

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

60880-2

Première édition
First edition
2000-12

**Logiciel pour les calculateurs de sûreté
des centrales nucléaires –**

**Partie 2:
Défense contre les défaillances de cause
commune provoquées par le logiciel,
utilisation d'outils logiciels et de logiciels
prédéveloppés**

**Software for computers important to safety
for nuclear power plants –**

**Part 2:
Software aspects of defence against common
cause failures, use of software tools and of
pre-developed software**



Numéro de référence
Reference number
CEI/IEC 60880-2:2000

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- Site web de la CEI (www.iec.ch)
- Catalogue des publications de la CEI

Le catalogue en ligne sur le site web de la CEI (www.iec.ch/catlg-f.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.

- IEC Just Published

Ce résumé des dernières publications parues (www.iec.ch/JP.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.

- Service clients

Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

Email: custserv@iec.ch
Tél: +41 22 919 02 11
Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- IEC Web Site (www.iec.ch)
- Catalogue of IEC publications

The on-line catalogue on the IEC web site (www.iec.ch/catlg-e.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- IEC Just Published

This summary of recently issued publications (www.iec.ch/JP.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- Customer Service Centre

If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC**

60880-2

Première édition
First edition
2000-12

**Logiciel pour les calculateurs de sûreté
des centrales nucléaires –**

**Partie 2:
Défense contre les défaillances de cause
commune provoquées par le logiciel,
utilisation d'outils logiciels et de logiciels
prédéveloppés**

**Software for computers important to safety
for nuclear power plants –**

**Part 2:
Software aspects of defence against common
cause failures, use of software tools and of
pre-developed software**

© IEC 2000 Droits de reproduction réservés — Copyright - all rights reserved

Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Electrotechnical Commission
Telefax: +41 22 919 0300

3, rue de Varembe Geneva, Switzerland
e-mail: inmail@iec.ch IEC web site <http://www.iec.ch>



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

W

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

	Pages
AVANT-PROPOS	6
INTRODUCTION	8
Articles	
1 Domaine d'application et objet.....	10
2 Références normatives.....	10
3 Définitions et abréviations	12
4 Prescriptions et recommandations.....	18
4.1 Moyens de défense contre les défaillances logicielles de cause commune.....	18
4.1.1 Introduction	18
4.1.2 Conception du logiciel pour éviter les CCF.....	20
4.1.3 Sources et effets des CCF logicielles.....	20
4.1.4 Mise en oeuvre de la diversité	22
4.1.5 Pondération des inconvénients et des avantages liés à l'utilisation de la diversité.....	24
4.2 Outils logiciels pour le développement de logiciels.....	24
4.2.1 Introduction	24
4.2.2 Sélection des outils	26
4.2.3 Prescriptions applicables aux outils	26
4.3 Qualification de logiciels prédéveloppés	36
4.3.1 Introduction.....	36
4.3.2 Prescriptions générales	38
4.3.3 Processus d'évaluation et d'agrément.....	38
4.3.4 Prescriptions liées à l'intégration dans le système et à la maintenance des LPD.....	50
Annexe A (informative) Considérations sur les CCF et la diversification.....	56
A.1 CCF logicielle	56
A.2 Causes et effets des CCF potentielles	56
A.3 Défense contre les CCF.....	58
A.4 Preuve de conformité	60
A.5 Caractéristiques de la diversité.....	60
A.6 Inconvénients, avantages et justification de la diversité.....	62
Annexe B (informative) Prescriptions de la CEI 60880 pour l'utilisation et la qualification des outils logiciels	64
Annexe C (informative) Outils pour la production et la vérification des spécifications, de la conception et du code	66
C.1 Outils constructifs.....	66
C.2 Outils analytiques	68

CONTENTS

	Page
FOREWORD	7
INTRODUCTION	9
Clause	
1 Scope and object	11
2 Normative references	11
3 Definitions and abbreviations.....	13
4 Requirements and recommendations.....	19
4.1 Defences against common cause failure due to software	19
4.1.1 Introduction	19
4.1.2 Design of software against CCF	21
4.1.3 Sources and effects of CCF due to software	21
4.1.4 Implementation of diversity	23
4.1.5 Balance of drawbacks and benefits connected with the use of diversity	25
4.2 Software tools for the development of software.....	25
4.2.1 Introduction	25
4.2.2 Selection of tools.....	27
4.2.3 Requirements for tools	27
4.3 Qualification of pre-developed software	37
4.3.1 Introduction	37
4.3.2 General requirements.....	39
4.3.3 Evaluation and assessment process	39
4.3.4 Requirements for integration in the system and maintenance of PDS	51
Annex A (informative) Considerations of CCF and diversity	57
A.1 CCF due to software.....	57
A.2 Potential CCF causes and effects	57
A.3 CCF defences	59
A.4 Demonstration of correctness	61
A.5 Diversity features.....	61
A.6 Drawbacks, benefits and justification of diversity.....	63
Annex B (informative) IEC 60880 requirements for the use and qualification of software tools	65
Annex C (informative) Tools for production and checking of specification, design and code ..	67
C.1 Constructive tools	67
C.2 Analytical tools	69

	Pages
Annexe D (informative) Prescriptions de la CEI 60880 concernant les LPD.....	70
D.1 Résumé des prescriptions de la CEI 60880 concernant les LPD	70
D.2 Documentation pour l'évaluation des LPD	70
D.3 Directives pour la sélection des prescriptions applicables de la CEI 60880	72
D.4 Directives pour le classement des non-conformités et des facteurs compensateurs.....	72
D.5 Recueil et validation des données relatives à l'historique d'exploitation	74
 Bibliographie	 78
 Figure 1 – Processus de qualification des logiciels prédéveloppés	 52
Figure 2 – Relations de l'évaluation et de l'estimation du LPD avec le plan de qualification du système dans lequel il est intégré	54

