NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60880

Deuxième édition
Second edition
2006-05

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

Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions

© IEC 2006 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, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XE

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

SOMMAIRE

AVANT-PROPOS 6
INTRODUCTION 10

1 Domaine d'application et objet 16
2 Références normatives 16
3 Termes et définitions 18
4 Symboles et abréviations 28
5 Exigences générales pour les projets logiciel 28
5.1 Généralités 28
5.2 Types de logiciel 32
5.3 Principe de développement du logiciel 34
5.4 Gestion du projet logiciel 38
5.5 Plan d'assurance qualité logiciel 38
5.6 Gestion de configuration 40
5.7 Sécurité du logiciel 42
6 Exigences du logiciel 46
6.1 Spécification des exigences du logiciel 46
6.2 Auto-surveillance 48
6.3 Test périodique 48
6.4 Documentation 50
7 Conception et réalisation 50
7.1 Principes pour la conception et la réalisation 52
7.2 Langages, traducteurs et outils associés 56
7.3 Recommandations détaillées 58
7.4 Documentation 62
8 Vérification du logiciel 62
8.1 Processus de vérification du logiciel 62
8.2 Activités de vérification du logiciel 64
9 Aspects logiciels de l'intégration du système 72
9.1 Aspects logiciels du plan d'intégration du système 74
9.2 Intégration du système 76
9.3 Vérification du système intégré 76
9.4 Procédures de résolution de défaut 78
9.5 Aspects logiciels du compte rendu de vérification du système intégré 78
10 Aspects logiciels du plan de validation 80
10.1 Aspects logiciels du plan de validation système 80
10.2 Validation du système 80
10.3 Aspects logiciels du compte rendu de validation du système 82
10.4 Procédures de résolution de défaut 82
11 Modification du logiciel 82
11.1 Procédure de demande de modification 84
11.2 Procédure d'exécution d'une modification du logiciel 86
11.3 Modification du logiciel après livraison 88

CONTENTS

FOREWORD 7
INTRODUCTION 11

1 Scope and object 17
2 Normative references 17
3 Terms and definitions 19
4 Symbols and abbreviations 29
5 General requirements for software projects 29
5.1 General 29
5.2 Software types 33
5.3 Software development approach 35
5.4 Software project management 39
5.5 Software quality assurance plan 39
5.6 Configuration management 41
5.7 Software security 43
6 Software requirements 47
6.1 Specification of software requirements 47
6.2 Self-supervision 49
6.3 Periodic testing 49
6.4 Documentation 51
7 Design and implementation 51
7.1 Principles for design and implementation 53
7.2 Language and associated translators and tools 57
7.3 Detailed recommendations 59
7.4 Documentation 63
8 Software Verification 63
8.1 Software verification process 63
8.2 Software verification activities 65
9 Software aspects of system integration 73
9.1 Software aspects of system integration plan 75
9.2 System integration 77
9.3 Integrated system verification 77
9.4 Fault resolution procedures 79
9.5 Software aspects of integrated system verification report 79
10 Software aspects of system validation 81
10.1 Software aspects of the system validation plan 81
10.2 System validation 81
10.3 Software aspects of the system validation report 83
10.4 Fault resolution procedures 83
11 Software modification 83
11.1 Modification request procedure 85
11.2 Procedure for executing a software modification 87
11.3 Software modification after delivery 89

12 Aspects logiciels de l'installation et de l'exploitation 90
12.1 Installation du logiciel sur site 90
12.2 Sécurité informatique sur site 90
12.3 Adaptation du logiciel aux conditions sur site 92
12.4 Formation des opérateurs 92
13 Moyens de défense contre les défaillances logicielles de cause commune 94
13.1 Généralités 94
13.2 Conception du logiciel pour éviter les CCF 96
13.3 Sources et effets des CCF logicielles 96
13.4 Mise en oeuvre de la diversité 98
13.5 Pondération des inconvénients et des avantages liés à l'utilisation de la diversité 98
14 Outils logiciels pour le développement de logiciels 98
14.1 Généralités 98
14.2 Sélection des outils 100
14.3 Exigences applicables aux outils 102
15 Qualification de logiciels prédéveloppés 112
15.1 Généralités 112
15.2 Exigences générales 112
15.3 Processus d'évaluation et d'agrément 114
15.4 Exigences liées à l'intégration dans le système et à la maintenance des PDS 130

