IEC 62671

Edition 1.0 2013-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées

IEC 62671:2013

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62671

Edition 1.0 2013-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX
XA

ICS 27.120.20
ISBN 978-2-83220-630-0

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – SELECTION AND USE OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY

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 62671 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/898/FDIS	45A/907/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 the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

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

The contents of the corrigendum of September 2016 have been included in this copy.

INTRODUCTION

a) Technical background, main issues and organisation of the Standard

This IEC standard specifically focuses on the selection and evaluation of pre-developed dedicated devices of limited, specific functionality and limited configurability for use in a nuclear power plant, where these devices incorporate either software or digital circuit designs specified using hardware description languages and where these devices have been produced to a recognized non-nuclear standard, but not to the SC 45A series of standards.

It is intended that the Standard be used by designers of NPPs, operators of NPPs (utilities), systems evaluators and by licensors.

The focus of this standard is on two aspects that are not addressed by other standards in the IEC SC 45A series:

- Other standards address the hardware aspects of devices containing software, or address complex devices such as PLCs containing software where that software has the potential to be much more complex[1] than in the devices covered by this standard, and
- Other standards focus on devices to be designed specifically for nuclear applications, whereas this standard focuses on the considerations necessary to apply devices in NPPs that have not been designed for nuclear use.

Designers of I&C systems for NPPs are increasingly forced to turn to such devices because of reasons such as equipment obsolescence, the small size of the nuclear market as compared to the industrial market, and the growing number of suppliers who choose to design to general safety standards such as IEC 61508.

Hence it has become vital for designers of these systems to have the guidance provided by this standard to be able to select and evaluate candidate devices for their suitability to applications in NPPs. This standard provides such guidance without which I&C designers would be required to consider how to interpret IEC 60880, IEC 62138 or IEC 62566 for this purpose.

b) Situation of the current Standard 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 the system level. It is supplemented by guidance at the device level by IEC 60987 for design of hardware, by IEC 60880 and IEC 62138 for software and by IEC 62566 for potentially complex devices. All of these standards focus on nuclear-specific designs and apply the concept of a life cycle.

IEC 62671 is a second level IEC SC 45A document tackling the specific issue of selecting and evaluating devices for use in NPPs where the candidate devices have been designed for non-nuclear use (and possibly certified as compliant with a widely-accepted general safety standard such as IEC 61508). Additionally, IEC 62671 addresses only devices that have dedicated limited and specific functionality, and limited configurability.

IEC 62671 is to be read in association with IEC 60880 (informative), IEC 62138 (informative), IEC 60987 (informative) and IEC 62566 (informative) which are the other appropriate IEC SC 45A documents which provide guidance on computer-based systems performing functions important to safety in NPPs.

---

[1] There is no agreed upon definition of “complexity”, but where devices support more functionality, there are associated increases in volume of code, contention for system resources, and timing-related phenomena that can lead to unexpected failures of the device. This standard addresses these problems by covering only devices with very restricted functionality.

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 the Standard

It is important to note that this Standard establishes no additional functional requirements for systems of class 1, 2 or 3.

Aspects for which specific requirements have been provided in this Standard are:

- The use of a planned process to select, and then evaluate candidate devices for use, as well as to include considerations of the integration of the device into plant systems.
- Criteria for evaluating the functional suitability of a device that contains embedded software or uses digital circuits designed with software-based tools such as HDL (Hardware Description Language).
- Criteria to consider and balance in an overall evaluation to obtain an appropriate level of assurance that the device will perform as specified when called upon.
- Considerations for the safe application of the selected device in plant systems.

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

Throughout this standard, the emphasis is on the review of evidence of the processes in place at the designer and the manufacturer (who may be different organisations) since they are the organisations that impact the acceptability of the candidate device for its intended application. This evidence may have to be obtained through the supplier with whom the end user has direct contact.

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 document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

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

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding nuclear safety. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 refers 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 (QA).

The IEC SC 45A standards series consistently implement and detail the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements NS-R-1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NOTE 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, that are based on the requirements of standards such as IEC 61508.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – SELECTION AND USE OF INDUSTRIAL DIGITAL DEVICES OF LIMITED FUNCTIONALITY

1 Scope

1.1 General

This International Standard addresses certain devices that contain embedded software or electronically-configured digital circuits that have not been produced to other IEC Standards which apply to systems and equipment important to safety in Nuclear Power Plants, but which are candidates for use in nuclear power plants. It provides requirements for the selection and evaluation of such devices where they have dedicated[2], limited, and specific functionality and limited configurability.

In accordance with IEC 61513, I&C systems important to safety of classes 1, 2 and 3 may be implemented using conventional hard-wired equipment, digital technology equipment (computer based or programmed hardware) or by using a combination of both types of equipment. This International Standard provides the acceptance criteria for the selection, evaluation and use of certain digital devices that have not been developed specifically for use in these nuclear I&C systems. Such devices are very often developed to meet IEC 61508, and this standard acknowledges that compliance with IEC 61508 can be a key positive factor when qualifying non-nuclear components for nuclear sector use.

Devices addressed by this Standard are dedicated devices of limited, specific functionality, that contain or may contain components driven by software or digital circuits designed using software-based tools. Examples are smart sensors, valve positioners, electrical protective devices or inverters that contain or may contain components driven by software or digital circuits designed using software-based tools. This standard does not address the software aspects of complex general-purpose devices that are addressed by other standards, such as IEC 60880 and IEC 62138 for software. This standard addresses the issues that should be considered when evaluating the suitability of these dedicated devices of limited, specific functionality for use in a nuclear power plant. The intent is to apply a graded approach to these issues, with more demanding requirements applied for higher classes.

These issues include:

- functional suitability (does the device perform the functions required, and are these functions suitably secure from interference from any other functions),
- the evidence required to demonstrate this suitability (such as the development process followed, and the operational experience and maturity of the device),
- aspects affecting integration of the device in existing systems (e.g. functional compatibility and impact on maintenance and operation), and
- requirements related to ensuring the device will retain its suitability for its required lifetime (such as the lifetime of the plant).

This Standard relies on other standards, especially IEC 60780, to address hardware qualification issues not related to the complexities of software, namely reliability aspects related to environmental qualification and failures due to aging or physical degradation. Other

---

2 "Dedicated" in the sense in which it is used in this standard refers to design for one specific function that cannot be changed in the field. Refer to 3.7.

standards such as IEC 61508 can be used as complementary guidance for the evaluation and assessment of components, but it is recognized that certification to non-nuclear standards alone is insufficient.

1.2 Background

The need for this standard arises from current trends in the I&C industry including the advancing obsolescence of existing devices presently in use in nuclear power plants. It is becoming increasingly difficult, if not impossible, to identify analog devices or replace many existing devices with identical ones because suppliers increasingly employ micro-controllers, ASICs etc. embedded within the candidate replacement devices, and analog devices are becoming increasingly unavailable.

There are various technical risks regarding the acceptance of these devices for use in nuclear plants, because:

- many of these devices do not duplicate the precise functionality of the obsolete device to be replaced, having in some cases less and in other cases more functionality, or even subtly different functionality that may be inconsistent with the original design intent,
- these differences in functionality are not always readily apparent. Examples exist of problems that have occurred because of the lack of guidance in this area, and are generally caused by the difference in design goals between nuclear plants and industrial applications for which equipment is designed, and
- they may have specific vulnerabilities or failure modes that did not exist with the original equipment and that need to be considered.

1.3 Use of this standard

This standard provides requirements for determining whether digital devices of industrial quality, that are of dedicated, limited and specific functionality and limited configurability, are suitable for use in a nuclear application. This will require the application of criteria similar to those applied to non-digital devices, but this standard provides additional criteria that apply to digital devices. It will also take into account the limits of feasibility given that limited or no change will be made to the evaluated industrial device.

This standard is intended for use in the context of a defined application for which the application designers seek suitable devices for its implementation. Very often, however, the application designer is forced to consider using devices not designed specifically for nuclear application. The objective of this standard is to help the application designer to select and use such devices in a way that is consistent with the safety class and requirements of the intended application.

Thus, this standard may be applied at different stages of the life cycle of system design as defined in IEC 61513. It may be applied early in the plant design life cycle, where the architecture of the specific I&C system is being drafted, and the availability of suitable devices may influence the system design. If applied somewhat later when the system design has been finalized, this standard can be used to assess candidate devices. Finally, this standard may also be applied to retrofit situations where a system is already in operation and some devices have to be replaced.

Classes 1, 2 and 3 are characterised by graded sets of requirements. This standard is intended to be interpreted in the context of the category of safety function being performed and the class of the system. This means that a graded interpretation of the requirements is appropriate and expected. It is also recognized that the tolerable modes of failure may be quite different in each plant application context, and this may determine the acceptability of a given device or its form of use. The interpretation and rigor in application of the requirements of this standard is assumed to be appropriately considered in each case.

Another issue frequently encountered is supplier resistance to providing evidence of correctness, such as details about the internal functions of the device, or how it was developed. This issue should be addressed as early as possible, possibly through pre-qualification of suppliers, and may require the selection of other vendors in order to comply with this standard.

The Evaluation and Application Plan (EAP)[3] sets the objectives of the evaluation and provides a guide to interpreting this standard for the specific device and application. This Plan identifies and justifies the approaches that will be used in problematic cases, including the kind of compensatory measures which will be taken to address issues such as discrepancies between required and available functionality or the lack of traditional evidence of correctness.

The final step in the evaluation process is the preparation of the Evaluation and Application Report (EAR). This Report identifies the device being qualified, the application(s) for which it is qualified and all the constraints that apply to its use.

1.4 Framework

This standard is organized as follows:

- Clause 5 addresses the applicability of this standard, and the evaluation process, defining:
  - the variation of device functionality which is covered by this standard, and
  - the degree of flexibility and configurability of the device which is covered by this standard, as well as
  - the inputs and outputs of the evaluation process and the EAP which will document how the evaluator(s) will apply the clauses of this standard,
  - the contents of the EAR document, the evidence reviewed and the results of the analysis of this evidence, and the conclusions reached as to the suitability of the device.
- Clause 6 addresses the elements of functionality and other requirements that shall be evaluated, such as
  - the minimal level of development documentation of the candidate device,
  - the ability of the candidate device to perform the required function(s),
  - the immunity of the candidate device's primary function to unwanted influences from superfluous functions,
  - the ability of the candidate device to function under all expected environmental conditions, following IEC 60780 and other identified standards,
  - the reliability and maintainability of the candidate device,
  - the adequacy of cyber security measures, and
  - the user documentation provided.
- Clause 7 addresses the criteria for providing confidence in the correctness of the design and manufacture of the device, identifying:
  - the usefulness of previous non-nuclear certifications,
  - methods to avoid systematic faults,
  - the application of a safety life cycle during the design of the device,
  - manufacturing quality assurance, and
  - permitted means to compensate for some weaknesses in the evidence of some of these concerns, by completing the case in favour of accepting a candidate device on

[3] The requirement for a Qualification Plan defined in IEC 61513 is met by the Evaluation and Application Plan.

the basis of product stability, focussed operating experience, improvements in the documentation or complementary testing and/or analysis.

- Clause 8 addresses criteria for the integration of the device into a plant I&C system, including:
  - restrictions on how the device may be used (such as the highest class of application for which it is qualified),
  - modifications that may be necessary to either the device or the target system in order to integrate the device into the target system, and
  - the integration and commissioning of the device in the plant safety systems.
- Clause 9 addresses considerations for preserving the acceptability of the device, such as:
  - notifications by the device designer or manufacturer to users of the device,
  - the support lifetime of the device,
  - preservation of maintenance tools and documentation, and
  - recommendations for the end-user.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60671:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer based systems performing category A functions*

IEC 60980, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 60987:2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer based systems*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

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

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

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

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

ISO 9001:2008, *Quality management systems – Requirements*

3 Terms and definitions

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

3.1
ancillary function
any function provided by the candidate device that supports its primary function

Note 1 to entry: Examples are functions of the candidate device used to support the function important to safety, such as providing an appropriate means to monitor its operating parameters or its continued correct operation as required for the safety application.

Note 2 to entry: See also “Primary function” and “Superfluous function”.

3.2
auditable
property of documented evidence that is readily available for review by independent personnel

3.3
category of an I&C function
one of three possible safety assignments (A, B, C) of I&C functions resulting from considerations of the safety relevance of the function to be performed. An unclassified assignment may be made if the function has no importance to safety

Note 1 to entry: See also “class of an I&C system”, “I&C function”.

Note 2 to entry: IEC 61226 defines categories of I&C functions. To each category corresponds a set of requirements applicable on both the I&C function (concerning its specification, design, implementation, verification and validation) and the whole chain of items which are necessary to implement the function (concerning the properties and the related qualification) regardless how these items are distributed in a number of interconnected I&C systems. For more clarity, this standard defines categories of I&C functions and classes of I&C systems and establishes a relation between the category of the function and the minimal required class for the associated systems and equipment.

[SOURCE: IEC 61513:2011, 3.4]

3.4
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 different safety relevance. An unclassified assignment is made if the I&C system does not implement functions important to safety

Note 1 to entry: See also “category of an I&C function”, “items important to safety”.

[SOURCE: IEC 61513:2011, 3.6]

3.5
Common Cause Failure
CCF
failure of two or more structures, systems or components due to a single event or cause

[SOURCE: IEC 61513:2011, 3.8]

3.6
computer-based system
I&C system whose functions are mostly dependent on, or completely performed by microprocessors, programmed electronic equipment or computers

Note 1 to entry: Equivalent to: software-based system, programmed system.

[SOURCE: IEC 61513:2011, 3.11]