SVENSK STANDARD SS-EN 62061

Fastställd	Utgåva	Sida	Ingår i
2005-05-23	1	1 (1+104)	SEK Område 44

Svenska Elektriska Kommissionen, SEK

Maskinsäkerhet – Funktionssäkerhet hos elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska styrsystem

Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

Som svensk standard gäller europastandarden EN 62061:2005. Den svenska standarden innehåller den officiella engelska språkversionen av EN 62061:2005.

Nationellt förord

Europastandarden EN 62061:2005

består av:

- **europastandardens ikraftsättningsdokument,** utabetat inom CENELEC
- **IEC 62061, First edition, 2005 - Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems**

  utarbetad inom International Electrotechnical Commission, IEC.

ICS 13.110; 25.040.99; 29.020

Denna standard är fastställd av Svenska Elektriska Kommissionen, SEK,
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@sekom.se. *Internet*: www.sekom.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

Svenska Elektriska Kommissionen, SEK, 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
Box 1284
164 29 Kista
Tel 08-444 14 00
www.sekom.se

EUROPEAN STANDARD **EN 62061**

NORME EUROPÉENNE

EUROPÄISCHE NORM April 2005

ICS 13.110; 25.040.99; 29.020

English version

Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
(IEC 62061:2005)

Sécurité des machines –
Sécurité fonctionnelle des systèmes
de commande électriques, électroniques
et électroniques programmables relatifs
à la sécurité
(CEI 62061:2005)

Sicherheit von Maschinen –
Funktionale Sicherheit
sicherheitsbezogener elektrischer,
elektronischer und programmierbarer
elektronischer Steuerungssysteme
(IEC 62061:2005)

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 62061:2005 E

Foreword

The text of document 44/460/FDIS, future edition 1 of IEC 62061, prepared by IEC TC 44, Safety of machinery - Electrotechnical aspects, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62061 on 2004-12-01.

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)	2005-11-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2007-12-01

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and covers essential requirements of EC Directive 98/37/EC. See Annex ZZ.

PROOF TEST INTERVAL AND LIFETIME

The following important information should be noted in relation to the requirements of this standard:

Where the probability of dangerous failure per hour (PFH_D) is highly dependent upon proof testing (i.e. tests intended to reveal faults not detected by diagnostic functions) then the proof test interval needs to be shown as realistic and practicable in the context of the expected use of the safety-related electrical control system (SRECS) (e.g. proof test intervals of less than 10 years can be unreasonably short for many machinery applications).

CEN/TC114/WG6 have used a proof test interval (mission time) of 20 years to support the estimation of mean time to dangerous failure ($MTTF_D$) for the realization of designated architectures in Annex B of prEN ISO 13849-1. Therefore, it is recommended that SRECS designers endeavour to use a 20 year proof test interval.

It is acknowledged that some subsystems and/or subsystem elements (e.g. electro-mechanical components with high duty cycles) will require replacement within the SRECS proof test interval.

Proof testing involves detailed and comprehensive checks that can, in practice, only be performed when the SRECS and/or its subsystems has been designed to facilitate proof testing (e.g. dedicated test ports) and provided with necessary information (e.g. proof test instructions).

To ensure the validity of the proof test interval specified by the designer it is important that any other necessary designated tests (e.g. functional tests) are also successfully performed at the SRECS.

Annexes ZA and ZZ have been added by CENELEC.

———————

Endorsement notice

The text of the International Standard IEC 62061:2005 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 Where an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 60204-1	- [1)]	Safety of machinery - Electrical equipment of machines Part 1: General requirements	EN 60204-1 + corr. September	1997 [2)] 1998
IEC 61000-6-2, mod.	- [1)]	Electromagnetic compatibility (EMC) Part 6-2: Generic standards - Immunity for industrial environments	EN 61000-6-2	2001 [2)]
IEC 61310	Series	Safety of machinery - Indication, marking and actuation	EN 61310	Series
IEC 61508-2	- [1)]	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001 [2)]
IEC 61508-3	- [1)]	Part 3: Software requirements	EN 61508-3	2001 [2)]
ISO 12100-1	2003	Safety of machinery Basic concepts, general principles for design -- Part 1: Basic terminology, methodology	EN ISO 12100-1	2003
ISO 12100-2	2003	Basic concepts, general principles for design -- Part 2: Technical principles	EN ISO 12100-2	2003
ISO 13849-1	1999	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design	-	-
ISO 13849-2	2003	Part 2: Validation	EN ISO 13849-2	2003
ISO 14121	- [1)]	Safety of machinery Principles of risk assessment	-	-

1) Undated reference.

2) Valid edition at date of issue.

CONTENTS

INTRODUCTION

As a result of automation, demand for increased production and reduced operator physical effort, Safety-Related Electrical Control Systems (referred to as SRECS) of machines play an increasing role in the achievement of overall machine safety. Furthermore, the SRECS themselves increasingly employ complex electronic technology.

Previously, in the absence of standards, there has been a reluctance to accept SRECS in safety-related functions for significant machine hazards because of uncertainty regarding the performance of such technology.

This International Standard is intended for use by machinery designers, control system manufacturers and integrators, and others involved in the specification, design and validation of a SRECS. It sets out an approach and provides requirements to achieve the necessary performance.

This standard is machine sector specific within the framework of IEC 61508. It is intended to facilitate the specification of the performance of safety-related electrical control systems in relation to the significant hazards (see 3.8 of ISO 12100-1) of machines.

This standard provides a machine sector specific framework for functional safety of a SRECS of machines. It only covers those aspects of the safety lifecycle that are related to safety requirements allocation through to safety validation. Requirements are provided for information for safe use of SRECS of machines that can also be relevant to later phases of the life of a SRECS.

There are many situations on machines where SRECS are employed as part of safety measures that have been provided to achieve risk reduction. A typical case is the use of an interlocking guard that, when it is opened to allow access to the danger zone, signals the electrical control system to stop hazardous machine operation. Also in automation, the electrical control system that is used to achieve correct operation of the machine process often contributes to safety by mitigating risks associated with hazards arising directly from control system failures. This standard gives a methodology and requirements to

- assign the required safety integrity level for each safety-related control function to be implemented by SRECS;
- enable the design of the SRECS appropriate to the assigned safety-related control function(s);
- integrate safety-related subsystems designed in accordance with ISO 13849 ;
- validate the SRECS.

This standard is intended to be used within the framework of systematic risk reduction described in ISO 12100-1 and in conjunction with risk assessment according to the principles described in ISO 14121 (EN 1050). A suggested methodology for safety integrity level (SIL) assignment is given in informative Annex A.

Measures are given to co-ordinate the performance of the SRECS with the intended risk reduction taking into account the probabilities and consequences of random or systematic faults within the electrical control system.

Figure 1 shows the relationship of this standard to other relevant standards.

Table 1 gives recommendations on the recommended application of this standard and the revision of ISO 13849-1.