Withdrawn

	Page
Annex D (informative) IEC 60880 requirements concerning PDS	71
D.1 Summary of IEC 60880 requirements concerning the PDS	71
D.2 Documentation for the evaluation of the PDS	71
D.3 Guidance for selecting applicable IEC 60880 requirements	73
D.4 Guidance for graduating non-conformities and compensating factors	73
D.5 Collection and validation of data on the operational history.....	75
 Bibliography	 79
 Figure 1 – Outline of the qualification process of pre-developed software	 53
Figure 2 – Relation of PDS evaluation and assessment with the qualification plan of the system in which it is integrated.....	55

Withdrawn

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

LOGICIEL POUR LES CALCULATEURS DE SÛRETÉ DES CENTRALES NUCLÉAIRES –

Partie 2: Défense contre les défaillances de cause commune provoquées par le logiciel, utilisation d'outils logiciels et de logiciels prédéveloppés

AVANT-PROPOS

- 1) La CEI (Commission Electrotechnique Internationale) 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. 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 intéressés sont représentés dans chaque comité d'études.
- 3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme normes, spécifications techniques, rapports techniques ou guides, et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale 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 60880-2 a été établie par le sous-comité 45A: Instrumentation des réacteurs, 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/402/FDIS	45A/406/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 3.

Les annexes A, B, C et D sont données uniquement à titre d'information.

Une fois révisée, la CEI 60880 (1986) paraîtra sous le numéro CEI 60880-1.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2006. A cette date, la publication sera

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SOFTWARE FOR COMPUTERS IMPORTANT TO SAFETY
FOR NUCLEAR POWER PLANTS –****Part 2: Software aspects of defence against common cause failures,
use of software tools and of pre-developed software**

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the 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, the IEC publishes International Standards. 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. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60880-2 has been prepared by subcommittee 45A: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/402/FDIS	45A/406/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 3.

Annexes A, B, C and D are for information only.

When IEC 60880 (1986) is revised, it will be published as IEC 60880-1.

The committee has decided that the contents of this publication will remain unchanged until 2006. At this date, the publication will be

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

INTRODUCTION

La présente partie de la CEI 60880 énonce les prescriptions applicables aux logiciels pour systèmes informatiques de sûreté dans les centrales nucléaires. Elle doit être lue conjointement avec la CEI 60880. Cette partie comprend des exigences sur différents sujets; ces exigences ont leur origine dans les progrès technologiques et l'expérience acquise sur les systèmes logiciels jouant un rôle en matière de sûreté, depuis la parution de la CEI 60880.

Il faut mettre en oeuvre une défense contre les défauts logiciels pouvant provoquer une défaillance de cause commune (CCF) des systèmes informatiques conformément à la Publication de la Série Sécurité N° 50-C-D de l'AIEA, et les prescriptions techniques qui en découlent sont données. Les outils de support logiciel ont connu une croissance rapide et des recommandations liées à leur utilisation sont fournies. L'utilisation pratique de logiciels pour systèmes informatiques importants pour la sûreté repose souvent sur l'utilisation de logiciels prédéveloppés, et des prescriptions et des recommandations sont fournies dans ce sens.

La présente partie de la CEI 60880 fait référence à la publication fondamentale de sécurité, la CEI 61513.

Cette partie s'applique aux fonctions I&C de catégorie A et aux systèmes et équipements associés (FSE) de la CEI 61226.

NOTE Conformément au schéma de classification de la CEI 61513, les fonctions de catégorie A sont réalisées au sein de systèmes de classe 1, qui correspondent aux systèmes de sûreté de l'AIEA.

Withdrawn

INTRODUCTION

This part of IEC 60880 provides requirements for software for computer-based safety systems in nuclear power plants and should be read in conjunction with IEC 60880. This part includes requirements on several topics arising from advances in technology and experience of software systems with a role in safety since the publication of IEC 60880.

Defence against software faults which can lead to Common Cause Failure (CCF) of computer-based systems has to be provided in accordance with the IAEA Safety Series No. 50-C-D, and technical requirements arising from these provisions are given. There has also been a rapid growth in the use of computerized support tools, and recommendations for their use are given. The practical use of software for computer-based safety systems often depends on the use of pre-developed software, and requirements and recommendations in this connection are given.

This part of IEC 60880 references the basic safety publication IEC 61513.

This part applies to Category A I&C functions and associated systems and equipment (FSE) of IEC 61226.

NOTE According to the classification scheme of IEC 61513, category A functions are implemented in class 1 systems, which correspond to the safety systems of the IAEA.

Withdrawn

LOGICIEL POUR LES CALCULATEURS DE SÛRETÉ DES CENTRALES NUCLÉAIRES –

Partie 2: Défense contre les défaillances de cause commune provoquées par le logiciel, utilisation d'outils logiciels et de logiciels prédéveloppés

1 Domaine d'application et objet

Les prescriptions de la présente partie de la CEI 60880 sont applicables aux logiciels des systèmes informatiques de sûreté dans les centrales nucléaires. Elle fournit des prescriptions pour les logiciels des fonctions de catégorie A et des systèmes et équipements associés (FSE). Elle porte sur

- les moyens de défense contre les défaillances de mode commun provoquées par les logiciels;
- les outils automatisés pour le développement de logiciels importants pour la sûreté; et
- l'utilisation de logiciels préexistants.

La préparation et la validation des données sont traitées dans le cadre de ces trois thèmes.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente partie de la CEI 60880. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de la CEI 60880 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de l'ISO et de la CEI possèdent le registre des Normes internationales en vigueur.

CEI 60880:1986, *Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires*

CEI 61226:1993, *Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61513:—, *Centrales nucléaires de puissance – Contrôle-commande des systèmes important pour la sûreté – Prescriptions générales pour les systèmes*¹⁾

ISO/IEC 9126:1991, *Technologies de l'information – Evaluation des produits logiciels – Caractéristiques de qualité et directives d'utilisation*

AIEA 50-C-D (rev 1):1989, *Code pour la sûreté des centrales nucléaires: Conception*

AIEA 50-SG-D11:1986, *Principes généraux de sûreté dans la conception des centrales nucléaires: Guide de sûreté*

IEEE 610:1990, *Lexique de la terminologie d'ingénierie logicielle* (disponible en anglais seulement)

¹⁾ A publier.