Annexe A (normative) Cycle de vie et de sûreté du logiciel et détails des exigences du logiciel 132
Annexe B (normative) Exigences et recommandations détaillées relatives à la conception et à la réalisation 136
Annexe C (informative) Exemple d'ingénierie à base de logiciel orienté application (développement de logiciel avec un langage orienté application) 162
Annexe D (informative) Langage, traducteur, éditeur de liens 170
Annexe E (informative) Vérification et test du logiciel 174
Annexe F (informative) Liste typique des documents relatifs au logiciel 190
Annexe G (informative) Considérations sur les CCF et la diversification 192
Annexe H (informative) Outils pour la production et la vérification des spécifications, de la conception et du code 200
Annexe I (informative) Exigences concernant les logiciels prédéveloppés (PDS) 206
Annexe J (informative) Correspondance entre la CEI 61513 et cette norme 210

12 Software aspects of installation and operation 91
12.1 On-site installation of the software 91
12.2 On-site software security 91
12.3 Adaptation of the software to on-site conditions 93
12.4 Operator training 93
13 Defences against common cause failure due to software 95
13.1 General 95
13.2 Design of software against CCF 97
13.3 Sources and effects of CCF due to software 97
13.4 Implementation of diversity 99
13.5 Balance of drawbacks and benefits connected with the use of diversity 99
14 Software tools for the development of software 99
14.1 Introduction 99
14.2 Selection of tools 101
14.3 Requirements for tools 103
15 Qualification of pre-developed software 113
15.1 General 113
15.2 General requirements 113
15.3 Evaluation and assessment process 115
15.4 Requirements for integration in the system and modification of PDS 131

Annex A (normative) Software safety life cycle and details of software requirements 133
Annex B (normative) Detailed requirements and recommendations for design and implementation 137
Annex C (informative) Example of application oriented software engineering (software development with application-oriented language) 163
Annex D (informative) Language, translator, linkage editor 171
Annex E (informative) Software verification and testing 175
Annex F (informative) Typical list of software documentation 191
Annex G (informative) Considerations of CCF and diversity 193
Annex H (informative) Tools for production and checking of specification, design and implementation 201
Annex I (informative) Requirements concerning pre-developed software (PDS) 207
Annex J (informative) Correspondence between IEC 61513 and this standard 211

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ASPECTS LOGICIELS DES SYSTÈMES PROGRAMMÉS RÉALISANT DES FONCTIONS DE CATÉGORIE A

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 60880 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.

Cette deuxième édition annule et remplace la première édition publiée en 1986 ainsi que la CEI 60880-2 publiée en 2000. Elle constitue une révision technique.

L'objectif de la révision de la norme est de:

- Prendre en compte le fait que les techniques de génie logiciel ont progressé de façon significative ces dernières années.
- Mettre en cohérence la norme avec les nouvelles révisions des documents de l'AIEA NS-R-1 et NS-G-1.3, ceci comprenant autant que possible une adaptation des définitions.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY A FUNCTIONS

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 60880 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1986 and IEC 60880-2 published in 2000. It constitutes a technical revision.

The revision of the standard is intended to accomplish the following:

- To take into account the fact that software engineering techniques advanced significantly in the intervening years.
- To align the standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3. This includes as far as possible adaptation of the definitions.

- Remplacer, autant que possible, les exigences associées aux normes publiées depuis la parution de la première édition de la CEI 60880, plus particulièrement la CEI 61513, la CEI 61226 édition 2, la CEI 62138 et la CEI 60987.
- Intégrer complètement au niveau des chapitres 13, 14, 15 et des Annexes G, H, I, la CEI 60880-2 publiée en 2000.
- Faire la revue des exigences existantes et mettre à jour les définitions et la terminologie.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/613/FDIS	45A/621/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.

- To replace, as far as possible, requirements associated with standards published since the first edition of IEC 60880, especially IEC 61513, IEC 61226 edition 2, IEC 62138 and IEC 60987.
- To fully integrate IEC 60880-2 published in 2000 as chapters 13, 14, 15 and annexes G, H, I.
- To review the existing requirements and to update the terminology and definitions.

