IEC 62138

Edition 2.0 2018-07

REDLINE VERSION

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-5927-6

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD....4
INTRODUCTION....6
1 Scope....9
2 Normative references....10
3 Terms and definitions ~~and abbreviations~~ 10
4 Symbols and abbreviated terms 19
5 Key concepts and assumptions 19
5.1 General....19
5.2 Types of software....19
5.3 Types of configuration data 21
5.4 Software and system safety lifecycles....21
5.5 Gradation principles 24
~~Requirements for the software of I&C systems performing category C functions ....~~
~~General requirements....~~
~~Selection of pre-developed software ....~~
~~Software requirements specification ....~~
~~Software design ....~~
~~Implementation of new software ....~~
~~Software aspects of system integration....~~
~~Software aspects of system validation ....~~
~~Installation of software on site ....~~
~~Anomaly reports....~~
~~Software modification....~~
6 Requirements for the software of class 2 and class 3 I&C systems ~~performing category B functions~~ 37
6.1 Applicability of the requirements....37
6.2 General requirements....37
6.2.1 Software safety lifecycle – Software quality assurance....37
6.2.2 Verification 38
6.2.3 Configuration management....39
6.2.4 Selection and use of software tools 40
6.2.5 Selection of languages....41
~~Security....~~
6.3 Selection of pre-developed software 43
6.3.1 General 43
6.3.2 Documentation for safety....43
6.3.3 Evidence of correctness 44
6.3.4 Functional suitability 51
~~Selection and use of dedicated devices with embedded software ....~~
6.3.5 Selection and use of digital devices of limited functionality....52
6.4 Software requirements specification 52
6.4.1 General 52
6.4.2 Objectives....52
6.4.3 Inputs 52
6.4.4 Contents 53
6.4.5 Properties 54

6.5 Software design 54
6.5.1 Objectives 54
6.5.2 Inputs 55
6.5.3 Contents 55
6.5.4 Properties 56
6.6 Implementation of software 57
6.6.1 General requirements 57
6.6.2 Configuration of software and of devices containing software 57
6.6.3 Implementation with application-oriented languages 57
6.6.4 Implementation with general-purpose languages 58
6.7 Software aspects of system integration 60
6.7.1 General 60
6.8 Software aspects of system validation 60
6.8.1 General 60
6.9 Installation of software on site 62
6.9.1 General 62
6.10 Anomaly reports 62
6.11 Software modification 63
6.11.1 General 63
6.12 Defences against common cause failure due to software 64
Annex A (informative) Typical list of software documentation 66
Annex B (informative) Correspondence between IEC 61513:2011 and this document 67
Annex C (informative) Relations of this document with IEC 61508 68
C.1 General 68
C.2 Comparison of scope and concepts 68
C.3 Correspondence between this document and IEC 61508-3:2010 69
Bibliography 70

~~Figure – Process for providing evidence of correctness for pre-developed software of an I&C system of safety class 2. .....~~

Figure 1 – Typical software parts in a computer-based I&C system 20
Figure 2 – Activities of the system safety lifecycle (as defined by IEC 61513:2011) 21
Figure 3 – Software related activities in the system safety lifecycle 22
Figure 4 – Development activities of the IEC 62138 software safety lifecycle 23
Figure 5 – Overview of the typical qualification process for pre-developed complete operational system software 46
Figure 6 – Overview of the typical qualification process for pre-developed software components 47

Table A.1 – Typical list of software documentation 66
Table B.1 – Correspondence between IEC 61513:2011 and this document 67
Table C.1 – Correspondence between this document and IEC 61508-3:2010 69

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT ~~FOR~~ 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.

DISCLAIMER
This Redline version is not an official Standard and is intended to provide the user with an indication of what changes have been made to the previous version. Only the IEC International Standard provided in this package is to be considered the official Standard.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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.

IMPORTANT – The “colour inside” logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this publication using a colour printer.

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.~~

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 ~~FOR~~ TO SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY B OR C FUNCTIONS

1 Scope

This document ~~provides~~ 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 ~~and IEC 60880-2~~, which provides 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 document: 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.~~

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 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 document is not intended to be used as a general-purpose software engineering guide. It ~~provides requirements that~~ applies to the software of I&C systems of safety classes 2 or 3 ~~must meet to achieve system nuclear safety objectives~~ 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 ~~systems~~ important ~~for~~ to safety – Classification of instrumentation and control functions*

IEC 61513:~~2001~~ 2011, *Nuclear power plants – Instrumentation and control ~~for systems~~ 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*

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



IEC 62138:2018-07(en-fr)

CONTENTS

FOREWORD....4
INTRODUCTION....6
1 Scope....8
2 Normative references....8
3 Terms and definitions....9
4 Symbols and abbreviated terms....17
5 Key concepts and assumptions....17
5.1 General....17
5.2 Types of software....17
5.3 Types of configuration data....18
5.4 Software and system safety lifecycles....19
5.5 Gradation principles....21
6 Requirements for the software of class 2 and class 3 I&C systems....22
6.1 Applicability of the requirements....22
6.2 General requirements....22
6.2.1 Software safety lifecycle – Software quality assurance....22
6.2.2 Verification....23
6.2.3 Configuration management....24
6.2.4 Selection and use of software tools....25
6.2.5 Selection of languages....26
6.3 Selection of pre-developed software....27
6.3.1 General....27
6.3.2 Documentation for safety....27
6.3.3 Evidence of correctness....28
6.3.4 Functional suitability....35
6.3.5 Selection and use of digital devices of limited functionality....35
6.4 Software requirements specification....35
6.4.1 General....35
6.4.2 Objectives....35
6.4.3 Inputs....36
6.4.4 Contents....36
6.4.5 Properties....37
6.5 Software design....38
6.5.1 Objectives....38
6.5.2 Inputs....38
6.5.3 Contents....39
6.5.4 Properties....40
6.6 Implementation of software....40
6.6.1 General requirements....40
6.6.2 Configuration of software and of devices containing software....40
6.6.3 Implementation with application-oriented languages....41
6.6.4 Implementation with general-purpose languages....41
6.7 Software aspects of system integration....43
6.7.1 General....43
6.8 Software aspects of system validation....43
6.8.1 General....43

6.9 Installation of software on site 45
6.9.1 General 45
6.10 Anomaly reports 45
6.11 Software modification 46
6.11.1 General 46
6.12 Defences against common cause failure due to software 47
Annex A (informative) Typical list of software documentation 48
Annex B (informative) Correspondence between IEC 61513:2011 and this document 49
Annex C (informative) Relations of this document with IEC 61508 50
C.1 General 50
C.2 Comparison of scope and concepts 50
C.3 Correspondence between this document and IEC 61508-3:2010 51
Bibliography 52

Figure 1 – Typical software parts in a computer-based I&C system 18
Figure 2 – Activities of the system safety lifecycle (as defined by IEC 61513:2011) 19
Figure 3 – Software related activities in the system safety lifecycle 20
Figure 4 – Development activities of the IEC 62138 software safety lifecycle 21
Figure 5 – Overview of the typical qualification process for pre-developed complete operational system software 30
Figure 6 – Overview of the typical qualification process for pre-developed software components 31

Table A.1 – Typical list of software documentation 48
Table B.1 – Correspondence between IEC 61513:2011 and this document 49
Table C.1 – Correspondence between this document and IEC 61508-3:2010 51

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*

SOMMAIRE

AVANT-PROPOS 56
INTRODUCTION 58
1 Domaine d'application 60
2 Références normatives 60
3 Termes et définitions 61
4 Symboles et termes abrégés 69
5 Concepts et présupposés 70
5.1 Généralité 70
5.2 Types de logiciels 70
5.3 Types de données de configuration 71
5.4 Cycles de vie et de sûreté du logiciel et du système 71
5.5 Principes de gradation 73
6 Exigences pour le logiciel des systèmes d'I&C de classe 2 et de classe 3 74
6.1 Applicabilité des exigences 74
6.2 Exigences générales 75
6.2.1 Cycle de vie et de sûreté du logiciel – Assurance qualité du logiciel 75
6.2.2 Vérification 76
6.2.3 Gestion de configuration 77
6.2.4 Sélection et utilisation des outils logiciels 77
6.2.5 Sélection des langages 79
6.3 Sélection des logiciels prédéveloppés 80
6.3.1 Généralités 80
6.3.2 Documentation pour la sûreté 80
6.3.3 Preuve de conformité 81
6.3.4 Adéquation fonctionnelle 88
6.3.5 Sélection et utilisation d'appareils numériques à fonctionnalité limitée 88
6.4 Spécification du logiciel 88
6.4.1 Généralités 88
6.4.2 Objectifs 88
6.4.3 Entrées 89
6.4.4 Contenu 89
6.4.5 Propriétés 90
6.5 Conception du logiciel 91
6.5.1 Objectifs 91
6.5.2 Entrées 91
6.5.3 Contenu 92
6.5.4 Propriétés 93
6.6 Réalisation du logiciel 93
6.6.1 Exigences générales 93
6.6.2 Configuration du logiciel et des équipements contenant du logiciel 94
6.6.3 Réalisation en langages orientés application 94
6.6.4 Réalisation en langages généralistes 95
6.7 Aspects logiciels de l'intégration du système 96
6.7.1 Généralités 96
6.8 Aspects logiciels de la validation du système 97
6.8.1 Généralités 97

