

© Copyright SEK. Reproduction in any form without permission is prohibited.

Kärnkraftanläggningar – Instrumentering och styrsystem av betydelse för säkerheten – Fordringar på konstruktion av hårdvara för datorbaserade system

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

Som svensk standard gäller europastandarden EN 60987:2009. Den svenska standarden innehåller den officiella engelska språkversionen av EN 60987:2009.

Nationellt förord

Europastandarden EN 60987:2009

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 60987, Second edition, 2007 - Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems**

utarbetad inom International Electrotechnical Commission, IEC.

Tidigare fastställd svensk standard SS-IEC 987, utgåva 1, 1994, gäller ej fr o m 2012-06-01.

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven 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

**Nuclear power plants -
Instrumentation and control important to safety -
Hardware design requirements for computer-based systems
(IEC 60987:2007, modified)**

Centrales nucléaires de puissance -
Instrumentation et contrôle-commande
importants pour la sûreté -
Exigences applicables à la conception
du matériel des systèmes informatisés
(CEI 60987:2007, modifiée)

Kernkraftwerke -
Leittechnische Systeme mit
sicherheitstechnischer Bedeutung -
Anforderungen an die
Hardware-Auslegung
rechnerbasierter Systeme
(IEC 60987:2007, modifiziert)

This European Standard was approved by CENELEC on 2009-06-01. 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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

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

CENELEC

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

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of the International Standard IEC 60987:2007, prepared by SC 45A, Instrumentation and control of nuclear facilities, of IEC TC 45, Nuclear instrumentation, together with the common modifications prepared by the Technical Committee CENELEC TC 45AX, Instrumentation and control of nuclear facilities, was submitted to the formal vote and was approved by CENELEC as EN 60987 on 2009-06-01.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2010-06-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2012-06-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 60987:2007 was approved by CENELEC as a European Standard with agreed common modifications as given below.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

The following referenced documents are indispensable for the application 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 When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60780	- ¹⁾	Nuclear power plants - Electrical equipment of the safety system - Qualification	-	-
IEC 60812	- ¹⁾	Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)	EN 60812	2006 ²⁾
IEC 60880	- ¹⁾	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions	-	-
IEC 61000	Series	Electromagnetic compatibility (EMC)	EN 61000	Series
IEC 61025	- ¹⁾	Fault tree analysis (FTA)	EN 61025	2007 ²⁾
IEC 61513	2001	Nuclear power plants - Instrumentation and control for systems important for safety - General requirements for systems	-	-
IEC 62138	- ¹⁾	Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions	-	-
ISO 9001	- ¹⁾	Quality management systems - Requirements	EN ISO 9001	2008 ²⁾
IAEA NS-G 1.3	- ¹⁾	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	-	-

1) Undated reference.

2) Valid edition at date of issue.

CONTENTS

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

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.

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

1 Scope

1.1 General

This International Standard is applicable to NPP computer-system hardware for systems of Class 1 and 2 (as defined by IEC 61513).

The structure of this standard has not changed significantly from the original 1989 issue; however, some issues are now covered by standards which have been issued in the interim (for example, IEC 61513 for system architecture design) and references to new standards have been provided where applicable. The text of the standard has also been modified to reflect developments in computer system hardware design, the use of pre-developed (for example, COTS) hardware and changes in terminology.

Computer hardware facilities used for software loading and checking are not considered to form an intrinsic part of a system important to safety and, as such, are outside the scope of this standard.

NOTE 1 Class 3 computer-system hardware is not addressed by this standard, and it is recommended that such systems should be developed to commercial grade standards.

NOTE 2 In 2006 the development of a new standard to address hardware requirements for “very complex” hardware was discussed within IEC SC 45A. If such a standard is developed then that standard would be used for the development of “very complex” hardware in preference to IEC 60987.

1.2 Use of this standard for pre-developed (for example, COTS) hardware assessment

Although the primary aim of this standard is to address aspects of new hardware development, the processes defined within this standard may also be used to guide the assessment and use of pre-developed hardware, such as COTS hardware. Guidance has been provided in the text concerning the interpretation of the requirements of this standard when used for the assessment of such components. In particular, the quality assurance requirements of 4.3, concerning configuration control, apply.

Pre-developed components may contain firmware (as defined in 3.8), and, where firmware software is deeply imbedded, and effectively “transparent” to the user, then IEC 60987 should be used to guide the assessment process for such components. An example of where this approach is considered appropriate is in the assessment of modern processors which contain a microcode. Such a code is generally an integral part of the “hardware”, and it is therefore appropriate for the processor (including the microcode) to be assessed as an integrated hardware component using this standard.

Software which is not firmware, as described above, should be developed or assessed according to the requirements of the relevant software standard (for example, IEC 60880 for Class 1 systems and IEC 62138 for Class 2 systems).

1.3 Applicability of this standard to programmable logic devices development

I&C components may include programmable logic devices that are given their specific application logic design by the designer of the I&C component, as opposed to the chip manufacturer. Examples of such devices include complex programmable logic devices (CPLD) and field programmable gate arrays (FPGA).

While the programmable nature of these devices gives the development processes used for these devices, some of the characteristics of a software development process and the design processes used for such devices, are very similar to those used to design logic circuits implemented with discrete gates and integrated circuit packages. Therefore, the design processes and design verification applied to programmable logic devices should comply with the relevant requirements of this standard (i.e. taking into account the particular features of the design processes of such devices). To the extent that software-based tools are used to support the design processes for programmable logic devices, those software tools should generally follow the guidance provided for software-based development tools in the appropriate software standard, i.e. IEC 60880 (Class 1 systems) or IEC 62138 (Class 2 systems).

2 Normative references

The following referenced documents are indispensable for the application 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 60780, *Nuclear power plants – Electrical equipment of the safety system – Qualification*

IEC 60812, *Analysis techniques for system reliability – Procedures for failure mode and effects analysis (FMEA)*

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61513:2001, *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*

ISO 9001, *Quality management systems – Requirements*

IAEA 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*