IEC 62566-2

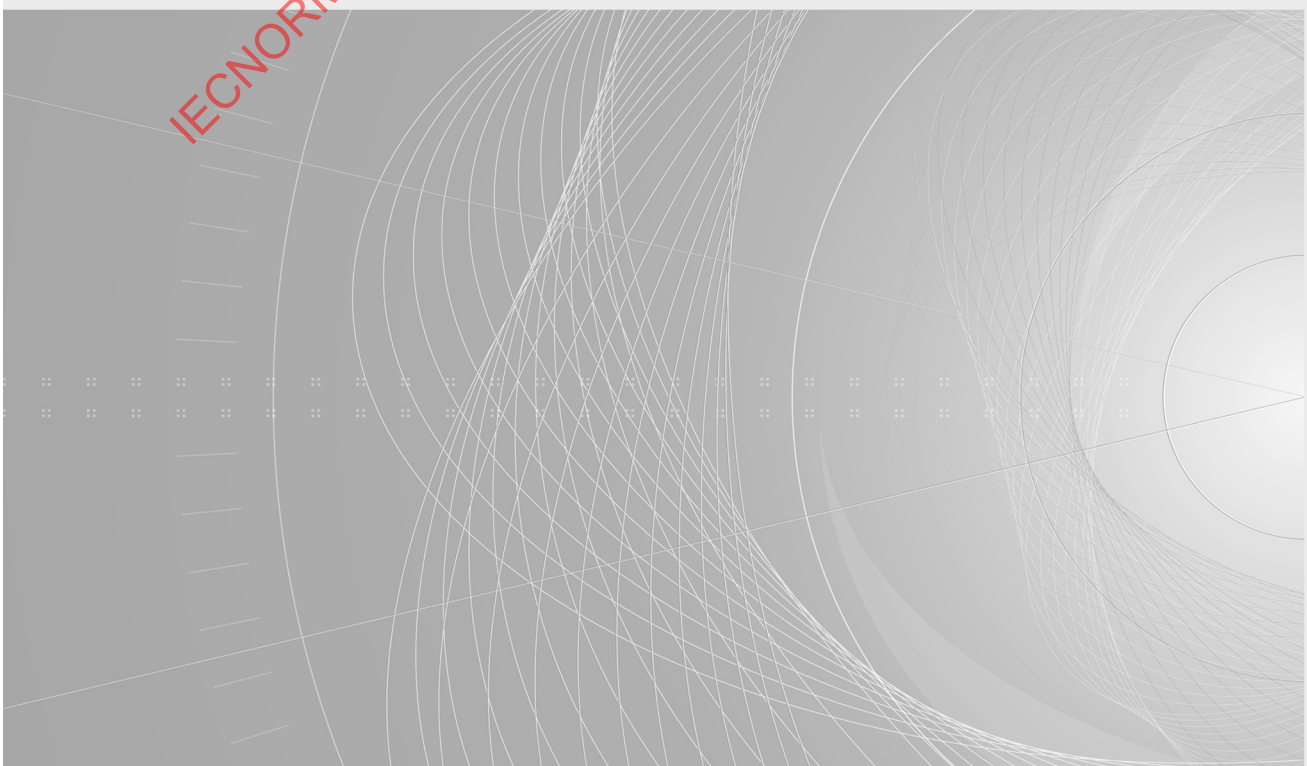
Edition 1.0 2020-05

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



IEC 62566-2:2020-05(en-fr)

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

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

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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
application function
function of an I&C system that performs a task related to the process being controlled rather than to the functioning of the system itself

[SOURCE: IEC 61513:2011, 3.1]

3.2
application-oriented language
computer language specifically designed to address a certain type of application and to be used by persons who are specialists of this type of application

Note 1 to entry: Equipment families usually feature application-oriented languages so as to provide easy to use capability for adjusting the equipment to specific requirements.

Note 2 to entry: Application-oriented languages may be used to specify the functional requirements of an I&C system, and/or to specify or design application software. They may be based on texts, on graphics, or on both.

Note 3 to entry: Examples: function block diagram languages, languages defined by IEC 61131-3.

Note 4 to entry: See also General-purpose language.

[SOURCE: IEC 60880:2006, 3.3]

3.3
application software
part of the software of an I&C system that implements the application functions

Note 1 to entry: For HPDs, application functions are not implemented using software and so the term “application software” might be replaced by “application functions implemented within the HPD design”.

Note 2 to entry: Application software contrasts with system software.

Note 3 to entry: See also system software.

[SOURCE: IEC 61513:2011, 3.2]

3.4
application specific integrated circuit
ASIC
integrated circuit designed for specific applications

Note 1 to entry: Specialized integrated circuit designed for the purpose of one company. It embeds bespoke functions defined by this company.

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

3.5
block
one of the parts that make up a design; a block may be subdivided into other blocks.

Note 1 to entry: A block is either a Pre-Developed Block or a Native Block or a block developed during the considered project.

[SOURCE: IEC 62566:2012, 3.2]

3.6
common cause failure
CCF
failure of two or more structures, systems or components due to a single specific event or cause.

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.7
configuration management
the process of identifying and documenting the characteristics of a facility’s structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation

[SOURCE: IAEA Safety Glossary, 2016 edition]

3.8
cybersecurity
set of activities and measures the objective of which is to prevent, detect, and react to:

– malicious disclosures of information (confidentiality) that could be used to perform malicious acts which could lead to an accident, an unsafe situation or plant performance degradation;
– malicious modifications (integrity) of functions that may compromise the delivery or integrity of the required service by I&C programmable digital systems (incl. loss of control) which could lead to an accident, an unsafe situation or plant performance degradation;

– malicious withholding or prevention of access to or communication of information, data or resources (incl. loss of view) that could compromise the delivery of the required service by I&C systems (availability) which could lead to an accident, an unsafe situation or plant performance degradation

Note 1 to entry: This definition is tailored with respect to the scope of IEC 62645 and the overall SC 45A document structure. It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors and protection against natural disasters. Those aspects – except human errors degrading cybersecurity – are not included in the concept of cybersecurity used in the SC 45A standard series. See annex A of IEC 62645 for more detail about such exclusions.

Note 2 to entry: Computer security, security and cybersecurity are considered synonymous in this document.

3.9
design specification
document or set of documents that describe the organisation and functioning of an item, and that are used as a basis for the implementation and the integration of the item

[SOURCE: IEC 62138:2018, 3.12]

3.10
documentation for safety
document or set of documents that specifies how a product can be safely used for applications important to safety

Note 1 to entry: This definition is used in the context of pre-developed components including programmable integrated circuits, native blocks and pre-developed blocks (see Clause 7).

[SOURCE: IEC 62138:2018, 3.13]

3.11
Electrical/Electronic/Programmable Electronic item
E/E/PE item
item based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

Note 1 to entry: In this term and its definitions, the word “item” can be replaced by the words: system or equipment or device.

[SOURCE: From IEC 61508-4:2010]

3.12
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 1 to entry: 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) or SystemVerilog (IEEE 1800).

[SOURCE: IEC 62566:2012, 3.4]

3.13
equipment family
set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). The development of plant specific configurations and of the related application software may be supported by software tools. An equipment family usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software

Note 1 to entry: An equipment family may also include HPD components.

Note 2 to entry: An equipment family may be a product of a defined manufacturer or a set of products interconnected and adapted by a supplier.

Note 3 to entry: The term “Equipment platform” is sometime used as a synonym of “Equipment family”.

[SOURCE: IEC 61513:2011, 3.17]

3.14
error
discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretical value or condition

Note 1 to entry: See also Human error, Fault, Failure.

[SOURCE: IEC 61513:2011, 3.18]

3.15
fault
defect in a hardware, software or system component

Note 1 to entry: Faults may be originated from random failures, that result e.g. from hardware degradation due to ageing, and may be systematic faults, e.g. software faults, which result from design errors.

Note 2 to entry: A fault (notably a design fault) may remain undetected in a system until specific conditions are such that the result produced does not conform to the intended function, i.e. a failure occurs.

Note 3 to entry: See also Human error, Error, Failure.

[SOURCE: IEC 61513:2011, 3.21]

3.16
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 1 to entry: 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.

[SOURCE: IEC 62566:2012, 3.5]

3.17
functional validation
verification of the correctness of the application functions specifications against the top level plant functional and performance requirements. It is complementary to the system validation that verifies the compliance of the system with the functions specification

[SOURCE: IEC 61513:2011, 3.23]

3.18
general-purpose language
computer language designed to address all types of usage

EXAMPLE Ada, C, Pascal.

Note 1 to entry: The system software of equipment families is usually implemented using general-purpose languages.

Note 2 to entry: See also Application-oriented language.

[SOURCE: IEC 60880:2006, 3.20]

3.19
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 1 to entry: The most widely used HDLs are VHDL (IEEE 1076) and Verilog (IEEE 1364).

[SOURCE: IEC 62566:2012, 3.6]

3.20
HDL-programmed device
HPD
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools.

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

Note 2 to entry: The development of HPDs can use Pre-Developed Blocks.

Note 3 to entry: HPDs are typically based on blank FPGAs (Field Programmable Gate Arrays) or similar programmable integrated circuits.

[SOURCE: IEC 62566:2012, 3.7]

3.21
human error
mistake
human action that produces an unintended result

Note 1 to entry: See also Fault, Error, Failure.

[SOURCE: IEC 61513:2011, 3.26]

3.22
I&C system
system, based on E/E/PE items, performing plant I&C functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: See also the definition of E/E/PE item and the associated notes.

Note 4 to entry: According to their typical functionality, IAEA distinguishes between automation / control systems, HMI systems, interlock systems and protection systems.

[SOURCE: IEC 62138:2018, 3.26]

3.23
integration
progressive aggregation and verification of components into a complete system

[SOURCE: IEC 62138:2018, 3.27]

3.24
mode of operation
functional state of an item where it provides a specific operational behaviour

EXAMPLE Initialisation mode, normal mode, degraded modes to be taken in case of error in the item.

[SOURCE: IEC 62138:2018, 3.29]

3.25
module
one of the parts that make up a design; a module may be subdivided into other modules.

Note 1 to entry: "Module" is a synonym of "Block"; "Block" is often used in the context of electronic design.

[SOURCE: IEC 62566:2012, 3.8]

3.26
native block
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.

[SOURCE: IEC 62566:2012, 3.9]

3.27
netlist
description of an electronic component in terms of interconnections between its terminal elements (e.g. native blocks).

[SOURCE: IEC 62566:2012, 3.10]

3.28
parameter
data item governing the behaviour of the I&C system and/or of its software, and that may be modified by operators during plant operation

Note 1 to entry: A parameter may also govern the behaviour of HPDs.

[SOURCE: IEC 62138:2018, 3.31]

3.29
pre-developed block
PDB
pre-developed functional block usable in a HDL description.

Note 1 to entry: 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 to entry: 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.

[SOURCE: IEC 62566:2012, 3.11]

3.30
programmable digital item
item that relies on software instructions or programmable logic to accomplish a function

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment or device

Note 2 to entry: The main kinds of programmable digital items are computer-based items and programmable logic items

Note 3 to entry: This term used by IEC SC 45A is equivalent to programmable electronic item (PE item) defined according to IEC 61508.

[SOURCE: IEC 62138:2018, 3.34]

3.31
programmable logic device
PLD
integrated circuit that consists of logic elements with an interconnection pattern, parts of which are user programmable.

Note 1 to entry: Different kinds of PLD exist, e.g. Erasable PLD or Complex PLD (CPLD).

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

[SOURCE: IEC 62566:2012, 3.13]

3.32
programmable logic item
item that relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable

Note 1 to entry: In this term and its definition, the term item can be replaced by the terms: system or equipment or device.

Note 2 to entry: A programmable logic item is a kind of programmable digital item.

Note 3 to entry: See also the definition of E/E/PE item and the associated notes.

[SOURCE: IEC 62138:2018, 3.35]

3.33
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

[SOURCE: IEC 62566:2012, 3.14]

3.34
self-supervision
automatic testing of system hardware performance and software consistency of a computer-based I&C system

Note 1 to entry: Self-supervision may also apply to HPDs or HPD-based I&C systems.

[SOURCE: IEC 60671:2007, 3.8]

3.35
system software
software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs, for example, operating systems, computers, utilities. System software is usually composed of operational system software and support software

Note 1 to entry: For HPDs, operational system functions are not implemented using software and so the term “operational system software” might be replaced by “operational system aspects of HPD design”.

Note 2 to entry: Operational system aspects of HPD design: aspects of the HPD design used during system operation, such as: communication interfaces, input/output management, on-line diagnostics.

Note 3 to entry: Support software: software that aids in the development, test, or maintenance of other software/HPDs and of the system such as synthesis tools, code generators, graphic editors, off-line diagnostics, verification and validation tools.

Note 4 to entry: See also application software.

[SOURCE: IEC 61513:2011, 3.58]

3.36
system validation
confirmation by examination and provision of other evidence that a system fulfils in its entirety the requirement specification as intended (functionality, response time, fault tolerance, robustness)

Note 1 to entry: The 2016 edition of the IAEA Safety Glossary gives the two following definitions:

> Validation: The process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation may involve a greater element of judgment than verification.
>
> Computer system validation: The process of testing and evaluating the integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements.

Firstly, the definition “system validation” is a specific case of validation. It refers to a specific product, namely to the validation of an I&C system. This is consistent with the IAEA definition. Secondly, the IEC definition specifies the reference of validation, namely the requirement specification whereas the IAEA definition only refers to the “intended function”.

[SOURCE: IEC 61513:2011, 3.59]

3.37
systematic fault
fault related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

[SOURCE: IEC 61513:2011, 3.60]

3.38
verification
confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

[SOURCE: IEC 61513:2011, 3.62]

4 Symbols and abbreviated terms

ASIC	Application Specific Integrated Circuit
CCF	Common Cause Failure
CPLD	Complex Programmable Logic Device
ESL	Electronic System Level
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
HPD	HDL-Programmed Device
IC	Integrated Circuit
I&C	Instrumentation and Control
PAL	Programmable Array Logic

PDB Pre-Developed Block
PLD Programmable Logic Device
RAM Random Access Memory
RTL Register Transfer Level
SRAM Static RAM
STA Static Timing Analysis
VHDL Very High Speed Integrated Circuit Hardware Description Language

5 General requirements for HPD projects

5.1 General

The present clause first places the HPD within the context of the I&C system as described by IEC 61513. Then it describes the HPD life-cycle which structures the HPD project.

Finally it provides requirements for HPD projects, for quality assurance and for configuration management, many of which are common with those of software development processes and are taken from IEC 62138 and which are supplemented by HPD specific requirements if needed.

With reference to Clause 1, the scope of this document excludes the development of micro-electronic technologies (blank integrated circuits). Therefore wordings such as “HPD development”, “HPD life-cycle”, “HPD design” or “HPD verification” refer to what is done within the I&C project, starting from these micro-electronic technologies in order to produce the specific HPD for use in the I&C system.

5.2 Life-cycle

The process of producing I&C systems for use in nuclear power plants is given in IEC 61513 that introduces the concept of system life-cycle. This is a vehicle by which the development process can be controlled and whose adoption should also result in evidence necessary to justify the correct operation of safety systems. It includes and places requirements on, but does not dictate the project arrangements to be used for, production of systems (see Figure 1).

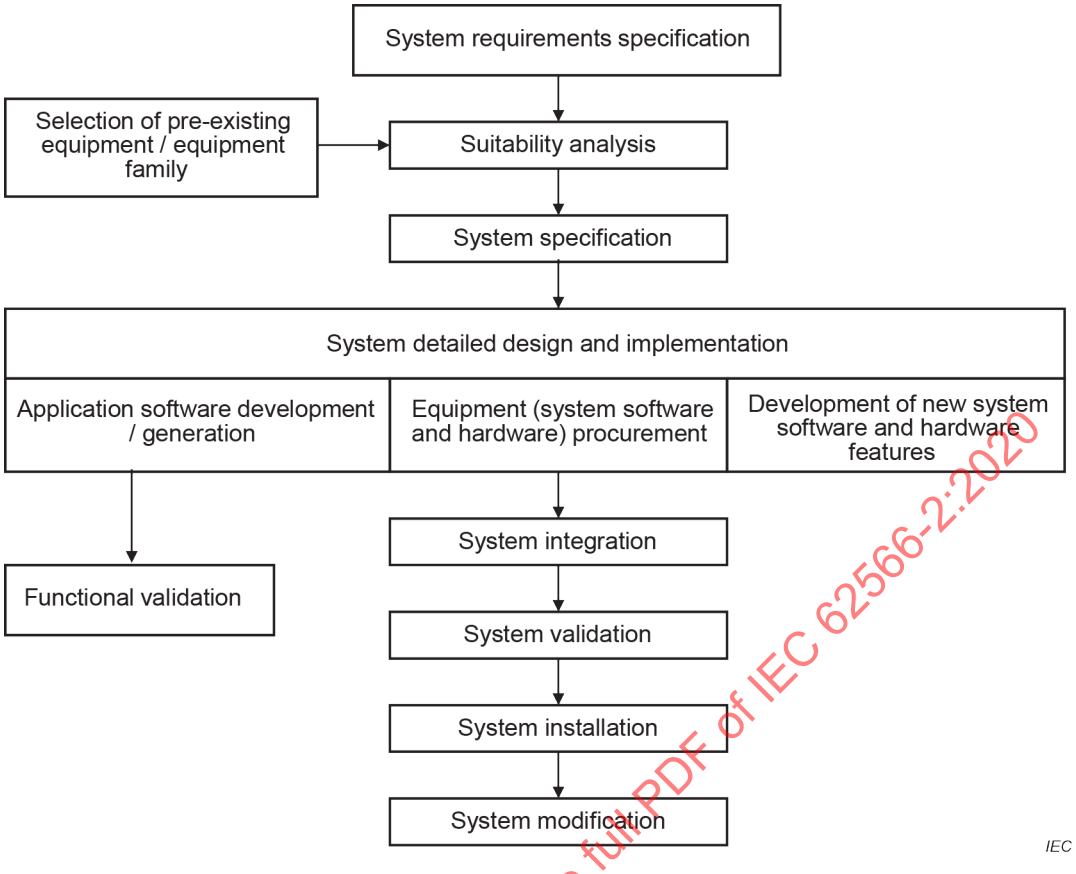


Figure 1 – System life-cycle (informative, as defined by IEC 61513)

The system life-cycle of IEC 61513 is complemented in IEC 60880 (for category A functions) and IEC 62138 (for category B and C functions) for software development, by IEC 62566 (for category A functions) and IEC 62566-2 (for category B and C functions) for HPD development and in IEC 60987 for hardware development of class 1 and 2 computer-based systems.

HPDs are developed by means of computer tools which tend to structure the development according to a cycle that includes activities dedicated to design and implementation, integration and validation, together with verification and test activities.

The system design and implementation phases of IEC 61513 shown in Figure 1 (particularly the “Equipment (system software and hardware) procurement” and “Development of new system software and hardware features”) are essential parts of the system life-cycle of IEC 61513. For system components which are HPDs, these phases are expanded Figure 2 to illustrate in more detail the phases between the specification of requirements and the validation.

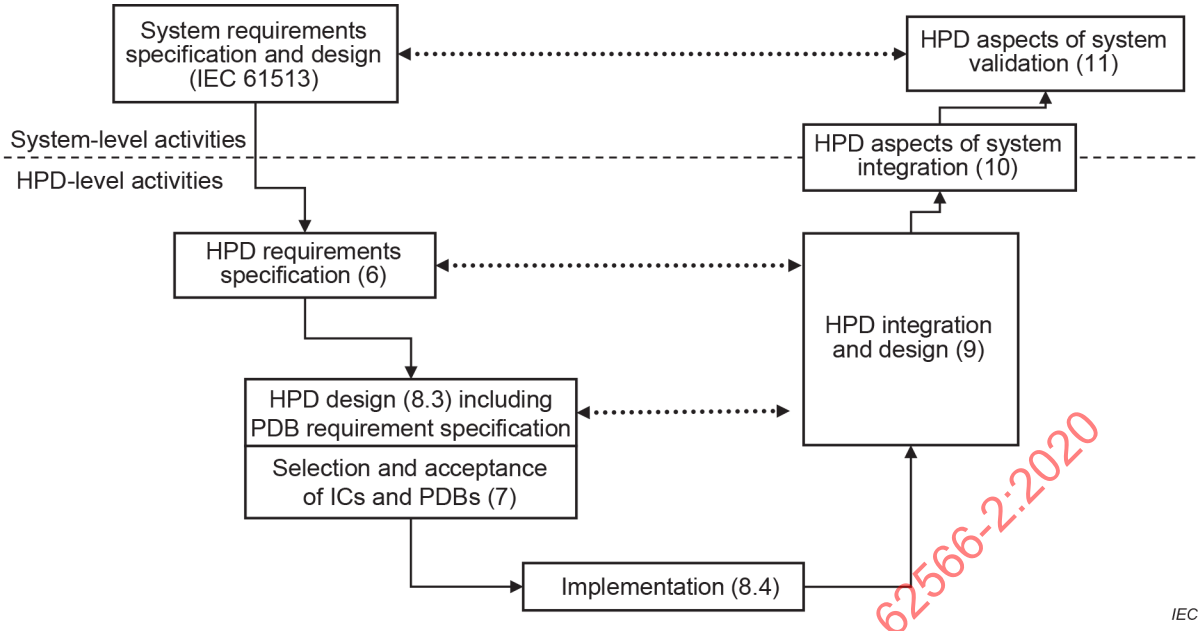


Figure 2 – HPD life-cycle

The HPD life-cycle described in Figure 2 shows the development of one HPD that might be undertaken in parallel with the development of other components (software or hardware) of the system as shown in Figure 1 but coming together at the integration and validation phases of the system life-cycle.

The following additional activities not represented in Figure 2 also support the development process of HPDs:

- quality assurance (5.4),
- configuration management (5.5),
- HPD verification (5.6),
- HPD modification activities (Clause 12),
- HPD production (Clause 13),
- Selection of tools (Clause 15).

5.3 Gradation principles

As a consequence of the gradation of safety relevance for functions of categories A, B and C (see IEC 61226), a suitable gradation has been adopted for the requirements applicable to the HPDs of I&C systems of safety classes 1, 2 and 3.

The application of the requirements of this standard to safety class 3 HPDs confers the basic level of confidence that is suitable for HPDs of an I&C system identified as important to safety. The principles followed are:

- reliance on quality assurance;
- attention given to the assurance that the HPD:
  - contributes as necessary to, and does not adversely affect, the functions important to safety;
  - satisfies the HPD requirements specification statements which define constraints important to safety;

- assurance that the operators of the I&C system are informed as early as reasonably possible of HPD errors and failures that might affect the functions identified as important to safety, so that any appropriate action can be taken;
- documented HPD requirements specifications, design specifications, integration plan, HPD test plan (i.e. simulation, functional testing), HPD aspects of the system validation plan and modification specifications.

