

**Nuclear power plants - Instrumentation and control
important to safety - Development of HDL-programmed
integrated circuits for systems performing category A
functions**

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 62566:2014 sisaldab Euroopa standardi EN 62566:2014 inglisekeelset teksti.	This Estonian standard EVS-EN 62566:2014 consists of the English text of the European standard EN 62566:2014.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 29.08.2014.	Date of Availability of the European standard is 29.08.2014.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 27.120.20

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:
Aru 10, 10317 Tallinn, Estonia; www.evs.ee; phone 605 5050; e-mail info@evs.ee

English Version

**Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions
(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
(CEI 62566:2012)

Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Entwicklung HDL-programmierter integrierter Schaltkreise für Systeme, die Funktionen der Kategorie A ausführen
(IEC 62566:2012)

This European Standard was approved by CENELEC on 2014-08-04. 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

This document (EN 62566:2014) consists of the text of IEC 62566:2012 prepared by SC 45A "Instrumentation, control and electrical systems of nuclear facilities" of IEC/TC 45 "Nuclear instrumentation".

The following dates are fixed:

- latest date by which this document has to be implemented (dop) 2015-08-04
at national level by publication of an identical
national standard or by endorsement
- latest date by which the national standards conflicting (dow) 2017-08-04
with this document have to be withdrawn

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 measures in the subject-matter covered by this standard.

Endorsement notice

The text of the International Standard IEC 62566:2012 was approved by CENELEC as a European Standard without any modification.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60671	-	Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing	EN 60671	-
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	2007	Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems	EN 60987	2009
IEC 61513	2011	Nuclear power plants - Instrumentation and control important to safety - General requirement for systems	EN 61513	2013
IEC 62138	-	Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions	EN 62138	-
IEC 62340	-	Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)	EN 62340	-
IAEA guide NS-G-1.3	2002	Instrumentation and control systems important to safety in nuclear power plants	-	-

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope and object.....	10
1.1 General.....	10
1.2 Use of this Standard.....	10
2 Normative references	11
3 Terms and definitions	11
4 Symbols and abbreviations.....	13
5 General requirements for HPD projects	14
5.1 General.....	14
5.2 Life-cycle.....	14
5.3 HPD project management.....	17
5.3.1 General	17
5.3.2 Additional requirements	17
5.4 HPD quality assurance plan	17
5.5 Configuration management.....	17
6 HPD requirements specification.....	18
6.1 General.....	18
6.2 Functional aspects of the requirement specification.....	18
6.3 Deterministic design.....	19
6.4 Fault detection and fault tolerance.....	19
6.5 Requirements capture using Electronic System Level tools	20
6.5.1 General	20
6.5.2 Requirements on the formalism of tools used at ESL level.....	20
6.5.3 Interface with design tools	20
6.6 Requirements analysis and review	20
7 Acceptance process for programmable integrated circuits, native blocks and pre-developed blocks.....	21
7.1 General.....	21
7.2 Component requirement specification.....	21
7.2.1 General	21
7.2.2 Requirements	21
7.2.3 Requirements analysis and review.....	21
7.3 Rules of use	22
7.4 Selection	22
7.4.1 General	22
7.4.2 Documentation review	22
7.4.3 Operating experience review	22
7.4.4 Specific requirements related to the blank integrated circuits.....	23
7.5 Acceptance justification.....	23
7.6 Modification for acceptance.....	24
7.7 Modification after acceptance.....	24
7.8 Acceptance documentation.....	24
8 HPD design and implementation.....	24
8.1 General.....	24
8.2 Hardware Description Languages (HDL) and related tools.....	24

