

**Nuclear power plants  
Instrumentation and control important to safety  
Hardware design requirements for computer-based  
systems**

EVS

**EESTI STANDARDI EESSÕNA****NATIONAL FOREWORD**

See Eesti standard EVS-EN 60987:2015 sisaldab Euroopa standardi EN 60987:2015 ingliskeelset teksti.	This Estonian standard EVS-EN 60987:2015 consists of the English text of the European standard EN 60987:2015.
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 20.02.2015.	Date of Availability of the European standard is 20.02.2015.
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](mailto: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; koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto: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; homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

English Version

Nuclear power plants - Instrumentation and control important to  
safety - Hardware design requirements for computer-based  
systems  
(IEC 60987:2007 + A1:2013)

Centrales nucléaires de puissance - Instrumentation et  
contrôle-commande importants pour la sûreté - Exigences  
applicables à la conception du matériel des systèmes  
informatisés  
(IEC 60987:2007 + A1:2013)

Kernkraftwerke - Leittechnische Systeme mit  
sicherheitstechnischer Bedeutung - Anforderungen an die  
Hardware-Auslegung rechnerbasierter Systeme  
(IEC 60987:2007 + A1:2013)

This European Standard was approved by CENELEC on 2015-02-16. 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, 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 60987:2015) consists of the text of IEC 60987:2007 + A1:2013 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 the document has to be implemented (dop) 2016-02-16  
at national level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2018-02-16

This document supersedes EN 60987:2009.

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.

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

## Endorsement notice

The text of the International Standard IEC 60987:2007 + A1:2013 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 61226      NOTE      Harmonized as EN 61226.

EVS

## 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](http://www.cenelec.eu)

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60780	-	Nuclear power plants - Electrical equipment of the safety system - Qualification	-	-
IEC 60812	-	Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)	EN 60812	-
IEC 60880	-	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions	EN 60880	-
IEC 61000	Series	Electromagnetic compatibility (EMC)	EN 61000	Series
IEC 61025	-	Fault Tree Analysis (FTA)	EN 61025	-
IEC 61513	2001 <sup>1)</sup>	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-
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 62671	-	Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality	-	-
ISO 2768-1	-	General tolerances - Part 1: Tolerances for linear and angular dimensions without individual tolerance indications	EN 22768-1	-
ISO 2768-2	-	General tolerances - Part 2: Geometrical tolerances for features without individual tolerance indications	EN 22768-2	-

<sup>1)</sup> Superseded by IEC 61513:2011.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
ISO 3951-1	-	Sampling procedures for inspection by variables - Part 1: Specification for single sampling plans indexed by acceptance quality limit (AQL) for lot-by-lot inspection for a single quality characteristic and a single AQL	-	-
ISO 3951-2	-	Sampling procedures for inspection by variables - Part 2: General specification for single sampling plans indexed by acceptance quality limit (AQL) for lot-by-lot inspection of independent quality characteristics	-	-
ISO 9001	-	Quality management systems - Requirements	EN ISO 9001	-
IAEA guide NS-G-1.3	-	Instrumentation and control systems important to safety in nuclear power plants	-	-
IAEA 50-C/SG-Q	1996	Quality assurance for safety in nuclear power plants and other nuclear installations	-	-

## CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	8
1.1 General.....	8
1.2 Use of this standard for pre-developed (for example, COTS) hardware assessment.....	8
1.3 Applicability of this standard to programmable logic devices development.....	9
2 Normative references .....	9
3 Terms and definitions .....	10
4 Project structure .....	12
4.1 General.....	12
4.2 Project subdivision .....	12
4.3 Quality assurance .....	12
5 Hardware requirements .....	13
5.1 General.....	13
5.2 Functional and performance requirements.....	14
5.3 Reliability/Availability requirements .....	15
5.4 Environmental withstand requirements .....	16
5.5 Documentation requirements.....	16
6 Design and development .....	17
6.1 General.....	17
6.2 Design activities .....	17
6.3 Reliability .....	18
6.4 Maintenance.....	18
6.5 Interfaces .....	19
6.6 Modification.....	19
6.7 Power failure .....	19
6.8 Component selection.....	19
6.9 Design documentation.....	19
7 Verification and validation .....	20
7.1 General.....	20
7.2 Verification plan .....	20
7.3 Independence of verification.....	21
7.4 Methods .....	21
7.5 Documentation .....	22
7.6 Discrepancies.....	22
7.7 Changes and modifications .....	22
7.8 Installation verification.....	22
7.9 Validation .....	22
7.10 Verification of pre-existing equipment platforms .....	22
8 Qualification .....	23
9 Manufacture .....	23
10 Installation and commissioning .....	23
11 Maintenance.....	23
11.1 Maintenance requirements .....	24

11.2 Failure data .....	24
11.3 Maintenance documentation .....	25
12 Modification .....	26
13 Operation .....	26
Annex A (informative) Overview of system life cycle .....	27
Annex B (informative) Outline of qualification.....	28
Annex C (informative) Example of maintenance procedure .....	29
Bibliography.....	30

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

---

### **NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – HARDWARE DESIGN REQUIREMENTS FOR COMPUTER-BASED SYSTEMS**

#### 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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 60987 has been prepared by subcommittee 45A: Instrumentation and control of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

This second edition cancels and replaces the first edition published in 1989. This edition includes the following significant technical changes with respect to the previous edition:

- account has been taken of the fact that computer design engineering techniques have advanced significantly in the intervening years;
- update of the format to align with the current IEC/ISO directives on the style of standards;
- alignment of the standard with the new revisions of IAEA documents NS-R-1 and NS-G-1.3, which includes as far as possible an adaptation of the definitions;

- replacement, as far as possible, of the requirements associated with standards published since the first edition, especially IEC 61513, IEC 60880, edition 2, and IEC 62138;
- review of the existing requirements and updating of the terminology and definitions.

The text of this standard is based on the following documents:

FDIS	Report on voting
45A/662/FDIS	45A/666/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

## INTRODUCTION

### a) Technical background, main issues and organization of the standard

The basic principles for the design of nuclear instrumentation, as specifically applied to the safety systems of nuclear power plants, were first interpreted in nuclear standards with reference to hardwired systems in IAEA Safety Guide 50-SG-D3 which has been superseded by IAEA Guide NS-G-1.3.

IEC 60987 was first issued in 1989 to cover the hardware aspects of digital systems design for systems important to safety, i.e. safety systems and safety-related systems.

Although many of the requirements within the original issue continue to be relevant, there were significant factors which justified the development of this revised edition of IEC 60987, in particular:

- a new standard has been produced which addresses in detail the general requirements for nuclear systems important to safety (IEC 61513);
- the use of pre-developed system platforms, rather than bespoke developments, has increased significantly.

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

The first-level IEC SC 45A standard for computer-based systems important to safety in nuclear power plants (NPPs) is IEC 61513. IEC 60987 is a second-level IEC SC 45A standard which addresses the generic issue of hardware design of computerized systems.

IEC 60880 and IEC 62138 are second-level standards which together cover the software aspects of computer-based systems used to perform functions important to safety in NPPs. IEC 60880 and IEC 62138 make direct reference to IEC 60987 for hardware design.

The requirements of IEC 60780 for equipment qualification are referenced within IEC 60987. For modules to be used in the design of a specific system important to safety, relevant and auditable operating experience from nuclear or other applications as described in IEC 60780, in combination with the application of rigorous quality assurance programmes, may be an acceptable method of qualification.

For more details on the structure of the 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 Class 1 or Class 2 systems (see IEC 61513 for system classification requirements).

Aspects for which special recommendations have been produced (so as to assure the production of highly reliable systems), are:

- a general approach to computing hardware development;
- a general approach to hardware verification and to the hardware aspects of computer system validation.

It is recognized that computer technology is continuing to develop and that it is not possible for a standard such as this 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 hardware design technologies. If new design techniques are developed then it should be possible to assess the suitability of such techniques by adapting and applying the design principles contained within this standard.

The scope of this standard covers digital systems hardware for Class 1 and Class 2 systems. This includes multiprocessor distributed systems and single processor systems; it covers the assessment and use of pre-developed items, for example, commercial off-the-shelf items (COTS), and the development of new hardware.

**d) Description of the structure of the SC 45A standard series and relationships with other IEC, IAEA and ISO documents**

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 direct 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 direct 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 referenced direct 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 45A standard series, corresponds to technical reports which are not normative documents.

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 9001 as well as to IAEA 50-C-QA (now replaced by IAEA 50-C/SG-Q) for topics related to quality assurance (QA).

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 of NS-R-1, establishing safety requirements related to the design of NPPs, and Safety Guide NS-G-1.3 dealing with instrumentation and control systems important to safety in NPPs. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.