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

FDIS	Report on voting
45A/613/FDIS	45A/621/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) Contexte technique, questions importantes et structure du document

Le développement des logiciels des systèmes de contrôle-commande numériques employés à des fins de sûreté nucléaire est un défi du fait des exigences de sûreté à satisfaire. Les logiciels de sûreté employés dans les centrales nucléaires, qui, souvent, ne sont sollicités qu'en cas d'urgence doivent être totalement validés et qualifiés avant leur mise en exploitation. Afin d'atteindre le haut niveau de fiabilité requis, une attention particulière doit être apportée durant tout le cycle de vie, depuis la spécification des exigences de base jusqu'à l'exploitation et la maintenance, en passant par les différentes étapes de conception et de V&V. L'objectif principal de cette norme est de traiter des différents aspects de sûreté correspondants et d'énoncer les exigences permettant d'atteindre le haut niveau de qualité logicielle nécessaire.

La première édition de cette norme, publiée en 1986, avait été développée pour interpréter les principes de sûreté de base jusqu'alors applicables aux systèmes câblés, pour les systèmes numériques – systèmes multiprocesseurs répartis, grands systèmes mono-processeurs – employés dans les systèmes de sûreté des centrales nucléaires.

Elle fut largement utilisée par l'industrie nucléai re pour fournir des exigences et des recommandations applicables aux logiciels des systèmes de contrôle commande des centrales nucléaires.

Bien que la plupart des exigences de cette première édition soient toujours pertinentes, des éléments significatifs ont justifié le développement de cette seconde édition:

– Depuis 1986 un certain nombre de nouvelles normes ont été produites; celles-ci traitent en détail des exigences générales portant sur les systèmes (CEI 61513) et des exigences relatives au matériel (CEI 60987). Une norme traite du logiciel des systèmes de contrôle-commande réalisant des fonctions de catégories B ou C pour les systèmes importants pour la sûreté des centrales nucléaire (CEI 62138). Le Guide de sûreté de l'AIEA 50-SG-D3 a été remplacé par le guide NS-G-1.3. Enfin, la CEI 60880-2 a été diffusée.
– Les techniques de génie logiciel ont progressé de façon significative au cours des dernières années.

Lors du développement de cette norme, le plus grand soin a été apporté au maintien de la transparence par rapport à la première édition. Lorsque cela a été possible, la formulation des exigences a été conservée, sinon elle a été modifiée tout en maintenant la traçabilité. De la même façon, la CEI 60880-2 traitant des aspects logiciels relatifs à la défense contre les défaillances de cause commune, à l'utilisation des d'outils logiciels et de logiciels prédéveloppés, a été intégrée de telle façon que la présente norme couvre aujourd'hui la totalité des sujets considérés.

L'objectif de cette norme est d'être utilisée par les développeurs de systèmes, les acheteurs et les utilisateurs de systèmes (exploitants), les évaluateurs de systèmes et autorités réglementaires.

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

La CEI 61513, qui traite des systèmes de contrôle-commande numériques de haute intégrité employés dans les systèmes de sûreté des centrales nucléaires de puissance fait référence à la CEI 60880.

La CEI 60880 est le document de deuxième niveau qui traite les aspects logiciels des systèmes de contrôle-commande réalisant des fonctions de catégorie A.

INTRODUCTION

a) Technical background, main issues and organisation of the standard

Engineering of software based Instrumentation and Control (I&C) systems to be used for nuclear safety purposes is a challenge due to the safety requirements to be fulfilled. The safety software used in nuclear power plants (NPP) which are often required only in emergency cases, have to be fully validated and qualified before being used in operation. In order to achieve the high reliability required, special care has to be taken throughout the entire life cycle, from the basic requirements, the various design phases and V&V procedures for operation and maintenance. It is the main aim of this standard to address the related safety aspects and to provide requirements for achieving the high software quality necessary.

The first edition of this standard was issued in 1986 to interpret the basic safety principles applied so far in hardwired systems for the utilisation of digital systems — multiprocessor distributed systems as well as larger scale central processor systems — in the safety systems of nuclear power plants.

It has been used extensively within the nuclear industry to provide requirements and guidance for software of NPP safety I&C systems.

Although many of the requirements within the first edition continued to be relevant, there were significant factors which justified the development of this second edition:

– Since 1986, a number of new standards have been produced which address in detail the general requirements for systems (IEC 61513), hardware requirements (IEC 60987) and a standard to address software for I&C systems performing category B or C functions for NPP systems important to safety (IEC 62138). The Safety Guide 50-SG-D3 of the IAEA has been superseded by the guide NS-G-1.3. Additionally, IEC 60880-2 has been issued.
– Software engineering techniques have advanced significantly in the intervening years.