8.3	Design.....	25
8.3.1	General	25
8.3.2	Defensive design	25
8.3.3	Structure	25
8.3.4	Language and coding rules.....	26
8.3.5	Synchronous vs asynchronous design	27
8.3.6	Power management.....	27
8.3.7	Initialization	28
8.3.8	Non-functional configurations	28
8.3.9	Testability.....	28
8.3.10	Design documentation	28
8.4	Implementation.....	29
8.4.1	General	29
8.4.2	Products	29
8.4.3	Files of parameters and constraints	29
8.4.4	Post-route analyses.....	30
8.4.5	Redundancies introduced or removed by the tools	30
8.4.6	Finite state machines.....	31
8.4.7	Static timing analysis.....	31
8.4.8	Implementation documentation	31
8.5	System level tools and automated code generation	32
8.6	Documentation	33
8.7	Design and implementation review	33
9	HPD verification	33
9.1	General	33
9.2	Verification plan	34
9.3	Verification of the use of the pre-developed items	35
9.4	Verification of the design and implementation.....	35
9.5	Test-benches	36
9.6	Test coverage	36
9.7	Test execution.....	37
9.8	Static verification.....	37
10	HPD aspects of system integration	37
10.1	General	37
10.2	HPD aspects of the system integration plan	38
10.3	Specific aspects of system integration.....	38
10.4	Verification of the integrated system.....	39
10.5	Fault resolution procedures	39
10.6	HPD aspects of the integrated system test report	39
11	HPD aspects of system validation.....	40
11.1	General	40
11.2	HPD aspects of the system validation plan	40
11.3	System validation	40
11.4	HPD aspects of the system validation report	40
11.5	Fault resolution procedures	41
12	Modification	41
12.1	Modification of the requirements, design or implementation.....	41
12.2	Modification of the micro-electronic technology	41

13	HPD production	41
13.1	General	41
13.2	Production tests	41
13.3	Programming files and programming activities	42
14	HPD aspects of installation, commissioning and operation	42
15	Software tools for the development of HPDs	42
15.1	General	42
15.2	Additional requirements for design, implementation and simulation tools	42
16	Design segmentation or partitioning	43
16.1	Background	43
16.2	Auxiliary or support functions	43
16.2.1	General	43
16.2.2	Partitioning of auxiliary or support functions of category other than A	43
17	Defences against HPD Common Cause Failure	44
17.1	Background	44
17.2	Requirements	44
	Annex A (informative) Documentation	45
	Annex B (informative) Development of HPDs	47
	Bibliography	52
	Figure 1 – System life-cycle (informative, as defined by IEC 61513)	15
	Figure 2 – Development life-cycle of HPD	16

INTRODUCTION

a) Technical background, main issues and organisation of the Standard

The electronic systems of class 1 (according to IEC 61513) used in Nuclear Power Plants (NPP) which are required in emergency situations, need to be fully validated and qualified before being used in operation.

In traditional systems that are computer-based, a separation can be drawn between the hardware and software portions. The hardware is mainly designed with standardised components having pre-defined electronic functions such as microprocessors, timers or network controllers, whereas software is used to coordinate the different parts of the hardware and to implement the application functions.

Nowadays, I&C designers may build application functions directly in one integrated circuit using devices such as FPGAs or similar technologies. The function of such an integrated circuit is not defined by the supplier of the physical component or micro-electronic technology but by the I&C designer.

The specific integrated circuits addressed by this Standard are:

- 1) based on pre-developed micro-electronic resources,
- 2) developed within an I&C project,
- 3) developed with Hardware Description Languages (HDL) and related tools used to implement the requirements in a proper assembly of the pre-developed micro-electronic resources.

Therefore these circuits are named “HDL-Programmed Devices”, (HPD). The HDL statements which describe a HPD can include the instantiation of Pre-Developed Blocks (PDB) which are typically provided as libraries, macros, or Intellectual Property cores.

HPDs can be effective solutions to implement functions required by an I&C project. However, the verification and validation may be limited by issues such as high number of internal paths and limited observability, if the HPD has not been developed with verifiability in mind.

In order to achieve the reliability required for safety I&C systems, the development of HPDs shall comply with strict process and technical requirements such as those provided by this Standard, including the specification of requirements, the selection of blank integrated circuits and PDBs, the design and implementation, the verification, and the procedures for operation and maintenance.

It is intended that this Standard be used by hardware designers, operators of NPPs (utilities), and by regulators. Regulatory bodies will find guidance to assess important aspects such as design, implementation, verification and validation of HPDs.

b) Situation of the current Standard in the structure of the IEC SC 45A Standard series

IEC 61513 is a first level IEC SC 45A document and gives guidance applicable to I&C at system level. It is supplemented by guidance at hardware level (IEC 60987) and software level (IEC 60880 and IEC 62138). IEC 62340 gives requirements in order to reduce and overcome the possibility of common cause failure of category A functions.