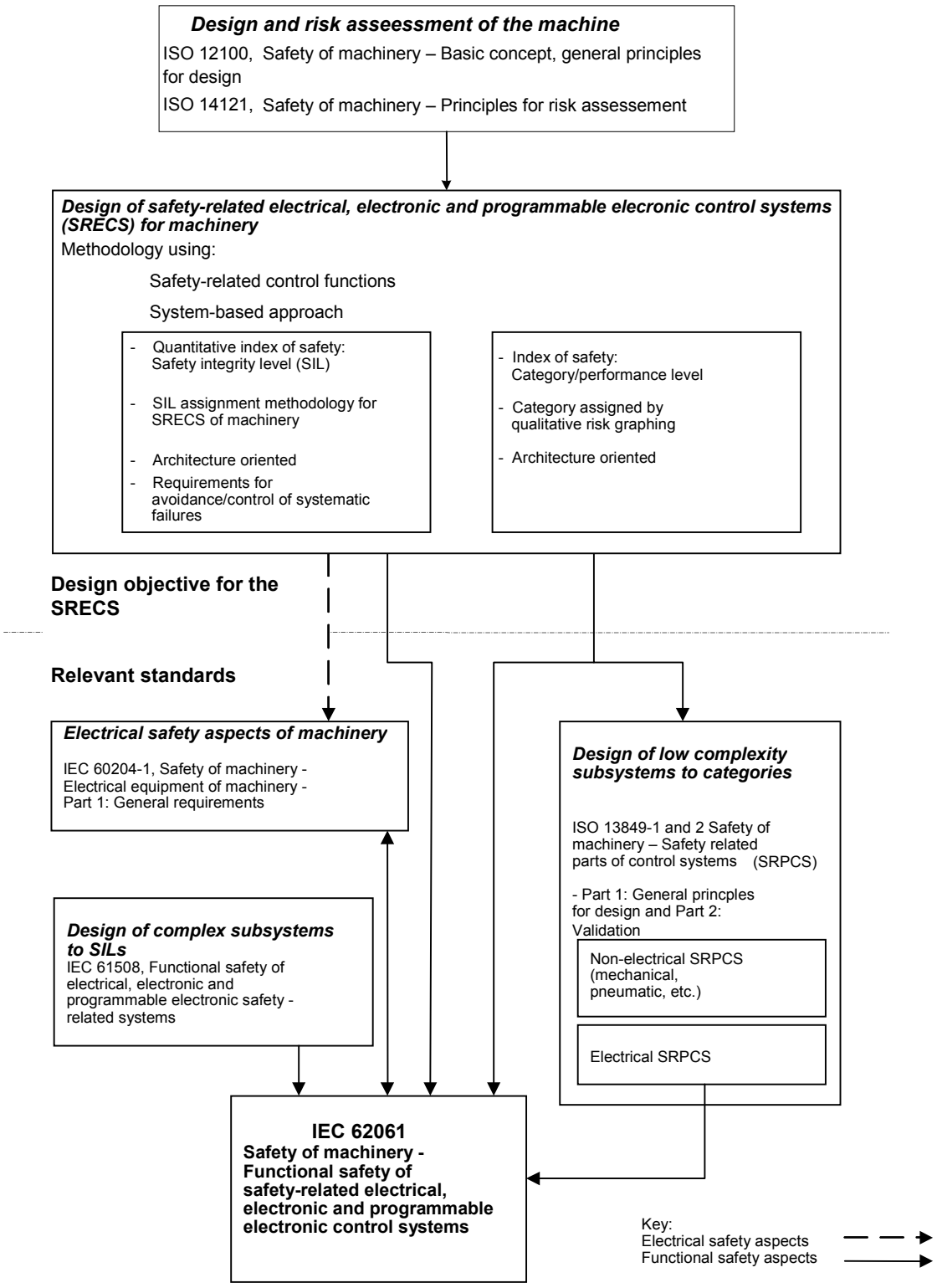

Figure 1 – Relationship of IEC 62061 to other relevant standards

Information on the recommended application of IEC 62061 and ISO 13849-1 (under revision)

IEC 62061 and ISO 13849-1 (under revision) specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. Table 1 summarises the scopes of IEC 62061 and ISO 13849-1(under revision).

NOTE ISO 13849-1 is currently under preparation by ISO TC 199 and CEN TC 114.

Table 1 – Recommended application of IEC 62061 and ISO 13849-1(under revision)

	Technology implementing the safety-related control function(s)	ISO 13849-1 (under revision)	IEC 62061
A	Non electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, or non complex electronics	Restricted to designated architectures (see Note 1) and up to PL=e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures (see Note 1) and up to PL=e	X see Note 3
E	C combined with B	Restricted to designated architectures (see Note 1) and up to PL=d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X see Note 2	X see Note 3

"X" indicates that this item is dealt with by the standard shown in the column heading.