In this standard, utmost care has been taken to keep transparency with respect to the first edition. Where possible, the phrasing of requirements has been kept, otherwise it has been extended in a traceable way. In the same manner, IEC 60880-2 dealing with software aspects of defence against common cause failures, use of software tools and pre-developed software has been integrated, so that now this current standard covers entirely the software safety issues to be addressed.

It is intended that the standard be used by systems developers, systems purchasers/users (utilities), systems assessors and by licensors.

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

IEC 60880 is directly referenced by IEC 61513 which deals with the system aspects of high integrity computer-based I&C used in safety systems of nuclear power plants together.

IEC 60880 is the second level SC 45A document tackling the issue of software aspects for I&C systems performing category A functions.

Le logiciel relatif aux fonctions de catégories B et C est traité dans la CEI 62138.

Prises ensemble, la CEI 60880 et la CEI 62138 couvrent les aspects logiciels relatifs aux systèmes numériques employés dans les centrales nucléaires de puissance pour réaliser les fonctions importantes pour la sûreté.

Cette seconde édition de la CEI 60880 doit être lue conjointement avec la CEI 60987 et la CEI 61226, qui sont les normes du SC 45A traitant des aspects matériels et du classement des systèmes.

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

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

Il est important de noter que cette norme n'établit pas d'exigences fonctionnelles supplémentaires pour les systèmes de sûreté.

Les aspects pour lesquels des exigences et des recommandations particulières ont été produites sont:

1) une approche générale du développement logiciel pour garantir une production de logiciel hautement fiable prenant en compte les interdépendances entre le matériel et le logiciel;
2) une approche générale pour la vérification du logiciel et pour les aspects logiciels de la validation du système programmé;
3) des procédures pour le contrôle des modifications et des configurations du logiciel;
4) des exigences applicables à l'utilisation des outils;
5) des procédures pour la qualification des logiciels prédéveloppés.

Il est reconnu que les techniques logicielles se développent de façon continue à un rythme soutenu et qu'il n'est pas possible, pour une norme, de faire référence à toutes les techniques et technologies nouvelles de conception.

Pour garantir la pertinence de la norme pour les années futures, l'accent a été mis sur les principes, plutôt que sur les techniques logicielles.

Si de nouvelles techniques sont développées, l'application des principes devrait permettre d'en apprécier l'utilité.

d) Description de la structure de la collection des normes du SC 45A 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 est la 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.

La CEI 61513 fait directement référence aux autres normes du SC 45A 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 CEI 61513, un ensemble documentaire cohérent.

Software for categories B and C functions is dealt with in IEC 62138.

IEC 60880 and IEC 62138 together cover the domain of the software aspects of computer-based systems used in nuclear power plants to perform functions important to safety.

This second edition of IEC 60880 is to be read in conjunction with IEC 60987 and IEC 61226, the appropriate SC 45A standards on computer hardware and on classification.

For more details on the structure of the SC 45A standard series see item d) of this introduction.

c) Recommendation and limitation regarding the application of this standard

It is important to note that this standard establishes no additional functional requirements for safety systems.

Aspects for which special requirements and recommendations have been produced, are:

1) a general approach to software development to assure the production of the highly reliable software required including hardware and software interdependencies;
2) a general approach to software verification and to the software aspects of the computer-based system validation;
3) procedures for software modification and configuration control;
4) requirements for use of tools;
5) procedures for qualification of pre-developed software.

It is recognised that software technology is continuing to develop at a rapid pace and that it is not possible for a standard such as this to include references to all modern design technologies and techniques.

To ensure that the standard will continue to be relevant in future years the emphasis has been placed on issues of principle, rather than specific software technologies.

If new techniques are developed then it should be possible to assess the suitability of such techniques by applying the safety principles contained within this standard.

d) Description of the structure of the SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top level document of the SC 45A standard series is IEC 61513. This standard deals with requirements for NPP I&C systems important to safety and lays out the SC 45A standards series.

IEC 61513 refers directly to other 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.

