SLOVENSKI STANDARD
oSIST prEN IEC 62566-2:2020

01-september-2020

Jedrske elektrarne - Merilna in nadzorna oprema za zagotavljanje varnosti - Razvoj HDL-programiranih integriranih vezij - 2. del: HDL-programirana integrirana vezja za sisteme, ki izvajajo funkcije kategorije B ali 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

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)

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

Ta slovenski standard je istoveten z: **prEN IEC 62566-2:2020**

ICS:

27.120.20	Jedrske elektrarne. Varnost	Nuclear power plants. Safety
31.200	Integrirana vezja, mikroelektronika	Integrated circuits. Microelectronics

oSIST prEN IEC 62566-2:2020 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN IEC 62566-2

July 2020

ICS 27.120.20

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 draft European Standard is submitted to CENELEC members for enquiry. Deadline for CENELEC: 2020-10-09.

The text of this draft consists of the text of IEC 62566-2:2020.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CENELEC 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, Denma 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to prov supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and sha be referred to as a European Standard.

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

European foreword

This document (prEN IEC 62566-2:2020) consists of the text of document IEC 62566-2:2020, prepared by IEC/TC 45 "Instrumentation, control and electrical power systems of nuclear facilities"

This document is currently submitted to the CENELEC Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dor + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dor + 36 months (to be confirmed or modified when voting)

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.

Bibliography

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 to be published

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

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.