For safety class 2 HPDs, in addition to the principles already stated for class 3 HPDs, the principles followed by this standard are:

- more stringent requirements for the selection of pre-developed blocks and native blocks;
- more stringent requirements for functional validation;
- more stringent requirements for verification, and for the selection and use of HPD development tools and languages;
- explicit requirements for simplicity, clarity, precision, verifiability, testability and modifiability.

When requirements are applicable to both safety classes, the extent of the justification required to confirm compliance with this standard may be moderated depending upon the safety class, i.e. for class 3, the extent of justification may be reduced compared to class 2. Also, the extent of justification for those functions which are 'not important to safety' in class 2 or 3 systems need only address how the design ensures that such functions do not jeopardise the functions which are identified as important to safety.

5.4 HPD quality assurance

5.4.1 General

Subclause 6.3.2.1 of IEC 61513:2011 provides general requirements for quality assurance at the level of an I&C system. The present subclause provides additional requirements specific, or of particular importance, to HPDs.

5.4.2 The development of HPDs shall be performed according to a HPD life-cycle. The provisions of this HPD life-cycle shall be specified in a quality assurance plan.

This quality assurance plan may be a part of the system quality assurance plan, or may be a separate HPD quality assurance plan.

5.4.3 If a separate HPD quality assurance plan is used, it shall be consistent with the system quality assurance plan. The applicable requirements of 6.3.2 of IEC 61513:2011 shall be addressed by the two plans.

5.4.4 The quality assurance plan shall divide the development phase of the HPD life-cycle into specified activities. These activities shall include the activities necessary to achieve the required HPD quality, and to verify and provide objective evidence that this quality is achieved.

5.4.5 The specification of an activity shall state:

a) its objectives;

b) its relationships and interactions with other activities;

c) its inputs and results;

d) the organisation and responsibilities relevant to the activity.

e) the verification activities associated as required by 5.6.

5.4.6 The contents and properties required of the inputs and results should also be specified.

5.4.7 The quality assurance plan shall require that:

a) the implementation of each activity is assigned to competent persons equipped with adequate resources.

b) modifications in approved documents are identified, reviewed and approved by authorised persons.

c) the methods, languages, tools, rules and standards used are identified and documented, known to, and within the competencies of the concerned development personnel.

d) if several methods, languages, tools, rules and/or standards are used, it is clear which ones have to be used for each activity.

e) project specific terms, expressions, abbreviations and conventions used are explicitly defined.

f) non-conformances raised are tracked and resolved.

g) records resulting from its application are produced. In particular, it shall require that the results of verifications and reviews are recorded together with the scope of the verifications or reviews, the conclusions reached and the resolutions agreed. Any deviation from the quality assurance plan shall be documented and justified.

h) the output documentation constitutes a set of appropriately cross-referenced mutually consistent documents, ensuring the traceability of the final design to the input requirements.

5.5 Configuration management

5.5.1 General

Subclause 6.3.2.3 of IEC 61513:2011 provides requirements for configuration management at the I&C system level. The present subclause provides additional requirements specific, or of particular importance, to HPDs.

5.5.2 Configuration management for HPDs shall be performed according to the provisions of a configuration management plan or of the quality assurance plan. These provisions shall be consistent with those for system level configuration management.

5.5.3 The configuration management shall record the following items:

a) documentation of modules (blocks) developed within the project and of PDBs,

b) identification marking of integrated circuits,

c) computer files used for simulation, verification and production allowing results to be reproduced and audited,

d) parameters used for the automated activities of the software tools (see Clause 15), such as “optimize timing, optimize density” for the place and route activity,

e) identification of the versions of all software tools (see Clause 15), including any “software patch” applied, as well as general purpose libraries and technology dependent libraries,

f) errata sheets containing warnings about identified bugs in software tools.

5.5.4 The configuration management plan shall specify technical means for the authentication of the HPD items under configuration management and of their versions.

5.5.5 The configuration management plan shall ensure that the version of the HPD attached to a given version of the system or equipment, and the versions of the items which together constitute this HPD version are uniquely identified.

5.6 HPD Verification

5.6.1 A verification plan shall define the scope of HPD verification and review activities.

5.6.2 The verification plan shall address the requirements of 6.3.2.2 of IEC 61513:2011 as they relate to HPDs.

5.6.3 Verifications and reviews shall be performed according to documented provisions. The verification plan shall ensure that:

a) the verification results are held under configuration management;

b) all verification activities have precisely identified inputs, and their results are consistent with these inputs;

c) the activities fulfil their specified objectives, and their results have the required contents and properties, and comply with any resolution agreed;

d) the results are clear, precise and up-to-date;

e) the results comply with any applicable rule;

f) the results comply with the applicable requirements of this standard.

"Precisely identified" means that the version is known without any ambiguity. "Clear" means that the individuals who need to read a document can fully understand it without excessive effort, even if they have not been involved earlier in the project, provided that they have the required knowledge. "Precise" means that there is no ambiguity.

The extent of the verification and review activities might depend on the scale and nature of the HPD and the results to be verified or reviewed, and on the methods and tools used. The extent of the verification and review activities might be more limited for the requirements that are not identified as important to safety (see requirement 6.2.5) and that cannot jeopardise the functions identified as important to safety.

5.6.4 The verification plan should ensure that records are produced such that the verification process is fully auditable, i.e. such that independent confirmation of the implementation of the verification plan may be performed.

5.6.5 The verification of the results of an activity shall be performed by competent persons who did not participate in the activity.

5.6.6 The verification of the results of an activity should include representatives of those concerned with the use of these results, as well as other experts, as necessary.

5.6.7 The HPD requirements specification, the HPD design specification and the HPD verification plan shall be verified.

5.6.8 HPD verification shall be performed by persons who did not develop the HPD being verified.

5.6.9 *For class 2, the application of design and implementation rules shall be verified (see 8.3.3 for recommended design rules).*

5.6.10 *For class 2, persons who do the verification should have managerial independence from the developers.*

6 HPD requirements specification

6.1 General

6.1.1 Overview

The present subclause completes and adds precision to the requirements of 6.2.3.4 of IEC 61513:2011.

6.1.2 A HPD requirements specification shall document the requirements of the HPD, either in the document itself or by referencing sets of requirements stated at system or subsystem level (e.g. the functional behaviour to be implemented).

6.1.3 The HPD requirements specification should be unequivocal, verifiable and achievable, including for temporal aspects

6.1.4 When the HPD implements a safety function, its requirements specification shall be derived from the requirements of the I&C system implementing this safety function and shall be part of the specification of the subsystem which uses the HPD.

6.1.5 The HPD requirements specification should describe what is to be done and not how it is to be done.

In principle, the objective of the HPD requirements specification is to specify what the HPD is to achieve without specifying how it shall do it. However, design and implementation constraints might have to be specified when this is required by considerations of the design of the I&C system or of the I&C architecture.

6.1.6 The HPD requirements specification shall be a reference for HPD design, HPD aspects of system validation, and, if applicable, HPD modifications.

The HPD requirements specification may reference input documentation directly, so as to avoid unnecessary duplications and minimise the risk of inconsistencies. It may also reference other pre-existing documents, such as the documentation of native blocks and other pre-developed blocks.

6.1.7 The HPD requirements specification shall provide traceability to its input documents.

6.1.8 The verification of the HPD requirements specification should check that it is consistent and complete with respect to all of its relevant input documents (see Figure 2).

6.1.9 The references, if any, made by the HPD requirements specification to other documents shall be precise so as to be unambiguous.

6.1.10 *For class 2, the notations, rules and/or standards used to describe the HPD requirements specification should contribute to its clarity and precision, and should be chosen taking into account those used in the inputs and those chosen for the design and implementation of the HPD.*

Since any particular specification format does not always allow a clear, precise and verifiable expression of all specification needs, different and complementary formats may be used in the same HPD requirements specification.

6.2 Functional aspects of the requirements specification

6.2.1 General

The present subclause describes the content of the requirements specification directly related to the functional needs.

6.2.2 The requirements specification shall specify:

a) the functions to be provided by the HPD,

b) the HPD's different modes, and the corresponding conditions of transition, including power-on, initialization and, when appropriate, the definition of safe states,

c) the HPD's interfaces and interactions with its environment (operators and other I&C components), including the roles, protocols, types, data formats, bit numbering, ranges and constraints of inputs and outputs,

d) any HPD parameters which can be modified manually during operation, and their roles,

e) the HPD's performance and, when appropriate, response time,

f) what the HPD shall not do or shall avoid, when appropriate,

g) the constraints or rules to be respected by HPD design and implementation for the sake of verifiability and robustness.

6.2.3 The HPD requirements specification should also specify the conditions of use (for example, the demand load), in particular the worst case conditions, provided to the HPD by its environment.

6.2.4 The HPD requirements specification should state the HPD quality objectives to be respected by HPD design and implementation for the sake of correctness and robustness.

6.2.5 The HPD requirements specification shall identify the safety category associated with the specified functions and the requirements.

6.2.6 *For class 2, the HPD requirements specification should avoid unnecessary functionality with respect to the system or subsystem-level requirements.*

In principle, it is preferable that the HPDs do not have more capabilities than required so as to minimise complexity. However, because current industrial practice is based on the use of pre-developed components, the inclusion of non-required capability may be justified.

Concerning requirements 6.2.2, 6.2.3 and 6.2.6, functions, interfaces and performance requirements might depend on the mode of operation, on the values of the parameters, on the configuration data and on the conditions provided to the HPD.

6.3 Fault detection and fault tolerance

The HPD requirements specification shall specify the modes of operation required when errors or failures are detected.

For example, this might include constraints:

a) to enhance the ability of the HPD and of the I&C system to tolerate faults (due to single event upsets, for example), to detect and signal errors and failures to operators, to perform actions or to take specified modes of operation following detected failures;

b) to give confidence that operator mistakes and failures of other systems or equipment with which the HPD interacts or shares resources will not lead to unacceptable effects.

6.4 Requirements capture using Electronic System Level tools

6.4.1 General

This document does not prescribe a specific method to capture the HPD requirements. If they are captured using tools at Electronic System Level (ESL, see Annex A), then the requirements of 6.4.2 and 6.4.3 apply to these tools and to their use.

In the case of use of ESL tools, if the requirement specification language is similar to implementation languages, requirement 6.1.5. (separation between what has to be done (the requirement) and how it is done (the design)) may be replaced by alternate means, e.g. comments to specify inputs, outputs and algorithms.

6.4.2 Requirements on the formalism of tools used at ESL level

6.4.2.1 When the HPD requirements are captured using an ESL tool:

a) this tool shall offer a formalism with a rigorous semantics and clarity (standardization of structure and presentation, modularity, sound comments);

b) the formalism used in the ESL tool shall be understandable for all participants;

c) if the tool offers flexible mechanisms to redefine functions and operators, then the actual characteristics of any given element should be clear to any involved participants.

6.4.2.2 The languages used at ESL level should allow taking due account of the system architecture, e.g. enable the assignment of functions to components, and support any fault tolerant design features.

6.4.3 Interface with design tools

The semantics of the languages used to express the requirements specification at ESL level might differ from the semantics of the HDL languages used during design. Examples where discrepancies might occur are in the interpretation of parallelism, the management of overflows, or the encoding of types and finite state machines.

a) If the semantics of the language used to express the requirements specification at ESL level differs from the semantics of the other languages used in the project, then discrepancies shall be identified for each involved item of the requirements specification;

b) each occurrence of a discrepancy within the requirements specification shall be documented. A generic list of discrepancies between the involved languages is a useful reference, but is not enough to clarify the requirements specification.

7 Acceptance process for programmable integrated circuits, native blocks and Pre-Developed Blocks

7.1 General

Subclause 6.2.3.2 of IEC 61513:2011 provides general requirements for the selection of pre-existing components (not necessarily HPD components). The present subclause provides additional requirements specific, or of particular importance, to HPDs.

7.2 Acceptance process for programmable integrated circuits and included native blocks

7.2.1 General

The general approach for the selection and acceptance of blank programmable integrated circuits and their included native blocks is given in Figure 3.

Some native blocks represent the configurable resources of the Integrated Circuit (IC) and are generally used in every HPD design. Such native blocks are accepted as part of the IC during the IC suitability analysis.

Other native blocks might represent higher-level design features such as multipliers and serial transmission controllers. Such native blocks are optional in that they have the defining feature that it is possible to not instantiate them in the HPD design. Such native blocks, if used, are to be evaluated and accepted according to PDB acceptance criteria (see 7.3).

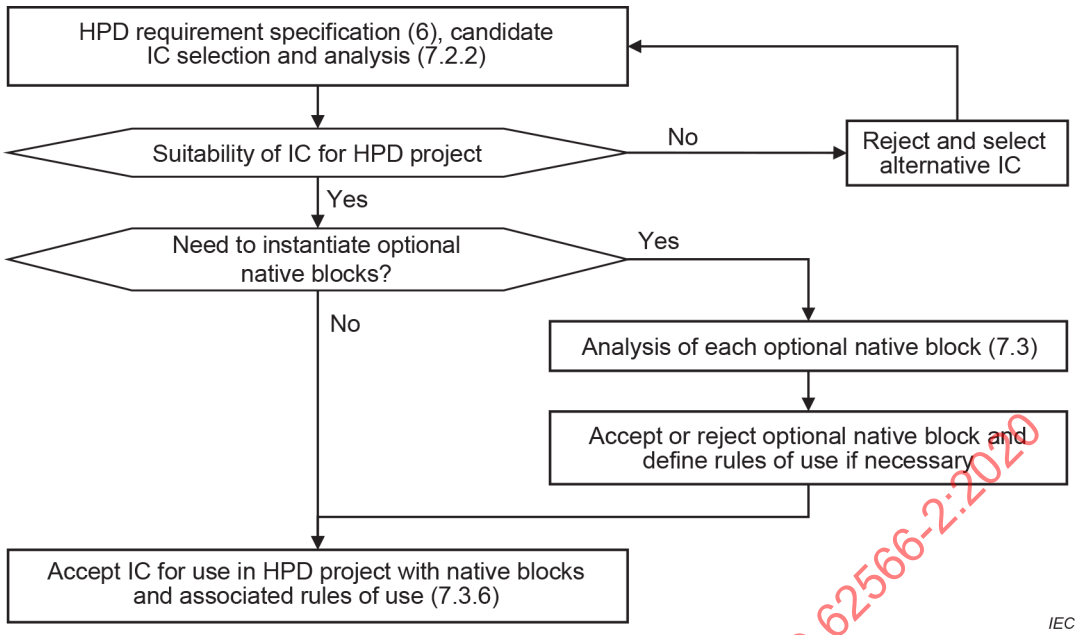


Figure 3 – Overview of selection and acceptance process for blank Integrated Circuits and native blocks

7.2.2 Integrated Circuit acceptance

7.2.2.1 The candidate integrated circuit shall be analysed with respect to the requirements of the HPD.

7.2.2.2 The analysis should consider the following properties of the candidate integrated circuit:

a) IC technology (CPLD, FPGA, etc.);
b) Configuration technology (antifuse, flash, SRAM, etc.);
c) Number of logic elements, resource utilization margin and suitability of internal architecture and native blocks;
d) Number of input/output pins, form factor and circuit packaging (quad flat package, ball grid array, etc.);
e) Power consumption;
f) Maximum operating frequency;
g) Hardware reliability and duration of retention of programmed configuration;
h) Environmental conditions;
i) Suitability of development tools with respect to the requirements of Clause 15 of the present standard.

Other factors which could be considered during the selection of candidate ICs are the quality management system of the manufacturer, the estimated future availability of the IC and the operational experience that it has.

7.2.2.3 If the candidate integrated circuit is not suitable for the given application then it shall be rejected and an alternative shall be found.

7.2.2.4 If one or more optional native blocks of the chosen IC are to be instantiated in the design of the HPD, then each one shall be accepted for use according to 7.3 of the present standard.

The refusal of the use of an optional native block in the HPD design does not imply the rejection of the IC itself.

7.3 Acceptance process for PDBs

7.3.1 General

The general approach for the selection and acceptance of PDBs is given in Figure 4.

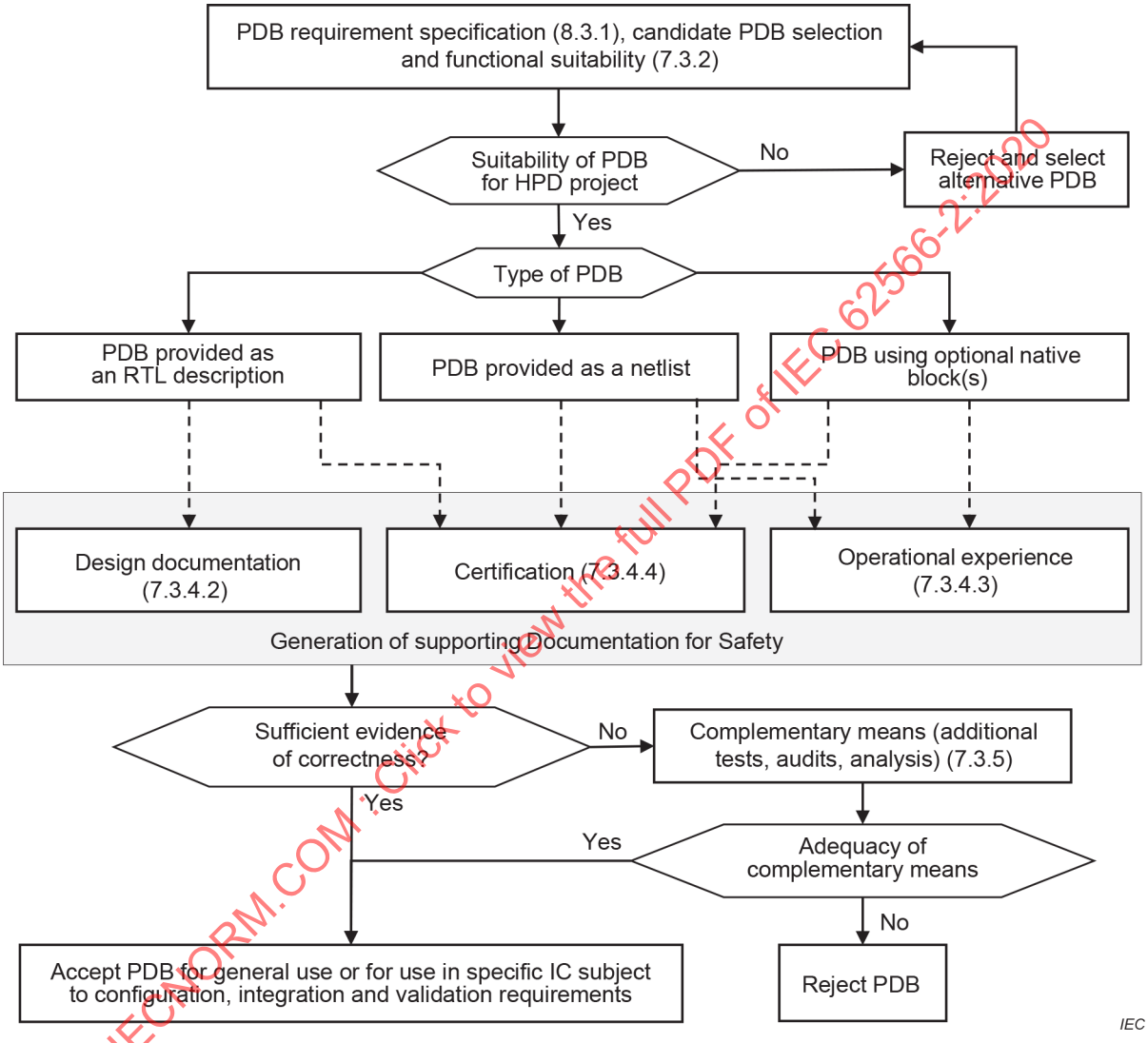


Figure 4 – Overview of selection and acceptance process for PDBs

7.3.2 PDB functional suitability

7.3.2.1 General

The objective of the present subclause is to ensure that the PDB is well-suited with respect to the PDB requirements.

7.3.2.2 The documentation for safety (7.3.3) of PDBs shall be evaluated with respect to the HPD requirements specification (Clause 6) and the PDB requirements specification (8.3.1.2). Inconsistencies shall be resolved.

7.3.2.3 *For class 2, the functions of the PDB which are not required to support the PDB requirements specification should be identified. A justification that these functions do not have a detrimental effect on safety should be provided*.

7.3.3 Documentation for safety of PDBs

7.3.3.1 The PDB documentation shall detail how designers are to use the PDBs consistently with their specifications and design characteristics.

In this standard, the corresponding document or set of documents is called documentation for safety. When the PDB is a part of an equipment or equipment family, this documentation may be a part of the documentation for safety of the equipment or equipment family.

Documentation for safety generally comprises more than the user documentation provided by the supplier of the PDB. For example, it might include information obtained from the PDB design, additional tests, measurements and/or analyses, and from operational experience.

7.3.3.2 Documentation for safety shall include a description of:

a) the functions provided;

b) the external interfaces;

c) the roles, types, formats, ranges and constraints of inputs, outputs, exception signals, parameters and configuration data, information concerning finite state machines, when appropriate;

d) the different modes of operation and the corresponding conditions of transition;

e) any constraint to be respected when using the PDB.

7.3.3.3 *For class 3, the documentation for safety should provide information regarding the performance (for example, in terms of response time) of the functions*.

7.3.3.4 *For class 2, when applicable, the constraints to be respected when using the PDB (see 7.3.3.2) should give adequate confidence in the correctness of the PDB and of the system design*.

7.3.3.5 *For class 2, the documentation for safety shall provide information regarding the performance (for example, in terms of response time) of the functions*.

7.3.4 Generation of supporting documentation for safety

7.3.4.1 General

7.3.4.1.1 A documented analysis of each PDB used in the HPD shall demonstrate that it fulfils the requirements allocated to it.

7.3.4.1.2 Evidence of correctness of PDBs with respect to their documentation for safety shall be provided.

7.3.4.1.3 PDBs provided in the form of a Register Transfer Level (RTL) description should be selected and approved through either a design documentation review (7.3.4.2) or through certification (7.3.4.4).

7.3.4.1.4 PDBs provided in the form of a netlist should be selected and approved through either an operational experience review (7.3.4.3) or through certification (7.3.4.4).

7.3.4.1.5 Optional native blocks should be selected and approved through either an operational experience review (7.3.4.3) or through certification (7.3.4.4).

7.3.4.1.6 In cases where complete evidence of correctness of PDBs cannot be provided through either a design documentation review, operational experience review or certification, or a combination of these methods, then complementary means shall be invoked according to 7.3.5 of the present standard.

7.3.4.1.7 The documentation shall specify if the PDB is subject to a generic acceptance, valid for use in any IC, or if the PDB is accepted for use only in the IC used within the HPD project.

7.3.4.2 Design documentation review

7.3.4.2.1 General

A design documentation review may be used to support the justification of correctness of PDBs under the following conditions:

7.3.4.2.2 The design documentation review shall demonstrate that the PDB is compliant with the requirements allocated to it as defined in its documentation for safety.

7.3.4.2.3 *For class 2, the analysis of the documentation shall demonstrate that any functions and modes of the pre-developed item not used within the HPD do not impede the used ones.*

7.3.4.3 Operating experience review

Relevant, sufficient and positive operational experience may be used to support the justification of correctness of PDBs under the following conditions:

If the operating experience is invoked then:

a) the analysis of the operating experience shall demonstrate that:
   i) its volume is commensurate to the reliability requirements,
   ii) it has been collected in operating conditions equivalent to those in which the PDB will be used,
   iii) the actual use of the PDB has been traced at the level of detail generally required by this document for the documentation;

b) for class 2, the means and procedures used to collect the operating experience shall ensure that any PDB failure that occurred in the analysed operation is recorded in such detail that a technical analysis can identify its cause as far as possible;

c) for class 2, evidence shall be provided that any identified failures of the candidate PDB were correctly analysed and the corresponding PDB faults have been either corrected or that there is an applicable constraint detailed in the documentation for safety;

d) for class 2, a documented technical analysis shall justify that all interactions of the PDB with its environment are included within those covered by the operating experience;

e) for class 2, the operating experience taken into consideration shall correspond to precisely identified versions of the PDB and, when this item is specific to equipment, of the equipment in which it operates;

f) for class 2, the operating experience should address the specific version of the pre-developed item or its sub-part used in the HPD; otherwise the differences between versions shall be analysed to demonstrate that the operating experience is relevant for the intended version.

7.3.4.4 Certification of PDBs

7.3.4.4.1 General

The evidence provided by certification of PDBs may support the justification of correctness of PDBs under the following conditions:

7.3.4.4.2 The safety standard used for the certification of the PDB shall address explicitly the PDB development process.

7.3.4.4.3 The certification taken into consideration shall be documented.

7.3.4.4.4 The precise identification of the certified PDB shall be documented. If it was certified as a part of a larger product (for example, as a part of an equipment or equipment family), the precise identification of this product shall also be documented.

7.3.4.4.5 *For class 2, the evidence supporting the certification shall be assessable, in particular:*

a) the conditions (for example, the conditions of use and the assumptions) of the certification;

b) the methods and tools used for the certification;

c) the results obtained (for example, the properties and/or measurements certified).

7.3.4.4.6 *For class 2, the relevance of these conditions and results to correctness and to the I&C system shall be justified.*

7.3.4.4.7 *For class 2, the effectiveness of the methods and tools used for the certification should be justified.*

7.3.4.4.8 *For class 2, the certifying authority shall be identified and shall be competent for the properties and/or measurements certified.*

7.3.4.4.9 *For class 2, the version of the certified PDB should be the same as the one used in the I&C system; otherwise the differences between versions shall be analysed to demonstrate that the certification is relevant for the intended version.*

7.3.5 Complementary means

7.3.5.1 In cases where the PDB cannot be completely justified according to design documentation review, operational experience review or certification, or a combination of these methods, complementary means (for example additional testing, analysis, audits) shall be used to support the justification of correctness of PDBs with an equivalent level of confidence.

7.3.5.2 When using complementary means for providing evidence of correctness, the acceptance criteria should be specified and justified in early stages of the HPD development. These criteria should be justified considering the requirements of this standard the compliance to which has not been adequately established.

7.3.5.3 In cases where complementary means do not provide adequate justification, the PDB shall be rejected.

7.3.6 Rules of use

7.3.6.1 General

The use of functions or modes of the PDBs that are required to implement the HPD might be constrained by rules in order to improve design properties such as safety or testability.

7.3.6.2 If the pre-developed item includes functions, configurations or operating modes that are not required to be implemented in the HPD, rules should be defined to prohibit the use of such functions and modes.

7.3.6.3 If rules of use are established:

a) they shall be documented,

b) the verification plan shall give assurance that their fulfilment is verified during the project.

7.3.7 Modification for acceptance

7.3.7.1 General

In general, modifications of PDBs by the HPD designer are only possible for PDBs supplied in the form of HDL source code.

7.3.7.2 If modifications of the PDB are necessary to achieve acceptance, they shall be specified, designed, implemented and verified.

7.3.7.3 These modifications shall be performed and documented in accordance with the requirements of this document regarding project structure and management, quality, specification of requirements, design, implementation and verification.

8 HPD design and implementation

8.1 General

The present clause provides requirements and recommendations based on good practice for design and implementation, in order to meet appropriate safety features such as fault-free as possible and amenability to verification.

The HPD design and implementation phases shall be documented.

The corresponding document or set of documents is composed of the HPD design specification (see 8.3.6) and the HPD implementation documentation (see 8.4.7).

8.2 Hardware Description Languages (HDL) and related tools

8.2.1 General

Even though the use of specific languages and tools cannot be required, the following may be considered as common basic rules for languages and tools used for the design and implementation of HPDs for class 2 and 3 systems.

8.2.2 Design and implementation should use Hardware Description Languages (HDL) and tools for simulation, synthesis, place and route.

NOTE When properly chosen and used, these tools improve essential aspects such as understandability of the descriptions, management of electrical and temporal constraints, verification, adequateness of coverage criteria, and documentation.

8.2.3 Even if 8.2.2 is not fulfilled, any documentation, analysis, or verification required by this document shall be provided.

8.2.4 The languages used:

a) shall follow strict (or well-defined) semantic and syntax rules;

b) shall have a syntax completely and clearly defined and documented;

c) should comply with a recognized Standard (e.g. IEEE 1076 for VHDL, IEEE 1364 for Verilog or IEEE 1800 for SystemVerilog).

8.3 Design

8.3.1 General

8.3.1.1 The inputs to the HPD design process shall include the HPD requirements specification.

They might also include other documents, such as project specific constraints, and/or applicable rules and standards.

8.3.1.2 The design phase shall produce

a) a description of the overall organisation of the HPD;

b) the identification of the integrated circuit to be used (the selection and acceptance of the integrated circuit to be used is to be based on the HPD requirements specification and carried out according to the requirements of 7.2 of the present standard);

c) a design description of the overall operation of the HPD under the conditions and operating modes required by the HPD requirements specification;

d) the requirements allocated to each block used in the design. For the blocks to be implemented using PDBs, these requirements are to be used for the selection and acceptance of PDBs according to the requirements of 7.3 of the present standard. For new blocks, these requirements are to be used for new developments;

8.3.1.3 The overall design description should provide information regarding:

a) The descriptions and configurations of RTL modules developed within the HPD project;

b) The main internal and external interfaces, including communication interfaces and links between HPD components and PDBs.

8.3.1.4 The description of the overall operation should provide information regarding:

a) Interactions, communication protocols and information flows;

b) Sequencing and timing constraints;

c) Use of resources;

d) Synchronisation between different design modules.

8.3.1.5 The HPD design shall be produced with the goal of ensuring modularity, testability and maintainability.

8.3.1.6 The HPD design specification shall provide evidence that the HPD requirements specification statements important to safety are taken into account in all specified conditions.

8.3.1.7 *For class 3, the HPD design specification should provide rules for HPD implementation.*

8.3.1.8 *For class 2, a top-down design approach should be preferred.*

8.3.1.9 *For class 2, the HPD design specification shall include the detailed design (RTL description), of any modules implemented in HDL.*

8.3.1.10 For class 2, for each module implemented in HDL, the HPD design specification should specify:

a) The functions to be provided by the module including its external interfaces, inputs, outputs and configuration data,

b) The requirements of the module regarding its environment,

c) Any relevant implementation constraints,

d) Any other information that the users of the module shall be aware of.

8.3.1.11 *For class 2, the HPD design specification shall provide information enabling correct predictions regarding the key safety significant elements of system performance, including notably the maximum response times of applications.*

Such information may be provided in the form of data, formulae and/or models.

8.3.1.12 *For class 2, the design should aim to ease verification.*

8.3.1.13 *For class 2, the HPD design specification shall provide rules for HPD implementation.*

8.3.1.14 *For class 2, non-compliances with design rules should be justified.*

8.3.2 Fault detection

8.3.2.1 The design shall take into account the arrangements selected in the requirements specification to detect the faults and to elaborate the corresponding information within the HPD.

8.3.2.2 The HPD design specification shall ensure that the adverse side effects of HPD errors and failures are cleared prior to returning to a normal mode of operation.

8.3.2.3 *For class 2, on fault detection, the HPD should behave in accordance with the corresponding specified requirements, in particular in ensuring that errors or failures do not propagate beyond the specified limits.*

8.3.2.4 *For class 2, the HPD design specification and the system design documentation shall state and justify the measures taken to mitigate the effects of the known or anticipated failure modes of any PDBs for which complementary means for providing evidence of correctness have been used.*

8.3.3 Language and coding rules

8.3.3.1 The list given below contains strongly recommended design considerations and techniques. However the list is not considered to be all-encompassing and parts might change with technology.

a) only synthesizable features of the language should be used in the design of the HPD. The test and simulation environment (9.2) may use all language features. Any native blocks (see 3.26) which are already synthesized and routed in the pre-developed integrated circuit may be instantiated as they are, if they comply with Clause 7;

b) dedicated resources or design features (e.g. predefined clock trees and clock conditioning circuits, power rails, reset trees, etc.) should be used when appropriate;

c) coding rules should cover all relevant aspects, in particular naming of modules and signals, use of the structuring features (such as packages, functions, procedures, project libraries, instantiation), organization of the computations on critical paths, organization of processes, recommended constructs and forbidden constructs;

d) functions using side effects ("impure") should be forbidden in the design description. (Rationale: such a function can return different values when called several times with the same parameters. It is therefore very difficult to test and verify, as it breaks the basic concept of a function, and in fact of determinism);

NOTE 1 An impure function might also have side effects such as modifying objects out of their scope.

e) constructs that could lead to differences between simulated and synthesized behaviours should be forbidden. Depending on the language used, examples of such constructs might be the incomplete or conflicting assignments, use of "don't care" character in comparisons, comparisons (higher or lower) involving enumerated types. (Rationale: simulation is an important verification method. If simulated and synthesized behaviours differ, then the verification chain is broken);

f) signals and variables should not be initialized at their declaration in the RTL description, but by an explicit mechanism such as reset (rationale: initialization in HDL might lead to differences between simulated and synthesized behaviours);

g) use of explicit delays should be forbidden in the design description, as such delays lead to differences between simulated and synthesized behaviours;

NOTE 2 This does not forbid the existence of delays at system level or in the Requirements of the HPD. It means that such delays cannot be implemented by a “delay” or “after” instruction in HDL, but e.g. by counters or shift registers.

h) creation of delays by means of combinatorial gates or by depending upon propagation delays along wires should be forbidden in the design description. If such design cannot be avoided, Static Timing Analyses (STA) shall be done to justify the usage of such design (Rationale: such delays are not stable over parameters such as temperature, voltage, or from one part to another, or from one area of the die to another);

i) the types of the interface signals of the HPD should be defined in a clear and non-ambiguous way, preferably standardized, independently of any tool or micro-electronic technology;

j) HDL level definitions should not allow different interpretations, to avoid variations when compiled under different conditions. E.g. inputs / outputs of the HPD should be explicitly assigned to known pins.

NOTE 3 This subclause does not apply to the design of library components, which are built to be instantiated in different locations of future designs with different input/output allocations.

To design HDL code that can be transferred between different technologies it is necessary for the pin allocation to be defined in a constraints file, not in the HDL code. Language features such as templates in VHDL-2008 might help doing this.

8.3.3.2 *For class 2, in order to make the design more understandable and to reduce the potential for differences between the simulated and the synthesized behaviours*:

a) a set of strict design rules which reflect the latest knowledge in terms of design safety and reliability shall be required by the quality plan and established;

b) the compliance with those design rules shall be enforced by appropriate means (e.g. review, tooling, etc.).

8.3.4 Synchronous vs. asynchronous design

8.3.4.1 General

Synchronous design consists of enforcing the change in the state of the internal registers and of the outputs simultaneously only at times defined by a clock. It favours a modular and understandable design, it minimizes the potential for wrong behaviours due to glitches, and it favours the best use of synthesis and verification tools.

8.3.4.2 In order to facilitate stable, robust, and clearly structured designs:

a) a synchronous architecture should be used;

b) non-compliances shall be justified.

8.3.4.3 The design shall ensure that signals at asynchronous interfaces are synchronized.

8.3.4.4 If an asynchronous architecture is used, a documented analysis of all paths shall demonstrate that the outputs comply with the requirements specification (Clause 6) and that there is no adverse glitch or metastability.

8.3.4.5 If an asynchronous architecture is used, it shall be demonstrated that an equivalent synchronous architecture cannot achieve the same goals.

8.3.4.6 The HPD behaviour shall not be subject to the actual values of the internal propagation delays along wires and through gates.

8.3.5 Power Management

8.3.5.1 *For class 2, the behaviour of the HPD during power-up/start-up, power-down and sudden loss of power shall comply with the HPD requirements specification.*

8.3.6 Design documentation

8.3.6.1 At the end of the design phase the corresponding documentation shall be completed.

8.3.6.2 The design documentation shall define the variant actually used for each instantiation of each library component, to avoid ambiguities when variants with different speeds or electrical characteristics exist.

8.3.6.3 The design documentation shall include the precise identification and configuration of native blocks and PDBs.

8.3.6.4 The HPD design specification documentation shall be a reference for HPD implementation and integration, and for possible HPD modifications.

8.3.6.5 *For class 2, the HPD design specification shall present the HPD design clearly and precisely.*

For class 2, the main approach recommended by this standard is a top-down approach, but some documents might also give information that highlights how aspects of particular importance (for example, tolerance to failures) are taken into account across the HPD or across the I&C system.

8.3.6.6 *For class 2, the design documentation shall include information allowing estimated maximum response times to be determined.*

8.4 Implementation

8.4.1 Products

8.4.1.1 The implementation shall generate all information necessary to produce the HPD in a systematic way and to verify that each produced part complies with the design.

8.4.1.2 It shall be verified that only the native blocks and PDBs which have been accepted according to the requirements of Clause 7.3 have been implemented.

8.4.1.3 *For class 2, the implementation shall produce timing information to supplement the RTL description ("back-annotations") in order to precisely simulate the temporal behaviour taking into account all delays associated with gates and wires.*

8.4.1.4 *For class 2, the back-annotated description shall be usable in the test-bench (9.1) and, when appropriate, in higher level tools such as board level simulation.*

8.4.2 Files of parameters and constraints

8.4.2.1 The files of parameters and constraints shall be documented, verified and placed under configuration management.

8.4.3 Post-route analyses

8.4.3.1 A post-route analysis shall demonstrate the compliance of the design and implementation with the technology rules defined by the suppliers of the design and implementation tools and of the micro-electronic technology.

8.4.4 Redundancies introduced or removed by the tools

8.4.4.1 The redundancies introduced or removed by the tools to meet timing or technology constraints shall be analysed in order to ensure that the fulfilment of HPD requirements is not compromised.

8.4.4.2 *For class 3, it should be demonstrated that the logic optimization performed by the tools has not removed fault detection and tolerance mechanisms such as redundancies or processing of cases normally unreachable.*

8.4.4.3 *For class 2, as redundancies introduce new states, these new states shall be analysed to demonstrate that the safe behaviour of the design cannot be affected.*

8.4.4.4 *For class 2, it shall be demonstrated that the logic optimization performed by the tools has not removed fault detection and tolerance mechanisms such as redundancies or processing of cases normally unreachable.*

8.4.5 Finite state machines

8.4.5.1 *For class 2, the robustness of the final implementation of finite state machines shall be analysed.*

8.4.5.2 *For class 2, finite state machines shall not have dead states other than those possibly specified in the HPD requirement specification.*

NOTE A dead state is a state from which the finite state machine cannot reach any other state.

8.4.5.3 *For class 2, the potential additional states introduced by some encoding methods (such as "one-hot") shall be taken into account in failure analysis.*

NOTE "one-hot" encoding uses one flip-flop per state to be represented; each particular state is represented by one specific flip-flop set to "true" and all others set to "false". Thus, only combinations with exactly one flip-flop set to "true" are valid. In case of failure, several flip-flops could be simultaneously set to "true", which would correspond to additional, undefined states.

8.4.6 Static Timing Analysis

8.4.6.1 A Static Timing Analysis (STA) shall be performed and documented for worst and best cases to calculate the margins, taking into account the timing information provided by the technology libraries and all relevant design and implementation tools.

8.4.6.2 *For class 2, if paths are excluded from STA (because seen as "false paths") or declared as multi-cycle paths, this decision shall be justified and documented.*

8.4.6.3 *For class 2, STA shall demonstrate that the frequency of each clocked block is compatible with all non-excluded paths (see subclause 8.4.6.2) with sufficient margin within the specified variability of the micro-electronic technology.*

8.4.6.4 *For class 2, the effect of the clock skew on critical structures such as shift registers shall be analysed and documented.*

NOTE The clock skew is the amount of time between the arrivals of the clock signal at different locations.

8.4.7 Implementation documentation

8.4.7.1 At the end of the implementation phase the corresponding documentation shall be completed.

8.4.7.2 The implementation documentation should include:

a) the gate-level description of the HPD, usable in the same test-bench as used at RTL level, including the identities and the versions of the various modules and elements used within the HPD design;

b) the technology specific description (e.g. “programming file”) necessary to program the HPD and to test each part (13.3);

c) the constraints and parameters provided to the tools,

d) any redundancy added or removed during implementation.

8.4.7.3 *For class 2 the implementation documentation shall describe*:

a) the back-annotations that take into account all delays associated with gates and wires;

b) the timings (such as frequency, set-up and hold times, rise and fall times, propagation times) predicted by the tools unless they are already defined in the datasheet;

c) the constraints and parameters provided to the tools;

d) any redundancy added or removed during implementation.

8.4.7.4 *For class 2, the documentation shall be detailed enough to allow an engineer not involved in the project to run the synthesis, place and route tools and get the same results (HPD and verification output), as well as to verify the completeness and the correctness of the post-route analyses*.

8.5 System level tools and automated code generation

8.5.1 General

The requirements of the different components of a system may be captured using ESL tools that provide a textual or graphical description.

8.5.2 The parts of the HPD requirements specification and/or of the HPD design specification that are used to generate an RTL description by automated means shall be considered to be written using ESL languages.

8.5.3 The generated products shall not be modified by direct manual action on the products.

8.5.4 The products shall be regenerated if anything has to be modified, for example with respect to findings from verification or review activities.

8.5.5 *For class 2, if a requirements specification written in an ESL language is used to automatically generate an RTL description of the HPD or a part of it*:

a) The generated RTL description shall be verified to be functionally correct and consistent with respect to the HPD requirement specification,

b) the generated description shall be straightforward and avoid unnecessary complexity;

c) this description should allow the behaviour of the device to be easily understood so that errors and ambiguities can be identified promptly by the HPD design engineers.

8.5.6 *For class 2, RTL descriptions generated using ESL design tools should conform to documented rules designed to improve clarity, modifiability and testability*.

9 HPD integration and testing

9.1 General

The HPD integration and testing described by the present clause is completely distinct from the HPD aspects of system-level integration and validation described by Clauses 10 and 11 respectively. The activities described by the present clause concern functional testing by means

of simulation of the HPD design at various stages of integration in a software environment before implementation onto the integrated circuit.

9.2 Test-benches for HPD functional simulation

9.2.1 A HPD integration and testing plan shall define the integration and testing strategy to be employed.

9.2.2 A HPD test programme shall be developed and documented according to the HPD integration and testing plan. As needed, this test programme might consist of several different test benches, each with a different scope and objective, e.g. some test-benches might be dedicated to module-level simulations and one or more to top-level simulations.

9.2.3 The team that writes the HPD test programme shall include at least one person who did not participate in the design and implementation.

9.2.4 The test programme shall include test-benches which exercise all the features mentioned in the HPD Requirement Specification such as functions, modes, finite state machines, algorithms, protocols and PDBs.

9.2.5 If PDBs are subject to individual functional validation as part of complementary means (see 7.3.5), the simulations and tests carried out shall demonstrate that the PDB behaves as is specified by its documentation for safety.

In cases where PDBs are provided in the form of RTL or a netlist, then their behaviour can be simulated in the same way as modules designed using general purpose HDL or ESL tools. In cases where PDBs use optional native blocks, then vendor-specific simulation files can be provided for the purposes of functional simulation and validation.

9.2.6 Functional validation tests shall be developed with respect to the functional requirements of the object under test and not solely to the internal structure of the object.

9.2.7 *For class 2, in test cases where accelerated simulation techniques are used, justifications should be provided to ensure the representativeness and the coverage of the tests.*

9.3 Test coverage

9.3.1 *For class 2, appropriate test coverage criteria shall be selected and documented according to the type of component under test.*

Such criteria might be related, for example, to instructions, decisions, expressions, paths, finite state machines, or processes. According to the type of component under test, certain coverage criteria might not be appropriate. For example, in cases where PDBs are provided in the form of optional native blocks, it might not be possible to define structural coverage criteria due to a lack of knowledge about the internal implementation of the PDB. This means that other types of coverage criteria might be chosen for class 2 (functional coverage, for example).

NOTE A path is a particular sequence of branches taken when executing the code.

9.3.2 *For class 2, a documented analysis of the test coverage criteria shall demonstrate that they are sufficient regarding the HPD requirement specification and design/implementation characteristics, and that the test-bench provides sufficient observability to make a pass/fail decision for each covered element.*

9.3.3 *For class 2, the coverage of each function by self-supervision shall be analysed with respect to the fault detection requirements (see 6.3) taking into account the effects the tools might have on the actual topology.*

9.4 Test execution

9.4.1 Tests shall be performed using the test-benches following the design phase on the RTL description, in order to confirm its correctness.

9.4.2 Test results (values, sequences, and timings) shall be documented.

9.4.3 For discrepancies that are determined to be unacceptable, the HPD design or test-benches shall be modified as required and the HPD integration and testing phase shall be repeated for impacted parts of the HPD design.

9.4.4 The sufficiency of the repeated parts of the HPD integration and testing phase shall be justified with respect to the modifications made to the HPD design or test-benches.

9.4.5 *For class 3, a documented analysis of any discrepancy should decide whether it is acceptable or not.*

9.4.6 *For class 2, tests shall be performed after the implementation phase to confirm that the post route description complies with the timing constraints in the best (shortest propagation time) and worst (longest propagation time) conditions, taking account of the timing information provided by the tools and libraries (back-annotations).*

9.4.7 *For class 2, a documented analysis of any discrepancy shall decide whether it is acceptable or not.*

10 HPD aspects of system integration

10.1 General

The integration of HPDs into the system is considered part of the system integration according to IEC 61513. The present clause complements subclauses 6.2.5, 6.3.4 and 6.4.5 of IEC 61513:2011 by providing additional requirements specific, or of particular importance, to HPDs.

