IEC 62566-2

Edition 1.0 2020-05

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL – Partie 2: Circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie B ou C

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-8032-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – DEVELOPMENT OF HDL-PROGRAMMED INTEGRATED CIRCUITS –

Part 2: HDL-programmed integrated circuits for 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 62566-2 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1304/FDIS	45A/1314/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.

A list of all parts in the IEC 62566 series, published under the general title *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits*, can be found on the IEC website.

In this document, the following print types are used:

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

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 the Standard

Electronic systems performing category B and C functions (according to IEC 61226) used in Nuclear Power Plants (NPPs) need to be fully validated and qualified according to their safety class. This International Standard provides requirements for the development of class 2 or 3 HDL (Hardware Description Language) Programmed Devices (HPDs) performing category B or C functions as defined by IEC 61226. It complements IEC 62566 which provides requirements for the development of HPDs performing category A functions.

In computer-based systems, a separation can be drawn between the hardware and software portions. The hardware is mainly designed with standardised components having pre-defined electronic functions such as microprocessors, timers or network controllers, whereas software is used to coordinate the different parts of the hardware and to implement the application functions.

I&C designers might build application functions using integrated circuits such as FPGAs or similar technologies. The function of such an integrated circuit is not defined by the supplier of the physical component or micro-electronic technology but by the I&C designer.

The specific integrated circuits addressed by this Standard are:

a) based on pre-developed micro-electronic technologies,

b) developed within an I&C project,

c) developed in Hardware Description Languages (HDL) by using appropriate and compatible development tools.

Therefore these circuits are named “HDL-Programmed Devices”, (HPD). The HDL statements which describe a HPD can include the instantiation of Pre-Developed Blocks (PDB) which are typically provided as libraries, macros, or intellectual property cores.

HPDs can be effective solutions to implement functions required by an I&C project. However, the verification and validation might be limited by issues such as high number of internal paths and limited observability, if the HPD has not been developed with verifiability in mind.

In order to achieve the reliability required for safety I&C systems, the development of HPDs shall comply with strict process and technical requirements such as those provided by this Standard, including the specification of requirements, the selection of blank integrated circuits and PDBs, the design and implementation, the verification, and the procedures for operation and maintenance.

It is intended that this Standard be used by HPD designers, operators of NPPs (utilities), and by regulators. Regulatory bodies will find guidance to assess important aspects such as design, implementation, verification and validation of HPDs.

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 hardware level (IEC 60987), software level (IEC 60880 and IEC 62138) and HPD level (IEC 62566 and IEC 62566-2). IEC 62340 gives requirements in order to reduce and overcome the possibility of common cause failure of category A functions.

IEC 62566-2 is a second level IEC SC 45A document which focuses on the activities when HPDs performing category B or C functions are developed. For HPDs performing category B functions, it complements IEC 60987 which deals with the generic issues of hardware design of computer-based systems.

c) Recommendations and limitations regarding the application of the Standard

It is important to note that this Standard establishes no additional functional requirements for safety systems.

Aspects for which special requirements and recommendations have been produced are:

a) an approach to specify the requirements of, to design, to implement and to verify “HDL-Programmed Devices” (HPD, 3.20), and to handle the corresponding aspects of system integration and validation;

b) an approach to analyse and select the blank integrated circuits, micro-electronic technologies and Pre-Developed Blocks (PDB, 3.29) used to develop HPDs;

c) procedures for the modification and configuration control of HPDs;

d) requirements for selection and use of software tools used to develop HPDs.

It is recognized that digital technology is continuing to develop at a rapid pace and that it is not possible for a Standard such as this one to include references to all modern design technologies and techniques.

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. If new techniques are developed then it should be possible to assess the suitability of such techniques by applying the safety principles contained within this Standard.

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 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 45 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 part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). 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, IEC 60964 is the entry document for the IEC/SC 45A control rooms standards and IEC 62342 is the entry document for the 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 of IEC/SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – DEVELOPMENT OF HDL-PROGRAMMED INTEGRATED CIRCUITS –

Part 2: HDL-programmed integrated circuits for systems performing category B or C functions

1 Scope

This part of IEC 62566 provides requirements for achieving highly reliable HDL-Programmed Devices (HPDs), for use in I&C systems of nuclear power plants performing functions of safety category B or C as defined by IEC 61226.

