l'Annexe B de la CEI 60880 a été rejetée.

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
P.O. Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch