# SLOVENSKI STANDARD
# oSIST prEN 62138:2019

**01-april-2019**

---

**Nuklearne elektrarne - Instrumenti in nadzorni sistemi za zagotavljanje varnosti - Značilnosti programske opreme računalniških sistemov, ki izvajajo funkcije kategorij B ali C (IEC 62138:2018)**

Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions (IEC 62138:2018)



Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2018)



Centrales nucléaires de puissance - Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté - Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C (IEC 62138:2018)

**Ta slovenski standard je istoveten z:** **prEN 62138:2019**

---

**ICS:**

| | | |
|---|---|---|
| 27.120.20 | Jedrske elektrarne. Varnost | Nuclear power plants. Safety |

**oSIST prEN 62138:2019** **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

**DRAFT**
**prEN IEC 62138**

February 2019

ICS 27.120.20

Will supersede EN 62138:2009

English Version

# Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions (IEC 62138:2018)

Centrales nucléaires de puissance - Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté - Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C (IEC 62138:2018)

Kernkraftwerke - Leittechnische Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorien B oder C (IEC 62138:2018)



This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2019-04-26.

The text of this draft consists of the text of IEC 62138:2018.

If this draft becomes a European Standard, 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.



This draft European Standard was established by CENELEC 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 CEN-CENELEC Management Centre has the same status as the official versions.

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

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.


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

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

## European foreword

This document (prEN IEC 62138:2019) consists of the text of IEC 62138:2018 prepared by IEC/SC 45A "Instrumentation, control and electrical power systems of nuclear facilities", of IEC/TC 45 "Nuclear instrumentation".

This document is currently submitted to the Enquiry.

The following dates are proposed:

| | | |
|---|---|---|
| • latest date by which the existence of this document has to be announced at national level | (doa) | dor + 6 months |
| • latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | dor + 12 months |
| • latest date by which the national standards conflicting with this document have to be withdrawn | (dow) | dor + 36 months (to be confirmed or modified when voting) |

This document will supersede EN 62138:2009.



As stated in the nuclear safety directive 2009/71/EURATOM, Chapter 1, Article 2, item 2, Member States are not prevented from taking more stringent safety measures in the subject-matter covered by the Directive, in compliance with Community law. In a similar manner, this European standard does not prevent Member States from taking more stringent nuclear safety and/or security measures in the subject-matter covered by this standard.

## Annex ZA
(normative)

## Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| IEC 60880 | 2006 | Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions | EN 60880 | 2009 |
| IEC 61226 | - | Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions | EN 61226 | - |
| IEC 61513 | 2011 | Nuclear power plants - Instrumentation and control important to safety - General requirements for systems | EN 61513 | 2013 |
| IEC 62671 | 2013 | Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality | - | - |

IEC 62138

Edition 2.0 2018-07

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE



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

## Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-5830-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO 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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 2004. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) align the standard with standards published or revised since the first edition, in particular IEC 61513, IEC 60880, IEC 62645 and IEC 62671;
b) merge Clause 5 and Clause 6 of the first edition into a single clause in order to avoid the repetition of the vast majority of the text which proves to be extremely difficult to maintain in consistency;

c) revise clause on the selection of pre-developed software based on experiences from the application of the first edition of the standard on industrial projects. More precise criteria are proposed for the evidence of correctness of pre-developed software;

d) introduce requirements on traceability in consistency with IEC 61513;

e) introduce an Annex A that gives a typical list of software documentation;

f) introduce an Annex B that establishes relationship between IEC 61513 and this document;

g) introduce an Annex C that establishes relationship between IEC 61508 and this document.

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

| FDIS | Report on voting |
|---|---|
| 45A/1201/FDIS | 45A/1209/RVD |

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

In this document, the following print types are used:

- *Requirements and recommendations applicable specifically to class 2 or to class 3 systems appear in italics in Clause 6.*



The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be



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

# INTRODUCTION

**a) Technical background, main issues and organisation of this document**

This International Standard provides requirements on the software aspects for computer-based instrumentation and control (I&C) systems performing category B or C functions as defined by IEC 61226. It complements IEC 60880 which provides requirements for the software of computer-based I&C systems performing category A functions.

It is consistent with, and complementary to, IEC 61513:2011. Activities that are mainly system level activities (for example, integration, validation and installation) are not addressed exhaustively by this document: requirements that are not specific to software are deferred to IEC 61513:2011.

This document 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 application-oriented languages.

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

IEC 61513 is a first level IEC SC 45A document and gives guidance applicable to I&C at system level.

IEC 62138 is a second level IEC SC 45A document that supplements IEC 61513 concerning software development of computer-based I&C systems performing category B or C functions.

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



**c) Recommendations and limitations regarding the application of this document**

This document is not intended to be used as a general-purpose software engineering guide. It applies to the software of I&C systems performing category B or C functions for new nuclear power plants as well as to I&C upgrading or back-fitting of existing plants.



For existing plants, only a subset of requirements is applicable and this subset has to be identified at the beginning of any project.

The purpose of the guidance provided by this document is to reduce, as far as possible, the potential for latent software faults to cause system failures, either due to single software failures or multiple software failures (i.e. Common Cause Failures due to software).

This document does not explicitly address how to protect software against those threats arising from malicious attacks, i.e. cybersecurity, for computer-based systems. IEC 62645 provides requirements for security programmes for computer-based systems.

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

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

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in nuclear power plants (NPPs). IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital

systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 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 IEC SC 45A standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance. At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirement for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 is published, this NOTE 2 of the introduction will be suppressed.

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

## 1 Scope

This document specifies requirements for the software of computer-based instrumentation and control (I&C) systems performing functions of safety category B or C as defined by IEC 61226. It complements IEC 60880 which provides requirements for the software of computer-based I&C systems performing functions of safety category A.

It is 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 document: requirements that are not specific to software are deferred to IEC 61513.

The link between functions categories and system classes is given in IEC 61513. 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 document are attached to the safety class of the I&C system (class 2 or class 3).



This document is not intended to be used as a general-purpose software engineering guide. It applies to the software of I&C systems of safety classes 2 or 3 for new nuclear power plants as well as to I&C upgrading or back-fitting of existing plants.



For existing plants, only a subset of requirements is applicable and this subset has to be identified at the beginning of any project.

The purpose of the guidance provided by this document is to reduce, as far as possible, the potential for latent software faults to cause system failures, either due to single software failures or multiple software failures (i.e. Common Cause Failures due to software).

This document does not explicitly address how to protect software against those threats arising from malicious attacks, i.e. cybersecurity, for computer-based systems. IEC 62645 provides requirements for security programmes for computer-based systems.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

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

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 62671:2013, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

## 3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

**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

[SOURCE: IEC 60880:2006, 3.1]

**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

[SOURCE: IEC 61513:2011, 3.1]



**3.3**
**application software**
part of the software of an I&C system that implements the application functions



Note 1 to entry: Application software contrasts with system software.

Note 2 to entry: Application software is plant specific, so it is not to be considered pre-developed software.

[SOURCE: IEC 61513:2011, 3.2 modified (modified notes to entry)]

**3.4**
**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 to entry: Equipment families usually feature application-oriented languages so as to provide easy to use capability for adjusting the equipment to specific requirements.

Note 2 to entry: 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 to entry: Examples: function block diagram languages, languages defined by IEC 61131-3.

Note 4 to entry: See also general-purpose language.

[SOURCE: IEC 60880:2006, 3.3 modified (addition of note 4 to entry)]

**3.5**
**common cause failure**
**CCF**
failure of two or more structures, systems or components due to a single specific event or cause