NOTE 1 Designated architectures are defined in Annex B of EN ISO 13849-1(rev.) to give a simplified approach for quantification of performance level.

NOTE 2 For complex electronics: Use of designated architectures according to EN ISO 13849-1(rev.) up to PL=d or any architecture according to IEC 62061.

NOTE 3 For non-electrical technology use parts according to EN ISO 13849-1(rev.) as subsystems.

SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED ELECTRICAL, ELECTRONIC AND PROGRAMMABLE ELECTRONIC CONTROL SYSTEMS

1 Scope

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machines (see Notes 1 and 2). It is applicable to control systems used, either singly or in combination, to carry out safety-related control functions on machines that are not portable by hand while working, including a group of machines working together in a co-ordinated manner.

NOTE 1 In this standard, the term “electrical control systems” is used to stand for ”Electrical, Electronic and Programmable Electronic (E/E/PE) control systems” and “SRECS” is used to stand for “safety-related electrical, electronic and programmable electronic control systems”.

NOTE 2 In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of a SRECS.

This standard is an application standard and is not intended to limit or inhibit technological advancement. It does not cover all the requirements (e.g. guarding, non-electrical interlocking or non-electrical control) that are needed or required by other standards or regulations in order to safeguard persons from hazards. Each type of machine has unique requirements to be satisfied to provide adequate safety.

This standard:

– is concerned only with functional safety requirements intended to reduce the risk of injury or damage to the health of persons in the immediate vicinity of the machine and those directly involved in the use of the machine;

– is restricted to risks arising directly from the hazards of the machine itself or from a group of machines working together in a co-ordinated manner;

  NOTE 3 Requirements to mitigate risks arising from other hazards are provided in relevant sector standards. For example, where a machine(s) is part of a process activity, the machine electrical control system functional safety requirements should, in addition, satisfy other requirements (e.g. IEC 61511) insofar as safety of the process is concerned.

– does not specify requirements for the performance of non-electrical (e.g. hydraulic, pneumatic) control elements for machines;

  NOTE 4 Although the requirements of this standard are specific to electrical control systems, the framework and methodology specified can be applicable to safety-related parts of control systems employing other technologies.

– does not cover electrical hazards arising from the electrical control equipment itself (e.g. electric shock – see IEC 60204–1).

The objectives of specific Clauses in IEC 62061 are as given in Table 2.

Table 2 – Overview and objectives of IEC 62061

Clause	Objective
4: Management of functional safety	To specify the management and technical activities which are necessary for the achievement of the required functional safety of the SRECS.
5: Requirements for the specification of safety-related control functions	To set out the procedures to specify the requirements for safety-related control functions. These requirements are expressed in terms of functional requirements specification, and safety integrity requirements specification.
6: Design and integration of the safety-related electrical control system	To specify the selection criteria and/or the design and implementation methods of the SRECS to meet the functional safety requirements. This includes: selection of the system architecture, selection of the safety-related hardware and software, design of hardware and software, verification that the designed hardware and software meets the functional safety requirements.
7: Information for use of the machine	To specify requirements for the information for use of the SRECS, which has to be supplied with the machine. This includes: provision of the user manual and procedures, provision of the maintenance manual and procedures.
8: Validation of the safety-related electrical control system	To specify the requirements for the validation process to be applied to the SRECS. This includes inspection and testing of the SRECS to ensure that it achieves the requirements stated in the safety requirements specification.
9: Modification of the safety-related electrical control system	To specify the requirements for the modification procedure that has to be applied when modifying the SRECS. This includes: modifications to any SRECS are properly planned and verified prior to making the change; the safety requirements specification of the SRECS is satisfied after any modifications have taken place.

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 60204–1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*