SOFTWARE FOR COMPUTERS IMPORTANT TO SAFETY FOR NUCLEAR POWER PLANTS –

Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software

1 Scope and object

This part of IEC 60880 is applicable to the software of computer-based safety systems in nuclear power plants. It gives requirements for software for category A functions, systems and associated equipment (FSE). It addresses

- defence against common cause failures, caused by software;
- automated tools for the development of software important to safety; and
- use of pre-developed software.

Preparation and confirmation of data is dealt with within these three topics as appropriate.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 60880. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of IEC 60880 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60880:1986, *Software for computers in the safety systems of nuclear power stations*

IEC 61226:1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61513: —, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*¹⁾

ISO/IEC 9126:1991, *Information technology – Software product evaluation – Quality characteristics and guidelines for their use*

IAEA 50-C-D (rev 1):1988, *Code on the safety of Nuclear Power Plants: Design*

IAEA 50-SG-D11:1986, *General design safety principles for nuclear power plants – A safety guide*

IEEE 610:1990, *Standard glossary of software engineering terminology*

¹⁾ To be published

3 Définitions et abréviations

Pour les besoins de la présente partie de la CEI 60880, les termes et définitions donnés dans la CEI 60880 et dans les publications de la Série Sécurité N° 50-C-D de l'AIEA, ainsi que les suivants, sont applicables.

NOTE 1 Les termes «doit/doivent», «il convient de» et «peut/peuvent» sont utilisés conformément aux prescriptions de la CEI.

NOTE 2 L'exemple suivant est donné afin de lever toute ambiguïté quant à l'utilisation des termes **erreur**, **défaut**, **défaillance** et **trajectoire de signal**:

Si une personne ou un processus commet une **erreur** dans la production de quelque chose, cela entraîne un **défaut** du produit. Lorsque le produit est utilisé, il peut être satisfaisant ou bien tomber en panne si le **défaut** n'est pas corrigé. Si l'utilisation sollicite le **défaut**, le produit tombera en panne si aucun autre moyen de défense n'empêche la **défaillance**. Une **défaillance** est due à la fois à un **défaut** et à une sollicitation, sans aucun autre moyen de défense en service. Dans le cas des logiciels, un **défaut** est sollicité par une **trajectoire de signal**.

3.1 animation

processus par lequel le comportement défini par une spécification est visualisé avec ses valeurs effectives dérivées des expressions de comportement établies et de certaines valeurs d'entrée

3.2 fonction d'application

fonction d'un système d'instrumentation et commande qui effectue une tâche relative au processus à commander plutôt qu'au fonctionnement du système lui-même
[dérivée de 2.1 de la CEI 60880]

3.3 canal

chemin séparé sur lequel les informations sont acheminées dans un système redondant ou réparti; ce chemin peut également avoir une redondance

3.4 défaillance de cause commune (CCF)

défaillance qui résulte d'un ou plusieurs événements, qui provoquent des défaillances simultanées de deux ou plusieurs canaux dans un système à canaux multiples ou dans plusieurs systèmes, conduisant à une défaillance du (des) système(s)
[3.6.10 de la CEI 61508-4, modifiée]

NOTE 1 Selon le contexte, une CCF peut être vue au niveau système ou au niveau des systèmes qui constituent un groupe de sûreté.

NOTE 2 Voir en 3.8 la définition de défaillance.

3.5 donnée

représentation d'une information ou d'instructions d'une manière adaptée pour la communication, l'interprétation ou le traitement au moyen d'un ordinateur
[définition adaptée de IEEE 610]

NOTE Les données qui sont nécessaires pour définir des paramètres et initier des fonctions d'application et de service dans le système, sont appelées «données d'application».

3 Definitions and abbreviations

For the purposes of this part of IEC 60880, the terms and definitions given in IEC 60880 and in the IAEA Safety Series No. 50-C-D, as well as the following terms and definitions apply.

NOTE 1 “Shall”, “should” and “may” are used in accordance with IEC conventions.

NOTE 2 For clarification of the terms **error**, **fault**, **failure** and **signal trajectory** the following example is given.

If a person or process makes an **error** in producing something, this will result in a **fault** in the product. When the product is used, it may be satisfactory, or it may fail, if the **fault** is not corrected. If the use challenges the **fault**, the product will fail if no other defence prevents the **failure**. A **failure** is due to both a **fault** and a challenge, with no other defence operating. For software, a challenge to a **fault** is provided by a **signal trajectory**.

3.1

animation

process by which the behaviour defined by a specification is displayed with actual values derived from the stated behaviour expressions and from some input values

3.2

application function

function of an I&C system that performs a task related to the process being controlled rather than to the functioning of the system itself
[derived from 2.1 of IEC 60880]

3.3

channel

separate path along which information flows through a redundant or distributed system. That path may also contain redundancy

3.4

common cause failure (CCF)

failure which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system or in multiple systems, leading to system(s) failure

[3.6.10 of IEC 61508-4, modified]

NOTE 1 Depending on the context, a CCF may be considered at the system level or at the level of the systems which constitute a safety group.

NOTE 2 See definition of failure (3.8).

3.5

data

representation of information or instructions in a manner suitable for communication, interpretation, or processing by computers

[adapted from IEEE 610]

NOTE Data which are required to define parameters and to instantiate application and service functions in the system are called “application data”.

