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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN 62138:2009 sisaldab Euroopa standardi EN 62138:2009 ingliskeelset teksti.	This Estonian standard EVS-EN 62138:2009 consists of the English text of the European standard EN 62138:2009.
Standard on kinnitatud Eesti Standardikeskuse 30.10.2009 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 30.10.2009 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 14.08.2009.	Date of Availability of the European standard text 14.08.2009.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

ICS 27.120.20

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62138

August 2009

ICS 27.120.20

English version

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

(IEC 62138:2004)

Centrales nucléaires - Instrumentation et contrôle-commande importants pour la sûreté - Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C (CEI 62138:2004)

Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie B oder C (IEC 62138:2004)

This European Standard was approved by CENELEC on 2009-07-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 62138:2009 E

Foreword

The text of the International Standard IEC 62138:2004, prepared by SC 45A, Instrumentation and control of nuclear facilities, of IEC TC 45, Nuclear instrumentation, was submitted to the formal vote and was approved by CENELEC as EN 62138 on 2009-07-01 without any modification.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2010-07-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2012-07-01

Annex ZA has been added by CENELEC.

———————

Endorsement notice

The text of the International Standard IEC 62138:2004 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61508-3	NOTE	Harmonized as EN 61508-3:2001 (not modified).
IEC 61508-4	NOTE	Harmonized as EN 61508-4:2001 (not modified).
IEC 61511-1	NOTE	Harmonized as EN 61511-1:2004 (not modified).
ISO 9000-3	NOTE	Harmonized as EN ISO 9000-3:1997 (not modified).
ISO 9001	NOTE	Harmonized as EN ISO 9001:2008 (not modified).

———————

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 61226	- [1)]	Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions	-	-
IEC 61513	2001	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-

[1)] Undated reference.

SOMMAIRE

AVANT-PROPOS 4
INTRODUCTION 8

1 Domaine d'application 10
2 Références normatives 10
3 Termes, définitions et abréviations 12
4 Concepts et présupposés 22
4.1 Types de logiciels 22
4.2 Types de données 24
4.3 Cycles de Vie et de Sûreté du Logiciel et du Système 24
4.4 Principes de gradation 30
5 Exigences pour le logiciel des systèmes d'I&C réalisant des fonctions de catégorie C 34
5.1 Exigences générales 34
5.2 Sélection du logiciel pré-développé 42
5.3 Spécification du logiciel 44
5.4 Conception du logiciel 48
5.5 Réalisation du logiciel nouveau 50
5.6 Aspects logiciels de l'intégration du système 52
5.7 Aspects logiciels de la validation du système 52
5.8 Installation du logiciel sur site 54
5.9 Rapports d'anomalie 54
5.10 Modification du logiciel 54
6 Exigences pour le logiciel des systèmes d'I&C réalisant des fonctions de catégorie B 56
6.1 Exigences générales 56
6.2 Sélection des logiciels prédéveloppés 64
6.3 Spécification du logiciel 74
6.4 Conception du logiciel 78
6.5 Réalisation du logiciel nouveau 82
6.6 Aspects logiciels de l'intégration du système 86
6.7 Aspects logiciels de la validation du système 86
6.8 Installation du logiciel sur site 88
6.9 Rapports d'anomalie 90
6.10 Modification du logiciel 90

Bibliographie 94

Figure 1 – Composants logiciels typiques d'un système d'I&C informatisé 22
Figure 2 – Activités du Cycle de Vie et de Sûreté du Système (selon la CEI 61513) 24
Figure 3 – Activités logicielles dans le Cycle de Vie et de Sûreté du Système 26
Figure 4 – Activités de développement du Cycle de Vie et de Sûreté du Logiciel selon la CEI 62138 28
Figure 5 – Processus pour établir que le logiciel pré-développé d'un système d'I&C de classe 2 est correct 30

CONTENTS

FOREWORD 5
INTRODUCTION 9

1 Scope 11
2 Normative references 11
3 Terms, definitions and abbreviations 13
4 Key concepts and assumptions 23
4.1 Types of software 23
4.2 Types of data 25
4.3 Software and System Safety Lifecycles 25
4.4 Gradation principles 31
5 Requirements for the software of I&C systems performing category C functions 35
5.1 General requirements 35
5.2 Selection of pre-developed software 43
5.3 Software requirements specification 45
5.4 Software design 49
5.5 Implementation of new software 51
5.6 Software aspects of system integration 53
5.7 Software aspects of system validation 53
5.8 Installation of software on site 55
5.9 Anomaly reports 55
5.10 Software modification 55
6 Requirements for the software of I&C systems performing category B functions 57
6.1 General requirements 57
6.2 Selection of pre-developed software 65
6.3 Software requirements specification 75
6.4 Software design 79
6.5 Implementation of new software 83
6.6 Software aspects of system integration 87
6.7 Software aspects of system validation 87
6.8 Installation of software on site 89
6.9 Anomaly reports 91
6.10 Software modification 91

Bibliography 95

Figure 1 – Typical software parts in computer-based I&C systems. 23
Figure 2 – Activities of the System Safety Lifecycle (as defined by IEC 61513). 25
Figure 3 – Software related activities in the System Safety Lifecycle 27
Figure 4 – Development activities of the IEC 62138 Software Safety Lifecycle. 29
Figure 5 – Process for providing evidence of correctness for pre-developed software of an I&C system of safety class 2. 31

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, those 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 importants 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*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, définitions et abréviation suivants s'appliquent.

3.1
animation
processus par lequel le comportement défini par une spécification est visualisé avec ses valeurs effectives dérivées des équations de comportement et des valeurs d'entrée

(CEI 60880-2)

3.2
fonction d'application
fonction d'un système d'I&C qui accomplit une tâche relative au processus sous contrôle plutôt qu'au fonctionnement du système lui-même

(CEI 61513)

3.3
langage orienté application
langage informatique spécifiquement conçu pour un certain type d'application et pour être utilisé par les spécialistes de ce type d'application

NOTE 1 Les familles d'équipements offrent en général des langages orientés application de façon à faciliter l'adaptation des équipements à des besoins particuliers.

NOTE 2 Les langages orientés application peuvent être utilisés pour la spécification d'exigences fonctionnelles que doit satisfaire un système d'I&C, ou pour spécifier ou concevoir le logiciel d'application. Ils peuvent être basés sur du texte, des diagrammes, ou une combinaison des deux.

NOTE 3 Exemples: les langages à blocs fonctionnels, les langages définis par la CEI 61131-3.

NOTE 4 Voir aussi Langage généraliste.

3.4
logiciel d'application
partie du logiciel d'un système d'I&C qui exécute des fonctions d'application

(CEI 61513)

NOTE Voir aussi Logiciel système, Logiciel système opérationnel.

3.5
catégorie d'une fonction d'I&C
une des trois affectations possibles (A, B ou C) des fonctions d'I&C, résultant de l'évaluation de l'importance pour la sûreté des fonctions à exécuter. Une affectation «non classée» peut être délivrée si la fonction n'est pas importante pour la sûreté

(CEI 61513)

NOTE Voir aussi Classe d'un système d'I&C.