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

IEC 62566:2012

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

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

About the IEC

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

About IEC publications

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

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Customer Service Centre - webstore.iec.ch/csc

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

A propos de la CEI

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

A propos des publications CEI

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

Liens utiles:

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

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

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

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

Service Clients - webstore.iec.ch/csc

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

IEC 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

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*

3 Terms and definitions

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

3.1
Application Specific Integrated Circuit , ASIC
integrated circuit designed for specific applications

[IEC 60050-521:2002, 521-11-18]

NOTE Specialized integrated circuit designed for the purpose of one company. It embeds bespoke functions defined by this company.

3.2
block
one of the parts that make up a design; a block may be subdivided into other blocks

NOTE A block is either a Pre-Developed Block or a Native Block or a block developed during the considered project.

3.3
Common Cause Failure, CCF
failure of two or more structures, systems or components due to a single specific event or cause

[IAEA Safety Glossary 2007 Edition]

NOTE Common causes may be internal or external to an I&C system.

[IEC 61513]

3.4
Electronic System Level, ESL
high-level description of an electronic system, based on a set of processes representing functionalities of components such as microprocessors, memories, specialized computing units, or communication channels

NOTE This description allows the designer to partition the system into components, to assess its performance under different mapping of functions to the components, and to establish the requirements for the components.

It is typically performed with languages such as SystemC (IEEE 1666), SystemVerilog (IEEE 1800), or Matlab (R).

3.5
Field Programmable Gate Array, FPGA
integrated circuit that can be programmed in the field by the I&C producer. It includes programmable logic blocks (combinatorial and sequential), programmable interconnections between them and programmable blocks for input and/or outputs. The function is then defined by the I&C designer, not by the integrated circuit supplier.

NOTE While FPGAs are essentially digital devices, some of them may integrate analog input/outputs and analog to digital converters. FPGAs may include advanced digital functions such as hardware multipliers, dedicated memory and embedded processor cores.

3.6
Hardware Description Language, HDL
language used to formally describe the functions and/or the structure of an electronic component for documentation, simulation or synthesis

NOTE The most widely used HDLs are VHDL (IEEE 1076) and Verilog (IEEE 1364).

3.7
HDL-Programmed Device, HPD
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools

NOTE 1 HDLs and related tools (e.g. simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

NOTE 2 The development of HPDs can use Pre-Developed Blocks.

NOTE 3 HPDs are typically based on blank FPGAs, PLDs or similar micro-electronic technologies.

3.8
module
one of the parts that make up a design; a module may be subdivided into other modules

NOTE Module" is a synonym of "Block"; "Block" is often used in the context of electronic design. "Module" is the term used by IEC 60880 and is needed in this Standard for references to IEC 60880.

3.9
native block
a Block which represents a pre-existing resource in the integrated circuit, e.g. an OR gate or a more complex block such as a multiplier or a serial transmission controller. By programming the HPD, the Native Blocks are configured and connected to provide the required function.

3.10
netlist
description of an electronic component in terms of interconnections between its terminal elements (e.g. Native Blocks)

3.11
Pre-Developed Block, PDB
pre-developed functional block usable in a HDL description

NOTE 1 PDBs are typically provided as libraries, macros, or Intellectual Property cores. They are used in the development of a HPD and incorporated in this HPD.

NOTE 2 A PDB may need significant work before incorporation in a HPD, e.g. synthesizing an electronic circuit from the HDL statements, mapping the notional components of this circuit on the hardware structures of the physical integrated circuit and routing the interconnections.

3.12
Pre-Developed Software, PDS
software part that already exists, is available as a commercial or proprietary product, and is being considered for use

[IEC 60880]

3.13
Programmable Logic Device, PLD
integrated circuit that consists of logic elements with an interconnection pattern, parts of which are user programmable.

[IEC 60050-521:2002, 521-11-01]

NOTE 1 Different kinds of PLD exist, e.g. Erasable PLD or Complex PLD (CPLD).

NOTE 2 The differences between “FPGA” and “PLD” are not well defined, but “PLD” usually refers to a simpler device than “FPGA”.

3.14
Register Transfer Level, RTL
synchronous parallel model of an electronic circuit, describing its behaviour by means of signals processed according to a combinatorial logic and transferred between registers on clock pulses. The RTL model is typically written in HDL or generated out of HDL source code.

4 Symbols and abbreviations

ASIC: Application Specific Integrated Circuit

CCF: Common Cause Failure

CPLD: Complex Programmable Logic Device

DRC: Design Rule Check

ESL: Electronic System Level

FPGA: Field Programmable Gate Array

HDL: Hardware Description Language

HPD: HDL-Programmed Device

IP: Intellectual Property