IEC 62566

Edition 1.0 2012-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XA

ICS 27.120.20

ISBN 978-2-88912-896-9

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope and object 10
1.1 General 10
1.2 Use of this Standard 10
2 Normative references 11
3 Terms and definitions 11
4 Symbols and abbreviations 13
5 General requirements for HPD projects 14
5.1 General 14
5.2 Life-cycle 14
5.3 HPD project management 17
5.3.1 General 17
5.3.2 Additional requirements 17
5.4 HPD quality assurance plan 17
5.5 Configuration management 17
6 HPD requirements specification 18
6.1 General 18
6.2 Functional aspects of the requirement specification 18
6.3 Deterministic design 19
6.4 Fault detection and fault tolerance 19
6.5 Requirements capture using Electronic System Level tools 20
6.5.1 General 20
6.5.2 Requirements on the formalism of tools used at ESL level 20
6.5.3 Interface with design tools 20
6.6 Requirements analysis and review 20
7 Acceptance process for programmable integrated circuits, native blocks and pre-developed blocks 21
7.1 General 21
7.2 Component requirement specification 21
7.2.1 General 21
7.2.2 Requirements 21
7.2.3 Requirements analysis and review 21
7.3 Rules of use 22
7.4 Selection 22
7.4.1 General 22
7.4.2 Documentation review 22
7.4.3 Operating experience review 22
7.4.4 Specific requirements related to the blank integrated circuits 23
7.5 Acceptance justification 23
7.6 Modification for acceptance 24
7.7 Modification after acceptance 24
7.8 Acceptance documentation 24
8 HPD design and implementation 24
8.1 General 24
8.2 Hardware Description Languages (HDL) and related tools 24

8.3 Design 25
8.3.1 General 25
8.3.2 Defensive design 25
8.3.3 Structure 25
8.3.4 Language and coding rules 26
8.3.5 Synchronous vs asynchronous design 27
8.3.6 Power management 27
8.3.7 Initialization 28
8.3.8 Non-functional configurations 28
8.3.9 Testability 28
8.3.10 Design documentation 28
8.4 Implementation 29
8.4.1 General 29
8.4.2 Products 29
8.4.3 Files of parameters and constraints 29
8.4.4 Post-route analyses 30
8.4.5 Redundancies introduced or removed by the tools 30
8.4.6 Finite state machines 31
8.4.7 Static timing analysis 31
8.4.8 Implementation documentation 31
8.5 System level tools and automated code generation 32
8.6 Documentation 33
8.7 Design and implementation review 33
9 HPD verification 33
9.1 General 33
9.2 Verification plan 34
9.3 Verification of the use of the pre-developed items 35
9.4 Verification of the design and implementation 35
9.5 Test-benches 36
9.6 Test coverage 36
9.7 Test execution 37
9.8 Static verification 37
10 HPD aspects of system integration 37
10.1 General 37
10.2 HPD aspects of the system integration plan 38
10.3 Specific aspects of system integration 38
10.4 Verification of the integrated system 39
10.5 Fault resolution procedures 39
10.6 HPD aspects of the integrated system test report 39
11 HPD aspects of system validation 40
11.1 General 40
11.2 HPD aspects of the system validation plan 40
11.3 System validation 40
11.4 HPD aspects of the system validation report 40
11.5 Fault resolution procedures 41
12 Modification 41
12.1 Modification of the requirements, design or implementation 41
12.2 Modification of the micro-electronic technology 41

13 HPD production 41
13.1 General 41
13.2 Production tests 41
13.3 Programming files and programming activities 42
14 HPD aspects of installation, commissioning and operation 42
15 Software tools for the development of HPDs 42
15.1 General 42
15.2 Additional requirements for design, implementation and simulation tools 42
16 Design segmentation or partitioning 43
16.1 Background 43
16.2 Auxiliary or support functions 43
16.2.1 General 43
16.2.2 Partitioning of auxiliary or support functions of category other than A 43
17 Defences against HPD Common Cause Failure 44
17.1 Background 44
17.2 Requirements 44
Annex A (informative) Documentation 45
Annex B (informative) Development of HPDs 47
Bibliography 52

Figure 1 – System life-cycle (informative, as defined by IEC 61513) 15
Figure 2 – Development life-cycle of HPD 16

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – DEVELOPMENT OF HDL-PROGRAMMED INTEGRATED CIRCUITS FOR SYSTEMS PERFORMING CATEGORY A 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 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/859/FDIS	45A/865/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.

