SLOVENSKI STANDARD
SIST EN 62138:2009

01-november-2009

Nuklearne elektrarne - Merilna in nadzorna oprema za zagotavljenje varnosti - Znaļ ilnosti programske opreme raļ unalniģkih sistemov, ki izvajajo kategoriji funkcij B ali C (IEC 62138:2004)

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

Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie B oder C

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

Ta slovenski standard je istoveten z: **EN 62138:2009**

ICS:

27.120.20	Jedrske elektrarne. Varnost	Nuclear power plants. Safety

SIST EN 62138:2009 **en,fr**

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.

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

CONTENTS

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.

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 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.

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.

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*

3 Terms, definitions and abbreviations

For the purposes of this document, the following terms, definitions and abbreviation apply.

3.1
animation
process by which the behaviour defined by a specification is displayed with actual values derived from the stated behaviour expressions and from some input values

(IEC 60880-2)

3.2
application function
function of an I&C system that performs a task related to the process being controlled rather than to the functioning of the system itself

(IEC 61513)

3.3
application-oriented language
computer language specifically designed to address a certain type of application and to be used by persons who are specialists of this type of application

NOTE 1 Equipment families usually feature application-oriented languages so as to provide easy to use capability for adjusting the equipment to specific requirements.

NOTE 2 Application-oriented languages may be used to specify the functional requirements of an I&C system, and/or to specify or design application software. They may be based on texts, on graphics, or on both.

NOTE 3 Examples: function block diagram languages, languages defined by IEC 61131-3.

NOTE 4 See also General-purpose language.

3.4
application software
part of the software of an I&C system that implements the application functions

(IEC 61513)

NOTE See also System software, Operational system software.

3.5
category of an I&C function
one of three possible safety assignments (A, B, C) of I&C functions resulting from considerations of the importance to safety of the functions to be performed. An unclassified assignment may be made if the function is not significant to safety

(IEC 61513)

NOTE See also Class of an I&C system.

3.6
class of an I&C system
one of three possible assignments (1, 2, 3) of I&C systems important to safety resulting from consideration of their requirement to implement I&C functions of differing importance to safety. An unclassified assignment is made if the I&C system does not implement functions important to safety

(IEC 61513)

NOTE See also Category of an I&C function.

3.7
complexity
degree to which a system or component has a design, implementation or behaviour that is difficult to understand and verify

(IEC 61513)

3.8
configuration management
discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control modifications to those characteristics, record and report changes in status, and verify compliance with specified requirements

(IEC 61513)

3.9
design specification
document or set of documents that describe the organisation and functioning of an item, and that are used as a basis for the implementation and the integration of the item

3.10
documentation for safety
document or set of documents that specifies how a product can be safely used for applications important to safety

3.11
equipment family
set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). The development of plant specific configurations and of the related application software may be supported by software tools. An equipment family usually provides a number of standard functionalities (application functions library) that may be combined to generate specific application software

(IEC 61513)

NOTE 1 An equipment family may be a product of a defined manufacturer or a set of products interconnected and adapted by a supplier.

NOTE 2 The term “Equipment platform” is sometime used as a synonym of “Equipment family”.

3.12
error
discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretical value or condition

(IEC 61513)

NOTE See also Mistake, Fault, Failure.

3.13
executable code
software that is included in the target system

NOTE Executable code usually includes instructions to be executed by the hardware of the target system, and associated data.

3.14
failure
deviation of the delivered service from the intended one

(IEC 61513)

NOTE See also Mistake, Fault, Error.

3.15
fault
defect in a hardware, software or system component

(IEC 61513)

NOTE 1 Faults may be subdivided into random faults and systematic faults. Random faults result from hardware degradation and cause failures at unpredictable times. Systematic faults result from design errors (for example, software faults) and, in identical conditions, lead systematically to the same failures.

NOTE 2 A fault (in particular a design fault) may remain undetected in a system until specific conditions are such that the result produced does not conform to the intended function, i.e. a failure occurs.

NOTE 3 See also Mistake, Error, Failure.

3.16
functional validation
verification of the correctness of the application functions specifications versus the plant functional and performance requirements. It is complementary to the system validation that verifies the compliance of the system with the functions specification

(IEC 61513)

3.17
general-purpose language
computer language designed to address all types of usage

NOTE 1 The system software of equipment families is usually implemented using general-purpose languages.

NOTE 2 Examples: Ada, C, Pascal.

NOTE 3 See also Application-oriented language.

3.18
integration
progressive aggregation and verification of components into a complete system

3.19
I&C architecture
organisational structure of the I&C systems of a plant which are important to safety

(IEC 61513)

3.20
mistake
human action (or inaction) that produces an unintended result

(IEC 60880-2)

NOTE See also Fault, Error, Failure.