SVENSK STANDARD SS-EN 60880

Fastställd	Utgåva	Sida	Ansvarig kommitté
2012-05-09	1	1 (1+109)	SEK TK 45

Kärnkraftanläggningar – Instrumentering och styrsystem av betydelse för säkerheten – Programvara för datorbaserade system för realisering av funktioner i kategori A

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

Som svensk standard gäller europastandarden EN 60880:2009. Den svenska standarden innehåller den officiella engelska språkversionen av EN 60880:2009.

Nationellt förord

Europastandarden EN 60880:2009

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
– **IEC 60880, Second edition, 2006 - Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions**

utarbetad inom International Electrotechnical Commission, IEC.

Tidigare fastställd svensk standard SS-IEC 880, utgåva 1, 1987 och SS-IEC 60880-2, utg 1, 2003, gäller ej fr o m 2012-07-01.

ICS 27.120.20

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@elstandard.se. *Internet*: www.elstandard.se

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

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60880

October 2009

ICS 27.120.20

English version

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

(IEC 60880:2006)

Centrales nucléaires de puissance - Instrumentation et contrôle-commande importants pour la sûreté - Aspects logiciels des systèmes programmés réalisant des fonctions de catégorie A
(CEI 60880:2006)

Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A
(IEC 60880:2006)

CENELEC

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

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 60880:2009 E

SEK Svensk Elstandard

Foreword

The text of the International Standard IEC 60880:2006, prepared by SC 45A, Instrumentation and control of nuclear facilities, of IEC TC 45, Nuclear instrumentation, was submitted to the formal vote and was approved by CENELEC as EN 60880 on 2009-07-01 without any modification.

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)	2010-07-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2012-07-01

CLC/TC 45AX experts draw attention to the readers of this European standard to the fact that it should be read in conjunction with IAEA document INSAG-10, 1996, “Defence in Depth in Nuclear Safety” which applies.

_____

Endorsement notice

The text of the International Standard IEC 60880:2006 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 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.

Publication	Year	Title	EN/HD	Year
IEC 60671	- [1)]	Nuclear power plants - Instrumentation and control systems important to safety - Surveillance testing	-	-
IEC 61069-2	1993	Industrial-process measurement and control - Evaluation of system properties for the purpose of system assessment - Part 2: Assessment methodology	EN 61069-2	1994
IEC 61226	- [1)]	Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions	-	-
IEC 61508-4	- [1)]	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2001 [2)]
IEC 61513	- [1)]	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-
ISO/IEC 9126	Series	Software engineering - Product quality	-	-
IAEA guide NS-G-1.2	- [1)]	Safety assessment and verification for nuclear power plants	-	
IAEA guide NS-G-1.3	- [1)]	Instrumentation and control systems important to safety in nuclear power plants	-	-

[1)] Undated reference.

[2)] Valid edition at date of issue.

CONTENTS

INTRODUCTION

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

Engineering of software based Instrumentation and Control (I&C) systems to be used for nuclear safety purposes is a challenge due to the safety requirements to be fulfilled. The safety software used in nuclear power plants (NPP) which are often required only in emergency cases, have to be fully validated and qualified before being used in operation. In order to achieve the high reliability required, special care has to be taken throughout the entire life cycle, from the basic requirements, the various design phases and V&V procedures for operation and maintenance. It is the main aim of this standard to address the related safety aspects and to provide requirements for achieving the high software quality necessary.

The first edition of this standard was issued in 1986 to interpret the basic safety principles applied so far in hardwired systems for the utilisation of digital systems — multiprocessor distributed systems as well as larger scale central processor systems — in the safety systems of nuclear power plants.

It has been used extensively within the nuclear industry to provide requirements and guidance for software of NPP safety I&C systems.