INTRODUCTION

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

The electronic systems of class 1 (according to IEC 61513) used in Nuclear Power Plants (NPP) which are required in emergency situations, need to be fully validated and qualified before being used in operation.

In traditional systems that are computer-based, 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.

Nowadays, I&C designers may build application functions directly in one integrated circuit using devices 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:

1) based on pre-developed micro-electronic resources,
2) developed within an I&C project,
3) developed with Hardware Description Languages (HDL) and related tools used to implement the requirements in a proper assembly of the pre-developed micro-electronic resources.

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 may 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 hardware 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 system level. It is supplemented by guidance at hardware level (IEC 60987) and software level (IEC 60880 and IEC 62138). IEC 62340 gives requirements in order to reduce and overcome the possibility of common cause failure of category A functions.

IEC 62566 is a second level IEC SC 45A document which focuses on the activities when HPDs are developed. It complements IEC 60987 which deals with the generic issues of hardware design of computer based systems. It refers to IEC 60880 when issues identical to that of software development are addressed.

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 safety systems.

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

1) an approach to specify the requirements of, to design, to implement and to verify “HDL-Programmed Devices” (HPD, 3.7), and to handle the corresponding aspects of system integration and validation;
2) an approach to analyse and select the blank integrated circuits, micro-electronic technologies and Pre-Developed Blocks (PDB, 3.11) used to develop HPDs;
3) procedures for the modification and configuration control of HPDs;
4) 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 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 and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In 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 for topics related to quality assurance.

The IEC SC 45A Standards series consistently implements and details 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.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – DEVELOPMENT OF HDL-PROGRAMMED INTEGRATED CIRCUITS FOR SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope and object

1.1 General

This International Standard provides requirements for achieving highly reliable “HDL-Programmed Devices” (HPD), for use in I&C systems of nuclear power plants performing functions of safety category A 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 FPGAs or similar micro-electronic technologies. General purpose integrated circuits such as microprocessors are not HPDs.

This Standard provides requirements on:

a) a dedicated development life-cycle addressing each phase of the development of HPDs, including specification of requirements, design, implementation, verification, integration and validation,

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

c) selection of pre-developed components. This includes micro-electronic resources (such as a blank FPGA or CPLD) and HDL statements representing Pre-Developed Blocks (PDB),

d) use of simplicity and deterministic principles, recognized to be of primary importance to achieve “fault free” implementation of category A functions,

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

This Standard does not put requirements on the development of the micro-electronic resources, 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 resources in an I&C project with HDLs and related tools.

This Standard 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 (CCF). The requirements within this Standard for clear and comprehensive documentation should facilitate the effective application of IEC 62340.

Reliability aspects related to environmental qualification and failures due to ageing or physical degradation are not handled in this Standard. Other Standards, especially IEC 60987, IEC 60780 and IEC 62342, address these topics.

Subclause 5.7 of IEC 60880:2006 provides security requirements that apply to the development of HPDs as applicable.

1.2 Use of this Standard

This Standard provides guidance and requirements to produce verifiable designs and implementations where justification is necessary due for example to the function performed or to the importance to safety of its behaviour. Class 1 I&C systems may use HPDs for which full demonstration of compliance with the requirements of this Standard is not mandatory, e.g.

when they do not implement the logic of a safety function. However, deviations from this Standard should be justified.

This Standard 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 61513 for system integration and validation when HPDs are included.