The programming of HPDs relies on Hardware Description Languages (HDL) and related software tools. They are typically based on blank Field Programmable Gate Arrays (FPGAs) or similar micro-electronic technologies such as Programmable Logic Devices (PLD), Complex Programmable Logic Devices (CPLDs), etc. General purpose integrated circuits such as microprocessors are not HPDs. Annex B.8 provides descriptions of a number of different types of integrated circuits.

This document provides requirements on:

a) a dedicated HPD life-cycle addressing each phase of the development of HPDs, including specification of requirements, design, implementation, integration and validation, as well as verification activities associated with each phase,

b) planning and complementary activities such as modification and production,

c) selection of pre-developed components. This includes micro-electronic technologies and Pre-Developed Blocks (PDBs),

d) tools used to design, implement and verify HPDs.

This document does not put requirements on the development of the micro-electronic technologies, which are usually available as "commercial off-the-shelf" items and are not developed under nuclear quality assurance standards. It addresses the developments made with these micro-electronic technologies in an I&C project with HDLs and related tools.

This document provides guidance to avoid as far as possible latent faults remaining in HPDs, and to reduce the susceptibility to single failures as well as to potential Common Cause Failures (CCFs).

Reliability aspects related to environmental qualification and failures due to ageing or physical degradation are not handled in this document. Other standards, especially IEC 60987, IEC/IEEE 60780-323 and IEC 62342, address these topics.

This document does not cover cybersecurity for HDL aspects of I&C systems. IEC 62645 provides requirements for security programmes for I&C programmable digital systems.

This document provides guidance and requirements to produce verifiable HPD designs and implementations requiring justification due for their role in carrying out category B or C safety functions. This document describes the activities to develop HPDs, organized in the framework of a dedicated life-cycle. It also describes activities and guidelines to be used in addition to the requirements of IEC 61226 for system classification and IEC 61513 for system integration and validation when HPDs are included.

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

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

IEC 62340, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – DÉVELOPPEMENT DES CIRCUITS INTÉGRÉS PROGRAMMÉS EN HDL –

Partie 2: Circuits intégrés programmés en HDL pour les systèmes 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 62566-2 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.

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

FDIS	Rapport de vote
45A/1304/FDIS	45A/1314/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.

Une liste de toutes les parties de la série IEC 62566, publiées sous le titre général *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL*, peut être consultée sur le site web de l'IEC.

Dans le présent document, les types de caractères d'imprimerie suivant sont employés:

– *Les exigences et les recommandations qui sont spécifiquement applicables aux systèmes de classes 2 et 3 apparaissent en italiques*

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 de la norme

Il est nécessaire que les systèmes électroniques réalisant des fonctions de catégories B et C (au sens de l'IEC 61226) utilisés dans les centrales nucléaires de puissance soient entièrement validés et qualifiés selon leur classe de sûreté. La présente Norme internationale énonce les exigences applicables au développement de circuits (HPD) de classe 2 ou 3 programmés en HDL ("Hardware Description Language", langage de description de matériel), assurant des fonctions de catégorie B ou C comme défini par l'IEC 61226. Elle complète l'IEC 62566 qui énonce les exigences applicables au développement de HPD assurant des fonctions de catégorie A.

Dans les systèmes programmés, il peut y avoir une distinction entre le matériel et le logiciel. Le matériel est principalement conçu avec des composants normalisés remplissant des fonctions électroniques prédéfinies tels que des microprocesseurs, des temporisateurs ou encore des contrôleurs de réseau, alors que le logiciel est utilisé pour coordonner les différentes parties du matériel et pour réaliser les fonctions de l'application nucléaire.

Les concepteurs d'instrumentation et de contrôle-commande (I&C) ont la possibilité de bâtir des fonctions d'application en utilisant des circuits tels que les FPGA ou des technologies similaires. La fonction d'un tel circuit intégré n'est pas définie par le fournisseur du composant physique ou de la technologie microélectronique, mais par le concepteur d'instrumentation et de contrôle-commande.

Les circuits intégrés traités dans la présente norme sont:

a) basés sur des technologies microélectroniques prédéveloppées;

b) développés au sein d'un projet d'I&C;

c) développés au moyen de langages de description de matériel (HDL), en faisant appel à des outils de développement adaptés et compatibles.

Par conséquent, ces circuits sont nommés "circuits intégrés programmés en HDL" (HPD). Les instructions HDL qui décrivent un HPD peuvent inclure l'instanciation de blocs prédéveloppés (PDB) qui sont typiquement fournis sous la forme de bibliothèques, de macros, ou de blocs de propriété intellectuelle.

