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

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 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

CONTENTS

Pages

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.

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.

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 calculateur
[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».