3.6

diversité

existence de deux ou plusieurs manières différentes d'atteindre un objectif donné. La diversité est en particulier assurée comme moyen de défense contre une défaillance de mode commun. Elle peut être réalisée par la mise en oeuvre des systèmes physiquement différents les uns des autres ou par une diversité fonctionnelle, dans laquelle des systèmes similaires réalisent l'objectif spécifié de manière différente [définition adaptée de la CEI 61226]

3.7

analyse dynamique

processus consistant à évaluer un système ou un composant sur la base de son comportement pendant l'exécution. S'oppose à l'analyse statique (voir IEEE 610)

3.8

défaillance

une défaillance survient lorsque le service réalisé s'écarte du service voulu

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

3.9

défaut

anomalie d'un composant matériel ou logiciel ou système. Les défauts sont divisés en défauts aléatoires (par exemple la conséquence d'une usure du matériel), et défauts systématiques (par exemple introduits dans la conception); pour le logiciel, ceux-ci comprennent les erreurs de codage et les erreurs de spécification

NOTE Un défaut (et en particulier un défaut de conception) peut rester non détecté dans une partie du système jusqu'à ce que des conditions spécifiques ou une trajectoire de signal affectant cette partie du système soient telles que le résultat produit ne soit pas conforme à la fonction désirée. Cela entraîne une défaillance de cette partie du système.

3.10

diversité fonctionnelle

application de la diversité au niveau fonctionnel (par exemple, actionnement d'un déclenchement sur la limite de pression et sur la limite de température)

3.11

fonctions, et systèmes et matériels associés (FSE)

les fonctions sont des actions effectuées dans un but ou afin de réaliser un objectif. Les systèmes et équipements associés sont les ensembles de composants et les composants eux-mêmes qui sont employés pour remplir les fonctions (voir l'article 3 de la CEI 61226)

3.12

erreur (ou faute) humaine

action humaine ou procédure produisant un résultat indésirable

3.13

bibliothèque

ensemble d'éléments logiciels connexes contenus dans un fichier unique, mais sélectionnés individuellement pour inclusion dans le produit logiciel final

3.14

logiciel à n versions ou multi-versions

ensemble de programmes différents, appelés versions, développé pour satisfaire une prescription commune et des tests communs d'acceptation. L'exécution simultanée et indépendante de ces versions se déroule, en général sur des matériels redondants. Des entrées identiques dans des systèmes de tests ou bien des entrées correspondantes dans des systèmes redondants sont utilisées. Une stratégie prédéterminée telle que le vote est utilisée pour choisir parmi des sorties contradictoires de versions différentes

3.6**diversity**

existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common mode failure. 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 (see clause 3 of IEC 61226)

3.7**dynamic analysis**

process of evaluating a system or component based on its behaviour during execution. In contrast to static analysis (see IEEE 610)

3.8**failure**

failure occurs when the delivered service deviates from the intended service

NOTE A failure is the result of a hardware fault, software fault, system fault, or operator or maintenance error, and the associated signal trajectory which results in the failure.

3.9**fault**

defect in a hardware, software, or system component. Faults are subdivided into random faults (for example, resulting from wearing out of hardware), and systematic faults (for example, introduced in the design), and for software these include coding errors and specification errors

NOTE A fault (notably a design fault) may remain undetected in a part of the system until specific conditions or signal trajectories affecting that part of the system, are such that the result produced does not conform to the intended function. This results in a failure of that part of the system.

3.10**functional diversity**

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

3.11**functions, and associated systems and equipment (FSE)**

functions are carried out for a purpose or to achieve a goal. The associated systems and equipment are the collections of components and the components themselves that are employed to achieve the functions (see clause 3 of IEC 61226)

3.12**human error (or mistake)**

human action or a procedure that produces an unintended result

3.13**library**

collection of related software elements that are grouped together, but which are individually selected for inclusion in the final software product

3.14**n-version or multi-version software**

set of different programs, known as versions, developed to meet a common requirement and common acceptance test. Concurrent and independent execution of these versions takes place, generally in redundant hardware. Identical inputs in test systems or corresponding inputs in redundant systems are used. A predetermined strategy such as voting is used to decide between conflicting outputs in different versions

3.15

logiciel système opérationnel

logiciel fonctionnant sur le processeur cible, par exemple pilotes et services d'entrée/sortie, gestion des interruptions, gestion de l'ordonnancement, pilotes de communication, bibliothèques orientées application, diagnostic en ligne, redondance et gestion des modes de marche dégradée

3.16

événements initiateurs hypothétiques (PIE)

événements qui entraînent des incidents de fonctionnement prévus ou des situations accidentelles et leurs combinaisons plausibles

[AIEA 50-C-D]

3.17

logiciel prédéveloppé (LPD)

logiciel existant, disponible dans le commerce ou en tant que produit protégé par des droits de propriété, dont l'utilisation est envisagée dans un système informatique

3.18

réutilisable

s'applique à un module logiciel qui peut être utilisé dans plusieurs programmes d'un ordinateur ou d'un système informatique (voir IEEE 610)

3.19

trajectoire de signal

l'historique temporel de tous les situations des équipements, états d'un matériel, signaux d'entrée et entrées de l'opérateur qui déterminent les sorties d'un système

3.20

version logicielle

nouvelle édition d'un produit logiciel consécutive à une modification ou à une correction d'un produit logiciel précédent

3.21

spécification

document qui spécifie de manière complète, précise et vérifiable les prescriptions, la conception, le comportement ou autres caractéristiques d'un système ou composant et, souvent, les procédures permettant de déterminer si ces dispositions ont été satisfaites (voir IEEE 610)

NOTE Il existe différents types de spécifications, par exemple les spécifications des exigences de logiciels et les spécifications de conception.

