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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

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

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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

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

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

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

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

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

FOREWORD 5
INTRODUCTION 7
1 Scope 10
2 Normative references 11
3 Terms and definitions 11
4 Symbols and abbreviated terms 18
5 General requirements for HPD projects 19
5.1 General 19
5.2 Life-cycle 19
5.3 Gradation principals 21
5.4 HPD quality assurance 22
5.4.1 General 22
5.5 Configuration management 23
5.5.1 General 23
5.6 HPD Verification 23
6 HPD requirements specification 24
6.1 General 24
6.1.1 Overview 24
6.2 Functional aspects of the requirements specification 25
6.2.1 General 25
6.3 Fault detection and fault tolerance 26
6.4 Requirements capture using Electronic System Level tools 26
6.4.1 General 26
6.4.2 Requirements on the formalism of tools used at ESL level 27
6.4.3 Interface with design tools 27
7 Acceptance process for programmable integrated circuits, native blocks and Pre-Developed Blocks 27
7.1 General 27
7.2 Acceptance process for programmable integrated circuits and included native blocks 27
7.2.1 General 27
7.2.2 Integrated Circuit acceptance 28
7.3 Acceptance process for PDBs 29
7.3.1 General 29
7.3.2 PDB functional suitability 29
7.3.3 Documentation for safety of PDBs 30
7.3.4 Generation of supporting documentation for safety 30
7.3.5 Complementary means 32
7.3.6 Rules of use 32
7.3.7 Modification for acceptance 33
8 HPD design and implementation 33
8.1 General 33
8.2 Hardware Description Languages (HDL) and related tools 33
8.2.1 General 33
8.3 Design 33
8.3.1 General 33

8.3.2 Fault detection 35
8.3.3 Language and coding rules 35
8.3.4 Synchronous vs. asynchronous design 36
8.3.5 Power Management 37
8.3.6 Design documentation 37
8.4 Implementation 37
8.4.1 Products 37
8.4.2 Files of parameters and constraints 37
8.4.3 Post-route analyses 37
8.4.4 Redundancies introduced or removed by the tools 38
8.4.5 Finite state machines 38
8.4.6 Static Timing Analysis 38
8.4.7 Implementation documentation 38
8.5 System level tools and automated code generation 39
8.5.1 General 39
9 HPD integration and testing 39
9.1 General 39
9.2 Test-benches for HPD functional simulation 40
9.3 Test coverage 40
9.4 Test execution 41
10 HPD aspects of system integration 41
10.1 General 41
10.2 Requirements 41
11 HPD aspects of system validation 42
11.1 General 42
11.2 Requirements 42
12 Modification 43
12.1 Modification of the requirements, design or implementation 43
12.1.1 General 43
12.2 Modification of the micro-electronic technology 45
13 HPD production 45
13.1 General 45
13.2 Production tests 45
13.3 Programming files and programming activities 45
14 HPD aspects of installation, commissioning and operation 46
14.1 General 46
14.1.1 Overview 46
14.2 Anomaly reports 46
15 Software tools for the development of HPDs 46
15.1 General 46
15.1.1 Overview 46
15.2 Additional requirements for design, implementation and simulation tools 47
16 Design segmentation or partitioning 48
16.1 Background 48
16.2 Auxiliary or support functions 48
16.2.1 General 48
16.2.2 Partitioning of auxiliary or support functions or functions of an inferior safety category 48

17 Defences against HPD Common Cause Failure 49
Annex A (informative) Documentation 50
A.1 General 50
A.2 Project 50
A.3 HPD requirement specification 50
A.4 Acceptance of blank integrated circuits, Native Blocks and PDBs 50
A.5 HPD design and implementation 50
A.6 HPD integration and testing 51
A.7 HPD aspects of system integration 51
A.8 HPD aspects of system validation 51
A.9 Modification 51
A.10 HPD production 51
A.11 Software tools for the development of HPDs 51
Annex B (informative) Development of HPDs 52
B.1 General 52
B.2 Optional capture of requirements at Electronic System Level 52
B.3 HPD and system life-cycle 52
B.4 Design 53
B.5 Acceptance process for programmable integrated circuits, native blocks and Pre-Developed Blocks 54
B.6 Implementation 54
B.7 HPD integration and testing 55
B.8 Types of specific integrated circuits 55
B.8.1 General 55
B.8.2 PAL (Programmable Array Logic) 56
B.8.3 PLD, CPLD (Programmable Logic Device, Complex PLD) 56
B.8.4 FPGA 56
B.8.5 Gate Array, or pre-diffused integrated circuit 57
B.8.6 Standard Cells 57
B.8.7 “Full custom ASIC”, or “raw ASIC” 57
Bibliography 58

Figure 1 – System life-cycle (informative, as defined by IEC 61513) 20
Figure 2 – HPD life-cycle 21
Figure 3 – Overview of selection and acceptance process for blank Integrated Circuits and native blocks 28
Figure 4 – Overview of selection and acceptance process for PDBs 29

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.