Those requirements of IEC 60987 that relate to programmable logic device development are applicable, in addition to those of this Standard, where HPDs are part of class 1 I&C systems.

NOTE In case of conflicting requirements, this Standard supersedes those in IEC 60987 about class 1 HPDs.

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, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

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

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

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

IEC 62138, *Nuclear power plants – Instrumentation and control important for 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)*

IAEA guide NS-G-1.3:2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*

SOMMAIRE

AVANT-PROPOS 57
INTRODUCTION 59
1 Domaine d'application et objet 62
1.1 Considérations générales 62
1.2 Utilisation de la présente norme 63
2 Références normatives 63
3 Termes et définitions 64
4 Symboles and abréviations 66
5 Exigences générales pour les projets HPD 66
5.1 Considérations générales 66
5.2 Cycle de vie 67
5.3 Gestion du projet HPD 69
5.3.1 Considérations générales 69
5.3.2 Autres exigences 69
5.4 Plan d'assurance qualité pour le HPD 69
5.5 Gestion de configuration 69
6 Spécification des exigences du HPD 70
6.1 Considérations générales 70
6.2 Aspects fonctionnels de la spécification des exigences 71
6.3 Conception déterministe 71
6.4 Détection des défauts et tolérance aux fautes 71
6.5 Capture des exigences avec des outils ESL 72
6.5.1 Considérations générales 72
6.5.2 Exigences relatives au formalisme des outils ESL 72
6.5.3 Interface avec les outils de conception 72
6.6 Analyse et revue des exigences 73
7 Processus d'acceptation des circuits intégrés programmables, des blocs natifs et des blocs prédéveloppés 73
7.1 Considérations générales 73
7.2 Spécification des exigences du composant 73
7.2.1 Considérations générales 73
7.2.2 Exigences 74
7.2.3 Analyse et revue des exigences 74
7.3 Règles d'utilisation 74
7.4 Sélection 74
7.4.1 Considérations générales 74
7.4.2 Revue de la documentation 75
7.4.3 Revue de l'expérience de fonctionnement 75
7.4.4 Exigences particulières pour les circuits intégrés vierges 75
7.5 Justification de l'acceptation 76
7.6 Modification pour l'acceptation 76
7.7 Modification après l'acceptation 76
7.8 Documentation d'acceptation 77
8 Conception et réalisation du HPD 77
8.1 Considérations générales 77
8.2 Langages de description de matériel (HDL) et outils associés 77

8.3 Conception 78
8.3.1 Considérations générales 78
8.3.2 Conception défensive 78
8.3.3 Structure 78
8.3.4 Langage et règles de codage 79
8.3.5 Conception synchrone ou asynchrone 80
8.3.6 Gestion de l'alimentation 80
8.3.7 Initialisation 81
8.3.8 Configurations non fonctionnelles 81
8.3.9 Testabilité 81
8.3.10 Documentation de conception 81
8.4 Réalisation 82
8.4.1 Considérations générales 82
8.4.2 Produits 82
8.4.3 Fichiers de paramètres et de contraintes 82
8.4.4 Analyses post-routage 83
8.4.5 Redondances introduites ou supprimées par les outils 84
8.4.6 Machines à états finis 84
8.4.7 Analyse temporelle statique 84
8.4.8 Documentation de réalisation 85
8.5 Outils de niveau système et génération automatique de code 85
8.6 Documentation 86
8.7 Revue de conception et de réalisation 87
9 Vérification du HPD 87
9.1 Considérations générales 87
9.2 Plan de vérification 88
9.3 Vérification de l'utilisation des éléments prédéveloppés 89
9.4 Vérification de la conception et de la réalisation 89
9.5 Bancs de test 89
9.6 Couverture des tests 90
9.7 Exécution des tests 90
9.8 Vérification statique 90
10 Aspects de l'intégration du système liés au HPD 91
10.1 Considérations générales 91
10.2 Aspects du plan d'intégration du système liés au HPD 91
10.3 Aspects spécifiques de l'intégration du système 92
10.4 Vérification du système intégré 93
10.5 Procédures de résolution des défauts 93
10.6 Aspects du rapport de test du système intégré lié au HPD 93
11 Aspects de la validation du système liés au HPD 93
11.1 Considérations générales 93
11.2 Aspects du plan de validation du système liés au HPD 94
11.3 Validation du système 94
11.4 Aspects du rapport de validation du système liés au HPD 94
11.5 Procédures de résolution des défauts 94
12 Modification 95
12.1 Modification des exigences, de la conception ou de la réalisation 95
12.2 Modification de la technologie micro-electronique 95

