Kärnkraftanläggningar –
Instrumentering och styrsystem av betydelse för säkerheten –
Utveckling av HDL-programmerade integrerade kretsar –
Del 2: Utveckling av HDL-programmerade integrerade kretsar för realisering av funktioner i kategori B eller C

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

Som svensk standard gäller europastandarden EN IEC 62566-2:2020. Den svenska standarden innehåller den officiella engelska språkversionen av EN IEC 62566-2:2020.

Nationellt förord

Europastandarden EN IEC 62566-2:2020

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
– **IEC 62566-2, First edition, 2020 - Nuclear power plants - Instrumentation and control systems important to safety - Development of HDL-programmed integrated circuits - Part 2: HDL-programmed integrated circuits for systems performing category B or C functions**

utarbetad inom International Electrotechnical Commission, IEC.

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62566-2

November 2020

English Version

Nuclear power plants - Instrumentation and control systems important to safety - Development of HDL-programmed integrated circuits - Part 2: HDL-programmed integrated circuits for systems performing category B or C functions
(IEC 62566-2:2020)

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)

Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Entwicklung HDL-programmierter integrierter Schaltkreise - Teil 2: HDL-programmierte integrierte Schaltkreise für Systeme, die Funktionen der Kategorie B oder C ausführen (IEC 62566-2:2020)

This European Standard was approved by CENELEC on 2020-11-16. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN IEC 62566-2:2020 E

European foreword

This document (EN IEC 62566-2:2020) consists of the text of document IEC 62566-2:2020, prepared by IEC/SC 45A "Instrumentation and control of nuclear facilities" of IEC/TC 45 "Nuclear instrumentation".

The following dates are fixed:

- latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement   (dop)   2021-11-16

- latest date by which the national standards conflicting with this document have to be withdrawn   (dow)   2023-11-16

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

As stated in the nuclear safety directive 2009/71/EURATOM, Chapter 1, Article 2, item 2, Member States are not prevented from taking more stringent safety measures in the subject-matter covered by the Directive, in compliance with Community law.

In a similar manner, this European standard does not prevent Member States from taking more stringent nuclear safety and/or security measures in the subject-matter covered by this standard.

Endorsement notice

The text of the International Standard IEC 62566-2:2020 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC/IEEE 60780-323:2016	NOTE	Harmonized as EN 60780-323:2017 (not modified)
IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified)
IEC 61508-2:2010	NOTE	Harmonized as EN 61508-2:2010 (not modified)
IEC 61508-3:2010	NOTE	Harmonized as EN 61508-3:2010 (not modified)
IEC 61508-4:2010	NOTE	Harmonized as EN 61508-4:2010 (not modified)
IEC 62645	NOTE	Harmonized as EN IEC 62645

2

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1   When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2   Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 60880	2006	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions	EN 60880	2009
IEC 60987	-	Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems	EN 60987	-
IEC 61226	-	Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions	EN 61226	-
IEC 61513	2011	Nuclear power plants - Instrumentation and control important to safety - General requirements for systems	EN 61513	2013
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	EN IEC 62138	2019
IEC 62340	-	Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)	EN 62340	-
IEC 62566	2012	Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions	EN 62566	2014

3

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*