SLOVENSKI STANDARD

SIST EN 62061:2005

december 2005

Varnost strojev – Funkcijska varnost na varnost vezanih električnih, elektronskih in programirljivih elektronskih krmilnih sistemov (IEC 62061:2005)

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

ICS 13.110; 25.040.40

Referenčna številka
SIST EN 62061:2005(en)

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)

This European Standard was approved by CENELEC on 2004-12-01. 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, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

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.

Annex ZZ
(informative)

Coverage of Essential Requirements of EC Directives

This European Standard has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association and within its scope the standard covers the following essential requirements out of those given in Annex I of the EC Directive 98/37/EC:

– 1.2.1;

– 1.2.7.

Compliance with this standard provides one means of conformity with the specified essential requirements of the Directive concerned.

WARNING: Other requirements and other EC Directives may be applicable to the products falling within the scope of this standard.

_____

IEC 62061

Edition 1.0 2005-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XD
CODE PRIX

ICS 13.110; 25.040.99; 29.020

ISBN 2-8318-7818-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED ELECTRICAL, ELECTRONIC AND PROGRAMMABLE ELECTRONIC CONTROL 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 62061 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

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

FDIS	Report on voting
44/460/FDIS	44/470/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.

The contents of the corrigendum of July 2005 have been included in this copy.

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.

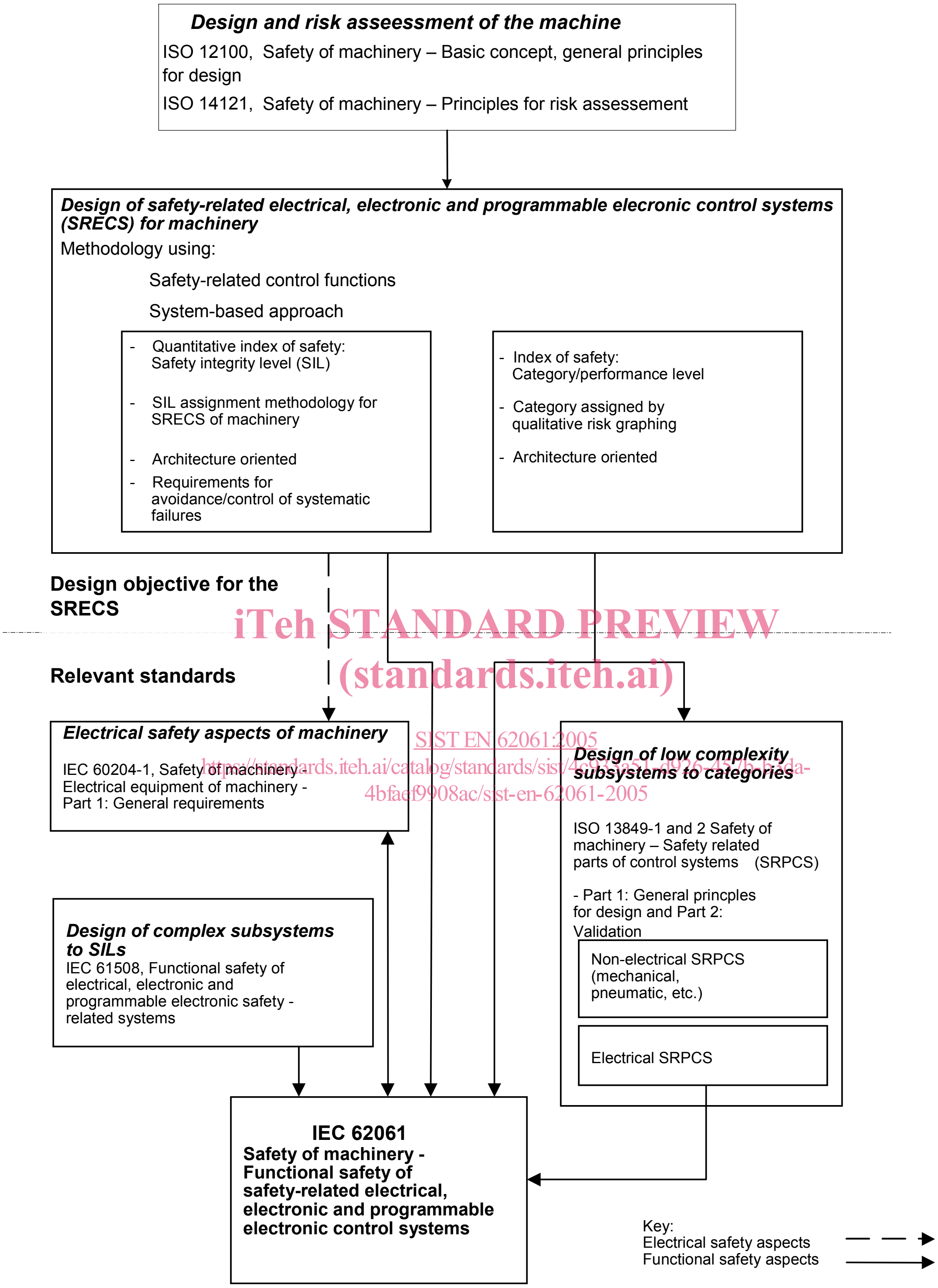

Figure 1 – Relationship of IEC 62061 to other relevant standards

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.