10.2 Requirements

10.2.1 HPD integration and/or inspections shall show that the integrated system and the HPD:

a) comply with the design provisions that ensure the satisfaction of the HPD requirements specification statements identified as important to safety;

b) satisfy the constraints stated by the HPD requirements specification with respect to correctness and robustness.

10.2.2 HPD integration shall be performed according to the provisions of the system integration plan or of a HPD integration plan.

10.2.3 Records of the application of the plan used for HPD integration shall be produced, for example, test results. In the event of HPD or system modifications being required, it shall be possible to repeat all, or a subset of, the integration tests to evaluate the extent of possible changes in behaviour.

10.2.4 *For class 3, traceability should be provided between the HPD design specification and the corresponding integration tests.*

10.2.5 *For class 2, when HPD validation testing is not considered to have sufficiently exercised the HPD, sufficient confidence of correct operation shall be obtained, either by performing additional HPD integration testing or by other means.*

10.2.6 *For class 2, traceability shall be provided between the HPD design specification and the corresponding integration tests*.

11 HPD aspects of system validation

11.1 General

Aspects of HPD functionality are tested during system validation. The present clause complements 6.2.6, 6.3.5 and 6.4.6 of IEC 61513:2011 by providing additional requirements specific, or of particular importance, to HPDs. Where discrepancies are revealed, validation may be continued with justification or may be stopped to correct the discrepancy before revalidation.

11.2 Requirements

11.2.1 HPD validation shall be performed according to the provisions of a plan that is preferably the system validation plan or a HPD validation plan.

11.2.2 The plan used for HPD validation shall specify the validation actions to be performed, and shall show that all the HPD aspects of system functionality, performance and interface are correctly taken into account. It shall also specify the main phases of the HPD validation (for example, an off-site phase followed by an on-site phase) and the corresponding means, methods and tools to be used.

11.2.3 Records of the application of the plan used for HPD validation shall be produced. In the event of HPD or system modifications being required, it shall be possible to repeat all, or a subset of, the validation tests to evaluate the extent of possible changes in behaviour.

11.2.4 These records shall document the configuration of the HPD being validated and the configuration of the validation environment (for example, the hardware environment and the tools, if any).

11.2.5 *For class 3, HPD validation shall show that, in the target I&C system, the integrated HPD conforms to the functional, performance and interface requirements that are identified as important to safety. This shall include justification that*:

a) the specified HPD functions important to safety are correctly performed when their parameters and inputs are in the ranges specified by the HPD requirements specification, in the conditions of use defined in the HPD requirements specification;

b) the system functions important to safety to which the HPD contributes are correctly performed in the conditions of use defined in the system requirements specification;

c) the HPD provides defences as required by the HPD requirements specification against operator mistakes and failures of other systems and equipment;

d) the HPD functions correctly in its different modes of operation;

e) the plant engineering data used by, or integrated in, the I&C system to implement functions important to safety is correct; in particular, the validation of the HPD shall show that this data defines the interface between the systems and equipment of the plant with which the HPD interacts or shares resources.

The validation tests are normally performed with the HPD integrated in the target I&C system. It may be acceptable to use a platform representative of the target I&C system to perform validation tests if adequate justification is provided.

The conditions of use of functions important to safety may include operation during high communication loading.

11.2.6 For class 3, the plan used for HPD validation should provide traceability between the HPD requirements specification and the corresponding validation actions.

11.2.7 For class 3, the results of HPD validation should be auditable by persons competent in the subjects addressed but not directly engaged in the validation process.

11.2.8 For class 2, HPD validation shall show that, in the target I&C system, the integrated HPD conforms to each functional, performance and interface statement of the HPD requirements specification, and contributes as designed to the satisfaction of the system requirements specification. This shall include justification that:

a) the specified HPD functions are correctly performed when their parameters and inputs are in the ranges specified by the HPD requirements specification, in the conditions of use defined in the HPD requirements specification;

b) the system functions to which the HPD contributes are correctly performed in the conditions of use defined in the system requirements specification;

c) the HPD provides defences as required by the HPD requirements specification against operator mistakes and failures of other systems and equipment;

d) the HPD functions correctly in its different modes of operation;

e) the plant engineering data used by, or integrated in, the I&C system is correct; in particular, the validation of the HPD shall show that this data defines the interface between the systems and equipment of the plant with which the HPD interacts or shares resources.

f) defences required to be performed by the system in the system requirements specification against operator mistakes and failures of other systems and equipment, and to which the HPD contributes, are correctly provided;

The validation tests are normally performed with the HPD integrated in the target I&C system. It may be acceptable to use a platform representative of the target I&C system to perform validation tests if adequate justification is provided.

The conditions of use of functions important to safety may include the concurrent operation of functions not important to safety notably the operation during high communication loading.

11.2.9 *For class 2, the plan used for HPD validation shall provide traceability between the HPD requirements specification and the corresponding validation actions*.

11.2.10 *For class 2, the results of HPD validation shall be auditable by persons competent in the subjects addressed but not directly engaged in the validation process*.

12 Modification

12.1 Modification of the requirements, design or implementation

12.1.1 General

The decision to proceed with HPD modifications depends upon their impact on the I&C system. Therefore, they are subject to the requirements of 6.2.8 and 6.4.7 of IEC 61513:2011. The present subclause provides additional requirements specific, or of particular importance, to HPDs.

12.1.2 HPD modifications shall be developed so as to maintain consistency with the requirements of Clauses 5, 6, 7, 8 and 9. They shall be installed on-site in accordance with the requirements of Clause 14.

12.1.3 HPD modifications should be integrated and validated in a manner consistent with Clauses 10 and 11.

12.1.4 When the extent of a modification does not require the full application of Clauses 10 and 11, the integration of the modified HPD shall be performed according to a regression HPD integration plan, and the validation shall be performed according to a regression HPD validation plan. The adequacy and thoroughness of these plans shall be justified taking into account the extent of any modifications made in the HPD requirements specification and in the HPD design specification. Records of the application of these plans shall be produced.

12.1.5 HPD modifications shall be comprehensively documented. In particular, all affected HPD documents shall be updated.

12.1.6 HPD modification documentation should state:

a) the objectives of the HPD modification, including any system-level objectives;

b) the HPD components affected or created by the modification;

c) identification of the versions of these components, both before and after modification.

The system level objectives of a modification are documented according to the requirements 6.4.7 of IEC 61513:2011.

12.1.7 The effects of a HPD modification on the rest of the I&C system and on the other systems with which it interacts or shares resources shall be assessed. Any necessary action shall be taken so as to ensure the correct operation of the I&C system.

12.1.8 The effects on HPDs of modifications in the rest of the I&C system or in the other systems with which it interacts or shares resources shall be assessed. Any necessary action shall be taken so as to ensure the correct operation of the I&C system.

12.1.9 *For class 2, when the regression approach is used, the regression HPD integration plan and the regression HPD validation plan shall give adequate confidence that the modified HPD conforms in all respects to the new HPD requirements specification, and that*:

a) the objectives of the modification are satisfied;

b) no fault is introduced;

c) the modified and/or newly introduced PDB behaves as specified by the corresponding documentation for safety and as expected by the modified HPD design specification;

d) the other modified and/or new HPD components conform to their specification.

12.1.10 *For class 2, HPD modification documentation should state in addition*:

a) any changes made to its specification;

b) any constraints that need to be respected when developing the modification;

c) the references of the modified design and/or implementation documents.

12.1.11 *For class 2, the level of detail of the documentation of a HPD modification shall be such that*:

– *it contributes as appropriate to the confidence in the correctness of the modified HPD and I&C system;*

– *compliance of the I&C system to the applicable requirements of IEC 61513 can be demonstrated.*

The IEC 61513:2011 requirements that might be concerned are mainly in 6.2.2.3, 6.2.2.4, 6.2.2.5, 6.2.3.3, 6.2.3.5 and 6.2.4.

12.2 Modification of the micro-electronic technology

12.2.1 If the supplier updates the micro-electronic technology (e.g. new version of a blank FPGA to increase the speed or to reduce the die size) and does not supply sufficient information justifying compatibility of the new integrated circuit with respect to the HPD requirements, the acceptance process (Clause 7.2) shall be performed again.

According to the information provided by the supplier, the compatibility of the new integrated circuit can be assumed and the acceptance process described by 7.2 might not need to be performed again.

12.2.2 An impact analysis shall be performed after modification of the integrated circuit technology to determine what verification and/or validation activities of the HPD and system lifecycle need to be performed to assess the assumed compatibility of the new integrated circuit technology.

12.2.3 The relevant verification and/or validation activities shall be performed according to the impact analysis and duly documented.

13 HPD production

13.1 General

The scope of this document excludes the design and manufacture of the pre-developed micro-electronic technologies (e.g. a blank FPGA) used as inputs by the development process of the HPD. “Production” in this Standard designates the final steps which deliver the integrated circuit ready for use in the I&C system.

13.2 Production tests

13.2.1 Production tests performed at board level (after assembly of the HPD onto the printed circuit board – e.g. by soldering) shall verify that the interface of the part is operational (such as “I/O pin stuck at” fault test, global functional test).

13.2.2 Each produced part shall pass the production tests or shall be rejected.

13.2.3 The test results shall be stored together with identification information such as batch number in order to support the diagnosis of potential process problems.

13.3 Programming files and programming activities

13.3.1 The programming files shall include error detection codes, and the programming equipment shall verify them.

13.3.2 For each produced part:

a) the configuration after programming shall be verified and;

b) relevant traceability information (such as batch number, programming log file, characteristics of programmable switches before and after programming) shall be stored.

13.3.3 All procedures and requirements given by the integrated circuit supplier shall be fulfilled (e.g. to prevent electrostatic discharge).

13.3.4 Only tools guaranteed and supported by the integrated circuit supplier shall be used.

14 HPD aspects of installation, commissioning and operation

14.1 General

14.1.1 Overview

Subclause 6.2.7 of IEC 61513:2011 provides requirements regarding the installation of the I&C system on site. The present subclause provides additional requirements specific, or of particular importance, to the installation of HPDs.

14.1.2 The procedure for installing HPDs on site shall be documented. It shall guarantee that the correct and complete version of the HPD is installed.

14.1.3 The procedure for installing HPDs on site shall include and specify on-site checks and tests to be performed before the I&C system is put into full operational use. In particular, the satisfaction of the conditions required for correct operation of the HPD shall be verified.

For example, these conditions may concern the hardware on which the HPD operates, or other systems with which the software interacts or shares resources.

14.2 Anomaly reports

14.2.1 If unexpected, apparently incorrect, unexplained or abnormal behaviour is experienced after acceptance into service, an anomaly report should be raised.

14.2.2 The anomaly report should give details of the behaviour, the HPD and hardware configurations and the activities in hand at the time. It should also include the originator, location, date, and a report identification.

14.2.3 The anomaly reports should be reviewed. Issues raised should be documented, tracked and resolved.

14.2.4 The anomaly should be reported to the designer and to the users.

15 Software tools for the development of HPDs

15.1 General

15.1.1 Overview

Software tools can play an important role in preventing the introduction of faults in HPDs or in system design, and in revealing existing faults. In particular, tools can aid or automate the development of HPDs.

Examples of tools associated with the development of HPDs are HDL generators, synthesis tools, timing analysers and test case generators.

15.1.2 The quality assurance plan shall precisely identify the software tools which might influence the correctness of HPDs.

15.1.3 User documentation shall be available for the users of such tools to ensure that they are used as intended.

15.1.4 The quality assurance plan shall distinguish the tools which might introduce faults in HPDs, such as HDL generators and synthesis tools, from those which might only lead to overlooking already existing faults, such as timing analysers and test case generators.

15.1.5 Evidence regarding tool quality and ability to produce correct results should be based on operational experience, tool qualification or certification, certification of their suppliers for appropriate development practices, guarantee of appropriate tool development processes, and/or tests. The required stringency of the evidence should be determined based upon the conditions of use of the tool, the extent of the verification of its outputs, the likelihood of tool errors to be detected, and the seriousness of the consequences of undetected erroneous results. Conversely, stringent evidence (for example, a tool qualification according to IEC 62566) may be used as a substitute for some of the verifications of outputs.

15.1.6 *For class 3, evidence should be provided regarding the quality of the software tools which might introduce faults in HPDs, and regarding their ability to produce correct results*.

15.1.7 *For class 2, the software tools which might introduce faults in HPDs shall be selected and used according to documented procedures and rules aiming at reducing or mitigating this risk. Evidence shall be provided regarding their quality and their ability to produce correct results. Where tools have been applied to generate a given item or information their use shall be recorded to identify them*.

15.1.8 *For class 2, the software tools which might fail to report faults in HPDs should be selected and used in a way which reduces this risk*.

15.1.9 *For class 2, the use of software tools which might fail to report faults in HPDs should be recorded*.

15.1.10 *For class 2, when a tool or tool version which has the potential to introduce faults in HPDs is substituted with another, precautions shall be taken to ensure that this does not have adverse effects on the correctness of the HPDs*.

For example, in addition to the quality and ability of the new tool to produce correct results, its compatibility with the previous tool might need to be assessed.

15.2 Additional requirements for design, implementation and simulation tools

15.2.1 Software tools shall give access to the parameters that control the logic synthesis and the implementation (e.g. through settings).

15.2.2 Software tools should not add structures not directly traceable to HDL source statements (e.g. gate duplication to match timing requirement) without warning.

15.2.3 The designers shall have previous knowledge of the software tools, in particular they shall know how they perform on the structures and constructs used in the project.

15.2.4 If a software tool requires command line arguments these shall be in a script file (placed under configuration management) to avoid manual invocation errors.

This is useful not only for the consistency; it also helps in assessing the origin of a fault, which might lie in the source code, in the tool or in the tool parameters. It might also be necessary in the assessment of the potential for Common Cause Failure (CCF) due to design and implementation tools.

15.2.5 When moving to a new version of a software tool that is responsible for a transformation of design information (e.g. logic synthesis or place and route), all affected simulation, analysis and verification activities shall be performed again.

It can be justified by documented analysis that a given modification of a tool cannot affect the abovementioned activities, e.g. correction of some inconsistent behaviour in the tool graphical user interface.

Activities which have been completed before the tool change do not need to be repeated.

16 Design segmentation or partitioning

16.1 Background

It is possible on some HPD devices to design and implement circuits that are allocated using physically different areas of the integrated circuit, have minimal or no interconnections together, and use no common hardware resources. Some HPDs support such areas, sometimes called “lakes”, with unused/unusable space between them. Some of the advantages of design segmentation or partitioning can include the implementation of auxiliary or support functions (this is not to be a replacement for redundant channels/trains in a design at system level).

16.2 Auxiliary or support functions

16.2.1 General

In general, auxiliary or support functions implemented on a HPD, even if not performing category B or C functions, have the potential to interfere with these functions of that HPD. Thus, unless it can be shown that the requirements of 16.2.2 are met, auxiliary or support functions shall be developed, implemented and verified according to the requirements of this document (i.e., as category B or C functions as required).

16.2.2 Partitioning of auxiliary or support functions or functions of an inferior safety category

This document recognizes that it might be possible with specific design measures and partitioning of the HPD to ensure that auxiliary or support functions are independent of those of category B or C and cannot inappropriately interfere with them. In such cases, provided the following requirements are met, auxiliary or support functions may be implemented on a class 2 or 3 HPD without the same rigour as for category B or C functions, respectively:

a) it shall be demonstrated by design, implementation, assessment and systematic verification that the operation or failure of such auxiliary or support functions or functions of an inferior safety category cannot interfere directly or indirectly with any category B or C function, whether the cause of the failure is internal or external to the HPD (e.g. induced by the power supplies, a short circuit on a connected line, etc.),

b) this demonstration shall address functional aspects of interference,

c) in particular the areas of the integrated circuit used to implement such auxiliary or support functions shall be physically different from those used to implement the category B or C functions,

d) in case of modification of the HPD, it shall be demonstrated that the requirements of 16.2.2 are still fulfilled,

e) the interface between circuits implementing category B or C functions and auxiliary or support functions or functions of an inferior safety category shall be simple and fully verifiable,

f) data received by category B or C functions from auxiliary or support functions or functions of an inferior safety category shall be limited to static parameter values (e.g. calibration constants, set-points),

g) category B or C functions shall not have any time dependence on reception of data from auxiliary or support functions or functions of an inferior safety category,

h) appropriate safety measures (e.g. safe communications protocols) shall be implemented for any communication between category B or C functions and auxiliary or support functions or functions of an inferior safety category such that all data transfer errors will be detected and a suitable safe response taken, or correct receipt of data is acknowledged.

17 Defences against HPD Common Cause Failure

Systematic faults introduced in any design and implementation process of a HPD due to human error (either in the developed part or in an included pre-existing design) could under some triggering event lead to the CCF of multiple instantiations of a HPD design.

The potential for CCF at system level is in the scope of higher level SC 45A Standards, in particular:

a) IEC 61513:2011,5.4.2.6 that addresses defence against CCF;

b) IEC 61513:2011,5.4.4.2 that addresses the assessment of reliability and defences against CCF;

c) IEC 62340 (for category A functions).

The present document defines development and verification processes and requirements which minimise the potential for HPDs to have systematic faults and therefore, as such faults can cause CCF, also minimise the potential for CCF due to HPDs.

Annex A
(informative)

Documentation

A.1 General

This annex identifies typical documentation for each of the main clauses of this document. The contents may be organized into a set of documents different from those suggested in this annex, provided that the sections are clearly identified.

A.2 Project

a) Quality assurance plan.

b) Configuration management plan.

c) Verification plan.

A.3 HPD requirement specification

a) HPD requirement specification.

A.4 Acceptance of blank integrated circuits, Native Blocks and PDBs

a) IC and PDB requirements specification(s).

b) Documentation for safety of PDBs.

c) Documents providing evidence of correctness of PDBs with respect to documentation for safety including, when applicable: design documentation review, operational experience review, certification review, documents concerning complementary means (audit reports, test reports, etc.).

d) Document containing the rules of use for PDBs.

A.5 HPD design and implementation

a) HPD design specification including:

   1) description of breakdown into main modules, design choices, identification of the integrated circuits, native blocks and PDBs.

   2) *for class 2, detailed design description including:*

      - *the RTL description of any modules implemented in HDL.*
      - *any information enabling correct predictions regarding the key safety significant elements of system performance, including notably the maximum response times of applications.*
      - *preliminary electrical characteristics and timings.*

b) HPD implementation documentation including:

   1) Gate-level description ("netlist"), technology specific description for production.

   2) Files of parameters and constraints.

   3) Description of redundancies introduced or removed.

   4) For class 2,

      - back annotations taking into account delays associated with gates and wires post-implementation.
      - electrical characteristics and detailed timings.

5) Post-route analyses report, STA report.

A.6 HPD integration and testing

a) HPD simulation and integration plan.

b) Document containing a description of the test-benches and, for class 2, the coverage criteria and justification of these coverage criteria.

c) Report including: test results and analysis (RTL level, post-synthesis, post-route), analysis of the fulfilment of the rules of use.

A.7 HPD aspects of system integration

a) System integration plan including: HPD aspects of system integration strategy and procedures, configuration management interface, test cases.

b) HPD aspects of integrated system test report, including identification of components and tools, test results and analysis, faults found and resolution.

A.8 HPD aspects of system validation

a) System validation plan including test cases specific to HPD aspects.

b) System validation report including aspects specific to HPDs: identification of components and tools, test results, test analysis, faults found and resolution.

A.9 Modification

All documents related to the development phases affected by the modification have to be updated. Otherwise, in cases where the extent of the modification does not require the full application of Clauses 10 and 11, the integration and validation of the modified HPD may be performed according to:

a) Regression HPD integration plan.

b) Regression HPD validation plan.

A.10 HPD production

a) Document containing the production tests.

b) Document containing the results of production tests, the part identification information and the part programming information.

A.11 Software tools for the development of HPDs

a) Tool selection report (analysis of tool support, evaluation, acceptance, limits of applicability).

b) User documentation.

c) Document describing the strategy for modification, upgrade or replacement.

Annex B
(informative)

Development of HPDs

B.1 General

The development activities addressed by this document are based on Hardware Description Languages (HDL) and design tools running on workstations, according to a flow whose broad outline is presented here to ease the understanding of the corresponding clauses of this document.

B.2 Optional capture of requirements at Electronic System Level

Capture of requirements is sometimes done by means of a high level description of the system to which the HPD belongs: this description includes the other hardware and software components. Each component is represented by a behavioural model, and these models exchange information through communication channels to simulate the intended system.

This description level is called "Electronic System Level", or ESL, and uses system description languages such as SystemC or System Verilog.

This description is typically executed (simulation) with functional test cases to estimate the relevance of different system architectures, select the best one, and finally set-up the requirements of each component including the HPD in terms of behaviour and interface.

Subclause 8.5 provides guidance applicable when an ESL description of the HPD requirements is used in an automated way to generate part or all of the HPD design. This generation is sometimes called “high-level synthesis”. Only limited effort is then necessary to transform the specification into HDL that can then be automatically translated into an RTL description or into a form suitable to be interpreted.

B.3 HPD and system life-cycle

The HPD life-cycle described in Figure 2 shows the development of one HPD that might be undertaken in parallel with the development of other components (software or hardware) of the system as shown in Figure 1, but coming together at the integration and validation phases of the system life-cycle.

The approach proposed to development is based on the traditional “V cycle” model as this approach has been reflected in other Standards and is also recommended in IAEA SSG-39, but allowing necessary adjustments recognizing that some phases of the development can be done automatically by tools and that development might be iterative.

There is often no clear separation and well-identified boundary between the integration of a given component and the system integration. Therefore, in this Standard, the integration of a given HPD within a system is considered to be part of the system integration. Similarly, the validation of a given HPD within a system is considered to be part of the system validation. This standard also addresses the integration of the HPD from its component parts and the testing steps associated with this process.

Depending on the function achieved by the HPD, the system or subsystem to consider during integration might range:

- from the I&C system when the HPD implements a safety function logic;

- to an electronic board or cabinet when it implements a function (internal to the board or cabinet) that has been demonstrated, by suitable analysis, to be incapable of affecting the outputs of any safety function in the wider system.

The situation usually most critical from a safety standpoint is when the HPD directly implements the safety function logic.

B.4 Design

Although presented in a linear manner in the present standard, the design and implementation phase described in Clause 8 does not necessarily directly follow the selection and acceptance process for predeveloped items as described by Clause 7. For the purposes of reusability, for example, the ICs and PBDs might already have been selected when beginning the initial design phase. In other cases, the selection and acceptance of ICs and PDBs might depend on the initial design decisions and can therefore only occur after the initial design phase has begun. In all cases, the HPD design phase (Clause 8) and selection and acceptance process for predeveloped items (Clause 7) as a whole is to be considered an iterative process.

