SVENSK STANDARD SS-EN 62138

Fastställd	Utgåva	Sida	Ansvarig kommitté
2012-05-09	1	1 (1+48)	SEK TK 45

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

Nuclear power plants –
Instrumentation and control important for safety –
Software aspects for computer-based systems performing category B or C functions

Som svensk standard gäller europastandarden EN 62138:2009. Den svenska standarden innehåller den officiella engelska språkversionen av EN 62138:2009.

Nationellt förord

Europastandarden EN 62138:2009

består av:

– **europastandardens ikraftsättningsdokument,** utarbetat inom CENELEC
– **IEC 62138, First edition, 2004 - Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions**

utarbetad inom International Electrotechnical Commission, IEC.

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 62138

August 2009

ICS 27.120.20

English version

Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category B or C functions

(IEC 62138:2004)

Centrales nucléaires - Instrumentation et contrôle-commande importants pour la sûreté - Aspects logiciels des systèmes informatisés réalisant des fonctions de catégorie B ou C (CEI 62138:2004)

Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie B oder C (IEC 62138:2004)

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 62138:2009 E

SEK Svensk Elstandard

Foreword

The text of the International Standard IEC 62138:2004, 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 62138 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

Annex ZA has been added by CENELEC.

———————

Endorsement notice

The text of the International Standard IEC 62138:2004 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61508-3	NOTE	Harmonized as EN 61508-3:2001 (not modified).
IEC 61508-4	NOTE	Harmonized as EN 61508-4:2001 (not modified).
IEC 61511-1	NOTE	Harmonized as EN 61511-1:2004 (not modified).
ISO 9000-3	NOTE	Harmonized as EN ISO 9000-3:1997 (not modified).
ISO 9001	NOTE	Harmonized as EN ISO 9001:2008 (not modified).

———————

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 61226	- [1)]	Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions	-	-
IEC 61513	2001	Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems	-	-

[1)] Undated reference.

CONTENTS

INTRODUCTION

Structure of the SC 45A standard series – Relationships with other IEC, IAEA and ISO documents

The entry point of the SC 45A standard series is IEC 61513. This standard deals with general requirements for instrumentation and control systems and equipment (I&C systems) that are used to perform functions important to safety in nuclear power plants (NPPs), and structures the SC45A standard 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, software aspects of computer-based systems, hardware aspect of computer-based systems, control rooms design and multiplexing. The standards referenced directly have to be considered together with IEC 61513 as a consistent document set.

The other SC 45A standards not directly referenced by IEC 61513 are standards related to particular equipment, technical methods or specific activities. Usually, those low level documents, which refer to the documents of the higher levels previously described for the general topics, can be used on their own.

IEC 61513 has adopted a presentation format similar to basic safety publication IEC 61508, with an overall safety lifecycle frame and a system safety lifecycle frame, and provides an interpretation of the general requirements of IEC 61508, parts 1, 2 and 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 that frame, IEC 60880 and IEC 62138 correspond to IEC 61508, part 3 for the nuclear application sector.

IEC 61513 refers to ISO as well as to IAEA 50-C-QA (now replaced by IAEA 50-C/SG-Q) for topics related to quality assurance.

The SC 45A standards series implements consistently and in detail the principles and basic safety aspects given 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 the SC 45A standards are consistent with that used by the IAEA.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT FOR SAFETY – SOFTWARE ASPECTS FOR COMPUTER-BASED SYSTEMS PERFORMING CATEGORY B OR C FUNCTIONS

1 Scope

This International Standard provides requirements for the software of computer-based I&C systems performing functions of safety category B or C as defined by IEC 61226. It complements IEC 60880 and IEC 60880-2, which provide requirements for the software of computer-based I&C systems performing functions of safety category A.

It is also consistent with, and complementary to, IEC 61513. Activities that are mainly system level activities (for example, integration, validation and installation) are not addressed exhaustively by this standard: requirements that are not specific to software are deferred to IEC 61513.

IEC 61513 defines the safety classes of I&C systems important to safety as follows:

- I&C systems of safety class 1 are basically intended to perform functions of safety category A, but may also perform functions of safety category B and/or C, and non safety-classified functions;
- I&C systems of safety class 2 are basically intended to perform functions of safety category B, but may also perform functions of safety category C, and non safety-classified functions;
- I&C systems of safety class 3 are basically intended to perform functions of safety category C, but may also perform non safety-classified functions.

Since a given safety-classified I&C system may perform functions of different safety categories and even non safety-classified functions, the requirements of this standard are attached to the safety class of the I&C system.

This standard takes into account the current practices for the development of software for I&C systems, in particular:

- the use of pre-developed software, equipment and equipment families that were not necessarily designed to nuclear industry sector standards;
- the use of dedicated “black-box” devices with embedded software;
- the use of application-oriented languages.

This standard is not intended to be used as a general-purpose software engineering guide. It provides requirements that the software of I&C systems of safety classes 2 or 3 must meet to achieve system nuclear safety objectives.

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 61226, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

IEC 61513:2001, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*