Au troisième niveau, les normes du SC 45A, qui ne sont généralement pas référencées directement par la 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 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 des parties 1, 2 et 4 de la CEI 61508 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, pour l'application au secteur nucléaire, à la CEI 61508-3.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A 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 le guide NS-R-1 «Safety of Nuclear Power Plants: Design – Requirements» et le guide NS-G-1.3 «Instrumentation and Control Systems Important to Safety in Nuclear Power Plants». La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

At a third level, 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 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 parts 1, 2 and 4, for the nuclear application sector. Compliance with this standard 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, part 3 for the nuclear application sector.

IEC 61513 refers to ISO standards as well as to IAEA 50-C-QA for topics related to quality assurance.

The SC 45A standards series consistently implement and detail the principles and basic safety aspects provided in the IAEA Code on the safety of nuclear power plants and in the IAEA safety series, in particular the Requirements NS-R-1, “Safety of Nuclear Power Plants: Design” and the Safety Guide NS-G-1.3, “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.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ASPECTS LOGICIELS DES SYSTÈMES PROGRAMMÉS RÉALISANT DES FONCTIONS DE CATÉGORIE A

1 Domaine d'application et objet

Cette Norme internationale énonce des exigences pour les logiciels des systèmes d'instrumentation et de contrôle-commande (I&C) programmés des centrales nucléaires de puissance, réalisant des fonctions de catégorie A telle que définie par la CEI 61226.

Selon la définition donnée par la CEI 61513, les systèmes d'I&C de sûreté de classe 1 sont, à la base, destinés aux fonctions de catégorie A, mais peuvent également réaliser des fonctions de catégories inférieures. Cependant, les exigences des systèmes sont toujours déterminées par les fonctions de la plus haute catégorie concernée.

Pour les logiciels des systèmes d'I&C réalisant uniquement des fonctions de catégories B et C, telles que définies par la CEI 61226, les exigences et recommandations de la CEI 62138 sont applicables.

La présente norme énonce des exigences pour la production de logiciels de haute fiabilité. Elle prend en compte chaque étape de développement et de documentation du logiciel, c'est-à-dire la spécification des exigences, la conception, le développement, la vérification, la validation et l'exploitation.

Les principes appliqués pour développer ces exigences comprennent:

– l'utilisation des meilleures pratiques existantes;
– l'utilisation de méthodes de conception descendante;
– la modularité;
– la vérification de chaque phase;
– la clarté de la documentation;
– la vérifiabilité des documents;
– la réalisation de tests de validation.

Des recommandations et informations supplémentaires sur la façon de se conformer aux exigences de la partie principale de cette norme sont données dans les Annexes A à I.

2 Références normatives

Les documents référencés ci-après sont indispensables à l'application de cette norme. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document référencé (y compris les amendements) s'applique.

CEI 60671, *Essais périodiques et surveillance du système de protection des réacteurs nucléaires*

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope and object

This International Standard provides requirements for the software of computer-based I&C systems of nuclear power plants performing functions of safety category A as defined by IEC 61226.

According to the definition in IEC 61513, I&C systems of safety class 1 are basically intended to support category A functions, but may also support functions of lower categories. However the system requirements are always determined by the functions of the highest category implemented.

For software of I&C system performing only category B and C functions in NPP as defined by IEC 61226, requirements and guidance of IEC 62138 are applicable.

This standard provides requirements for the purpose of achieving highly reliable software. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation.

The principles applied in developing these requirements include:

– best available practices;
– top-down design methods;
– modularity;
– verification of each phase;
– clear documentation;
– auditable documents;
– validation testing.

Additional guidance and information on how to comply with the requirements of the main part of this standard is given in Annexes A to I.

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, *Periodic tests and monitoring of the protection system of nuclear reactors*

CEI 61069-2:1993, *Mesure et commande dans les processus industriels – Appréciation des propriétés d'un système en vue de son évaluation – Partie 2: Méthodologie à appliquer pour l'évaluation*

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

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

ISO/CEI 9126, *Génie logiciel – Qualité du produit*

Guide AIEA NS-G-1.2, *Evaluation de sûreté et vérification pour les centrales nucléaires*

Guide AIEA NS-G-1.3, *Instrumentation et systèmes de commande importants pour la sûreté dans les centrales nucléaires*

IEC 61069-2:1993, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

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

IEC 61508-4, *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*

ISO/IEC 9126, *Software engineering – Product quality*

IAEA guide NS-G-1.2, *Safety Assessment and Verification for Nuclear power Plant*

IAEA guide NS-G-1.3, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*