Starting from the requirements, this activity initially aims at defining the main design principles, such as the partition in pre-developed or custom modules, the organization of the self-supervision and the identification of the micro-electronic technology (including its native blocks) and PDBs that could be used.

Then an RTL (Register Transfer Level) description is built and tested by simulation. HDLs such as VHDL or Verilog are used. This is mostly not dependant on the micro-electronic technology that will be used.

This high level description is a synchronous parallel model of the HPD, describing its behaviour by means of signals transformed by combinatorial functions and sequentially transferred between registers triggered by one or more clocks.

The RTL description has structural aspects, showing the logical relations between modules which can be designed specifically or taken from libraries. It also has behavioural aspects, making it possible to describe the function of a module by means of algorithmic descriptions. This description is carried out by means of a HDL (Hardware Description Language), typically VHDL (IEEE 1076) or Verilog (IEEE 1364).

The RTL description needs to be synthesizable, which means that it can be translated automatically into a set of interconnected electronic gates. To achieve this property, the designer uses only a subset of the HDL language, while the full language may be used for example to create simulation environments.

In parallel to the design, it is of use to develop a "test-bench" with the same language: the RTL description of the HPD is included in a broader HDL program, which sends it input sequences and reads its outputs in order to test it by simulation. The test-bench may use non-synthesizable language features to ease the design of the tests (e.g.: access to files, printing, explicit time management). The test-bench is then used to check the RTL description, and can be associated with various tools for test generation and coverage measurement.

Static analysis tools are being introduced to provide complementary verification approach. They typically make it possible to prove whether some expected properties hold or not on an HDL description. Examples of static analyses are: checking of properties, assertion based verification, checking of equivalence between different design levels (e.g. RTL and netlist), or Static Timing Analysis.

B.5 Acceptance process for programmable integrated circuits, native blocks and Pre-Developed Blocks

When developing HPDs, it is necessary to select and assess pre-developed items including blank integrated circuits, native blocks and/or PDBs incorporated in the final HPD. Some types of native blocks such as logic gates are used in every HPD design. More complex native blocks, referred to in this standard as optional native blocks, such as multipliers or serial transmission controllers might or might not be used according to HPD design choices. The use of optional native blocks and PDBs is common industrial practice. This document does not however presuppose that the use of such optional native blocks or PDBs is necessary or desired within any given HPD project.

In the present document, PDBs are categorised according to the format in which they are provided. PDBs provided in the form of an RTL description can be integrated by the HPD designer into any target IC. PDBs provided in the form of a netlist can also be integrated into any target IC. In such cases, however, the supplier of the PDB typically provides a netlist file which has been synthesised for a specific IC as specified by the HPD designer. Such netlist files are therefore not directly usable by the HPD designer in other ICs. PDBs provided in the form of optional native blocks represent existing hardware within the IC with no possibility of modification but which, if used, need to be instantiated and configured using a software wizard or other software tools.

In cases where pre-developed items (or components) include features not required for the HPD, the elaboration and the enforcement of specific “rules of use” is recommended in order to restrict their use to what is needed and safe.

Although the selection and acceptance processes for ICs and PDBs are presented in a linear manner, this does not suggest that the selection and acceptance of the IC (7.2) shall take place before the selection and acceptance of PDBs (7.3). In some cases, the need to use a specific PDB might restrict the choice of possible ICs. In other cases, the need to use a specific IC might restrict the choice of PDBs which can be used in the HPD design. The choice of appropriate ICs and PDBs therefore is to be made based on an iterative process, starting from the HPD requirements specification and initial design decisions according to the requirements of 8.3.

B.6 Implementation

Starting from the RTL description in addition to the native blocks and PDBs used in the HPD design, the implementation synthesizes the RTL description in order to produce a gate-level description (netlist) of the HPD. Then place and route is performed according to the target integrated circuit and results in the physical description needed to produce the HPD, such as a programming file or "bitstream".

The different families of components such as FPGAs, standard cells, and so on provide different pre-characterizations of the physical behaviour of the final product. Thus, while the activities described hereafter are intrinsically necessary, they may or not be handled automatically by the associated tools. The following description gives an overview of these activities for a design based on standard cells.

The logic synthesis transforms the RTL description into a network of logic cells of the micro-electronic technology, called "netlist". Depending on this micro-electronic technology, these cells might be only elementary gates (such as AND, OR) or might include larger functions (such as counters).

Although tools similar to software compilers are used to perform the synthesis, the designer directs the process by providing information on the expected performance (such as clock frequency, delay between two signals, power consumption) and on how critical signals such as clocks are to be handled. This information is typically stored in "constraint files" which can be very large. Their elaboration can thus be difficult, and an error or omission might result in generating a circuit suffering from subtle non-reproducible faults, almost impossible to detect by simulation. The verification of the constraint files is thus an essential activity.

The place and route stage defines the physical location of the cells on the silicon die, and inter-connects them taking into account the technological constraints (existence and capacity of predefined routing channels) as well as the application constraints (such as maximum propagation delay between two given nodes).

As the number of gates increases, more and more of them are inter-connected. So, more and more inter-connections have to be routed across the die. Additionally the requirements for speed usually impose to keep short some paths. This last constraint might lead to modifying the placement of some gates, which in turn reacts on the whole routing scheme. Finding the "best" solution is a very hard problem (in the sense of computability), so only approximations might be found by the tools, which need to use advanced and evolutionary algorithms.

The description after place and route is produced in a format which depends on the micro-electronic technology. As the physical layout is known at this stage, the propagation times might be refined by taking into account the resistance and capacitance of each path. This information is typically used to back-annotate again the description, in order to simulate it in the test-bench with realistic propagation times for cells and wiring.

Moreover, the supplier of the micro-electronic technology provides the propagation times of the cells included in its library, using formats such as VHDL-VITAL (IEEE 1076.4). This timing information is included as "back-annotation" of the netlist description, and is taken into account in the “post implementation” simulation.

In addition to the verification by "post implementation simulation”, tools for static analysis make it possible to check the propagation times (STA: Static Timing Analysis) or the equivalence between different description levels.

B.7 HPD integration and testing

Clause 9 addresses the testing of the HPD through the use of test benches at higher and higher levels of HPD integration in accordance with the structure of the HPD design. Initial behavioural simulations might be carried out at the level of individual HDL modules using appropriate test benches and test scenarios to provide suitable levels of functional and structural coverage as required by the validation plan. Then, HDL modules might be integrated together, resulting in the need for different test scenarios exercising relevant aspects of the HPD behaviour according to the overall HPD requirements specification.

B.8 Types of specific integrated circuits

B.8.1 General

The evolving technology offers many variants of specific integrated circuits, so this document provides requirements based on principles and not on specific details of each variant.

This clause provides an overview of the main available variants (note: their names are not always used consistently in the industry).

From a theoretical point of view, any computable function can be implemented with only one type of well-chosen elementary gate such as “NAND” (“*A nand B*” is “*not (A and B)*”). Therefore, the range of functions which can be implemented within a given circuit depends essentially on its size (number of gates) and on its internal connectivity which allows a more or less efficient use of the gates.

B.8.2 PAL (Programmable Array Logic)

PALs are low-size devices typically organized in OR/AND array in order to implement logic equations having the form of sum of products such as: *output = (A and B and not C) or (not B and not C) or (D).*

PALs are made specific by configuring connections, typically by blowing fuses or in some cases by configuring reprogrammable switches.

The AND structure is programmable, i.e. the product expression before programming is: *(A and not A and B and not B and C and not C)*, where each term corresponds to one configurable connection. According to the functional requirement, the unneeded terms are removed to produce e.g. *(A and not C).*

The OR structure is fixed: the inputs of the “OR” are a fixed number of such programmable products, e.g. *(A and not C) or (A and not B) or (D).*

Low-level languages such as PALASM are typically used to configure PALs: the designer inputs the logic equations to be implemented and the tool translates them into a map of connections. No behavioural description such as in VHDL or Verilog is possible with such languages.

PALs typically provide a few inputs and outputs (e.g. 10 inputs, 8 outputs) and they are equivalent to a few hundreds gates at most. Due to this limited size they are not in the scope of this document.

B.8.3 PLD, CPLD (Programmable Logic Device, Complex PLD)

PLDs and CPLDs are essentially large arrays of PALs interconnected together, but new families might offer additional features.

Like PALs, they are based on sum of products with fixed structure, thus the signal routing from input to output is fixed and propagation delay times are quite constant. Of course, when additional features such as feedback paths or specialized logic are offered this property might be lost.

The size of CPLDs reach the equivalent of tens of thousands of gates.

B.8.4 FPGA

FPGAs are organized as a large number of programmable logic blocks including provisions for combinatorial logic and storage. These blocks are interconnected by a hierarchy of programmable interconnects, and programmable input/output pads are provided (direction, impedance, voltage, and memorization are typically programmable). Specific paths are usually provided for critical signals such as clocks. FPGAs might in addition include specialized logic blocks such as memory, processor core, standardized interfaces, etc.

The gate equivalence of FPGAs is not really relevant because their complex and different structures make it difficult to predict how many blocks are needed for a given function. Some FPGAs include hundreds of thousands of programmable blocks, hundreds of inputs/outputs, and are made of billions of transistors.

FPGAs might retain their function (“configuration”) by using means such as:

a) Static RAM (the configuration is volatile, copied at start-up from an external memory),

b) Flash memory (the configuration is stored in non-volatile but reprogrammable internal memory elements),

c) Anti-fuse (the configuration is permanent; such devices are “One Time Programmable”).

The susceptibility of the configuration to single event upsets and neutron/alpha radiation is, relatively, high for static RAM, low for flash, and very low for anti-fuse parts.

B.8.5 Gate Array, or pre-diffused integrated circuit

The integrated circuit supplier prepares in advance standard integrated circuits in which all transistors are already made but are not interconnected. The specific function to be implemented is synthesized into a specific interconnection of the transistors.

This approach involves non-recurring costs associated with the production of the specific masks for the metal layers (interconnection), but might offer a lower part cost compared to FPGAs because no silicon is used to implement the programmable circuitry. However, this technology seems to be increasingly replaced by FPGAs.

B.8.6 Standard Cells

The supplier offers a micro-electronic technology and designs with it a range of “standard cells” such as elementary combinatorial gates, flip-flops, adders, counters, etc. These cells have known characteristics such as area, input current, capacitance and propagation delay. They are designed in such a way that they have the same height and different width, so they can be placed on the integrated circuit in rows in order to ease routing and power supplying.

The functional and physical characteristics of the cells are described in the “technology library”, which is provided to the I&C designer. This library is used during logic synthesis (see B.6) which transforms the RTL description into a netlist of these cells, which are then placed on the integrated circuit and interconnected. After completion of functional and technology related verifications, the masks needed to produce the integrated circuits are fabricated and the production may begin.

This approach involves higher non-recurring costs compared to gate-arrays because all masks are specific, but offers a lower part cost because the size of the integrated circuit is exactly what is needed. The availability of different cells for each type, optimizing different aspects such as speed, area, or power consumption, allows a better optimization of each area of the design, still under control of the I&C designer with only HDL related tools.

B.8.7 “Full custom ASIC”, or “raw ASIC”

This technology involves a specific design of all aspects of the integrated circuit, down to the transistor level, with specific tools. This implies very high non-recurring costs which need large volumes to be economically justified. These circuits are not in the scope of this document.

Bibliography

IEC/IEEE 60780-323:2016, *Nuclear facilities – Electrical equipment important to safety – Qualification*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 62342:2007, *Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing*

IEC 62645, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

IAEA Safety Standard Series No. SSR-2/1:2016, *Safety of Nuclear Power Plant: Design*

IAEA Safety Guide SSG-39:2016, *Design of instrumentation and control systems in Nuclear Power Plants*

IAEA Safety Glossary:2016, *Terminology used in nuclear safety and radiation protection*

IAEA Safety Standard Series, N° GS-G-3.5:2009, *The Management System for Nuclear Installations*

IEEE Std 7-4.3.2:2010, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*

IEEE 1076-2008, *IEEE Standard VHDL Language Reference Manual*

IEEE 1364-2005, *IEEE Standard for Verilog Hardware Description Language*

IEEE 1666-2011, *IEEE Standard for Standard SystemC Language Reference Manual*

IEEE 1800-2017, *IEEE Standard for SystemVerilog – Unified Hardware Design, Specification, and Verification Language*

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*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
fonction d'application
fonction d'un système d'I&C qui accomplit une tâche relative au processus sous contrôle plutôt qu'au fonctionnement du système lui-même

[SOURCE: IEC 61513:2011, 3.1]

3.2
langage orienté application
langage informatique spécifiquement conçu pour un certain type d'application et pour être utilisé par les spécialistes de ce type d'application

Note 1 à l'article: Les familles d'équipements offrent en général des langages orientés application de façon à faciliter l'adaptation des équipements à des exigences spécifiques.

Note 2 à l'article: Les langages orientés application peuvent être utilisés pour la spécification d'exigences fonctionnelles auxquelles doit satisfaire un système d'I&C, et/ou pour spécifier ou concevoir le logiciel d'application. Ils peuvent être basés sur du texte, des diagrammes ou une combinaison des deux.

Note 3 à l'article: Par exemple, les langages à blocs fonctionnels, les langages définis par l'IEC 61131-3.

Note 4 à l'article: Voir aussi "langage généraliste".

[SOURCE: IEC 60880:2006, 3.3]

3.3
logiciel d'application
partie du logiciel d'un système d'I&C qui exécute les fonctions d'application

Note 1 à l'article: Pour les HPD, les fonctions d'application ne sont pas mises en œuvre par logiciel. Par conséquent, il y a lieu de remplacer le terme "logiciels d'application" par "fonctions d'application réalisées dans le cadre de la conception des HPD".

Note 2 à l'article: le logiciel d'application est à mettre en regard avec le "logiciel système".

Note 3 à l'article: Voir également "logiciel système".

[SOURCE: IEC 61513:2011, 3.2]

3.4
circuit intégré spécifique
ASIC
circuit intégré conçu pour des applications spécifiques

Note 1 à l'article: Il s'agit d'un circuit intégré spécialisé conçu pour les besoins d'une société. Il intègre des fonctions sur mesure définies par cette société.

Note 2 à l'article: L'abréviation "ASIC" est dérivée du terme anglais développé correspondant "application specific integrated circuit".

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

3.5
bloc
une des parties constituant une conception; un bloc pouvant se décomposer en d'autres blocs

Note 1 à l'article: Un bloc est soit un bloc prédéveloppé, soit bloc natif, soit un bloc développé au cours du projet concerné.

[SOURCE: IEC 62566:2012, 3.2]

3.6
défaillance de cause commune
DCC
défaillance d'au moins deux structures, systèmes ou composants due à un seul événement ou une seule cause spécifique

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.7
gestion de la configuration
processus consistant à identifier et à consigner les caractéristiques des structures, systèmes et composants (y compris des systèmes programmés et des logiciels) d'une installation, et à s'assurer que les modifications de ces caractéristiques sont correctement élaborées, évaluées, approuvées, publiées, mises en œuvre, vérifiées, enregistrées et incorporées dans la documentation relative à cette installation

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2016]

3.8
cybersécurité
ensemble des activités et des mesures dont l'objectif est d'empêcher, de détecter et de réagir:

– à la divulgation malveillante d'informations (confidentialité) susceptibles d'être utilisées pour commettre des actes malveillants, ce qui pourrait entraîner un accident, une situation non sûre ou une dégradation des performances de la centrale;
– aux modifications malveillantes (intégrité) de fonctions pouvant porter atteinte à la fourniture ou à l'intégrité d'un service demandé par des systèmes numériques programmables d'I&C (y compris la perte de contrôle), ce qui pourrait entraîner un accident, une situation non sûre ou une dégradation des performances de la centrale;
– à la rétention ou à la prévention malveillante de l'accès à ou de la communication d'informations, de données ou de ressources (y compris la perte de visibilité) susceptibles de compromettre la fourniture du service demandé par des systèmes d'I&C (disponibilité), ce qui pourrait entraîner un accident, une situation non sûre ou une dégradation des performances de la centrale

Note 1 à l'article: Cette définition est harmonisée par rapport au domaine d'application de la norme IEC 62645, ainsi qu'à la structure générale des documents du SC 45A. Il est reconnu que le terme "cybersécurité" à un sens plus large dans d'autres normes et recommandations, où il englobe souvent les menaces non malveillantes, les erreurs humaines et la protection contre les catastrophes naturelles. A l'exception des erreurs humaines compromettant la cybersécurité, ces aspects ne relèvent pas du concept de cybersécurité utilisé dans la série de normes du SC 45A. Pour plus de détails sur ces exclusions, se reporter à l'Annexe A de l'IEC 62645.

Note 2 à l'article: Les termes "sécurité informatique", "sécurité" et "cybersécurité" sont utilisés comme des synonymes dans le présent document.

3.9
spécification de conception
document ou ensemble de documents qui décrivent l'organisation et le fonctionnement d'un élément, et qui sont utilisés comme base de la mise en œuvre et pour l'intégration de l'élément

[SOURCE: IEC 62138:2018, 3.12]

3.10
documentation de sûreté
document ou ensemble de documents qui spécifient comment un produit peut être utilisé de façon sûre dans une application importante pour la sûreté

Note 1 à l'article: Cette définition s'utilise dans le contexte des composants prédéveloppés, y compris les circuits intégrés programmables, les blocs natifs et les blocs prédéveloppés (voir Article 7).

[SOURCE: IEC 62138:2018, 3.13]

3.11
élément électrique/électronique/électronique programmable
élément E/E/PE
élément réalisé à partir de technologie électrique (E) et/ou électronique (E) et/ou électronique programmable (PE)

Note 1 à l'article: Dans ce terme et sa définition, le mot "élément" peut être remplacé par les mots "système", "équipement" ou "dispositif".

[SOURCE: Rédigée à partir de IEC 61508-4:2010]

3.12
niveau système électronique
ESL
description de haut niveau d'un système électronique, basée sur un ensemble de processus représentant les fonctionnalités de composants tels que des microprocesseurs, des mémoires, des unités de calcul spécialisées ou des canaux de transmission

Note 1 à l'article: Cette description permet au concepteur de répartir le système en composants, d'évaluer ses performances pour différentes affectations de fonctions aux composants, et d'établir les exigences relatives aux composants. Elle est typiquement réalisée avec des langages tels que SystemC (IEEE 1666) ou SystemVerilog (IEEE 1800).

Note 2 à l'article: L'abréviation "ESL" est dérivée du terme anglais développé correspondant "electronic system level".

[SOURCE: IEC 62566:2012, 3.4]

3.13
famille d'équipements
un ensemble de composants matériels et logiciels pouvant travailler de manière complémentaire dans une ou plusieurs architectures définies (configurations). Le développement des configurations spécifiques à la centrale et du logiciel d'application associé peut être réalisé par des outils logiciels. Une famille d'équipements fournit normalement un certain nombre de fonctionnalités normales (bibliothèque des fonctions d'application) qui peuvent être combinées pour générer un logiciel d'application spécifique

Note 1 à l'article: Une famille d'équipements peut aussi comprendre des composants HPD.

Note 2 à l'article: Une famille d'équipements peut être un produit provenant d'un fabricant ou un ensemble de produits interconnectés et adaptés par un fournisseur.

Note 3 à l'article: Le terme "plateforme d'équipements" est parfois utilisé comme synonyme de "famille d'équipements".

[SOURCE: IEC 61513:2011, 3.17]

3.14
erreur
différence entre une valeur ou condition calculée ou mesurée et la valeur ou condition réelle, spécifiée ou théorique

Note 1 à l'article: Voir aussi "erreur humaine", "défaut", "défaillance".

[SOURCE: IEC 61513:2011, 3.18]

3.15
défaut
imperfection dans un composant matériel, logiciel ou système

Note 1 à l'article: Les défauts peuvent provenir de défauts aléatoires, par exemple consécutifs au vieillissement du matériel, et peuvent être systématiques, par exemple des défauts logiciels, consécutifs à des erreurs de conception.

Note 2 à l'article: Un défaut (notamment un défaut de conception) peut ne pas être détecté dans le système jusqu'à l'apparition d'une situation pour laquelle le résultat produit n'est pas conforme à ce qui était prévu pour la fonction, c'est-à-dire qu'une défaillance se produit.

Note 3 à l'article: Voir aussi "erreur humaine", "erreur", "défaillance".

[SOURCE: IEC 61513:2011, 3.21]

3.16
réseau de portes programmable sur site
FPGA
circuit intégré qui peut être programmé sur site par le fabricant de contrôle-commande. Il comprend des blocs logiques programmables (combinatoires et séquentiels), des interconnexions programmables entre ceux-ci, et des blocs programmables pour les entrées et/ou les sorties. La fonction est ensuite définie par le concepteur du contrôle-commande, et non par le fabricant du circuit intégré

Note 1 à l'article: Bien que les FPGA soient essentiellement des dispositifs numériques, certains peuvent inclure des entrées et sorties analogiques ainsi que des convertisseurs de signaux analogiques/numériques. Les FPGA peuvent inclure des fonctions numériques avancées telles que des multiplieurs, des mémoires dédiées et des cœurs de microprocesseurs.

Note 2 à l'article: L'abréviation "FPGA" est dérivée du terme anglais développé correspondant "field programmable gate array".

[SOURCE: IEC 62566:2012, 3.5]

3.17
validation fonctionnelle
vérification de la conformité des spécifications des fonctions d'application aux exigences fonctionnelles et de performance de haut niveau de la centrale. Elle est complémentaire de la validation du système (qui vérifie la conformité du système à la spécification des fonctions)

[SOURCE: IEC 61513:2011, 3.23]

3.18
langage généraliste
langage informatique conçu pour s'adresser à tout type de besoin

EXEMPLE Ada, C, Pascal.

Note 1 à l'article: Le logiciel système d'une famille d'équipements est en général réalisé à l'aide de langages généralistes.

Note 2 à l'article: Voir aussi "langage orienté application".

[SOURCE: IEC 60880:2006, 3.20]

3.19
langage de description de matériel
HDL
langage permettant de décrire formellement les fonctions et/ou la structure d'un composant électronique, à des fins documentaires, de simulation ou de synthèse

Note 1 à l'article: Les HDL les plus utilisés sont VHDL (IEEE 1076) et Verilog (IEEE 1364).

Note 2 à l'article: L'abréviation "HDL" est dérivée du terme anglais développé correspondant "hardware description language".

[SOURCE: IEC 62566:2012, 3.6]

3.20
circuit intégré programmé en HDL
HPD
circuit intégré configuré (pour des systèmes d'I&C de centrales nucléaires de puissance) au moyen de langages de description de matériel et d'outils associés

Note 1 à l'article: Les HDL et outils associés (par exemple simulateur, synthétiseur) sont utilisés pour réaliser les exigences par un assemblage adéquat de ressources microélectroniques prédéveloppées.

Note 2 à l'article: Le développement de HPD peut utiliser des blocs prédéveloppés.

