NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
62138

Première édition
First edition
2004-01

Centrales nucléaires – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C

Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions

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 X

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ASPECTS LOGICIELS DES SYSTÈMES INFORMATISÉS RÉALISANT DES FONCTIONS DE CATÉGORIE B OU C

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 62138 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/507/FDIS	45A/521/RVD

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

Cette publication a été rédigée selon la Partie 2 des Directives ISO/CEI.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT FOR SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY B OR C 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 62138 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

FDIS	Report on voting
45A/507/FDIS	45A/521/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.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2009. A cette date, la publication sera

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

The committee has decided that the contents of this publication will remain unchanged until 2009. At this date, the publication will be:

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- withdrawn;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

INTRODUCTION

Structure de la collection de normes du SC 45A – Relations avec les documents de la CEI, de l'AIEA et de l'ISO

Le point d'entrée de la collection de normes produite 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 aspects logiciels et les aspects matériels pour les systèmes informatisés, la conception des salles de commande et le multiplexage. Ces normes directement référencées forment avec la CEI 61513 un ensemble documentaire cohérent.

Les normes du SC 45A qui ne sont pas référencées directement par la CEI 61513 sont relatives à des matériels particuliers, à des méthodes, à des techniques ou à des activités spécifiques. Généralement, ces documents de bas niveau font référence aux documents de plus haut niveau décrits précédemment pour les activités génériques, et peuvent être utilisés de façon isolée.

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.

La CEI 61513 fait référence aux normes ISO ainsi qu'au document AIEA 50-C-QA (qui a depuis été remplacé par le document AIEA 50-C/SG-Q) 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 – Safety Guide". La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

INTRODUCTION

Structure of the SC 45A standard series – Relationships with other IEC, IAEA and ISO documents

The entry point of the SC 45A standard series is IEC 61513. This standard deals with general requirements for instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs), and structures the SC45A standard 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, software aspects of computer-based systems, hardware aspect of computer-based systems, control rooms design and multiplexing. The standards referenced directly have to be considered together with IEC 61513 as a consistent document set.

The other SC 45A standards not directly referenced by IEC 61513 are standards related to particular equipment, technical methods or specific activities. Usually, these low level documents, which refer to the documents of the higher levels previously described for the general topics, can be used on their own.

IEC 61513 has adopted a presentation format similar to basic safety publication IEC 61508, with an overall safety lifecycle frame and a system safety lifecycle frame, and provides an interpretation of the general requirements of IEC 61508, parts 1, 2 and 4, for the nuclear application sector. Compliance with IEC 61513 will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In that frame, IEC 60880 and IEC 62138 correspond to IEC 61508, part 3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA 50-C-QA (now replaced by IAEA 50-C/SG-Q) for topics related to quality assurance.

The SC 45A standards series implements consistently and in detail the principles and basic safety aspects given 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 the SC 45A standards are consistent with that used by the IAEA.

CENTRALES NUCLÉAIRES – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – ASPECTS LOGICIELS DES SYSTÈMES INFORMATISÉS RÉALISANT DES FONCTIONS DE CATÉGORIE B OU C

1 Domaine d'application

Cette Norme internationale énonce des exigences sur les logiciels des systèmes d'instrumentation et de contrôle-commande (I&C) informatisés réalisant des fonctions de sûreté de catégorie B ou C, selon la définition donnée par la CEI 61226. Elle est complémentaire à la CEI 60880 et à la CEI 60880-2, qui énoncent des exigences sur le logiciel des systèmes d'I&C informatisés réalisant des fonctions de sûreté de catégorie A.

Elle est également cohérente et complémentaire à la CEI 61513. Les activités de nature essentiellement système (comme l'intégration, la validation et l'installation sur site) n'y sont pas traitées exhaustivement: les exigences qui ne sont pas spécifiques au logiciel sont à chercher dans la CEI 61513.

La CEI 61513 définit ainsi la classe des systèmes d'I&C importante pour la sûreté:

- les systèmes d'I&C de classe 1 sont principalement prévus pour réaliser des fonctions de catégorie A, mais peuvent aussi réaliser des fonctions de catégorie B et/ou C, ainsi que des fonctions non classées;
- les systèmes d'I&C de classe 2 sont principalement prévus pour réaliser des fonctions de catégorie B, mais peuvent aussi réaliser des fonctions de catégorie C, ainsi que des fonctions non classées;
- les systèmes d'I&C de classe 3 sont principalement prévus pour réaliser des fonctions de catégorie C, mais peuvent aussi réaliser des fonctions non classées.

Un système d'I&C classé de sûreté pouvant réaliser des fonctions de catégories différentes, ainsi que des fonctions non classées, les exigences de cette Norme sont directement attachées à la catégorie de sûreté des fonctions supportées, mais à la classe de sûreté du système.

Cette Norme prend en compte les pratiques de développement actuellement mises en oeuvre pour les logiciels de systèmes d'I&C, et en particulier:

- l'utilisation de logiciels, d'équipements et de familles d'équipements pré-développés, mais pas nécessairement selon les normes de l'industrie nucléaire;
- l'utilisation de «boîtes noires» contenant du logiciel;
- l'utilisation de langages orientés application.

Cette Norme n'est pas conçue comme un guide général de génie logiciel. Elle énonce les exigences que les logiciels des systèmes d'I&C de classe 2 et 3 doivent satisfaire afin d'atteindre les objectifs de sûreté nucléaire du système.

2 Références normatives

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

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT FOR SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY B OR C FUNCTIONS

1 Scope

This International Standard provides requirements for the software of computer-based I&C systems performing functions of safety category B or C as defined by IEC 61226. It complements IEC 60880 and IEC 60880-2, which provide requirements for the software of computer-based I&C systems performing functions of safety category A.

It is also consistent with, and complementary to, IEC 61513. Activities that are mainly system level activities (for example, integration, validation and installation) are not addressed exhaustively by this standard: requirements that are not specific to software are deferred to IEC 61513.

IEC 61513 defines the safety classes of I&C systems important to safety as follows:

- I&C systems of safety class 1 are basically intended to perform functions of safety category A, but may also perform functions of safety category B and/or C, and non safety-classified functions;
- I&C systems of safety class 2 are basically intended to perform functions of safety category B, but may also perform functions of safety category C, and non safety-classified functions;
- I&C systems of safety class 3 are basically intended to perform functions of safety category C, but may also perform non safety-classified functions.

Since a given safety-classified I&C system may perform functions of different safety categories and even non safety-classified functions, the requirements of this standard are attached to the safety class of the I&C system.

This standard takes into account the current practices for the development of software for I&C systems, in particular:

- the use of pre-developed software, equipment and equipment families that were not necessarily designed to nuclear industry sector standards;
- the use of dedicated “black-box” devices with embedded software;
- the use of application-oriented languages.

This standard is not intended to be used as a general-purpose software engineering guide. It provides requirements that the software of I&C systems of safety classes 2 or 3 must meet to achieve system nuclear safety objectives.

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.

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

CEI 61513:2001, *Centrales nucléaires – Instrumentation et contrôle commande des systèmes importants pour la sûreté – Prescriptions générales pour les systèmes*

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

IEC 61513:2001, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*