Les HPD peuvent constituer des solutions efficaces pour réaliser les fonctions exigées par un projet d'I&C. Cependant, il se peut que la vérification et la validation soient limitées en raison du grand nombre de chemins internes et de leur observabilité limitée, si le HPD n'a pas été conçu en pensant à sa vérifiabilité.

Afin d'atteindre la fiabilité élevée exigée pour les systèmes d'I&C importants pour la sûreté, le développement des HPD doit respecter des exigences de procédé et des exigences techniques strictes, telles que celles indiquées dans la présente norme, concernant notamment la spécification des exigences, le choix des circuits intégrés vierges et des PDB, la conception et la réalisation, la vérification, et les procédures de fonctionnement et de maintenance.

La présente norme est destinée aux concepteurs de HPD, aux opérateurs de centrales nucléaires de puissance (producteurs d'électricité) et aux autorités de sûreté. Les organismes réglementaires y trouveront des recommandations pour évaluer des aspects importants comme la conception, la réalisation, la vérification et la validation des HPD.

b) Position de la présente norme dans la série de normes du SC 45A de l'IEC

L'IEC 61513 est le document de premier niveau du SC 45A de l'IEC qui fournit les recommandations applicables à l'I&C au niveau système. Elle est complétée par des recommandations au niveau matériel (IEC 60987), au niveau logiciel (IEC 60880 et IEC 62138) et au niveau HPD (IEC 62566 et IEC 62566-2). L'IEC 62340 fournit des exigences visant à réduire et surmonter la possibilité d'une défaillance de cause commune de fonctions de catégorie A.

L'IEC 62566-2 est un document de deuxième niveau de la série de normes du SC 45A de l'IEC qui concerne les activités de développement des HPD assurant des fonctions de catégorie B ou C. Pour les HPD assurant des fonctions de catégorie B, elle complète l'IEC 60987 qui aborde les problèmes génériques de la conception du matériel des systèmes informatisés.

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

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

Des exigences et recommandations spéciales ont été produites pour les aspects suivants:

a) approche de spécification des exigences, de conception, de réalisation, de vérification des circuits intégrés programmés en HDL (HPD, voir 3.20), ainsi que des aspects de l'intégration et de la validation du système liés aux HPD;
b) approche d'analyse et de choix des circuits intégrés vierges, technologies microélectroniques et blocs prédéveloppés (PDB, voir 3.29) utilisés pour développer les HPD;
c) procédures de modification et de contrôle de configuration des HPD;
d) exigences relatives au choix et à l'utilisation des outils logiciels utilisés pour développer les HPD.

Il est reconnu que les techniques numériques se développent à un rythme soutenu, et qu'il n'est pas possible pour une norme de faire référence à toutes les techniques nouvelles de conception.

Pour garantir la pertinence de la présente norme dans les années futures, l'accent a été mis sur les principes plutôt que sur des technologies spécifiques. Si de nouvelles techniques apparaissent, il devrait être possible d'évaluer leur adéquation en appliquant les principes de sûreté contenus dans la présente norme.

d) Description de la structure de la série de 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 série de normes du SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. La norme 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. La norme IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique; elle couvre les systèmes d'alimentation électrique, y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être prises en compte ensemble et au même niveau. Les normes IEC 61513 et IEC 63046 structurent la série de normes du SC 45A de l'IEC et forment un cadre complet 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, la 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 tenir compte 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 pas référencées directement par les normes IEC 61513 ou IEC 63046, se rapportent à des équipements, des méthodes techniques ou 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 série de normes du SC 45A de l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

Les normes produites 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 série de l'AIEA pour la sécurité nucléaire (NSS). Cela inclut en particulier le document d'exigences SSR-2/1 de l'AIEA qui établit les exigences de sûreté relatives à la conception des centrales nucléaires de puissance, le Guide de sûreté SSG-30 de l'AIEA qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires de puissance, le Guide de sûreté SSG-39 de l'AIEA qui aborde la conception des systèmes d'instrumentation et de contrôle-commande des centrales nucléaires de puissance, le Guide de sûreté SSG-34 de l'AIEA qui concerne la conception des systèmes d'alimentation électrique des centrales nucléaires de puissance et le Guide d'implémentation NSS17 qui porte sur la sécurité informatique des 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 6150-1, 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 partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité. Au second niveau, la norme IEC 62645 est le document chapeau du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée à partir des principes pertinents de haut niveau des normes ISO/IEC 27001 et ISO/IEC 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée étroitement avec la norme IEC 62443. Au second niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et la norme IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est admis par 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), des normes nationales ou internationales s'appliquent.