Note 3 à l'article: Les HPD sont typiquement basés sur des FPGA ("Field Programmable Gate Arrays", réseaux de portes programmables sur site) vierges ou sur des circuits intégrés programmables similaires.

Note 4 à l'article: L'abréviation "HPD" est dérivée du terme anglais développé correspondant "HDL-programmed device".

[SOURCE: IEC 62566:2012, 3.7]

3.21
erreur humaine
faute humaine
action humaine conduisant à un résultat indésirable

Note 1 à l'article: Voir aussi "défaut", "erreur", "défaillance".

[SOURCE: IEC 61513:2011, 3.26]

3.22
système d'I&C
système réalisé sur la base d'éléments E/E/PE, exécutant des fonctions d'I&C de la centrale ainsi que des fonctions de service et de surveillance liées au fonctionnement du système lui-même

Note 1 à l'article: Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de communication, les interfaces vers les actionneurs et autres dispositifs de sortie. Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées.

Note 2 à l'article: Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

Note 3 à l'article: Voir aussi la définition d'élément E/E/PE et les notes associées.

Note 4 à l'article: Selon leurs fonctionnalités propres, l'AIEA fait la distinction entre les systèmes de contrôle et de commande, les systèmes d'IHM, les systèmes de verrouillage et les systèmes de protection.

[SOURCE: IEC 62138:2018, 3.26]

3.23
intégration
agrégation et vérification progressives des composants pour former un système complet

[SOURCE: IEC 62138:2018, 3.27]

3.24
mode de fonctionnement
état de fonctionnement d'un élément qui adopte dans ce cas un comportement opérationnel particulier

EXEMPLE Mode d'initialisation, mode normal ou modes dégradés à adopter en cas d'erreur dans l'élément.

[SOURCE: IEC 62138:2018, 3.29]

3.25
module
une des parties constituant une conception; un module pouvant se décomposer en d'autres modules

Note 1 à l'article: "Module" est synonyme de "bloc", le terme "bloc" étant souvent utilisé dans le contexte de la conception électronique.

[SOURCE: IEC 62566:2012, 3.8]

3.26
bloc natif
bloc représentant une ressource préexistante du circuit intégré, par exemple une porte logique ou un bloc plus complexe tel qu'un multiplicateur ou un contrôleur de transmission série. La programmation du HPD configure et connecte les blocs natifs pour réaliser la fonction exigée

[SOURCE: IEC 62566:2012, 3.9]

3.27
liste d'interconnexions
netlist
description d'un composant électronique par des interconnexions entre ses éléments terminaux (par exemple les blocs natifs)

[SOURCE: IEC 62566:2012, 3.10]

3.28
paramètre
donnée gouvernant le comportement du système d'I&C et/ou de son logiciel, et pouvant être modifiée par les opérateurs durant l'exploitation

Note 1 à l'article: Un paramètre peut également piloter le comportement du HPD.

[SOURCE: IEC 62138:2018, 3.31]

3.29
bloc prédéveloppé
PDB
bloc fonctionnel prédéveloppé utilisable dans une description en HDL

Note 1 à l'article: Les PDB sont typiquement fournis sous la forme de bibliothèques, de macros ou de blocs de propriété intellectuelle. Ils sont utilisés pour le développement du HPD et incorporés dans celui-ci.

Note 2 à l'article: L'incorporation d'un PDB dans un HPD peut nécessiter un travail significatif, par exemple la synthèse d'un circuit électronique à partir de ses instructions HDL, le placement des composants de ce circuit sur les structures matérielles du circuit intégré physique et le routage des interconnexions.

Note 3 à l'article: L'abréviation "PDB" est dérivée du terme anglais développé correspondant "pre-developed block".

[SOURCE: IEC 62566:2012, 3.11]

3.30
élément numérique programmable
élément qui s'appuie sur des instructions logicielles ou une logique programmable pour accomplir une fonction

Note 1 à l'article: Le terme "élément" peut ici être remplacé par le terme "système", "équipement" ou "dispositif".

Note 2 à l'article: Les principaux types d'éléments numériques programmables sont les éléments informatisés et les éléments logiques programmables.

Note 3 à l'article: Ce terme utilisé par le SC 45A de l'IEC équivaut au terme "élément électronique programmable" (élément PE) utilisé dans l'IEC 61508.

[SOURCE: IEC 62138:2018, 3.34]

3.31
réseau logique programmable
PLD
circuit intégré composé d'éléments logiques avec un motif d'interconnexions, dont des parties sont programmables par l'utilisateur

Note 1 à l'article: Il existe différents types de PLD, par exemple les EPLD (PLD effaçables) et les CPLD (PLD complexes).

Note 2 à l'article: Les différences entre FPGA et PLD ne sont pas strictement définies, mais "PLD" désigne habituellement un dispositif plus simple que "FPGA".

Note 3 à l'article: L'abréviation "PLD" est dérivée du terme anglais développé correspondant "programmable logic device".

[SOURCE: IEC 62566:2012, 3.13]

3.32
élément à logique programmable
élément qui s'appuie sur circuit intégré composé d'éléments logiques avec un motif d'interconnexions, dont des parties sont programmables par l'utilisateur

Note 1 à l'article: Le terme "élément" peut ici être remplacé par le terme "système", "équipement" ou "dispositif".

Note 2 à l'article: Un élément à logique programmable est un type d'élément numérique programmable.

Note 3 à l'article: Voir aussi la définition d'élément E/E/PE et les notes associées.

[SOURCE: IEC 62138:2018, 3.35]

3.33
niveau transfert de registre
RTL
modèle parallèle synchrone d'un circuit électronique, décrivant son comportement au moyen de signaux traités selon une logique combinatoire et transférés entre registres sur des impulsions d'horloge. Le modèle RTL est typiquement écrit en HDL ou généré à partir d'un code source HDL

Note 1 à l'article: L'abréviation "RTL" est dérivée du terme anglais développé correspondant "register transfer level".

[SOURCE: IEC 62566:2012, 3.14]

3.34
auto-surveillance
essai automatique des performances matérielles et de la cohérence logicielle d'un système d'I&C informatisé

Note 1 à l'article: L'auto-surveillance peut également s'appliquer à des HPD ou à des systèmes d'I&C basés sur HPD.

[SOURCE: IEC 60671:2007, 3.8]

3.35
logiciel système
logiciel conçu pour un système programmé particulier ou pour une famille de systèmes programmés afin de faciliter le fonctionnement et la maintenance de ces systèmes et des programmes connexes, par exemple systèmes d'exploitation, ordinateurs, services. Le logiciel système est généralement composé de logiciels opérationnels et de logiciels de soutien

Note 1 à l'article: Pour les HPD, les fonctions de système opérationnel ne sont pas mises en œuvre par logiciel. Par conséquent, il y a lieu de remplacer le terme "logiciels système opérationnels" par "aspects opérationnels système de la conception des HPD".

Note 2 à l'article: Aspects opérationnels système de la conception des HPD: aspects de la conception des HPD utilisés pendant le fonctionnement du système, comme par exemple les interfaces de communication, la gestion des entrées/sorties et les diagnostics en ligne.

Note 3 à l'article: Logiciels de soutien: logiciels d'aide au développement, aux essais ou à la maintenance des autres logiciels/HPD et du système, tels que les outils de synthèse, les générateurs de codes, les éditeurs graphiques, les diagnostics hors-ligne, les outils de vérification et de validation.

Note 4 à l'article: Voir également "logiciel d'application".

[SOURCE: IEC 61513:2011, 3.58]

3.36
validation système
confirmation par examen et apport d'autres éléments justificatifs qu'un système satisfait à la totalité des exigences spécifiées (fonctionnalités, temps de réponse, tolérance aux fautes, robustesse)

Note 1 à l'article: L'édition 2016 du Glossaire de sûreté de l'AIEA donne les deux définitions suivantes:

> Validation: Processus visant à déterminer si un produit ou un service est capable de remplir sa fonction prévue de façon satisfaisante. La validation peut impliquer un élément d'appréciation plus important que la vérification.
>
> Validation du système informatique: Processus consistant à soumettre à essai et à évaluer le système informatique intégré (matériel et logiciel) afin de garantir sa conformité par rapport aux exigences fonctionnelles, aux exigences relatives aux performances et à celles concernant les interfaces.

Tout d'abord, cette définition de "validation système" est un cas particulier de validation. Elle fait référence à un produit particulier, à savoir la validation d'un système d'I&C. Ceci est cohérent avec la définition de l'AIEA. Ensuite, la définition IEC précise la référence de validation, à savoir les spécifications d'exigences, alors que la définition de l'AIEA ne fait référence qu'à la "fonction prévue".

[SOURCE: IEC 61513:2011, 3.59]

3.37
défaut systématique
défaut relié de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

[SOURCE: IEC 61513:2011, 3.60]

3.38
vérification
confirmation par examen et apport d'éléments objectifs que les résultats d'une activité sont conformes aux objectifs et exigences établis pour cette activité

[SOURCE: IEC 61513:2011, 3.62]

4 Symboles et termes abrégés

ASIC	Circuit intégré spécifique (Application Specific Integrated Circuit)
DCC	Défaillance de cause commune
CPLD	Réseau logique programmable complexe (Complex Programmable Logic Device)
ESL	Niveau système électronique (Electronic System Level)
FPGA	Réseau de portes programmable sur site (Field Programmable Gate Array)
HDL	Langage de description de matériel (Hardware Description Language)
HPD	Circuit intégré programmé en HDL (HDL-Programmed Device)
CI	Circuit intégré
I&C	Instrumentation et contrôle-commande (Instrumentation and Control)
PAL	Réseau logique programmable (Programmable Array Logic)
PDB	Bloc prédéveloppé (Pre-Developed Block)
PLD	Réseau logique programmable (Programmable Logic Device)
RAM	Mémoire vive (Random Access Memory)
RTL	Niveau transfert de registre (Register Transfer Level)
SRAM	Mémoire vive statique (Static RAM)
STA	Analyse temporelle statique (Static Timing Analysis)
VHDL	HDL pour circuits intégrés très rapides (Very High Speed Integrated Circuit HDL)

5 Exigences générales pour les projets HPD

5.1 Généralités

Le présent article commence par situer le HPD dans le contexte relatif aux systèmes d'I&C décrit par l'IEC 61513. Il décrit ensuite le cycle de vie du HPD qui structure le projet du HPD.

Enfin, il énonce des exigences pour les projets HPD, pour l'assurance qualité et pour la gestion de configuration, dont un grand nombre reprend celles des processus de développement logiciel et provient de l'IEC 62138, avec un complément éventuel pour les exigences propres aux HPD, si nécessaire.

Le domaine d'application du présent document, défini à l'Article 1, exclut le développement des technologies microélectroniques et des circuits intégrés vierges. En conséquence, les formulations comme "développement du HPD", "cycle de vie du HPD", "conception du HPD" ou "vérification du HPD" désignent ce qui est effectué au sein du projet d'I&C, en partant de ces technologies microélectroniques pour réaliser le HPD spécifique destiné à être utilisé dans le système d'I&C.

5.2 Cycle de vie

Le processus de réalisation des systèmes d'I&C destinés aux centrales nucléaires de puissance est précisé dans l'IEC 61513 qui introduit le concept de cycle de vie de sûreté d'un système. Ce cycle de vie de sûreté est un moyen par lequel le processus de développement peut être contrôlé et dont il convient que l'adoption permette également d'obtenir les preuves nécessaires à la justification du fonctionnement correct des systèmes de sûreté. Il définit des exigences sur la production de systèmes, mais n'impose pas d'organisation spécifique du projet (voir Figure 1).

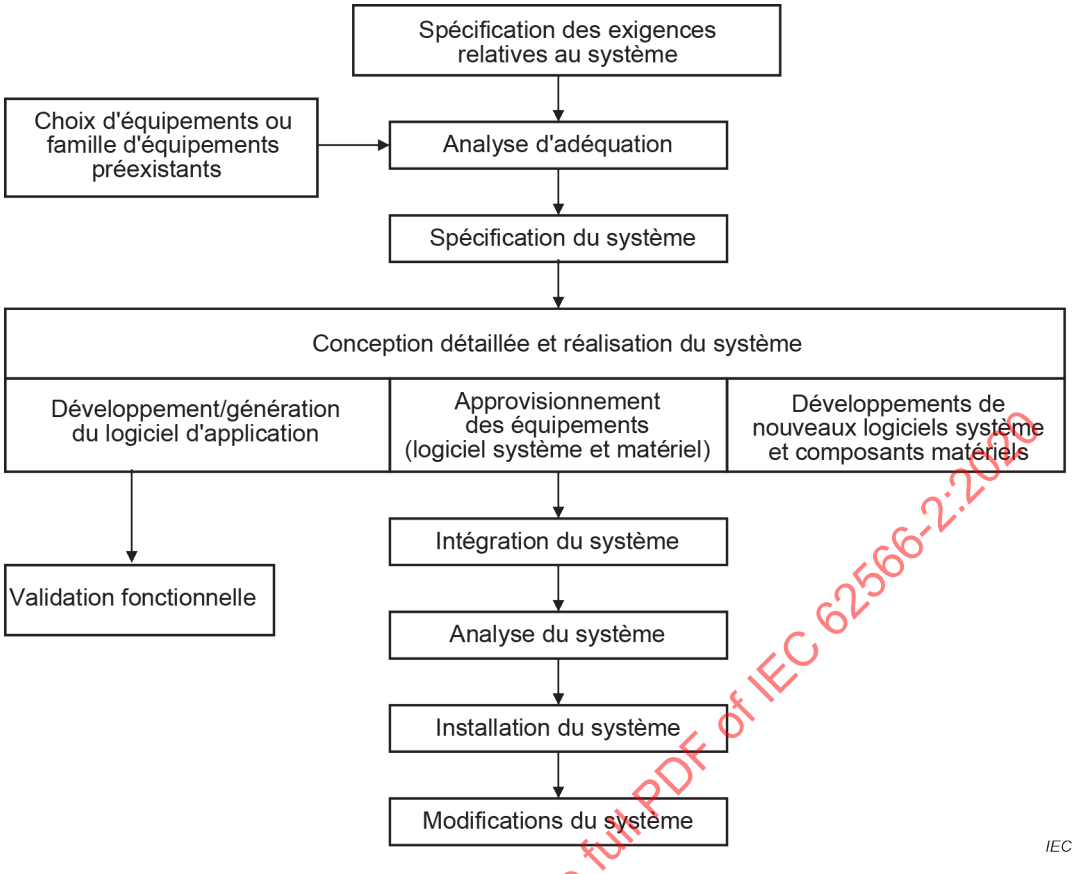


Figure 1 – Cycle de vie d'un système (informatif, tel que défini par l'IEC 61513)

Le cycle de vie d'un système de l'IEC 61513 est complété dans l'IEC 60880 (pour les fonctions de catégorie A) et dans l'IEC 62138 (pour les fonctions de catégories B et C) pour le développement des logiciels, par l'IEC 62566 (pour les fonctions de catégorie A) et l'IEC 62566-2 (pour les fonctions de catégories B et C) pour le développement des HPD et dans l'IEC 60987 pour le développement du matériel des systèmes programmés de classe 1 et 2.

Le développement des HPD fait appel à des outils informatiques qui tendent à structurer le processus de développement selon un cycle comportant des activités dédiées à la conception et à la réalisation, à l'intégration et à la validation, combinées aux activités de vérification et d'essai.

Les phases de conception et de réalisation d'un système de l'IEC 61513 représentées à la Figure 1 (notamment "Approvisionnement des équipements (matériel et logiciel système)" et "Développement des nouveaux matériels et logiciels systèmes opérationnels") constituent des phases essentielles du cycle de vie d'un système de l'IEC 61513. Pour les composants du système qui sont des HPD, ces phases sont décrites à la Figure 2 pour préciser les phases qui se situent entre la spécification des exigences et la validation.

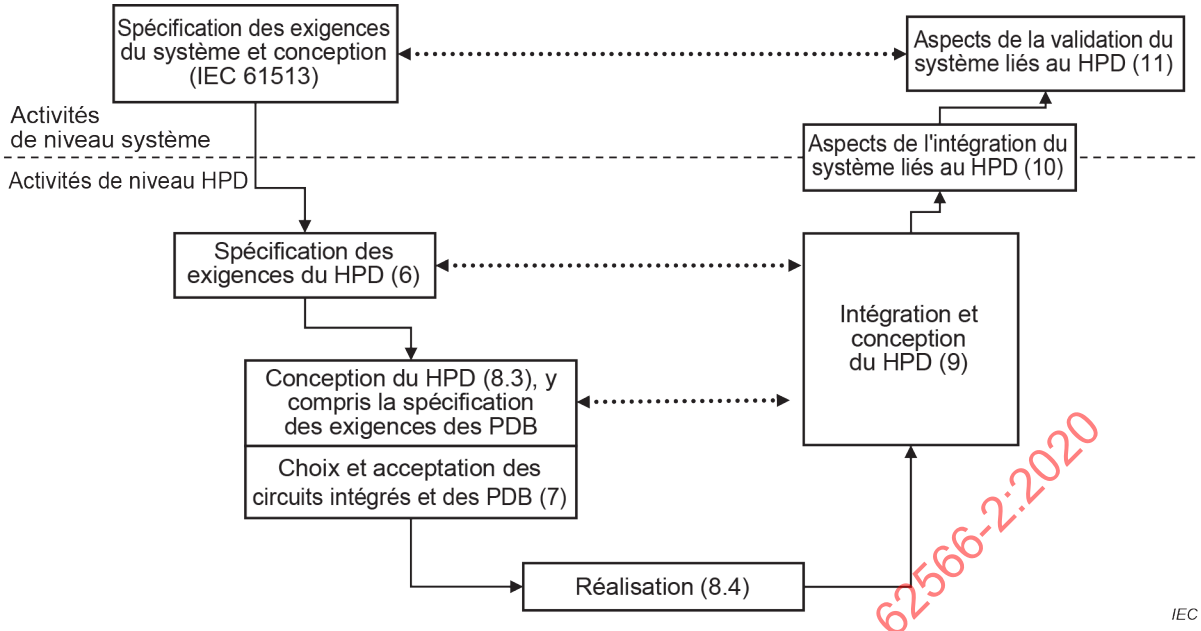


Figure 2 – Cycle de vie du HPD

Le cycle de vie du HPD représenté à la Figure 2 concerne le développement d'un HPD, qui peut être effectué parallèlement à celui d'autres composants (logiciels ou matériels) du système comme le montre la Figure 1. L'ensemble de ces développements converge toutefois lors des phases d'intégration et de validation du cycle de vie du système.

Les activités complémentaires suivantes non représentées sur la Figure 2 viennent aussi en appui du processus de développement des HPD:

- assurance qualité (voir 5.4);
- gestion de configuration (voir 5.5);
- vérification du HPD (voir 5.6);
- activités de modification du HPD (voir Article 12);
- production du HPD (voir Article 13);
- choix d'outils (voir Article 15).

5.3 Principes de gradation

En conséquence de la gradation de l'importance pour la sûreté des fonctions de catégories A, B et C (voir l'IEC 61226), une gradation adéquate a été définie pour les exigences applicables aux HPD des systèmes d'I&C de classes de sûreté 1, 2 et 3.

L'application des exigences du présent document aux HPD de la classe de sûreté 3 confère un niveau de confiance de base adapté aux HPD d'un système d'I&C identifié comme important pour la sûreté. Les principes retenus sont:

- le fait de s'appuyer sur l'assurance qualité;
- une attention particulière accordée à l'assurance que les HPD:
  - contribuent autant que nécessaire aux fonctions de sûreté et n'ont pas d'effet négatif sur elles;
  - sont conformes aux énoncés de la spécification des exigences du HPD définissant les contraintes importantes pour la sûreté;

- l'assurance que les opérateurs du système d'I&C seront informés aussi tôt que raisonnablement possible des erreurs et défaillances du HPD susceptibles d'affecter les fonctions identifiées comme importantes pour la sûreté, de façon à permettre toute action appropriée;
- la documentation des spécifications d'exigences et de conception, du plan d'intégration, du plan d'essai du HPD (à savoir simulation, essai fonctionnel), des aspects HPD du plan de validation du système et des spécifications de modification.

Pour les HPD de la classe de sûreté 2, en plus des principes déjà mentionnés pour les HPD de la classe 3, les principes retenus par la présente norme sont les suivants:

- des exigences plus sévères pour le choix des blocs prédéveloppés et des blocs natifs;
- des exigences plus sévères pour la validation fonctionnelle;
- des exigences plus sévères pour la vérification, le choix et l'utilisation des outils et des langages de développement du HPD;
- des exigences explicites pour la simplicité, la clarté, la précision, la vérifiabilité, et l'aptitude à l'essai et à la modification.

Lorsque des exigences sont applicables pour les deux classes de sûreté, l'étendue de la justification de la conformité à la présente norme peut être modulée en fonction de la classe de sûreté, c'est-à-dire que pour la classe 3, l'étendue pourra être plus faible que pour la classe 2. De plus, l'étendue de la justification pour les fonctions qui ne sont pas "importantes pour la sûreté" réalisées dans des systèmes de classe 2 ou 3 peut se limiter à la manière dont la conception assure que de telles fonctions ne mettent pas en péril les fonctions qui sont identifiées comme importantes pour la sûreté.

5.4 Assurance qualité pour HPD

5.4.1 Généralités

Le 6.3.2.1 de l'IEC 615:2011 énonce des exigences générales pour l'assurance qualité au niveau d'un système d'I&C. Le présent paragraphe énonce des exigences complémentaires spécifiques ou d'une importance particulière pour les HPD.

5.4.2 Le développement des HPD doit être réalisé selon un cycle de vie du HPD. Les dispositions de ce cycle de vie du HPD doivent être spécifiées dans un plan d'assurance qualité.

Ce plan d'assurance qualité peut faire partie du plan d'assurance qualité du système, ou être un plan d'assurance qualité HPD spécifique.

5.4.3 Si un plan d'assurance qualité HPD spécifique est utilisé, il doit être cohérent avec le plan d'assurance qualité du système. Les deux plans doivent répondre aux exigences applicables du 6.3.2 de l'IEC 61513:2011.

5.4.4 Le plan d'assurance qualité doit décomposer la phase de développement du cycle de vie du HPD en activités spécifiées. Ces activités doivent comprendre les activités nécessaires pour obtenir le niveau de qualité HPD exigé, et pour vérifier et démontrer que cette qualité a été obtenue.

5.4.5 La spécification d'une activité doit préciser:

a) ses objectifs;

b) ses relations et ses interactions avec les autres activités;

c) ses entrées et ses résultats;

d) l'organisation et les responsabilités pertinentes pour cette activité;

e) les activités de vérification associées, comme exigé par le 5.6.