3.22

analyse statique

processus d'évaluation d'un système ou d'un composant basé sur sa forme, sa structure, son contenu ou sa documentation. S'oppose à l'analyse dynamique

3.23

logiciel de support

logiciel d'aide au développement, au test ou à la maintenance d'autres logiciels, comme par exemple les compilateurs, les générateurs de codes, les simulateurs, le diagnostic hors ligne, les initialiseurs (voir 4.2)

3.24

logiciel système

logiciel conçu pour un système programmé ou une famille spécifique de systèmes programmés afin de faciliter l'exploitation et la maintenance du système programmé et des programmes associés, par exemple systèmes d'exploitation, compilateurs, utilitaires. Le logiciel système se compose en général du logiciel système opérationnel et du logiciel de support

3.15**operational system software**

software running on the target processor during operation, such as input/output drivers and services, interrupt management, scheduler, communication drivers, application-oriented libraries, on-line diagnostic, redundancy and graceful degradation management

3.16**postulated initiating event (PIE)**

identified events that lead to anticipated operational occurrences or accident conditions and their consequential failure effects

[IAEA 50-C-D]

3.17**pre-developed software (PDS)**

software which already exists is available as commercial or proprietary product and is being considered for use in a computer-based system

3.18**reusable**

pertaining to a software module that can be used in more than one computer program or software system (derived from IEEE 610)

3.19**signal trajectory**

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

3.20**software version**

instance of a software product derived by modification or correction of a preceding software product

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 (see IEEE 610)

NOTE There are different types of specifications, for example, software requirements specification or design specification.

3.22**static analysis**

process of evaluating a system or component based on its form, structure, content or documentation. In contrast to dynamic analysis

3.23**support software**

software that aids in the development, test, or maintenance of other software such as compilers, code generators, simulators, off-line diagnostic, initializers (see 4.2)

3.24**system software**

software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs, for example, operating systems, compilers, utilities. System software is usually composed of operational system software and support software

4 Prescriptions et recommandations

Dans la suite le terme «exigences» est utilisé pour désigner à la fois les exigences et les recommandations. La distinction apparaît au niveau de chaque paragraphe, où les exigences sont exprimées par «doit» et les recommandations par «il convient que».

4.1 Moyens de défense contre les défaillances logicielles de cause commune

Ce paragraphe émet des exigences en matière de moyens de défense contre les défauts de conception et codage qui peuvent amener à des défaillances de cause commune (CCF) de fonctions classées dans la Catégorie A, conformément à la CEI 61226.

4.1.1 Introduction

Une CCF peut intervenir dans les systèmes et équipements de l'architecture d'I&C qui réalisent différentes lignes de défense pour le même PIE (voir 5.3.1 de la CEI 61513). Le logiciel par lui-même n'a pas une CCF. Une CCF est à mettre en relation avec des défaillances qui ont leur origine dans des erreurs des exigences fonctionnelles, de la conception du système ou du logiciel.

Pour toutes les activités de sûreté, qu'elles soient relatives à l'organisation, au comportement ou à la conception, l'AIEA demande d'appliquer la défense en profondeur (voir 204 de la 50-C-D de l'AIEA), pour assurer que ces activités ont des recouvrements, de façon que si une défaillance intervient dans un sous-système, elle puisse être compensée ou corrigée dans le système total.

Le critère de défaillance unique (voir 329 à 336 de la 50-C-D de l'AIEA) stipule que l'ensemble des systèmes de sûreté doivent pouvoir remplir leur mission malgré une défaillance aléatoire unique pouvant intervenir n'importe où dans cet ensemble.

Les défauts logiciels sont des défauts systématiques et non des défauts aléatoires. Par conséquent, le critère de défaillance unique ne peut pas être appliqué à la conception d'un système de la même manière qu'il a été appliqué pour le matériel. Ainsi, lorsque le concept de défense en profondeur est appliqué, il convient de prendre en compte les éventuels effets des CCF logicielles dans chacune des couches de défense et entre couches redondantes. Il convient d'adopter des contre-mesures appropriées pendant le processus de développement et dans le processus d'évaluation, par exemple

- a) dans le développement, la vérification et la validation de chacune des couches de défense; et
- b) dans l'évaluation de l'indépendance et de la diversité des couches de défense redondantes.

L'utilisation de la diversité est un des moyens pour améliorer la fiabilité de certains systèmes et pour réduire le risque de certaines CCF (voir 337 à 339 de la 50-C-D de l'AIEA).

4.1.1.1 Prescriptions de la CEI 60880

Le paragraphe 4.2 de la CEI 60880 stipule que les prescriptions de fiabilité du système doivent servir de toile de fond à la description de la configuration du système informatique et renvoie à A.2.2 de la CEI 60880. Ce paragraphe donne une liste des facteurs pertinents (y compris la défense en profondeur, le repli en mode de fonctionnement dégradé, la gestion des défaillances, la diversité fonctionnelle et la diversité logicielle, la séparation et décomposition en modules, le découplage, la séparation logique) qui peuvent être utilisés pour éviter les CCF, mais ne traite pas ces facteurs de manière spécifique. Par conséquent, le paragraphe 4.1 de cette partie de la CEI 60880 spécifie comment déterminer les CCF potentielles provoquées par les logiciels ainsi que les techniques pour éviter l'apparition des CCF.

4 Requirements and recommendations

In the following, the term "requirements" is used as an inclusive term for both requirements and recommendations. The distinction appears at the level of the individual clauses where requirements are expressed by "shall" and recommendations by "should".

4.1 Defences against common cause failure due to software

This subclause provides requirements for defences against software design and coding faults which can lead to common cause failures (CCF) of functions classified as category A according to IEC 61226.

4.1.1 Introduction

CCF may occur in the I&C architecture's systems and equipment implementing different lines of defence against the same PIE (see 5.3.1 of IEC 61513). Software by itself does not have a CCF mode. CCF is related to system failures arising from faults in the functional requirements, system design, or in the software.

Defence in depth is required by the IAEA (see 204 of IAEA 50-C-D) to be applied to all safety activities, whether organizational, behavioural or design related, to ensure that there are overlapping defences so that if a failure should occur in a subsystem, it would be compensated for, or corrected in the integral system.

The single-failure criterion (see 329 to 336 of IAEA 50-C-D) requires that the assembly of safety systems have the ability to meet its purpose despite a single random failure assumed to occur anywhere in the assembly.