6.9 Installation du logiciel sur site 99
6.9.1 Généralités 99
6.10 Rapports d'anomalie 99
6.11 Modification du logiciel 99
6.11.1 Généralités 99
6.12 Défenses contre les défaillances de cause commune liées au logiciel 100
Annexe A (informative) Liste typique d'une documentation logicielle 102
Annexe B (informative) Correspondance entre l'IEC 61513:2011 et le présent document 103
Annexe C (informative) Relations du présent document avec l'IEC 61508 104
C.1 Généralités 104
C.2 Comparaison des domaines et des concepts 104
C.3 Correspondance entre le présent document et l'IEC 61508-3:2010 105
Bibliographie 106

Figure 1 – Composants logiciels typiques d'un système d'I&C informatisé 70
Figure 2 – Activités du cycle de vie de sûreté du système (selon l'IEC 61513:2011) 71
Figure 3 – Activités logicielles dans le cycle de vie et de sûreté du système 72
Figure 4 – Activités de développement du cycle de vie et de sûreté du logiciel selon l'IEC 62138 73
Figure 5 – Vue d'ensemble d'un processus typique de qualification de logiciel système opérationnel complet prédéveloppé 83
Figure 6 – Vue d'ensemble d'un processus typique de qualification de composants logiciels prédéveloppés 84

Tableau A.1 – Liste typique d'une documentation logicielle 102
Tableau B.1 – Correspondance entre l'IEC 61513:2011 et le présent document 103
Tableau C.1 – Correspondance entre le présent document et l'IEC 61508-3:2010 105

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC 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, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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 l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62138 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Cette deuxième édition annule et remplace la première édition publiée en 2004. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) aligner la présente norme sur les normes publiées ou révisées depuis sa première édition, en particulier l'IEC 61513, l'IEC 60880, l'IEC 62645 et l'IEC 62671;

b) fusionner les Articles 5 et 6 de la première édition en un seul article pour éviter la répétition d'une grande partie du texte dont le maintien de la cohérence s'est avéré très difficile;

c) réviser l'article portant sur la sélection des logiciels prédéveloppés sur la base du retour d'expérience issu de l'application de la première édition de la norme pour des projets industriels. Des critères plus précis sont proposés pour ce qui concerne la preuve de conformité des logiciels prédéveloppés;

d) introduire des exigences portant sur la traçabilité en cohérence avec l'IEC 61513;

e) introduire une Annexe A fournissant une liste typique de documentation des logiciels;

f) introduire une Annexe B établissant les relations liant l'IEC 61513 au présent document;

g) introduire une Annexe C établissant les relations liant l'IEC 61508 au présent document.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1201/FDIS	45A/1209/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 internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Dans ce document, les caractères suivant sont utilisés:

- *Les exigences et recommandations applicables uniquement aux systèmes de classes 2 et 3 apparaissent en italique à l'Article 6.*

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

INTRODUCTION

a) Contexte technique, questions importantes et structure du présent document

La présente norme internationale établit des exigences portant sur les aspects logiciels des systèmes d'instrumentation et de contôle-commande (I&C) informatisés réalisant des fonctions de catégorie B ou C, telles que définies par l'IEC 61226. Elle complète l'IEC 60880 qui établit les exigences pour les logiciels des systèmes d'I&C informatisés réalisant des fonctions de catégorie A.

Elle est cohérente et complémentaire avec l'IEC 61513:2011. Les activités se situant principalement au niveau système (par exemple l'intégration, la validation et l'installation) ne sont pas couvertes de façon exhaustive par le présent document; les exigences qui ne sont pas spécifiques au logiciel sont reportées dans l'IEC 61513:2011.

Le présent document prend en compte les pratiques de développement actuellement mises en œuvre pour les logiciels de systèmes d'I&C, et en particulier:

– l'utilisation de logiciels, d'équipements et de familles d'équipements prédéveloppés qui n'ont pas nécessairement été conçus selon les normes de l'industrie nucléaire;

– l'utilisation de langages orientés application.

b) Position du présent document dans la collection de normes du SC 45A de l'IEC

L'IEC 61513 est le document de premier niveau du SC 45A qui fournit les recommandations applicables pour l'I&C au niveau système.

L'IEC 62138 est le document de deuxième niveau du SC 45A qui complète l'IEC 61513 pour ce qui est du développement logiciel pour les systèmes d'I&C informatisés réalisant des fonctions de catégorie B ou C.