5.4.6 Il convient que le contenu et les propriétés exigés des entrées et des résultats soient également spécifiés.

5.4.7 Le plan d'assurance qualité doit exiger que:

a) la réalisation de chacune de ces activités soit assignée à des personnes compétentes dotées de ressources adéquates.

b) les modifications de documents approuvés soient identifiées, revues et approuvées par des personnes autorisées.

c) les méthodes, langages, outils, règles et normes utilisés soient identifiés et documentés, connus et dans le domaine de compétence des personnes impliquées dans le développement.

d) si plusieurs méthodes, langages, outils, règles et/ou normes sont utilisés, ceux qui sont à utiliser pour chaque activité soient clairement identifiés.

e) les termes, expressions, abréviations et conventions utilisés dans un sens spécifique au projet soient explicitement définis.

f) les non-conformités rencontrées soient suivies et résolues.

g) des enregistrements résultant de son application soient produits. En particulier, il doit exiger que les résultats des vérifications et revues soient enregistrés y compris leur portée, les conclusions atteintes et les décisions prises. Les non-conformités au plan d'assurance qualité doivent être documentées et justifiées.

h) la documentation produite constitue un ensemble approprié et cohérent de documents se référençant les uns les autres, garantissant la traçabilité de la conception finale par rapport aux exigences d'entrée.

5.5 Gestion des configurations

5.5.1 Généralités

Le 6.3.2.3 de l'IEC 61513:2011 énonce des exigences pour la gestion de configuration au niveau du système d'I&C. Le présent paragraphe énonce des exigences complémentaires spécifiques ou d'une importance particulière pour les HPD.

5.5.2 La gestion de configuration pour les HPD doit être réalisée conformément aux dispositions d'un plan de gestion de configuration ou du plan d'assurance qualité. Ces dispositions doivent être cohérentes avec celles du niveau du système.

5.5.3 La gestion de configuration doit enregistrer les éléments suivants:

a) documentation des modules (blocs) développés dans le cadre du projet et des PDB;

b) marquage identifiant les circuits intégrés;

c) fichiers d'ordinateur utilisés pour la simulation, la vérification et la production, permettant de reproduire et d'auditer les résultats;

d) paramètres des activités automatisées des outils logiciels (voir Article 15), comme "optimisation des temps de propagation, optimisation de la densité" pour l'activité de placement et routage;

e) identification des versions de tous les outils logiciels (voir Article 15), y compris les "correctifs" appliqués, et des bibliothèques générales ou liées à des technologies particulières;

f) fiches d'errata contenant des avertissements sur les bogues identifiés dans les outils logiciels.

5.5.4 Le plan de gestion de configuration doit spécifier les moyens techniques permettant l'authentification des éléments HPD gérés en configuration, ainsi que de leurs versions.

5.5.5 Le plan de gestion de configuration doit assurer une identification non ambiguë de la version du HPD attachée à une version donnée du système ou d'un équipement, ainsi que des versions de ses éléments constitutifs.

5.6 Vérification du HPD

5.6.1 Un plan de vérification doit définir la portée des vérifications et des revues devant être réalisées sur le HPD.

5.6.2 Le plan de vérification doit répondre aux exigences du 6.3.2.2 de l'IEC 61513:2011 lorsqu'elles sont relatives aux HPD.

5.6.3 Les vérifications et revues doivent être réalisées conformément à des dispositions documentées. Le plan de vérification doit assurer que:

a) les résultats de la vérification sont gérés en configuration;

b) toutes les activités de vérification ont des entrées précisément identifiées et que les résultats sont cohérents avec ces entrées;

c) les activités satisfont aux objectifs spécifiés, que les résultats présentent le contenu et les propriétés exigés et qu'ils sont conformes aux décisions prises;

d) les résultats sont clairs, précis et à jour;

e) les résultats sont conformes aux règles applicables;

f) les résultats sont conformes aux exigences applicables du présent document.

"Précisément identifiées" signifie que la version est connue sans ambiguïté. "Clairs" signifie que les personnes qui ont à lire un document peuvent le comprendre sans effort excessif même si elles n'ont pas été précédemment impliquées dans le projet, à condition qu'elles disposent des connaissances nécessaires. "Précis" signifie qu'il n'y a pas ambiguïté.

Il se peut que l'étendue des activités de vérification et de revue dépende de la taille et de la nature du HPD et des résultats à vérifier ou à revoir, ainsi que des méthodes et outils utilisés. Il se peut que l'étendue des activités de vérification et de revue soit moins importante pour les exigences non identifiées comme importantes pour la sûreté (voir exigence 6.2.5) et ne pouvant pas nuire aux fonctions identifiées comme importantes pour la sûreté.

5.6.4 Il convient que le plan de vérification garantisse que les enregistrements soient produits de façon à ce que le processus de vérification puisse faire l'objet d'audit complet, c'est-à-dire qu'il soit possible de confirmer de façon indépendante la mise en œuvre du plan de vérification.

5.6.5 La vérification des résultats d'une activité doit être réalisée par des personnes compétentes n'ayant pas participé à cette activité.

5.6.6 Il convient d'inclure dans la vérification des résultats d'une activité des représentants de ceux concernés par l'usage de ces résultats, ainsi que d'autres experts si nécessaire.

5.6.7 La spécification des exigences du HPD, la spécification de conception du HPD et le plan de validation du HPD doivent être vérifiés.

5.6.8 La vérification du HPD doit être effectuée par des personnes n'ayant pas participé au développement de ce HPD.

5.6.9 *Pour la classe 2, l'application des règles de conception et de réalisation doit être vérifiée (voir 8.3.3 pour les règles de conception recommandées).*

5.6.10 *Pour la classe 2, les personnes qui effectuent la vérification devraient avoir une indépendance de gestion par rapport aux développeurs.*

6 Spécification des exigences du HPD

6.1 Généralités

6.1.1 Vue d'ensemble

Le présent paragraphe complète et précise les exigences du 6.2.3.4 de l'IEC 61513:2011.

6.1.2 Un document de spécification des exigences du HPD doit donner toutes les exigences du HPD, soit dans le document lui-même, soit par renvoi à des ensembles d'exigences établies au niveau système ou sous-système (par exemple, comportement fonctionnel à implémenter).

6.1.3 Il convient que la spécification des exigences du HPD soit non ambiguë, vérifiable et réalisable, y compris pour les aspects temporels.

6.1.4 Si le HPD réalise une fonction de sûreté, sa spécification des exigences doit découler des exigences du système d'I&C hébergeant cette fonction et doit faire partie de la spécification du sous-système qui utilise le HPD.

6.1.5 Il convient que la spécification des exigences du HPD décrive ce qu'il y a à faire, et non la manière dont cela doit être fait.

En principe, l'objectif de la spécification des exigences du HPD est de préciser ce que le HPD doit accomplir sans spécifier comment. Cependant, il se peut que des contraintes de conception et de réalisation doivent être spécifiées si cela est nécessaire compte tenu de la conception du système d'I&C ou de l'architecture d'I&C.

6.1.6 La spécification des exigences du HPD doit être une référence pour la conception du HPD, les aspects HPD de la validation système et, le cas échéant, les modifications du HPD.

La spécification des exigences du HPD peut faire référence directement à des documents d'entrée de façon à éviter des duplications inutiles et à réduire le plus possible les risques d'incohérence. Elle peut aussi faire référence à des documents déjà existants, tels que la documentation de blocs natifs et d'autres blocs prédéveloppés.

6.1.7 La spécification des exigences du HPD doit assurer la traçabilité par rapport à ses documents d'entrée.

6.1.8 Il convient de vérifier que la spécification des exigences du HPD est cohérente et complète par rapport à tous ses documents d'entrée (voir Figure 2).

6.1.9 Les références éventuelles faites par la spécification des exigences du HPD à d'autres documents doivent être précises de façon à éviter toute ambiguïté.

6.1.10 *Pour la classe 2, il convient que les notations, règles et normes utilisées pour la spécification des exigences du HPD contribuent à sa clarté et à sa précision, et qu'elles soient choisies en tenant compte de celles utilisées pour les entrées et de celles retenues pour la conception et la réalisation du HPD.*

Une méthode de spécification unique ne permettant pas toujours d'exprimer clairement, précisément et de façon vérifiable tout besoin de spécification, plusieurs méthodes complémentaires peuvent être utilisées dans une même spécification des exigences du HPD.

6.2 Aspects fonctionnels de la spécification des exigences

6.2.1 Généralités

Le présent paragraphe décrit le contenu de la spécification des exigences directement lié aux besoins fonctionnels.

6.2.2 La spécification des exigences doit préciser:

a) les fonctions devant être assurées par le HPD;

b) les différents modes de fonctionnement du HPD ainsi que les conditions de transition correspondantes, y compris la mise sous tension, l'initialisation et, le cas échéant, la définition des états sûrs;

c) les interfaces du HPD et ses interactions avec son environnement (opérateurs et autres composants d'I&C), y compris les rôles, protocoles, types, formats, numérotation des bits, domaines de valeur et contraintes des entrées et des sorties;

d) les paramètres du HPD qui peuvent être modifiés manuellement en cours de fonctionnement et leurs rôles;

e) les performances et, le cas échéant, le temps de réponse du HPD;

f) ce que le HPD ne doit pas faire ou doit éviter, le cas échéant;

g) les contraintes et les règles à respecter lors de la conception et de la réalisation du HPD à des fins de vérifiabilité et de robustesse.

6.2.3 Il convient que la spécification des exigences du HPD précise également les conditions d'utilisation (par exemple les taux de sollicitation), notamment les conditions les plus défavorables imposées au HPD par son environnement.

6.2.4 Il convient que la spécification des exigences du HPD établisse les objectifs de qualité du HPD à respecter par la conception et la réalisation du HPD à des fins de conformité et de robustesse.

6.2.5 La spécification des exigences du HPD doit identifier la catégorie de sûreté associée aux fonctions spécifiées et aux exigences.

6.2.6 *Pour la classe 2, il convient que la spécification des exigences évite les fonctionnalités inutiles en ce qui concerne les exigences au niveau système ou sous-système.*

En principe, il est préférable que les HPD n'aient pas plus de fonctionnalités que ce qui est exigé afin de réduire le plus possible la complexité. Cependant, les pratiques industrielles actuelles étant basées sur l'utilisation de composants prédéveloppés, l'introduction de capacités non exigées peut être justifiée.

En ce qui concerne les 6.2.2, 6.2.3 et 6.2.6, il se peut que les exigences de fonctionnalité, d'interface et de performance dépendent du mode de fonctionnement, des valeurs des paramètres, des données de configuration et des conditions imposées au HPD.

6.3 Détection des défauts et tolérance aux fautes

La spécification des exigences du HPD doit spécifier les modes de fonctionnement exigés en cas de détection d'erreurs ou de défaillances.

Par exemple, ceci peut inclure des contraintes visant:

a) à augmenter la capacité du HPD et du système d'I&C à tolérer les défauts (dus à des événement perturbant unique, par exemple), à détecter et signaler aux opérateurs les erreurs et les défaillances, à effectuer des actions ou à adopter les modes de fonctionnement spécifiés à la suite d'une détection de défaillances;

b) à garantir que les erreurs des opérateurs et les défaillances des autres systèmes et équipements avec lesquels le HPD interagit ou partage des ressources n'auront pas de conséquences inacceptables.

6.4 Capture des exigences avec des outils ESL

6.4.1 Généralités

La présente norme ne prescrit pas de méthode spécifique pour la capture des exigences du HPD. Si elles sont capturées avec des outils au niveau système électronique (ESL, voir Annexe A), les exigences des 6.4.2 et 6.4.3 s'appliquent à ces outils et à leur utilisation.

Dans le cas de l'utilisation d'outils ESL, si le langage de spécification des exigences est semblable aux langages de réalisation, l'exigence 6.1.5 (séparation entre ce qui doit être fait (l'exigence) et la manière de le faire (la conception)) peut être remplacé par d'autres moyens, par exemple des commentaires pour spécifier les entrées, les sorties et les algorithmes.

6.4.2 Exigences relatives au formalisme des outils ESL

6.4.2.1 Si les exigences du HPD sont capturées à l'aide d'un outil ESL:

a) cet outil doit offrir un formalisme doté d'une sémantique rigoureuse et compréhensible (normalisation de la structure et de la présentation, modularité, commentaires pertinents);

b) le formalisme de l'outil ESL doit être compréhensible par tous les participants;

c) si l'outil propose des mécanismes flexibles pour redéfinir les fonctions et opérateurs, il convient que les caractéristiques réelles de tout élément donné soient claires pour tous les participants.

6.4.2.2 Il convient que les langages ESL utilisés permettent la prise en compte de l'architecture du système, par exemple en permettant l'assignation de fonctions à des composants, et supportent les caractéristiques de conception tolérantes aux fautes.

6.4.3 Interface avec les outils de conception

La sémantique des langages utilisés pour exprimer la spécification des exigences au niveau ESL pourra différer de celle des langages HDL employés pour la conception. Des exemples d'écarts possibles sont l'interprétation du parallélisme, la gestion des dépassements de capacité ou le codage des types et des machines à états finis.

a) Si la sémantique du langage utilisé pour exprimer la spécification des exigences au niveau ESL diffère de la sémantique des autres langages employés dans le projet, les écarts doivent être identifiés pour chaque élément concerné de la spécification des exigences;

b) chaque occurrence d'écart au sein de la spécification des exigences doit être documentée. Une liste générique d'écarts entre les langages concernés constitue une référence utile, mais ne suffit pas à clarifier la spécification des exigences.

7 Processus d'acceptation des circuits intégrés programmables, des blocs natifs et des blocs prédéveloppés

7.1 Généralités

Le 6.2.3.2 de l'IEC 61513:2011 énonce des exigences générales pour le choix de composants préexistants (pas nécessairement des composants du HPD). Le présent paragraphe énonce des exigences complémentaires spécifiques ou d'une importance particulière pour les HPD.

7.2 Processus d'acceptation des circuits intégrés programmables et des blocs natifs incorporés

7.2.1 Généralités

L'approche générale pour le choix et l'acceptation de circuits intégrés programmables vierges et leurs blocs natifs incorporés est donnée à la Figure 3.

Certains blocs natifs représentent les ressources configurables du circuit intégré et sont généralement utilisés dans toute conception du HPD. De tels blocs natifs sont acceptés comme une partie du circuit intégré pendant l'analyse d'adéquation de ce dernier.

D'autres blocs natifs pourront représenter des éléments de conception de plus haut niveau, tels que multiplicateurs et contrôleurs de transmission en série. Ces blocs natifs sont optionnels dans le sens où il est possible de ne pas les instancier lors de la conception du HPD. Lorsqu'ils sont employés, ces blocs natifs doivent être évalués et acceptés conformément aux critères d'acceptation des PDB (voir 7.3).

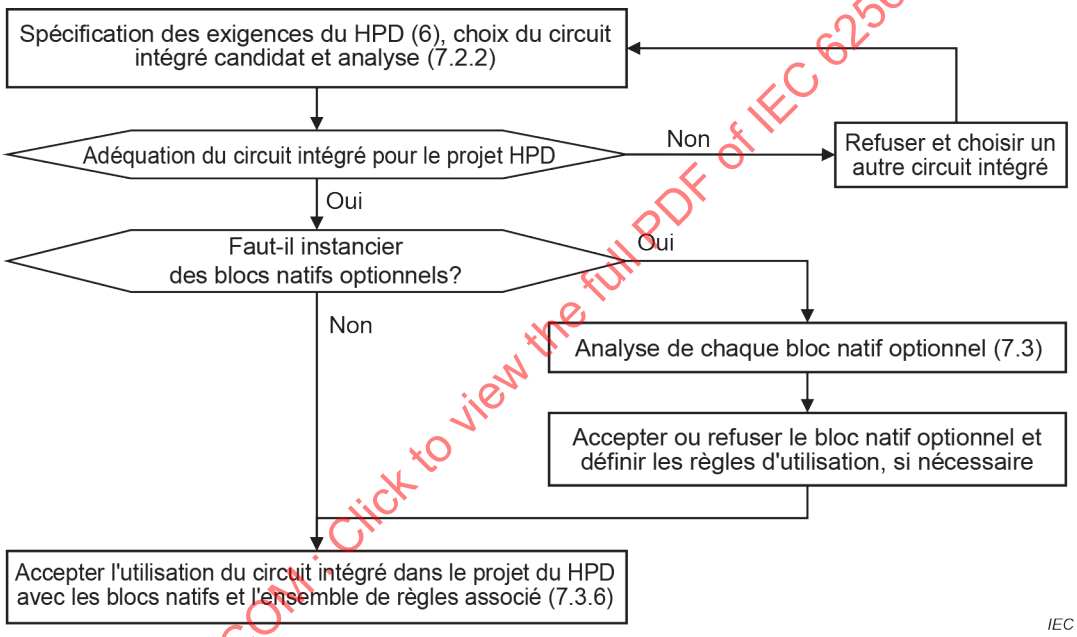


Figure 3 – Aperçu du processus de choix et d'acceptation pour les circuits intégrés vierges et les blocs natifs

7.2.2 Acceptation du circuit intégré

7.2.2.1 Le circuit intégré candidat doit être analysé du point de vue des exigences du HPD.

7.2.2.2 Il convient que l'analyse tienne compte des propriétés suivantes du circuit intégré candidat:

a) technologie de circuit intégré (CPLD, FPGA, etc.);

b) technologie de configuration (antifusible, flash, SRAM, etc.);

c) nombre d'éléments logiques, marge d'utilisation des ressources et adéquation de l'architecture interne et des blocs natifs;

d) nombre de broches d'entrée/sortie, facteur de forme et boîtier de circuit intégré (boîtier Quad Flat, matrice de billes, etc.);

e) consommation;

f) fréquence de fonctionnement maximale;

g) fiabilité du matériel et durée de conservation de la configuration programmée;

h) conditions d'environnement;

i) adéquation des outils de développement en ce qui concerne les exigences de l'Article 15.

D'autres facteurs pouvant être considérés durant la sélection des candidats de circuits intégrés sont le système de gestion de la qualité du fabricant, la disponibilité estimée dans le futur des circuits intégrés et de leurs retours d'expérience.

7.2.2.3 Si le circuit intégré candidat ne convient pas à l'application concernée, il doit être refusé et une autre solution doit être trouvée.

7.2.2.4 Si un ou plusieurs blocs natifs optionnels du circuit intégré choisi doivent être instanciés lors de la conception du HPD, chacun d'eux doit être accepté pour cette utilisation conformément au 7.3.

Le refus d'utiliser un bloc natif optionnel lors de la conception du HPD n'implique pas le refus du circuit intégré lui-même.

7.3 Processus d'acceptation pour les PDB

7.3.1 Généralités

L'approche générale pour le choix et l'acceptation des PDB est donnée à la Figure 4.

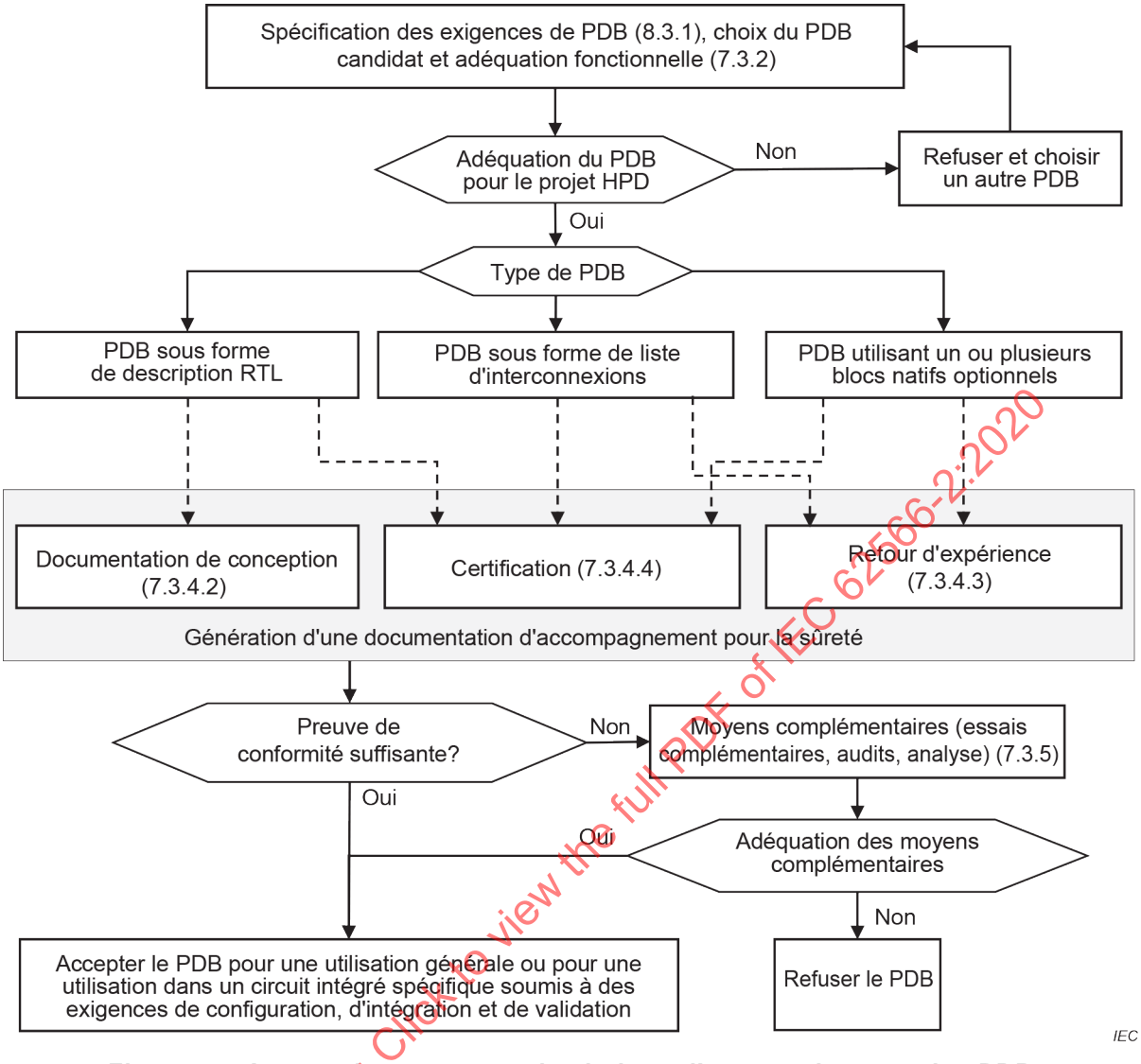


Figure 4 – Aperçu du processus de choix et d'acceptation pour les PDB

7.3.2 Adéquation fonctionnelle des PDB

7.3.2.1 Généralités

Le présent paragraphe a pour objectif d'assurer que le PDB répond bien aux exigences qui lui sont applicables.

7.3.2.2 La documentation de sûreté (voir 7.3.3) des PDB doit être évaluée par rapport à la spécification des exigences du HPD (voir Article 6) et par rapport à la spécification des exigences des PDB (voir 8.3.1.2). Les incohérences doivent être résolues.

7.3.2.3 *Pour la classe 2, il convient d'identifier les fonctions du PDB non nécessaires pour satisfaire à la spécification des exigences des PDB. Il convient de justifier que ces fonctions ne dégradent pas la sûreté.*

7.3.3 Documentation de sûreté des PDB

7.3.3.1 La documentation des PDB doit préciser comment les concepteurs utiliseront les PDB en accord avec leurs spécifications et leurs caractéristiques de conception.

Dans la présente norme, le document ou l'ensemble de documents correspondant est appelé documentation de sûreté. Quand le PDB fait partie d'un équipement ou d'une famille d'équipements, cette documentation peut être incluse dans la documentation de sûreté de l'équipement ou de la famille d'équipements.

La documentation de sûreté comprend généralement plus que la documentation d'utilisation délivrée par le fournisseur du PDB. Par exemple, elle peut comporter des informations obtenues à partir de la conception des PDB, d'essais, de mesures, et/ou d'analyses complémentaires, ou par le retour d'expérience.

7.3.3.2 Une documentation de sûreté doit comprendre la description:

a) des fonctions incluses;

b) des interfaces externes;

c) des rôles, types, formats, domaines de valeur et contraintes des entrées, sorties, signaux d'exception, paramètres et données de configuration, des informations concernant des machines à états finis, le cas échéant;

d) des différents modes de fonctionnement et des conditions de transition correspondantes;

e) de toute contrainte devant être respectée lors de l'utilisation du PDB.

7.3.3.3 *Pour la classe 3, il convient que la documentation de sûreté fournisse des informations sur les performances des fonctions (les temps de réponse, par exemple)*.

7.3.3.4 *Pour la classe 2, le cas échéant, il convient que les contraintes à respecter lorsqu'on utilise des PDB (voir 7.3.3.2) permettent de s'assurer convenablement de la conformité du PDB et de la conception du système*.

7.3.3.5 *Pour la classe 2, la documentation de sûreté doit fournir des informations sur les performances des fonctions (les temps de réponse, par exemple)*.

7.3.4 Production d'une documentation de sûreté d'accompagnement

7.3.4.1 Généralités

7.3.4.1.1 Une analyse documentée de chaque PDB utilisé dans le HPD doit démontrer qu'il remplit les exigences qui lui sont affectées.

7.3.4.1.2 La preuve de la conformité des PDB par rapport à leur documentation de sûreté devra être apportée.

7.3.4.1.3 Il convient que les PDB fournis sous la forme d'une description RTL soient choisis et approuvés au moyen d'une revue de la documentation de conception (voir 7.3.4.2) ou d'une certification (voir 7.3.4.4).

7.3.4.1.4 Il convient que les PDB fournis sous la forme d'une liste d'interconnexions soient choisis et approuvés au moyen d'une revue du retour d'expérience (voir 7.3.4.3) ou d'une certification (voir 7.3.4.4).

7.3.4.1.5 Il convient que les blocs natifs optionnels soient choisis et approuvés au moyen d'une revue du retour d'expérience (voir 7.3.4.3) ou d'une certification (voir 7.3.4.4).

7.3.4.1.6 En cas d'impossibilité d'apporter la preuve complète de la conformité des PDB au moyen d'une revue de la documentation de conception, d'une revue du retour d'expérience ou d'une certification, ou d'une combinaison de ces méthodes, des moyens complémentaires doivent être mis en œuvre conformément au 7.3.5 de la présente norme.

7.3.4.1.7 La documentation doit préciser si le PDB est soumis à une acceptation générique, valide pour une utilisation dans tout type de circuit intégré, ou si le PDB est accepté uniquement pour une utilisation dans le circuit intégré utilisé dans le cadre du projet du HPD.

7.3.4.2 Revue de la documentation de conception

7.3.4.2.1 Généralités

Une revue du retour d'expérience peut être utilisée en appui de la justification de conformité des PDB dans les conditions suivantes:

7.3.4.2.2 La revue de la documentation de conception doit démontrer que le PDB est conforme aux exigences qui lui sont appliquées, comme précisé dans sa documentation de sûreté.

7.3.4.2.3 *Pour la classe 2, l'analyse de la documentation doit démontrer que les fonctions et les modes de l'élément prédéveloppé non utilisés dans le HPD ne perturbent pas ceux qui sont utilisés.*

7.3.4.3 Revue du retour d'expérience

Un retour d'expérience pertinent, suffisant et favorable peut être utilisé en appui de la justification de conformité des PDB dans les conditions suivantes:

Si le retour d'expérience est invoqué:

a) l'analyse du retour d'expérience doit démontrer que:
   i) son volume est proportionné aux exigences de fiabilité;
   ii) il a été obtenu dans des conditions de fonctionnement équivalentes à celles dans lesquelles le PCB sera utilisé;
   iii) l'utilisation réelle du PDB a été observée au niveau de détail généralement exigé par le présent document pour la documentation;

b) pour la classe 2, les moyens et procédures utilisés pour recueillir le retour d'expérience doivent garantir que toute défaillance du PDB lors de la période prise en compte est enregistrée avec suffisamment de détails pour qu'une analyse technique puisse en identifier la cause lorsque c'est possible;

c) pour la classe 2, la démonstration doit être apportée que toute défaillance identifiée sur le PDB candidat a été correctement analysée et que les défauts de PDB correspondants ont été corrigés ou qu'il existe une contrainte applicable précisée dans la documentation de sûreté;

d) pour la classe 2, une analyse technique documentée doit justifier que toutes les interactions du PDB avec son environnement sont comprises dans celles que couvre le retour d'expérience;

e) pour la classe 2, le retour d'expérience pris en compte doit correspondre à des versions précisément identifiées du PDB et, lorsque cet élément est spécifique à un équipement, à des versions précisément identifiées de l'équipement dans lequel il opère;

f) pour la classe 2, il convient que le retour d'expérience concerne la version spécifique de l'élément prédéveloppé ou de sa sous-partie utilisée dans le HPD. Sinon, les différences entre les deux versions doivent être analysées pour démontrer que le retour d'expérience est pertinent pour la version envisagée.

7.3.4.4 Certification de PDB

7.3.4.4.1 Généralités

Les démonstrations apportées par la certification des PDB peuvent appuyer la justification de conformité des PDB dans les conditions suivantes:

7.3.4.4.2 La norme de sûreté utilisée pour la certification du PDB doit couvrir explicitement le processus de développement du PDB.

7.3.4.4.3 La certification prise en compte doit être documentée.

7.3.4.4.4 L'identification précise du PDB certifié doit être documentée. S'il a été certifié dans le cadre d'un produit plus large (par exemple dans le cadre de la certification d'un équipement ou d'une famille d'équipements), l'identification précise de ce produit doit aussi être documentée.

7.3.4.4.5 *Pour la classe 2, les démonstrations supportant la certification doivent pouvoir être évaluées, en particulier:*

a) les conditions de la certification (par exemple les conditions d'utilisation et les hypothèses retenues);

b) les méthodes et les outils utilisés pour la certification;

c) les résultats obtenus (par exemple les propriétés et/ou les mesures certifiées).

7.3.4.4.6 *Pour la classe 2, la pertinence de ces conditions et de ces résultats pour l'établissement de la conformité et pour le système I&C doit être justifiée.*

7.3.4.4.7 *Pour la classe 2, il convient que l'efficacité des méthodes et des outils utilisés pour la certification soit établie.*

7.3.4.4.8 *Pour la classe 2, l'entité certificatrice doit être identifiée et doit être compétente pour les propriétés et/ou les mesures certifiées.*

7.3.4.4.9 *Pour la classe 2, il convient que la version du PDB certifié soit la même que celle qui est utilisée dans le système d'I&C. Sinon, les différences entre les deux versions doivent être analysées pour démontrer la pertinence de la certification pour la version envisagée.*

7.3.5 Moyens complémentaires

7.3.5.1 Lorsque la justification du PDB conformément à une revue de la documentation de conception, d'une revue du retour d'expérience ou d'une certification, ou d'une combinaison de ces méthodes ne peut être complète, des moyens complémentaires (par exemple des essais supplémentaires, une analyse, des audits) doivent être mis en œuvre en support de la justification de la conformité des PDB, avec un niveau de confiance équivalent.

7.3.5.2 Lorsque des moyens complémentaires sont utilisés pour fournir la preuve de conformité, il convient que les critères d'acceptation soient spécifiés et justifiés dans les premières phases de développement du HPD. Il convient que ces critères soient justifiés en prenant en compte les exigences de la présente norme vis-à-vis desquelles la conformité n'a pas été établie de manière adéquate.

7.3.5.3 Lorsque les moyens complémentaires ne parviennent pas à apporter une justification appropriée, le PDB doit être rejeté.

7.3.6 Règles d'utilisation

7.3.6.1 Généralités

L'utilisation de fonctions ou de modes de fonctionnement des PDB exigés pour réaliser le HPD pourra être contrôlée par des règles afin d'améliorer des propriétés de conception telles que la sûreté ou l'aptitude à l'essai.

7.3.6.2 Si l'élément prédéveloppé comporte des fonctions, des configurations ou des modes de fonctionnement non exigés dans le HPD, il convient que des règles d'utilisation soient définies pour empêcher l'utilisation de ces fonctions et modes.

7.3.6.3 Si des règles d'utilisation sont établies:

a) elles doivent être documentées;

b) le plan de vérification doit garantir que leur application est vérifiée dans le cadre du projet.

7.3.7 Modification pour l'acceptation

7.3.7.1 Généralités

En général, les modifications des PDB par le concepteur du HPD sont uniquement possibles pour les PDB fournis sous la forme de code source HDL.

7.3.7.2 Si des modifications du PDB sont nécessaires pour son acceptation, elles doivent être spécifiées, conçues, réalisées et vérifiées.

7.3.7.3 Ces modifications doivent être effectuées et documentées conformément aux exigences de ce document en matière de structuration et de gestion du projet, de qualité, de spécification des exigences, de conception, de réalisation et de vérification.

8 Conception et réalisation du HPD

8.1 Généralités

Le présent article précise les exigences et les recommandations issues des bonnes pratiques de conception et de réalisation afin d'obtenir un HPD ayant les caractéristiques de sûreté appropriées, aussi exempt de défaut que possible et apte à la vérification.

La phase de conception et de réalisation du HPD doit être documentée.

Le document ou l'ensemble de documents correspondant se compose de la spécification de conception du HPD (voir 8.3.6) et de la documentation de réalisation du HPD (voir 8.4.7).

8.2 Langages de description de matériel (HDL) et outils associés

8.2.1 Généralités

Même si l'utilisation de langages et d'outils spécifiques ne peut pas être exigée, les points suivants peuvent être pris en compte comme des règles de base communes aux langages et aux outils employés pour la conception et la réalisation des HPD pour les systèmes de classe 2 et 3.

8.2.2 Il convient que la conception et la réalisation utilisent des langages de description de matériel (HDL) et des outils pour la simulation, la synthèse, le placement et le routage.

NOTE Des outils convenablement choisis et utilisés améliorent des aspects essentiels tels que l'intelligibilité des descriptions, la gestion des contraintes électriques et temporelles, la vérification, la pertinence des critères de couverture et la documentation.

8.2.3 Même si le 8.2.2 n'est pas respecté, tous les documents et toutes les analyses ou vérifications exigés par la présente norme doivent être fournis.

8.2.4 Les langages utilisés:

a) doivent suivre des règles strictes (ou bien définies) de sémantique et de syntaxe;

b) doivent avoir une syntaxe définie et documentée de façon claire et exhaustive;

c) il convient qu'ils respectent en principe une norme reconnue (par exemple IEEE 1076 pour VHDL, IEEE 1364 pour Verilog ou IEEE 1800 pour SystemVerilog).

8.3 Conception

8.3.1 Généralités

8.3.1.1 Les entrées du processus de conception du HPD doivent comprendre la spécification des exigences du HPD.

Elles peuvent également comprendre d'autres documents, tels que les contraintes spécifiques du projet et/ou les règles et normes applicables.

8.3.1.2 La phase de conception doit produire:

a) une description de l'organisation générale du HPD;

b) l'identification du circuit intégré à utiliser (le choix et l'acceptation du circuit intégré à utiliser devant être basés sur la spécification d'exigences du HPD et être réalisés selon les exigences du 7.2);

c) une description de la conception du fonctionnement global du HPD dans les conditions et modes de fonctionnement exigés par la spécification des exigences du HPD;

d) les exigences affectées à chaque bloc utilisé lors de la conception. Pour les blocs à mettre en œuvre en utilisant des PDB, ces exigences nécessitent d'être utilisées pour le choix et l'acceptation des PDB conformément aux exigences du 7.3 de la présente norme. Pour les nouveaux blocs, ces exigences nécessitent d'être utilisées pour les nouveaux développements.

8.3.1.3 Il convient que la description de la conception globale donne des informations sur:

a) les descriptions et les configurations des modules RTL développés dans le cadre du projet du HPD;

b) les principales interfaces internes et externes, y compris les interfaces de communication et les liaisons entre composants du HPD et PDB.

8.3.1.4 Il convient que la description du fonctionnement d'ensemble donne des informations sur:

a) les interactions, les protocoles de communication et les flux d'informations;

b) les ordonnancements et les contraintes temporelles;

c) l'utilisation des ressources;

d) la synchronisation entre les différents modules de conception.

8.3.1.5 La conception du HPD doit être produite dans le but d'assurer modularité, et l'aptitude à l'essai et à la maintenance.

8.3.1.6 La documentation de conception du HPD doit permettre d'établir que les énoncés de la spécification des exigences du HPD importants pour la sûreté sont pris en compte dans toutes les conditions spécifiées.

8.3.1.7 *Pour la classe 3, il convient que la spécification de conception du HPD énonce des règles pour la réalisation du HPD*.

8.3.1.8 *Pour l Pour la classe 2, il convient de privilégier une approche de conception descendante*.

8.3.1.9 *a classe 2, la spécification de conception du HPD doit comprendre la conception détaillée (description RTL) de tout module mis en œuvre en HDL*.

8.3.1.10 *Pour la classe 2, pour chaque module réalisé en HDL, il convient que la spécification de conception du HPD spécifie*:

a) les fonctions à fournir par le module, y compris ses interfaces externes, entrées, sorties et données de configuration;

b) les exigences du module concernant son environnement;

c) toute contrainte de réalisation pertinente;

d) toute information que les utilisateurs du module doivent connaître.

8.3.1.11 *Pour la classe 2, la spécification des exigences du HPD doit fournir les informations permettant de prévoir de manière correcte les caractéristiques clés pour la sûreté concernant les performances du système, notamment les temps de réponse maximaux des applications*.

De telles informations peuvent être fournies sous la forme de données, formules et/ou modèles.

8.3.1.12 *Pour la classe 2, il convient que la conception facilite les vérifications*.

8.3.1.13 *Pour la classe 2, la spécification de conception du HPD doit énoncer des règles pour la réalisation du HPD*.

8.3.1.14 *Pour la classe 2, il convient de justifier les écarts par rapport aux règles de conception*.

8.3.2 Détection des défauts

8.3.2.1 La conception doit tenir compte des dispositions retenues dans la spécification des exigences pour détecter les défauts et pour élaborer les informations correspondantes à l'intérieur du HPD.

8.3.2.2 La spécification de conception du HPD doit garantir que les effets de bord négatifs des erreurs et des défaillances du HPD sont éliminés avant le retour à un mode de fonctionnement normal.

8.3.2.3 *Pour la classe 2, lors de la détection d'un défaut, il convient que le HPD se comporte conformément aux exigences spécifiées, notamment en garantissant que les erreurs ou défaillances ne se propagent pas au-delà des limites spécifiées*.

8.3.2.4 *Pour la classe 2, la spécification de conception du HPD et la documentation de conception du système doivent énoncer et justifier les mesures prises pour limiter les effets des modes de défaillance connus ou prévus des PDB pour lesquels des moyens complémentaires de démonstration de conformité ont été utilisés*.

8.3.3 Langage et règles de codage

8.3.3.1 La liste suivante contient des approches et techniques de conception fortement conseillées. Toutefois, la liste n'est pas réputée exhaustive et des parties pourront évoluer avec la technologie.

a) Il convient que la conception du HPD n'utilise que des éléments synthétisables du langage. L'environnement d'essais et de simulation (voir 9.2) peut utiliser tous les éléments du langage. Les blocs natifs (voir 3.26) déjà synthétisés et routés dans le circuit intégré prédéveloppé peuvent être instanciés tels qu'ils sont, s'ils sont conformes à l'Article 7.

b) Il convient d'utiliser, le cas échéant, les ressources dédiées ou les éléments de conception fournis (par exemple arbres d'horloge prédéfinis et circuits de conditionnement d'horloge, rails d'alimentation, arbres de réinitialisation, etc.).

c) Il convient que ces règles de codage couvrent tous les aspects concernés, en particulier l'appellation des modules et des signaux, l'utilisation des éléments de structuration (comme les packages, les fonctions, les procédures, les bibliothèques du projet, l'instanciation), l'organisation des traitements sur les chemins critiques, l'organisation des processus, les constructions recommandées et les constructions interdites.

d) Il convient d'interdire les fonctions utilisant des effets de bords ("impures") dans la description de la conception (Justification: une telle fonction peut retourner des valeurs différentes quand elle est appelée plusieurs fois avec les mêmes paramètres. Elle est donc très difficile à soumettre à essai et à vérifier, car elle brise le concept de fonction et, en fait, de déterminisme).

NOTE 1 Il se peut qu'une fonction impure ait aussi des effets de bord comme la modification d'objets en dehors de sa portée.

e) Il convient d'interdire les constructions qui pourraient induire des différences entre les comportements simulés et synthétisés. Selon le langage utilisé, de telles constructions peuvent par exemple être des affectations incomplètes ou conflictuelles, l'utilisation du caractère "peu importe" dans des comparaisons, des comparaisons (supérieures ou inférieures) impliquant des types énumérés (Justification: la simulation est une méthode de vérification importante. Si les comportements simulés et synthétisés diffèrent, la chaîne de vérification est rompue).

f) Il convient d'initialiser les signaux et les variables non pas dans leur déclaration de la description RTL, mais par un mécanisme explicite tel qu'une initialisation (Justification: il se peut que l'initialisation en HDL induise des différences entre les comportements simulés et synthétisés).

g) Il convient d'interdire l'utilisation de retards explicites dans la description de la conception, car ces retards engendrent des différences entre les comportements simulés et synthétisés.

NOTE 2 Cela n'empêche pas l'existence de retards au niveau système ou dans les exigences du HPD. Cela signifie que de tels retards ne peuvent pas être réalisés par des instructions HDL comme "delay" ou "after" mais, par exemple, par des compteurs ou des registres à décalage.

h) Il convient d'interdire dans la description de la conception la création de retards au moyen de portes combinatoires ou de retards dépendant des temps de propagation dans les interconnexions. Si cela ne peut être évité, des analyses temporelles statiques (STA) doivent justifier l'utilisation d'une telle conception (Justification: ces retards ne sont pas stables par rapport à des paramètres tels que la température, la tension, ou d'un exemplaire du circuit intégré à l'autre, ou d'une zone du circuit intégré à une autre).

i) Il convient que les types des signaux d'interface du HPD aient une définition claire et exempte d'ambiguïté, de préférence normalisée, indépendante de tout outil ou technologie microélectronique.

j) Il convient que les définitions au niveau HDL ne puissent pas être interprétées de plusieurs manières, pour éviter des variations lorsque la compilation est répétée dans des conditions différentes. Par exemple, il convient que les entrées/sorties du HPD soient explicitement assignées à des broches connues.

NOTE 3 Cette disposition ne s'applique pas à la conception des composants des bibliothèques, qui sont prévus pour être instanciés à différents emplacements de conceptions futures avec des assignations différentes des entrées/sorties.

Pour concevoir du code HDL portable sur différentes technologies, il est nécessaire que l'assignation des broches soit définie dans un fichier de contraintes et non dans le code HDL. Des éléments du langage tels que les "templates" en VHDL-2008 pourront y aider.

8.3.3.2 *Pour la classe 2, afin d'améliorer la compréhensibilité de la conception et de réduire la possibilité de différences entre les comportements simulés et synthétisés*:

a) Un ensemble de règles de conception strictes reflétant les connaissances les plus récentes en matière de sûreté de conception et de fiabilité doit être exigé par le plan qualité et mis en place;

b) Le respect de ces règles doit être assuré par des moyens appropriés (par exemple revues, outils, etc.).

8.3.4 Conception synchrone ou asynchrone

8.3.4.1 Généralités

La conception synchrone consiste à modifier l'état des registres internes et des sorties simultanément et seulement à des moments définis par une horloge. Cela favorise une conception modulaire et compréhensible, tout en réduisant le plus possible le risque de comportements erronés dus à des aléas temporels ("glitch"); cela favorise également la meilleure utilisation des outils de synthèse et de vérification.

8.3.4.2 Afin de favoriser des conceptions stables, robustes et clairement structurées:

a) Il convient d'utiliser une architecture strictement synchrone;

b) Les écarts doivent être justifiés.

8.3.4.3 La conception doit garantir la synchronisation des signaux aux interfaces asynchrones.

8.3.4.4 Si une architecture asynchrone est utilisée, une analyse documentée de tous les chemins doit démontrer que les sorties respectent la spécification des exigences (voir Article 6) et qu'il n'existe ni aléas temporels ni métastabilité néfastes.

8.3.4.5 Si une architecture asynchrone est utilisée, il doit être démontré qu'une architecture synchrone équivalente ne peut pas atteindre les mêmes buts.

8.3.4.6 Le comportement du HPD ne doit pas dépendre des valeurs réelles des temps de propagation internes à travers les portes et les interconnexions.

8.3.5 Gestion de l'alimentation

8.3.5.1 *Pour la classe 2, le comportement du HPD à la mise sous tension, au démarrage et lors d'une perte soudaine d'alimentation doit être conforme à la spécification des exigences du HPD.*

8.3.6 Documentation de conception

8.3.6.1 A la fin de la phase de conception, la documentation correspondante doit être rédigée.

8.3.6.2 La documentation de conception doit définir la variante effectivement utilisée pour chaque instanciation d'un composant de bibliothèque, pour éviter les ambiguïtés dues à l'existence de variantes ayant des caractéristiques électriques ou temporelles différentes.

8.3.6.3 La documentation de conception doit comporter l'identification et la configuration précises des blocs natifs et des PDB.

8.3.6.4 La documentation de la spécification de conception du HPD doit être une référence pour la réalisation et l'intégration du HPD, ainsi que pour les modifications du HPD éventuelles.

8.3.6.5 *Pour la classe 2, les spécifications de conception du HPD doivent présenter la conception du HPD de façon claire et précise.*

Pour la classe 2, l'approche principale recommandée par la présente norme est une approche descendante, mais il se peut que certains documents soulignent aussi comment des points d'une importance particulière (par exemple la tolérance aux défaillances) sont pris en compte sur l'ensemble du HPD ou du système d'I&C.