Software faults are systematic, not random, faults and, therefore, the single-failure criterion can not be applied to the software design of a system in the same manner as it has been applied for hardware. When the defence-in-depth concept is applied, possible effects of CCF due to software inside each defence layer and between redundant layers have to be considered and appropriate counter-measures have to be adopted throughout the development process and in the evaluation processes, for example,

- a) in the development, verification and validation of each individual defence layer; and
- b) in the evaluation of the independence and diversity of redundant defence layers.

A means of enhancing the reliability of some systems and reducing the potential for certain CCFs is the use of diversity (see 337 to 339 of IAEA 50-C-D Rev 1).

4.1.1.1 Requirements of IEC 60880

Subclause 4.2 of IEC 60880 requires the system reliability requirements to be the background to the description of the computer system configuration, and refers to A.2.2 of IEC 60880. This latter subclause indicates relevant factors (including defence in depth, graceful degradation, management of failures, functional diversity, software diversity, spatial separation and modularization, decoupling, logical separation) that might be used to avoid CCF, but does not specifically address all these factors. Therefore, 4.1 of this part of IEC 60880 specifies the way to assess the potential for CCF caused by software and also specifies techniques to avoid the occurrence of CCF.

4.1.1.2 Principes directeurs de la défense contre les CCF logicielles

Les principes directeurs de la défense contre les CCF logicielles énoncent que tout défaut logiciel restera dans le système ou la voie concernés jusqu'à ce qu'il soit détecté et corrigé, et qu'il causera une défaillance si une trajectoire de signal préjudiciable la sollicite. Si deux systèmes ou canaux ou plus, qui réalisent différentes lignes de défense pour le même PIE (voir 5.3.1.5 de la CEI 61513), contiennent le défaut et sont sollicités par des trajectoires de signal spécifiques au cours d'une période sensible, les deux (ou tous/toutes) systèmes ou voies connaîtront une défaillance. Une description plus détaillée de ces états est donnée à l'article A.1.

Il convient donc de prendre en compte le risque potentiel de CCF logicielle lors de la conception. Si des conditions de CCF hypothétiques peuvent être prévues, des changements de conception et des fonctionnalités de défense, y compris la diversité logicielle, peuvent être nécessaires pour assurer la protection contre les CCF logicielles.

Le degré d'amélioration des défenses contre les CCF et les améliorations de la fiabilité qui peuvent être obtenues grâce à la diversité ne peuvent pas être quantifiées. Le concepteur utilisera son meilleur jugement sur la base d'une évaluation qualitative de la fiabilité que peut assurer le logiciel.

Les erreurs humaines intervenant avant le début de la conception logicielle donnent lieu à des défauts de prescriptions et à des défaillances potentielles du système contre lesquelles le seul génie logiciel ne peut prémunir. La défense contre ces types de CCF est traitée au niveau système en 5.3.1.5 de la CEI 61513.

Des erreurs humaines intervenant pendant le processus de génie logiciel peuvent donner lieu à des défauts logiciels et à des défaillances potentielles. Lorsque de tels défauts provoquent la défaillance de plus d'une ligne de défense, les défaillances sont considérées comme des CCF logicielles.

4.1.2 Conception du logiciel pour éviter les CCF

Le moyen de défense élémentaire et le plus important contre les CCF logicielles est de produire des logiciels de la plus haute qualité, c'est-à-dire contenant le moins d'erreurs possible. L'étendue de la couverture des moyens d'autocontrôle, tels que la surveillance de plausibilité des données, le contrôle d'échelle des paramètres, la temporisation cyclique, etc. (voir 4.8, 5.1 et A.2.8 de la CEI 60880), constituent un autre facteur important pour limiter les CCF logicielles potentielles.

Des exigences pour obtenir une haute fiabilité du logiciel sont données dans la CEI 60880 et dans les paragraphes suivants de la présente norme.

L'utilisation de méthodes éprouvées de génie logiciel avec des outils d'aide au développement et à la vérification du logiciel peuvent réduire le nombre de décisions humaines dans la conception et peuvent ainsi réduire le nombre de défauts dans le logiciel produit.

4.1.3 Sources et effets des CCF logicielles

4.1.3.1 Une analyse documentée des CCF logicielles potentielles doit être effectuée et documentée au niveau du système et/ou au niveau de l'architecture globale des systèmes d'I&C importants pour la sûreté.

NOTE 1 Des exigences sur l'architecture I&C sont données en 5.3.1 de la CEI 61513.

NOTE 2 Des exigences sur l'architecture des systèmes individuels d'I&C sont données en 6.1.2 de la CEI 61513.

4.1.1.2 Rationale for defence against CCF due to software

The rationale for defence against software faults is that any software fault will remain in the system or channel concerned until detected and corrected, and can cause failure if a specific signal trajectory challenges it. If two or more systems or channels implementing different lines of defence for the same PIE (see 5.3.1.5 of IEC 61513) contain the fault, and are exposed to specific signal trajectories within a sensitive time period, both (or all) systems or channels can fail, which is called a CCF. A more detailed description of these conditions is given in clause A.1.

The potential for CCF due to software should therefore be considered during design. If postulated conditions of CCF can be foreseen, design changes and defence features, including software diversity, may be needed for protection against CCF due to software.

The degree of improvement of defence against CCF and improvement in reliability that can be achieved by diversity cannot be quantified. Judgement is required based on an evaluation of the qualitative reliability which the software can achieve.

If human errors are made before software design starts, they may lead to faults of requirements and potential system failures against which software engineering alone cannot provide a defence. Defence against such CCF is discussed at the system level in 5.3.1.5 of IEC 61513.

If human errors are made during the software engineering process, they may lead to software faults and potential system failures. Where such faults lead to the failure of more than one line of protection the failures are considered to be CCFs due to software.

4.1.2 Design of software against CCF

The basic, and most important, defence against CCF due to software is to produce software of the highest quality, i.e. as error-free as possible. The extent of coverage of self-monitoring features, such as for data plausibility, parameter range checking, and loop timing etc. as addressed by 4.8, 5.1 and A.2.8 in IEC 60880 is a further important factor in limiting the potential for CCF due to software.