13 Production du HPD 95
13.1 Considérations générales 95
13.2 Tests de production 95
13.3 Fichiers de programmation et activités de programmation 96
14 Aspects de l'installation, du démarrage et du fonctionnement liés au HPD 96
15 Outils logiciels pour le développement des HPD 96
15.1 Considérations générales 96
15.2 Exigences additionnelles pour les outils de conception, réalisation et simulation 97
16 Segmentation de la conception ou partitionnement 97
16.1 Bases 97
16.2 Fonctions auxiliaires ou support 97
16.2.1 Considérations générales 97
16.2.2 Partitionnement de fonctions auxiliaires ou support de catégorie autre que A 97
17 Défense contre les défaillances de cause commune dues aux HPD 98
17.1 Bases 98
17.2 Exigences 98
Annexe A (informative) Documentation 100
Annexe B (informative) Développement des HPD 102
Bibliographie 107

Figure 1 – Cycle de vie de sûreté du système (informatif, tel que défini par la CEI 61513) 67
Figure 2 – Cycle de vie de développement du HPD 68

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

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 62566 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/859/FDIS	45A/865/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.

INTRODUCTION

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

Les systèmes électroniques de classe 1 (selon la CEI 61513) employés dans les centrales nucléaires de puissance et qui sont nécessaires dans les situations d'urgence doivent être entièrement validés et qualifiés avant d'être utilisés en phase d'exploitation.

Dans les systèmes programmés classiques, on peut distinguer le matériel du logiciel. Le matériel est principalement conçu avec des composants standardisés 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.

Aujourd'hui, les concepteurs d'instrumentation et de contrôle-commande (I&C) peuvent bâtir des fonctions d'application directement à l'intérieur d'un circuit intégré, 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 micro-électronique, mais par le concepteur d'instrumentation et de contrôle-commande.

Les circuits intégrés traités dans la présente norme sont:

1) basés sur des ressources micro-électroniques prédéveloppées,
2) développés au sein d'un projet d'I&C,
3) développés au moyen de Langages de Description de Matériel (HDL) et d'outils associés, utilisés pour réaliser les exigences par un assemblage adéquat des ressources micro-électroniques prédéveloppées.

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 requises par un projet d'I&C. Cependant, la vérification et la validation peuvent être 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, la sélection 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 matériel, 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 collection de normes du SC 45A de la CEI

La CEI 61513 est un document de premier niveau de la collection des normes du SC 45A de la CEI et fournit des recommandations applicables à l'I&C au niveau du système. Elle est complétée par des recommandations au niveau matériel (CEI 60987) et logiciel (CEI 60880 et CEI 62138). La CEI 62340 fournit des exigences visant à réduire et surmonter la possibilité d'une défaillance de cause commune de fonctions de catégorie A.

La CEI 62566 est un document de deuxième niveau de la collection des normes du SC 45A de la CEI qui concerne les activités de développement des HPD. Elle complète la CEI 60987 qui aborde les problèmes génériques de la conception du matériel des systèmes informatisés. Elle renvoie à la CEI 60880 quand des questions identiques à celles du développement des logiciels sont traitées.