NOTE 2 Le domaine de l'IEC/SC 45A a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015, des discussions se sont tenues au sein de l'IEC/SC 45A afin de décider de quelle manière et à quel niveau devaient être abordées les exigences générales relatives à la conception des systèmes électriques. Les experts du SC 45A de l'IEC ont recommandé d'élaborer au même niveau que l'IEC 61513 une norme indépendante visant à établir les exigences générales relatives aux systèmes électriques. Le projet IEC 63046 est lancé pour atteindre cet objectif. Lorsque la norme IEC 63046 sera publiée, la présente NOTE 2 de l'introduction sera supprimée.

CENTRALES NUCLÉAIRES DE PUISSANCE – INSTRUMENTATION ET CONTRÔLE-COMMANDE IMPORTANTS POUR LA SÛRETÉ – DÉVELOPPEMENT DES CIRCUITS INTÉGRÉS PROGRAMMÉS EN HDL –

Partie 2: Circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie B ou C

1 Domaine d'application

La présente partie de l'IEC 62566 énonce des exigences pour atteindre une haute fiabilité dans les "circuits intégrés programmés en HDL" (HPD) destinés aux systèmes d'I&C des centrales nucléaires de puissance réalisant des fonctions de sûreté de catégorie B ou C telles que définies par l'IEC 61226.

La programmation des HPD repose sur des langages de description de matériel (HDL) et des outils logiciels associés. Les HPD sont typiquement basés sur des réseaux de portes programmables sur site (FPGA) vierges ou sur des technologies microélectroniques similaires telles que les réseaux logiques programmables (PLD), les réseaux logiques programmables complexes (CPLD), etc. Les circuits intégrés d'usage général tels que les microprocesseurs ne sont pas des HPD. Des descriptions correspondant à différents types de circuits intégrés sont fournis en B.8.

Le présent document énonce des exigences sur:

a) un cycle de vie de HPD dédié concernant chaque phase du développement des HPD, notamment la spécification des exigences, la conception, la réalisation, l'intégration et la validation, ainsi que les activités de vérification associées à chacune des phases;

b) la planification et les activités complémentaires telles que la modification et la production;

c) le choix des composants prédéveloppés, notamment les technologies microélectroniques et les blocs prédéveloppés (PDB);

d) les outils utilisés pour concevoir, réaliser et vérifier les HPD.

Le présent document n'impose pas d'exigence sur le développement des technologies microélectroniques, qui sont généralement disponibles dans le commerce sous forme d'éléments "sur étagère", et ne sont pas développées selon des normes d'assurance qualité nucléaire. Il concerne les développements effectués à partir de ces technologies microélectroniques dans un projet d'I&C, avec des HDL et des outils associés.

Le présent document fournit des recommandations visant à éviter autant que possible les défauts latents résiduels dans les HPD, et à réduire la susceptibilité aux défaillances uniques et aux défaillances de cause commune (DCC) potentielles.

Les aspects de la fiabilité liés à la qualification environnementale et aux défaillances dues au vieillissement ou à la dégradation physique ne sont pas abordés dans le présent document. D'autres normes traitent de ces aspects, en particulier l'IEC 60987, l'IEC/IEEE 60780-323 et l'IEC 62342.

Le présent document ne couvre pas la cybersécurité pour les aspects HDL des systèmes d'I&C. L'IEC 62645 énonce des exigences portant sur les programmes de sécurité applicables aux systèmes numériques programmables d'I&C.

Le présent document fournit des recommandations et des exigences visant à produire des conceptions de HPD vérifiables et des mises en œuvre nécessitant les justifications liées à leur rôle dans la réalisation des fonctions de sûreté de catégorie B ou C. Le présent document décrit les activités visant à développer les HPD, organisées en un cycle de vie dédié. Il décrit également les activités et les lignes directrices à suivre en complément des exigences de l'IEC 61226 pour le classement des systèmes et de l'IEC 61513 pour l'intégration et la validation des systèmes lorsqu'ils incluent des HPD.

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 60987, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

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

IEC 62340, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Exigences permettant de faire face aux défaillances de cause commune (DCC)*

IEC 62566:2012, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Développement des circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie A*