Requirements to achieve highly reliable software with self-monitoring features are given in IEC 60880 and the following paragraphs of this standard.

The use of well-developed software engineering methods with software tool support for software development and verification can help to reduce the number of human design decisions and so potentially reduce the number of faults in the developed software.

4.1.3 Sources and effects of CCF due to software

4.1.3.1 An analysis of the potential for CCF due to software shall be performed and documented at the system level and/or at the level of the total I&C architecture of the I&C systems important to safety of the NPP.

NOTE 1 Requirements on the I&C architecture are given in 5.3.1 of IEC 61513.

NOTE 2 Requirements on the architecture of the individual I&C systems are given in 6.1.2 of IEC 61513.

4.1.3.2 Il convient que l'analyse comprenne les étapes suivantes:

- a) identification des composants logiciels utilisés dans le système ou dans l'architecture du contrôle commande;
- b) analyse des CCF potentielles dues à ces composants dans le cadre du système ou de l'architecture du contrôle commande;
- c) analyse des effets possibles de ces CCF.

NOTE L'analyse des effets potentiels des défauts ne supprime pas le besoin d'effectuer les activités de vérification et validation requise par la CEI 60880. Le but d'une telle analyse est de mettre en évidence toutes les faiblesses dans la conception, afin d'y initier des changements et/ou d'améliorer la confiance dans la conception du logiciel.

4.1.3.3 Les modules communs utilisés dans plusieurs systèmes doivent être identifiés et l'assurance de la fiabilité de ces modules doit être démontrée. Des méthodes pour mener cette démonstration sont donnés à l'article A.4.

4.1.3.4 Les données transmises à l'intérieur du système informatique ou entre différents systèmes informatiques doivent être identifiées. Une analyse doit être effectuée pour déterminer si des données erronées peuvent provoquer une CCF dans les processeurs ou les systèmes en réception.

4.1.3.5 La possibilité que, dans certaines conditions propres à la centrale, des mêmes logiciels implantés dans différents matériels soient soumis simultanément à des trajectoires de signaux identiques et qu'un même défaut logiciel apparaisse dans plusieurs canaux ou chemins fonctionnels, doit être évaluée.

NOTE Les défaillances peuvent être provoquées par des trajectoires de signaux qui n'ont pas été pris en compte lors de la conception, de la vérification et de la validation des logiciels des canaux individuels ou systèmes.

4.1.3.6 Les activités de maintenance du logiciel constituent une source potentielle de CCF. Il convient que la procédure de modification du logiciel ou des données donne l'assurance que ces types de défauts ne sont pas introduits.

4.1.3.7 Une analyse des sources potentielles de CCF logicielles doit être faite et documentée dans le cadre du jugement sur la défense contre les CCF propre à la conception de l'architecture I&C (voir 5.3.3 de la CEI 61513).

4.1.3.8 Si l'analyse identifie une menace inacceptable résultant de CCF provoquées par le logiciel, la conception du logiciel ou de l'architecture du contrôle commande doit être améliorée. Des méthodes pour la réalisation de défenses contre les CCF sont données à l'article A.3, et des méthodes pour la mise en œuvre de la diversité sont données à l'article A.5.

4.1.4 Mise en oeuvre de la diversité

4.1.4.1 Il convient que la mise en oeuvre de la diversité utilise des systèmes indépendants avec diversité fonctionnelle. Si la diversité fonctionnelle n'est pas appropriée ou possible, il convient de prendre en considération la diversité des systèmes, la diversité des caractéristiques des logiciels et la diversité des approches de conception. Les caractéristiques importantes sont données dans l'article A.5. Les techniques utilisées pour la défense contre les CCF doivent être documentées et justifiées par rapport à l'analyse qui a été effectuée.

4.1.4.2 Au niveau du logiciel, il convient que la défense contre les CCF soit basée sur un ensemble de techniques approprié, comme:

- a) des garanties sur la diversification des conditions d'exploitation du logiciel;
- b) des protections contre les erreurs et la propagation des défaillances;

4.1.3.2 The analysis should include the following steps:

- a) identification of the software components used in the system or I&C architecture;
- b) analysis of the potential CCF due to these components within the system or the I&C architecture;
- c) analysis of the possible effects of these CCF.

NOTE Performing an analysis of the potential effects of faults does not obviate the need to perform verification and validation activities as required by IEC 60880. The purpose of such an analysis is to reveal any weaknesses in the design, and hence initiate changes to the design, and/or to improve confidence in the software design.

4.1.3.3 If common modules are used in more than one system, they shall be identified and assurance of the reliability of such common modules shall be assessed. Methods supporting the demonstration of correctness are given in clause A.4.

4.1.3.4 Data transmitted inside a computer-based system or between computer-based systems shall be identified. An analysis shall be performed to determine if faulty data can lead to a CCF in receiving computers or systems.

4.1.3.5 The potential for plant conditions to subject the same software running in different hardware to identical and simultaneous signal trajectories and hence reveal the same software fault in several channels or functional paths shall be assessed.

NOTE Failures may be caused by signal trajectories which were not considered during the design, verification and validation of the software of the individual channels or systems.

4.1.3.6 Software maintenance activities have the potential to cause CCF and the processes used for software or data change assessment should provide assurance that such faults are not introduced.

4.1.3.7 The analysis of potential CCF due to software shall be performed and documented as part of the assessment of the defence against CCF of the design of the I&C architecture (see 5.3.3 of IEC 61513).

4.1.3.8 If the analysis identifies an unacceptable threat arising from CCF due to software then the design of the software or of the I&C architecture shall be improved. Methods supporting the implementation of CCF defences are given in clause A.3 and methods supporting the implementation of diversity features are given in clause A.5.

4.1.4 Implementation of diversity

4.1.4.1 Implementation of diversity should use independent systems with functional diversity. If functional diversity is not appropriate or possible, the use of system diversity, diverse software features and diverse design approaches should be considered. Features of importance are given in clause A.5. The techniques chosen for defence against CCF shall be documented and justified according to the analysis made.