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

c) Recommandations et limites relatives à l'application du présent document

Il n'est pas prévu que le présent document soit utilisé comme un guide de génie logiciel généraliste. Elle est applicable pour les logiciels des systèmes d'I&C réalisant des fonctions de catégorie B ou C pour les nouvelles centrales nucléaires de puissance comme pour les mises à jour ou les rénovations d'I&C de centrales existantes.

Pour les centrales existantes, seul un sous ensemble d'exigences est applicable et ce sous ensemble a à être identifié au début de chaque projet.

L'objectif des recommandations fournies par le présent document est de réduire, autant que faire se peut, le potentiel de défauts logiciels latents pouvant causer des défaillances système, dues à des défaillances logicielles uniques ou bien à des défaillances logicielles multiples (c'est-à-dire Défaillances de Cause Commune dues au logiciel).

Le présent document ne traite pas explicitement de la protection des logiciels contre les menaces liées à des attaques malveillantes des systèmes informatisés, c'est-à-dire de cybersécurité. L'IEC 62645 fournit des exigences portant sur les programmes de sécurité applicables pour les systèmes informatisés.

Afin d'assurer la pertinence du présent document pour les années à venir, l'accent est mis sur les questions de principes plutôt que sur les technologies particulières.

d) Description de la structure de la collection des normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC, et d'autres organisations (AIEA, ISO)

Les documents de niveau supérieur de la collection de normes produites par le SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. L'IEC 61513 traite des exigences générales 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. L'IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; elle couvre les systèmes d'alimentation électrique jusqu'à et y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être considérées ensemble et au même niveau. Les normes IEC 61513 et IEC 63046 structurent la collection de normes du SC 45A de l'IEC et forment un cadre

complet, cohérent et consistant établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

Les normes IEC 61513 et IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, la défense contre les défaillances de cause commune, la conception des salles de commande, compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes numériques programmables, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes, de second niveau, forment, avec les normes IEC 61513 et IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont généralement pas référencées directement par les normes IEC 61513 ou IEC 63046, 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 de l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

Les normes de la collection produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires, avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle-commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en œuvre NSS17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à l'IEC 61508-3 pour le secteur nucléaire. Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, l'IEC 62645 est le document chapeau des normes du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée sur les principes pertinents de haut niveau de l'ISO/IEC 27001 et l'ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec l'IEC 62443. Au second niveau, l'IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et l'IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est fait l'hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) on applique des normes nationales ou internationales.

NOTE 2 Le domaine du SC 45A de l'IEC a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein du SC 45A de l'IEC pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts du SC 45A de l'IEC ont recommandé que pour établir des exigences générales pour les systèmes électriques une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque l'IEC 63046 sera publiée, la présente NOTE 2 de l'introduction sera supprimée.

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

1 Domaine d'application

Le présent document spécifie 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 l'IEC 61226. Il est complémentaire à l'IEC 60880 qui énonce des exigences sur le logiciel des systèmes d'I&C informatisés réalisant des fonctions de sûreté de catégorie A.

Il est également cohérent et complémentaire à l'IEC 61513. Les activités de nature essentiellement système (par exemple 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 reportées dans l'IEC 61513.

La relation entre les catégories des fonctions et les classes des systèmes est fournie par l'IEC 61513. Un système d'I&C classé de sûreté pouvant réaliser des fonctions de catégories différentes, ainsi que des fonctions non classées, les exigences du présent document sont attachées à la classe de sûreté du système d'I&C (classe 2 ou classe 3).

Il n'est pas prévu que le présent document soit utilisé comme un guide de génie logiciel généraliste. Il est applicable pour les logiciels des systèmes d'I&C de classe de sûreté 2 ou 3 pour les nouvelles centrales nucléaires de puissance comme pour les mises à jour ou les rénovations d'I&C de centrales existantes.

Pour les centrales existantes, seul un sous ensemble d'exigences est applicable et ce sous ensemble a à être identifié au début de chaque projet.

L'objectif des recommandations fournies par le présent document est de réduire, autant que faire se peut, le potentiel d'avoir des défauts logiciels latents pouvant causer des défaillances système, due à des défaillances logicielles uniques ou bien à des défaillances logicielles multiples (c'est-à-dire Défaillances de Cause Commune dues au logiciel).

Le présent document ne traite pas explicitement de la protection des logiciels contre les menaces liées à des attaques malveillantes des systèmes informatisés, c'est-à-dire de cybersécurité. L'IEC 62645 fournit des exigences portant sur les programmes de sécurité applicables pour les systèmes informatisés.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences 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).

IEC 60880:2006, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A*

IEC 61226, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Classement des fonctions d'instrumentation et de contrôle-commande*

IEC 61513:2011, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 62671:2013, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées*