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

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*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – SÉLECTION ET UTILISATION DES APPAREILS NUMÉRIQUES À FONCTIONNALITÉS LIMITÉES

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI 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 la CEI. La CEI 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de brevet. La CEI 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 CEI 62671 a été établie par le sous-comité 45A: Instrumentation et contrôle-commande des installations nucléaires, du comité d'études 45 de la CEI: Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/898/FDIS	45A/907/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.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

Le contenu du corrigendum de septembre 2016 a été pris en considération dans cet exemplaire.

INTRODUCTION

a) Contexte technique, questions importantes et structure de la présente norme

La présente norme CEI s'intéresse plus particulièrement à la sélection et à l'évaluation des appareils dédiés prédéveloppés, présentant des fonctionnalités particulières et limitées ainsi que des possibilités de configuration limitées, devant être utilisés dans des centrales nucléaires de puissance. La conception de ces appareils intègre du logiciel ou des circuits numériques spécifiés à l'aide de langage de description du matériel. Lesdits appareils ont été produits en respectant des normes non nucléaires reconnues, mais pas des normes de la série du SC 45A de la CEI.

L'objectif de la présente norme est d'être utilisée par les concepteurs de centrales nucléaires, les exploitants de centrales nucléaires, les évaluateurs de système et par les régulateurs.

La présente norme s'intéresse à deux aspects qui ne sont pas couverts par les autres normes de la série du SC 45A de la CEI, en effet:

– d'autres de ces normes couvrent les aspects liés au matériel des appareils contenant du logiciel ou couvrent des appareils de type complexe tels que les PLCs qui contiennent du logiciel qui peut être beaucoup plus complexe[1] que celui contenu dans les appareils couverts par la présente norme,

– d'autres de ces normes s'intéressent aux appareils conçus spécifiquement pour les applications nucléaires alors que l'objectif de la présente norme est de s'intéresser aux points qu'il est nécessaire de considérer pour pouvoir utiliser dans des centrales nucléaires de puissance des appareils qui n'ont pas été conçus pour être utilisés dans ce cadre.

Les concepteurs des systèmes d'I&C des centrales nucléaires de puissance sont de plus en plus forcés d'avoir recours à ce type d'appareil pour des raisons liées par exemple à l'obsolescence des équipements, à la petite taille du marché nucléaire comparé à d'autres marchés industriels, et aussi à cause du nombre grandissant de fournisseurs qui choisissent de concevoir leurs produits en faisant référence à des normes génériques de sûreté telles que celles de la séries CEI 61508.

Ainsi, il devient vital pour les concepteurs de ces systèmes d'avoir les recommandations établies par la présente norme, afin d'être capable de choisir et d'évaluer les appareils candidats pour juger de leur aptitude à être employés dans les centrales nucléaires de puissance. La présente norme fournit des recommandations sans lesquelles les concepteurs seraient obligés de s'interroger sur la façon d'interpréter les CEI 60880, CEI 62138 ou CEI 62566 pour les sujets couverts.

b) Position de la présente norme dans la collection de normes du SC 45A de la CEI

La CEI 61513 est la norme du SC 45A de la CEI de premier niveau qui fournit des recommandations applicables à l'I&C au niveau système. Elle est complétée par des recommandations applicables au niveau appareil par la CEI 60987 pour la conception du matériel et par les CEI 60880 et CEI 62138 pour le logiciel et par la CEI 62566 pour des appareils potentiellement complexes. Toutes ces normes couvrent des conceptions qui sont spécifiquement nucléaires et appliquent le concept de cycle de vie.

La CEI 62671 est le document du SC 45A de la CEI de deuxième niveau qui traite de la question particulière du choix et de l'évaluation des appareils à utiliser dans les centrales

---

[1] Il n'y a pas de définition reconnue de la « complexité », mais lorsque les appareils sont support de beaucoup de fonctionnalités, il s'en suit une augmentation de la quantité de code, des contraintes sur les ressources du système, des phénomènes liés à la synchronisation qui peuvent entraîner des défaillances non prévues. Cette norme traite de ces problèmes dans le cas des appareils à fonctionnalité très limitée.

nucléaires de puissance lorsque ces appareils ont été conçus pour être utilisés dans des applications non nucléaires (et qu'ils sont potentiellement certifiés conformes à une norme de sûreté générique largement reconnue telle que la CEI 61508). De plus, la norme CEI 62671 couvre seulement les appareils qui présentent des fonctionnalités dédiés, limitées et particulières et une possibilité de configuration limitée.

La CEI 62671 doit être lue avec la CEI 60880 (informative), la CEI 62138 (informative), la CEI 60987 (informative) et la CEI 62566 (informative) qui sont les autres documents pertinents du SC 45A de la CEI qui fournissent des recommandations applicables aux systèmes programmés réalisant des fonctions importantes pour la sûreté et qui sont utilisés dans les centrales nucléaires de puissance.

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

c) Recommandations et limites relatives à l'application de présente norme

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté de classe 1, 2 ou 3.

La présente norme fournit des exigences particulières pour les aspects suivants:

- l'utilisation d'un processus planifié pour choisir, et pour évaluer les appareils candidats à l'utilisation, de même que pour intégrer l'appareil dans les systèmes de tranche,
- les critères d'évaluation de l'aptitude fonctionnelle d'un appareil contenant des logiciels embarqués ou utilisant des circuits numériques conçus à l'aide d'outils logiciels tel que HDL (Langage de description de matériel),
- les critères à considérer lors d'une évaluation d'ensemble pour obtenir un niveau d'assurance suffisant concernant le fait que l'appareil fonctionnera tel que prévu lorsqu'il sera sollicité,
- les considérations relatives à l'emploi sûr de l'appareil retenu dans les systèmes de tranche.

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

Dans la présente norme, l'accent est mis sur la revue des preuves afférentes aux processus mis en place par les concepteurs et les fabricants (qui peuvent être des organisations différentes), sachant que ces deux organisations ont de l'influence sur décision d'accepter ou non l'appareil candidat pour réaliser l'application prévue. Ces preuves peuvent avoir été obtenues par le truchement du fournisseur avec lequel l'utilisateur final est en contact direct.

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

Le document de niveau supérieur de la collection de normes produites par le SC 45A de la CEI est la norme CEI 61513. Cette norme traite des exigences relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires, et structure la collection de normes du SC 45A de la CEI.

La CEI 61513 fait directement référence aux autres normes du SC 45A de la CEI traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, les défaillances de cause commune, les aspects logiciels et les aspects matériels relatifs aux systèmes programmés, et la conception des salles de commande. Il convient de considérer que ces normes, de second niveau, forment, avec la norme CEI 61513, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de la CEI, qui ne sont généralement pas référencées directement par la norme CEI 61513, 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 la CEI correspond aux rapports techniques qui ne sont pas des documents normatifs.

La CEI 61513 a adopté une présentation similaire à celle de la CEI 61508, avec un cycle de vie de sûreté d'ensemble et un cycle de vie de sûreté des systèmes. Au niveau sûreté nucléaire, elle est l'interprétation des exigences générales des parties 1, 2 et 4 de la CEI 61508 pour le secteur nucléaire, pour ce qui concerne le domaine de la sûreté nucléaire. Dans ce domaine, la CEI 60880 et la CEI 62138 correspondent à la CEI 61508-3 pour le secteur nucléaire. La CEI 61513 fait référence aux normes ISO ainsi qu'aux documents AIEA GS-R-3, AIEA GS-G-3.1 et AIEA GS-G-5.1 pour ce qui concerne l'assurance qualité.

Les normes produites par le SC 45A de la CEI sont élaborées de façon à être en accord avec les principes de sûreté fondamentaux du Code AIEA sur la sûreté des centrales nucléaires, ainsi qu'avec les guides de sûreté de l'AIEA, en particulier avec le document d'exigences NS-R-1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires et avec le guide de sûreté NS-G-1.3 qui traite de l'instrumentation et du contrôle commande importants pour la sûreté des centrales nucléaires. La terminologie et les définitions utilisées dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

NOTE 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, dont les exigences sont comparables à des normes telles que la CEI 61508.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – SÉLECTION ET UTILISATION DES APPAREILS NUMÉRIQUES À FONCTIONNALITÉS LIMITÉES

1 Domaine d'application

1.1 Généralités

La présente Norme internationale couvre les appareils qui contiennent des logiciels embarqués ou des circuits numériques configurés électroniquement qui n'ont pas été produits conformément aux normes CEI applicables aux systèmes et équipements importants pour la sûreté des centrales nucléaires de puissance, mais qui sont candidats pour être utilisés dans des centrales nucléaires de puissance. Elle établit des exigences pour le choix et l'évaluation de tels appareils lorsque ceux-ci présentent des fonctionnalités spécifiques, limitées et dédiées[2] et que leur configuration est limitée.

Conformément à la CEI 61513, les systèmes d'I&C importants pour la sûreté de classe 1, 2 ou 3 peuvent être mis en œuvre en utilisant des équipements câblés conventionnels, des équipements numériques (programmables ou intégrant des matériels programmés) ou en utilisant une combinaison des deux types d'équipement. La présente norme fournit des critères d'acceptation pour le choix, l'évaluation et l'utilisation de certains des appareils numériques qui n'ont pas été développés spécifiquement pour être utilisés dans les systèmes d'I&C nucléaires. De tels appareils sont souvent conformes à la CEI 61508 ce qui peut être un facteur clé positif lorsqu'on qualifie des équipements non conçus pour le nucléaire pour les employer dans le secteur nucléaire.

Les appareils couverts par la présente norme sont des appareils dédiés présentant des fonctionnalités limitées particulières, qui intègrent ou peuvent intégrer des composants pilotés par logiciel ou des circuits numériques conçus en utilisant des outils logiciel. Des exemples sont: les capteurs intelligents, les positionneurs de vanne, les appareils de protection électriques ou les onduleurs qui peuvent contenir des composants pilotés par logiciel ou des circuits numériques conçus en utilisant des outils logiciels. La présente norme ne couvre pas les aspects relatifs au logiciel des appareils "tous usages" complexes qui sont couverts par d'autres normes, telles que la CEI 60880 et la CEI 62138 pour le logiciel. La présente norme traite des questions qu'il convient de prendre en compte lorsqu'on fait l'évaluation de l'aptitude de ces appareils dédiés à fonctionnalités spécifiques limitées pour être utiliser dans des centrales nucléaires de puissance. L'objectif de la présente norme est de proposer une approche graduelle de ces questions, avec l'application d'exigences plus contraignantes pour les classes de sûreté les plus élevées.

Ces questions comprennent:

- L'aptitude fonctionnelle (Est-ce qu'un appareil réalise les fonctions prévues ? Ces fonctions sont-elles protégées de façon suffisamment sûre des interactions avec les autres fonctions ?),
- Les preuves exigées pour démontrer cette aptitude (telles que le processus de développement suivi, le retour d'expérience collecté sur le terrain et le niveau de maturité atteint par l'appareil),

---

2 « Dédiés » dans le sens utilisé dans la présente norme fait référence à une conception pour une fonction particulière qui ne peut pas être modifiée sur le terrain, voir 3.7.

- Les aspects ayant un impact sur l'intégration de l'appareil dans des systèmes existants (par exemple compatibilité fonctionnelle et impacts sur la maintenance et l'exploitation), et
- Les exigences relatives à l'assurance que l'aptitude de l'appareil sera maintenue dans le temps et ceci pour sa durée de vie requise (telle que la durée de vie de la centrale).

La présente norme s'appuie sur d'autres normes, plus particulièrement la CEI 60780, pour traiter des questions de qualification du matériel, sans lien avec la complexité du logiciel, à savoir les aspects de fiabilité liés à la qualification environnementale, aux défaillances dues au vieillissement ou à des dommages physiques. D'autres normes telles que la CEI 61508 peuvent être utilisées comme recommandations complémentaires pour l'évaluation et l'appréciation de la qualité des équipements, mais il est reconnu que la seule certification par rapport à des normes non nucléaires est insuffisante.

1.2 Contexte

Le besoin à l'origine du développement de la présente norme est né d'une tendance apparue dans le secteur industriel fournisseur des systèmes d'I&C; ce besoin est en particulier lié au problème grandissant de l'obsolescence des appareils existants qui sont couramment utilisés dans les centrales nucléaires. En effet, il devient de plus en plus difficile, sinon impossible, de trouver des systèmes analogiques ou de remplacer la plupart des appareils existants à l'identique car les fournisseurs emploient de plus en plus de microcontrôleurs, d'ASICs, etc., embarqués dans les appareils proposés en remplacement, et les appareils analogiques sont de moins en moins disponibles sur le marché.

Il existe différents risques techniques potentiels lorsqu'on choisit d'utiliser ces appareils dans des centrales nucléaires, car:

- beaucoup de ces appareils ne reproduisent pas la fonctionnalité exacte que réalisait l'appareil obsolète à remplacer, pêchant ainsi dans certains cas par défaut et dans d'autres par excès, ou même présentant des fonctionnalités qui peuvent être légèrement incompatibles avec les objectifs de conception originaux;
- ces différences de fonctionnalités ne sont pas toujours immédiatement apparentes. Des exemples existent de problèmes qui sont apparus du fait du manque de recommandations dans le domaine. Ces problèmes trouvent généralement leur origine dans les différences existant entre les objectifs de conception de la centrale nucléaire et ceux des applications industrielles pour lesquelles l'appareil est conçu;
- les appareils peuvent présenter des faiblesses ou des modes de défaillances qui n'existaient pas dans l'équipement d'origine et qui doivent être prise en compte.

1.3 Utilisation de la présente norme

La présente norme établit des exigences permettant de déterminer si un appareil numérique de qualité industrielle, qui présente des fonctionnalités limitées dédiées et particulières ainsi que des possibilités de configuration limitées, est apte à être utilisé dans le cadre d'une application nucléaire. Ceci nécessitera l'application de critères similaires à ceux utilisés pour les appareils non numériques, mais la présente norme fournit en plus des critères applicables aux systèmes numériques. Elle tiendra aussi compte les limites associées à la faisabilité, étant donné que l'appareil industriel qualifié ne peut pas être modifié ou seulement de façon limitée.

La présente norme est conçue pour pouvoir être utilisée dans le cadre d'une application définie pour laquelle le concepteur recherche des appareils aptes à servir pour sa mise en œuvre. Très souvent, néanmoins, le concepteur de l'application est forcé de considérer l'emploi d'appareils qui n'ont pas été conçus spécifiquement pour le domaine nucléaire. L'objectif de la présente norme est d'aider le concepteur d'application à choisir et à utiliser de tels appareils conformément au classement de sûreté et aux exigences de l'application considérée.

Ainsi la présente norme peut être appliquée à différents niveaux du cycle de vie de la conception du système tel que défini dans la CEI 61513. Elle peut être appliquée tôt dans le cycle de vie de conception de la centrale, lorsque l'architecture du système d'I&C en question est élaborée, et la disponibilité d'appareils adaptés peut avoir une influence sur sa conception. En cas d'application ultérieure lorsque la conception du système est terminée, la présente norme peut être utilisée pour évaluer les appareils candidats. Finalement, la présente norme peut aussi être appliquée pour des opérations de rénovation lorsque le système est déjà en exploitation et que certains appareils sont à remplacer.

Les classes de sûreté 1, 2 et 3 sont caractérisées par des ensembles d'exigences gradués. L'objectif de la présente norme est d'être interprétée dans le cadre de la catégorie d'une fonction de sûreté à réaliser et du classement du système. Ceci veut dire qu'une interprétation graduée des exigences est appropriée et attendue. Il est aussi reconnu que les modes de défaillance tolérables peuvent être notablement différents suivant les applications de tranche considérées, et que ceci peut déterminer l'acceptabilité d'un appareil ou de sa forme d'utilisation. L'interprétation et la rigueur dans l'application des exigences de la présente norme sont supposées être prises en compte de façon adaptée dans chacun des cas.

Un autre problème fréquemment rencontré est la résistance des fournisseurs à fournir des preuves concernant les caractéristiques précises et exactes de l'appareil, telles que les détails concernant les fonctions internes de l'appareil, ou la façon dont il a été développé. Il convient de traiter cette question dès que possible, si possible lors de la pré-qualification des fournisseurs, et celle-ci pouvant nécessiter le choix d'autres fournisseurs afin de satisfaire à la présente norme.

Le Plan d'Evaluation et d'Application (PEA)[3] définit les objectifs et est un guide d'interprétation de la présente norme pour un appareil particulier et une application particulière. Ce plan identifie et justifie les approches qui seront utilisées en cas de problèmes, y compris les types des mesures compensatoires qui seront mises en œuvre afin de corriger les problèmes rencontrés tels que les différences entre les fonctionnalités demandées et celles disponibles, ou encore le manque de preuves, concernant les caractéristiques précises et exactes de l'appareil habituellement demandées.

L'étape finale du processus d'évaluation est la préparation du Rapport d'Evaluation et d'Application (REA). Ce compte rendu identifie l'appareil qui a été qualifié, l'application pour laquelle il l'a été et toutes les contraintes s'appliquant à son utilisation.

1.4 Structure

La présente norme est organisée comme suit:

- L'Article 5 traite de l'applicabilité de la présente norme, et du processus d'évaluation en considérant:
  - les écarts au niveau des fonctionnalités de l'appareil couvert par la présente norme,
  - le degré de flexibilité et de configurabilité de l'appareil couvert par la présente norme,
  - les entrées et les sorties du processus d'évaluation et le PEA qui documente comment les évaluateurs appliqueront les exigences de présente norme,
  - le contenu du document REA, les preuves qui ont fait l'objet de revue, et les résultats d'analyse de ces preuves, les conclusions tirées sur l'adéquation des aptitudes de l'appareil.
- L'Article 6 traite des éléments relatifs aux fonctionnalités et autres exigences qui doivent être évalués, tels que

---

[3] L'exigence de la CEI 61513 concernant l'existence d'un Plan de Qualification est satisfaite par l'existence du Plan d'Evaluation et d'Application.

  - le niveau minimum de documentation de développement de l'appareil candidat,
  - l'aptitude de l'appareil candidat à réaliser la ou les fonctions attendues,
  - l'immunité de la fonction principale de l'appareil candidat vis-à-vis des influences non souhaitées des fonctions superflues,
  - l'aptitude de l'appareil candidat à fonctionner en présence de toutes les conditions environnementales prévues, conformément à la CEI 60780 ou aux autres normes identifiées,
  - la fiabilité et l'aptitude de l'appareil candidat à la maintenance,
  - la pertinence des mesures relatives à la cybersécurité mises en place, et
  - la documentation utilisateur fournie.
- L'Article 7 traite des critères permettant d'établir la confiance en ce qui concerne les caractéristiques relevant de la précision et de l'exactitude de la conception et de la fabrication de l'appareil, en considérant:
  - l'utilité des certifications précédemment acquises pour des applications non nucléaires,
  - les méthodes d'évitement des défauts systématiques,
  - l'application d'un cycle de vie de sûreté pour la conception de l'appareil, et
  - l'assurance qualité associée à la fabrication, et
  - les moyens autorisés pour afin de compenser l'éventuelle faiblesse des preuves apportées pour couvrir points ci-dessus, en complétant le dossier d'acceptation de l'appareil candidat sur sa base de la stabilité, de son expérience en exploitation, en améliorant sa documentation ou en réalisant des essais ou des analyses complémentaires.
- L'Article 8 traite des critères relatifs à l'intégration de l'appareil dans les systèmes d'I&C de la centrale, en considérant:
  - les restrictions concernant la façon d'utiliser l'appareil (telles que le classement maximum de sûreté de l'application pour laquelle l'appareil est qualifié),
  - les modifications qu'il peut être nécessaire de réaliser ou sur l'appareil ou sur le système cible pour pouvoir intégrer l'appareil dans le système cible, et
  - l'intégration et la recette de l'appareil au niveau des systèmes de sûreté de la centrale.
- Le paragraphe 9 traite de considérations visant à maintenir le caractère acceptable de l'appareil, telles que:
  - les notifications faites à l'utilisateur par le concepteur de l'appareil ou par le fabricant,
  - le support technique offert pour l'appareil pour sa durée de vie,
  - la préservation des outils et de la documentation de maintenance, et
  - les recommandations destinées à l'utilisateur final.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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).

CEI 60671:2007, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

CEI 60780, *Centrales nucléaires – Equipements électriques de sûreté – Qualification*

CEI 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*

CEI 60980, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 60987:2007, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté*

CEI 61000 (toutes les parties), *Compatibilité électromagnétique (CEM)*

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

CEI 61508-7:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

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

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

ISO 9001:2008, *Systèmes d'assurance qualité - Exigences*