Although many of the requirements within the first edition continued to be relevant, there were significant factors which justified the development of this second edition:

– Since 1986, a number of new standards have been produced which address in detail the general requirements for systems (IEC 61513), hardware requirements (IEC 60987) and a standard to address software for I&C systems performing category B or C functions for NPP systems important to safety (IEC 62138). The Safety Guide 50-SG-D3 of the IAEA has been superseded by the guide NS-G-1.3. Additionally, IEC 60880-2 has been issued.
– Software engineering techniques have advanced significantly in the intervening years.

In this standard, utmost care has been taken to keep transparency with respect to the first edition. Where possible, the phrasing of requirements has been kept, otherwise it has been extended in a traceable way. In the same manner, IEC 60880-2 dealing with software aspects of defence against common cause failures, use of software tools and pre-developed software has been integrated, so that now this current standard covers entirely the software safety issues to be addressed.

It is intended that the standard be used by systems developers, systems purchasers/users (utilities), systems assessors and by licensors.

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

IEC 60880 is directly referenced by IEC 61513 which deals with the system aspects of high integrity computer-based I&C used in safety systems of nuclear power plants together.

IEC 60880 is the second level SC 45A document tackling the issue of software aspects for I&C systems performing category A functions.

Software for categories B and C functions is dealt with in IEC 62138.

IEC 60880 and IEC 62138 together cover the domain of the software aspects of computer-based systems used in nuclear power plants to perform functions important to safety.

This second edition of IEC 60880 is to be read in conjunction with IEC 60987 and IEC 61226, the appropriate SC 45A standards on computer hardware and on classification.

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

c) Recommendation and limitation regarding the application of this 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) a general approach to software development to assure the production of the highly reliable software required including hardware and software interdependencies;
2) a general approach to software verification and to the software aspects of the computer-based system validation;
3) procedures for software modification and configuration control;
4) requirements for use of tools;
5) procedures for qualification of pre-developed software.

It is recognised that software technology is continuing to develop at a rapid pace 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 software 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 SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top level document of the SC 45A standard series is IEC 61513. This standard deals with requirements for NPP I&C systems important to safety and lays out the SC 45A standards series.

IEC 61513 refers directly to other 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, 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 SC 45A 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 parts 1, 2 and 4, for the nuclear application sector. Compliance with this standard 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, part 3 for the nuclear application sector.

IEC 61513 refers to ISO standards as well as to IAEA 50-C-QA for topics related to quality assurance.

The SC 45A standards series consistently implement and detail the principles and basic safety aspects provided in the IAEA Code on the safety of nuclear power plants and in the IAEA safety series, in particular the Requirements NS-R-1, “Safety of Nuclear Power Plants: Design” and the Safety Guide NS-G-1.3, “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 SYSTEMS IMPORTANT TO SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY A FUNCTIONS

1 Scope and object

This International Standard provides requirements for the software of computer-based I&C systems of nuclear power plants performing functions of safety category A as defined by IEC 61226.

According to the definition in IEC 61513, I&C systems of safety class 1 are basically intended to support category A functions, but may also support functions of lower categories. However the system requirements are always determined by the functions of the highest category implemented.

For software of I&C system performing only category B and C functions in NPP as defined by IEC 61226, requirements and guidance of IEC 62138 are applicable.

This standard provides requirements for the purpose of achieving highly reliable software. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation.

The principles applied in developing these requirements include:

– best available practices;
– top-down design methods;
– modularity;
– verification of each phase;
– clear documentation;
– auditable documents;
– validation testing.

Additional guidance and information on how to comply with the requirements of the main part of this standard is given in Annexes A to I.

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 60671, *Periodic tests and monitoring of the protection system of nuclear reactors*

IEC 61069-2:1993, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

IEC 61226, *Nuclear power plants – Instrumentation and control systems important for safety – Classification of instrumentation and control functions*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

ISO/IEC 9126, *Software engineering – Product quality*

IAEA guide NS-G-1.2, *Safety Assessment and Verification for Nuclear power Plant*

IAEA guide NS-G-1.3, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*