IEC 62566 is a second level IEC SC 45A document which focuses on the activities when HPDs are developed. It complements IEC 60987 which deals with the generic issues of hardware design of computer based systems. It refers to IEC 60880 when issues identical to that of software development are addressed.

For more details on the structure of the IEC SC 45A Standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the Standard

It is important to note that this Standard establishes no additional functional requirements for safety systems.

Aspects for which special requirements and recommendations have been produced are:

- 1) an approach to specify the requirements of, to design, to implement and to verify “HDL-Programmed Devices” (HPD, 3.7), and to handle the corresponding aspects of system integration and validation;
- 2) an approach to analyse and select the blank integrated circuits, micro-electronic technologies and Pre-Developed Blocks (PDB, 3.11) used to develop HPDs;
- 3) procedures for the modification and configuration control of HPDs;
- 4) requirements for selection and use of software tools used to develop HPDs.

It is recognized that digital technology is continuing to develop at a rapid pace and that it is not possible for a Standard such as this one to include references to all modern design technologies and techniques.

To ensure that the Standard will continue to be relevant in future years the emphasis has been placed on issues of principle, rather than specific technologies. If new techniques are developed then it should be possible to assess the suitability of such techniques by applying the safety principles contained within this Standard.

d) Description of the structure of the IEC SC 45A Standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level document of the IEC SC 45A Standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A Standard series.

IEC 61513 refers directly to other IEC SC 45A Standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The Standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A Standards not directly referenced by IEC 61513 are Standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45 Standard series, corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework and provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. Compliance with IEC 61513 will facilitate consistency with the requirements of IEC 61508 as they have been interpreted for the nuclear industry. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 for topics related to quality assurance.

The IEC SC 45A Standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements NS-R-1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A Standards are consistent with those used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – DEVELOPMENT OF HDL-PROGRAMMED INTEGRATED CIRCUITS FOR SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope and object

1.1 General

This International Standard provides requirements for achieving highly reliable “HDL-Programmed Devices” (HPD), for use in I&C systems of nuclear power plants performing functions of safety category A as defined by IEC 61226.

The programming of HPDs relies on Hardware Description Languages (HDL) and related software tools. They are typically based on blank FPGAs or similar micro-electronic technologies. General purpose integrated circuits such as microprocessors are not HPDs.

This Standard provides requirements on:

- a) a dedicated development life-cycle addressing each phase of the development of HPDs, including specification of requirements, design, implementation, verification, integration and validation,
- b) planning and complementary activities such as modification and production,
- c) selection of pre-developed components. This includes micro-electronic resources (such as a blank FPGA or CPLD) and HDL statements representing Pre-Developed Blocks (PDB),
- d) use of simplicity and deterministic principles, recognized to be of primary importance to achieve “fault free” implementation of category A functions,
- e) tools used to design, implement and verify HPDs.

This Standard does not put requirements on the development of the micro-electronic resources, which are usually available as “commercial off-the-shelf” items and are not developed under nuclear quality assurance Standards. It addresses the developments made with these micro-electronic resources in an I&C project with HDLs and related tools.

This Standard provides guidance to avoid as far as possible latent faults remaining in HPDs, and to reduce the susceptibility to single failures as well as to potential Common Cause Failures (CCF). The requirements within this Standard for clear and comprehensive documentation should facilitate the effective application of IEC 62340.

Reliability aspects related to environmental qualification and failures due to ageing or physical degradation are not handled in this Standard. Other Standards, especially IEC 60987, IEC 60780 and IEC 62342, address these topics.

Subclause 5.7 of IEC 60880:2006 provides security requirements that apply to the development of HPDs as applicable.

1.2 Use of this Standard

This Standard provides guidance and requirements to produce verifiable designs and implementations where justification is necessary due for example to the function performed or to the importance to safety of its behaviour. Class 1 I&C systems may use HPDs for which full demonstration of compliance with the requirements of this Standard is not mandatory, e.g.