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

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

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

Les aspects pour lesquels des exigences et des recommandations particulières ont été produites sont les suivants:

1) approche de spécification des exigences, de conception, de réalisation et de vérification des circuits intégrés programmés en HDL (HPD, voir 3.7), ainsi que des aspects de l'intégration et de la validation du système liés aux HPD;
2) approche d'analyse et de sélection des circuits intégrés vierges, technologies micro-électroniques et Blocs Prédéveloppés (PDB, voir 3.11) utilisés pour développer les HPD;
3) procédures de modification et de contrôle de configuration des HPD;
4) exigences relatives à la sélection 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 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 publication fondamentale de sécurité 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 de la CEI 61508-1, de la CEI 61508-2 et de la CEI 61508-4 pour le secteur 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 et AIEA GS-G-3.1 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.

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

1 Domaine d'application et objet

1.1 Considérations générales

La présente Norme internationale énonce des exigences pour atteindre une fiabilité élevée 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 A telles que définies par la CEI 61226.

La programmation des HPD repose sur des Langages de Description de Matériel (HDL) et des outils logiciels associés. Ils sont typiquement basés sur des FPGA vierges ou des technologies micro-électroniques similaires. Les circuits intégrés d'usage général tels que les microprocesseurs ne sont pas des HPD.

La présente norme énonce des exigences sur:

a) un cycle de vie de développement dédié concernant chaque phase du développement des HPD, notamment la spécification des exigences, la conception, la réalisation, la vérification, l'intégration et la validation,

b) la planification et des activités complémentaires telles que la modification et la production,

c) la sélection des composants prédéveloppés, notamment les ressources micro-électroniques (telles que FPGA ou CPLD vierges) et les instructions HDL représentant des Blocs Prédéveloppés (PDB),

d) l'utilisation de principes de simplicité et de déterminisme reconnus pour leur importance dans l'atteinte d'une réalisation « exempte de défauts » des fonctions de catégorie A,

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

La présente norme n'impose pas d'exigence sur le développement des ressources micro-électroniques, 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. Elle concerne les développements effectués à partir de ces ressources micro-électroniques dans un projet d'I&C, avec des HDL et des outils associés.

La présente norme fournit des recommandations visant à éviter autant que possible les défauts latents résiduels dans les HPD, et à réduire la susceptibilité aux simples défauts et aux défaillances de cause commune (DCC) potentielles. Les exigences de la présente norme pour une documentation claire et complète devraient faciliter l'application efficace de la CEI 62340.

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 la présente norme. D'autres normes traitent de ces aspects, en particulier la CEI 60987, la CEI 60780 et la CEI 62342.

Le paragraphe 5.7 de la CEI 60880:2006 contient des exigences au sujet de la sécurité qui concernent le développement des HPD lorsqu'elles sont applicables.

1.2 Utilisation de la présente norme

La présente norme énonce des lignes directrices et des exigences pour des conceptions et réalisations vérifiables, lorsque qu'une justification est nécessaire par exemple en raison de la fonction exécutée ou de l'importance pour la sûreté de son comportement. Les systèmes d'I&C de classe 1 peuvent utiliser des HPD ne nécessitant pas une démonstration complète de conformité aux exigences de la présente norme, par exemple lorsqu'ils n'implémentent pas la logique d'une fonction de sûreté. Toutefois, il convient que les écarts par rapport aux exigences de la présente norme soient justifiés.

La présente norme décrit les activités visant à développer les HPD, organisées en un cycle de vie dédié. Elle décrit également les activités et les recommandations à suivre en complément des exigences de la CEI 61513 pour l'intégration et la validation des systèmes lorsqu'ils incluent des HPD.

Les exigences de la CEI 60987 relatives au développement de dispositifs logiques programmables sont applicables, en plus de celles de la présente norme, pour les HPD inclus dans des systèmes d'I&C de classe 1.

NOTE En cas d'exigences contradictoires, celles de la présente norme remplacent celles de la CEI 60987 pour les HPD de classe 1.

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

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 60987:2007, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences applicables à la conception du matériel des systèmes informatisés*

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

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

CEI 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)*

AIEA guide NS-G-1.3:2005, *Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté des centrales nucléaires*