4.1.4.2 At the software level, defences against CCF should be based on an appropriate selection of techniques, such as

- a) guarantee of diversified operational conditions of the software;
- b) defences against error and failure propagation;

- c) la réduction des effets négatifs des CCF;
- d) l'utilisation de logiciels diversifiés répondant à des spécifications différentes, pour des réalisations différentes de la même exigence fonctionnelle.

NOTE 1 Il convient de prendre en considération la possibilité de différencier les méthodes de conception et implémentation mais ceci n'est pas une exigence.

NOTE 2 La technique de la N programmation n'est pas recommandée.

4.1.5 Pondération des inconvénients et des avantages liés à l'utilisation de la diversité

Si la diversité logicielle est utilisée et affirmée, il convient que les inconvénients et avantages sur la fiabilité globale du logiciel soient justifiés sur la base de l'analyse ci-dessus, et documentés (voir 339 de la 50-C-D de l'AIEA, et 4.6.2 de la 50-SG-D11 de l'AIEA). Les avantages, inconvénients et aspects liés à la justification sont donnés à l'article A.6.

4.2 Outils logiciels pour le développement de logiciels

4.2.1 Introduction

Le présent paragraphe développe les prescriptions existantes de la CEI 60880 pour les outils logiciels utilisés dans le développement de logiciels destinés aux calculateurs des systèmes de sûreté des centrales nucléaires.

4.2.1.1 Prescriptions de la CEI 60880 liées aux outils logiciels

Les prescriptions de la CEI 60880 spécifiquement applicables à l'utilisation, la vérification et l'évaluation des outils logiciels sont listées dans l'annexe B de la présente norme.

4.2.1.2 Utilisation des outils logiciels

L'utilisation des outils logiciels appropriés peut augmenter l'intégrité du processus de développement du logiciel, et donc la fiabilité du produit logiciel, en réduisant le risque d'introduction d'erreurs pendant le processus. L'utilisation d'outils peut également présenter des avantages économiques car le temps et le travail nécessaires à la production du logiciel peuvent être réduits. Les outils peuvent être utilisés pour contrôler automatiquement le respect des règles et normes de construction, générer des enregistrements adéquats et une documentation cohérente aux formats standards, et permettre le contrôle des modifications. Les outils peuvent également réduire les travaux de test et permettre la tenue automatique de journaux. Les outils peuvent aussi être nécessaires car requis par une méthode spécifique de développement.

Les outils sont particulièrement puissants lorsqu'ils sont définis pour fonctionner conjointement. Il convient de prendre garde à ne pas attendre des outils qu'ils réalisent des tâches qui dépassent leurs capacités. En d'autres termes, ils ne peuvent pas remplacer l'homme lorsqu'il convient de faire appel à son jugement. Dans certains cas, le soutien par des outils est mieux adapté que l'automatisation complète du processus. Lors de la sélection d'un outil, il convient de faire la balance entre les avantages et les risques liés à son utilisation et les avantages et les risques liés à sa non-utilisation. Le principe important est de choisir des outils qui limitent les possibilités d'introduction d'erreurs mais qui maximisent la capacité à les détecter.

Les outils qui entrent dans le cadre de cette partie de la CEI 60880 sont ceux utilisés pour permettre la capture des prescriptions et ceux utilisés pour permettre la transformation des prescriptions en codes et en données système finals (il peut y avoir un grand nombre d'étapes intermédiaires). Cette partie recouvre également les outils utilisés pour permettre de procéder directement à la vérification, à la validation et au test, les outils utilisés pour la préparation et le contrôle des données d'application (voir 4.2.3.5), et enfin les outils utilisés pour la gestion et le contrôle des processus et des produits concernés par le développement des logiciels.

- c) reduction of the negative effects of CCF;
- d) use of software diversified by different specifications for different implementations of the same functional requirement.

NOTE 1 Differences in design and implementation methods should be considered for inclusion but are not required.

NOTE 2 N-version programming is not recommended.

4.1.5 Balance of drawbacks and benefits connected with the use of diversity

If diverse software is used and claimed, the drawbacks and benefits on the overall reliability of the software should be justified on the basis of the above analysis, and documented (see 339 of IAEA 50-C-D, and 4.6.2 of IAEA 50-SG-D11). Potential benefits, drawbacks and justification aspects are given in clause A.6.

4.2 Software tools for the development of software

4.2.1 Introduction

This subclause expands on the existing requirements of IEC 60880 for software tools used in the development of software for computers in safety systems of nuclear power plants.

4.2.1.1 IEC 60880 requirements for software tools

The IEC 60880 requirements that specifically apply to the use, verification and assessment of software tools are listed in annex B of this standard.

4.2.1.2 Rationale for the use of software tools

The use of appropriate software tools can increase the integrity of the software development process, and hence software product reliability, by reducing the risk of introducing faults in the process. The use of tools can also have economic benefits as they can reduce the time and human effort required to produce software. Tools can be used to automatically check for adherence to rules of construction and standards, to generate proper records and consistent documentation in standard formats, and to support change control. Tools can also reduce the effort required for testing and to maintain automatic logs. Tools can also be necessary because a specific development methodology requires their use.

Tools are most powerful when they are defined to work co-operatively with each other. Care should be taken not to require tools to undertake tasks beyond their capability, for example, they cannot substitute humans when judgement is involved. In some cases, tool support is more appropriate than complete automation of the process. When selecting a tool, the benefits and risk of using a tool must be balanced against the benefits and risk of not using a tool. The important principle is to choose tools that limit the opportunity for making errors and introducing faults, but maximize the opportunity for detecting faults.

Tools within the scope of this part of IEC 60880 include those used to support the capture of requirements and those used to support the transformation of requirements into the final system code and data (there may be many intermediate steps). The scope also includes those tools used to directly support the performance of verification, validation and testing, tools for the preparation and control of application data (see 4.2.3.5), and tools for the management and control of the processes and products involved in the software development.