

**Masinate ohutus. Ohutust mõjutavad osad  
juhtimissüsteemides. Osa 1: Kavandamise  
üldpõhimõtted**

Safety of machinery - Safety-related parts of control  
systems - Part 1: General principles for design

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

Käesolev Eesti standard EVS-EN ISO 13849-1:2008 sisaldab Euroopa standardi EN ISO 13849-1:2008 ingliskeelset teksti.

Standard on kinnitatud Eesti Standardikeskuse 21.07.2008 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.

Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 11.06.2008.

Standard on kättesaadav Eesti standardiorganisatsioonist.

This Estonian standard EVS-EN ISO 13849-1:2008 consists of the English text of the European standard EN ISO 13849-1:2008.

This standard is ratified with the order of Estonian Centre for Standardisation dated 21.07.2008 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.

Date of Availability of the European standard text 11.06.2008.

The standard is available from Estonian standardisation organisation.

ICS 13.110

Võtmesõnad:

### Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:  
Aru 10 Tallinn 10317 Eesti; [www.evs.ee](http://www.evs.ee); Telefon: 605 5050; E-post: [info@evs.ee](mailto:info@evs.ee)

English Version

**Safety of machinery - Safety-related parts of control systems -  
Part 1: General principles for design (ISO 13849-1:2006)**

Sécurité des machines - Parties des systèmes de  
commande relatives à la sécurité - Partie 1: Principes  
généraux de conception (ISO 13849-1:2006)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von  
Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO  
13849-1:2006)

This European Standard was approved by CEN on 18 May 2008.

CEN 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 CEN Management Centre or to any CEN 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 CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

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



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

## Foreword

The text of ISO 13849-1:2006 has been prepared by Technical Committee ISO/TC 199 "Safety of machinery" of the International Organization for Standardization (ISO) and has been taken over as EN ISO 13849-1:2008 by Technical Committee CEN/TC 114 "Safety of machinery" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by December 2008, and conflicting national standards shall be withdrawn at the latest by December 2009.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 13849-1:2006.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EC Directive(s).

For relationship with EC Directive(s), see informative Annexes ZA and ZB, which are integral part of this document.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

### Endorsement notice

The text of ISO 13849-1:2006 has been approved by CEN as a EN ISO 13849-1:2008 without any modification.

## **Annex ZA** (informative)

### **Relationship between this European Standard and the Essential Requirements of EU Directive 98/37/EC, amended by Directive 98/79/EC**

This European Standard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association to provide a means of conforming to Essential Requirements of the New Approach Directive 98/37/EC, amended by Directive 98/79/EC.

Once this standard is cited in the Official Journal of the European Communities under that Directive and has been implemented as a national standard in at least one Member State, compliance with the normative clauses of this standard confers, within the limits of the scope of this standard, a presumption of conformity with Essential Requirements 1.2.1 and 1.2.7 of Annex I of that Directive and associated EFTA regulations.

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

## **Annex ZB** (informative)

### **Relationship between this European Standard and the Essential Requirements of EU Directive 2006/42/EC**

This European Standard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association to provide a means of conforming to Essential Requirements of the New Approach Directive Machinery 2006/42/EC.

Once this standard is cited in the Official Journal of the European Communities under that Directive and has been implemented as a national standard in at least one Member State, compliance with the normative clauses of this standard confers, within the limits of the scope of this standard, a presumption of conformity with Essential Requirements 1.2.1 of Annex I of that Directive and associated EFTA regulations.

**WARNING —** Other requirements and other EU Directives may be applicable to the product(s) falling within the scope of this standard.

# Contents

Page

Foreword.....	v
Introduction.....	vi
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms, definitions, symbols and abbreviated terms.....</b>	<b>2</b>
3.1 Terms and definitions.....	2
3.2 Symbols and abbreviated terms .....	8
<b>4 Design considerations .....</b>	<b>9</b>
4.1 Safety objectives in design.....	9
4.2 Strategy for risk reduction .....	11
4.2.1 General.....	11
4.2.2 Contribution to the risk reduction by the control system .....	11
4.3 Determination of required performance level ( $PL_r$ ).....	14
4.4 Design of SRP/CS .....	14
4.5 Evaluation of the achieved performance level PL and relationship with SIL .....	15
4.5.1 Performance level PL .....	15
4.5.2 Mean time to dangerous failure of each channel ( $MTTF_d$ ) .....	17
4.5.3 Diagnostic coverage (DC) .....	18
4.5.4 Simplified procedure for estimating PL.....	18
4.6 Software safety requirements .....	21
4.6.1 General.....	21
4.6.2 Safety-related embedded software (SRESW) .....	21
4.6.3 Safety-related application software (SRASW) .....	22
4.6.4 Software-based parameterization .....	25
4.7 Verification that achieved PL meets $PL_r$ .....	26
4.8 Ergonomic aspects of design.....	26
<b>5 Safety functions .....</b>	<b>26</b>
5.1 Specification of safety functions .....	26
5.2 Details of safety functions .....	28
5.2.1 Safety-related stop function .....	28
5.2.2 Manual reset function.....	29
5.2.3 Start/restart function .....	29
5.2.4 Local control function .....	30
5.2.5 Muting function.....	30
5.2.6 Response time .....	30
5.2.7 Safety-related parameters .....	30
5.2.8 Fluctuations, loss and restoration of power sources .....	31
<b>6 Categories and their relation to <math>MTTF_d</math> of each channel, <math>DC_{avg}</math> and CCF.....</b>	<b>31</b>
6.1 General.....	31
6.2 Specifications of categories .....	32
6.2.1 General.....	32
6.2.2 Designated architectures .....	32
6.2.3 Category B .....	32
6.2.4 Category 1 .....	33
6.2.5 Category 2 .....	34
6.2.6 Category 3 .....	35
6.2.7 Category 4 .....	36
6.3 Combination of SRP/CS to achieve overall PL .....	39

<b>7</b>	<b>Fault consideration, fault exclusion.....</b>	<b>40</b>
<b>7.1</b>	<b>General.....</b>	<b>40</b>
<b>7.2</b>	<b>Fault consideration.....</b>	<b>40</b>
<b>7.3</b>	<b>Fault exclusion.....</b>	<b>41</b>
<b>8</b>	<b>Validation.....</b>	<b>41</b>
<b>9</b>	<b>Maintenance.....</b>	<b>41</b>
<b>10</b>	<b>Technical documentation.....</b>	<b>41</b>
<b>11</b>	<b>Information for use.....</b>	<b>42</b>
<b>Annex A (informative)</b>	<b>Determination of required performance level (PL<sub>r</sub>).....</b>	<b>44</b>
<b>Annex B (informative)</b>	<b>Block method and safety-related block diagram.....</b>	<b>47</b>
<b>Annex C (informative)</b>	<b>Calculating or evaluating MTTF<sub>d</sub> values for single components.....</b>	<b>49</b>
<b>Annex D (informative)</b>	<b>Simplified method for estimating MTTF<sub>d</sub> for each channel.....</b>	<b>57</b>
<b>Annex E (informative)</b>	<b>Estimates for diagnostic coverage (DC) for functions and modules.....</b>	<b>59</b>
<b>Annex F (informative)</b>	<b>Estimates for common cause failure (CCF).....</b>	<b>62</b>
<b>Annex G (informative)</b>	<b>Systematic failure.....</b>	<b>64</b>
<b>Annex H (informative)</b>	<b>Example of combination of several safety-related parts of the control system.....</b>	<b>67</b>
<b>Annex I (informative)</b>	<b>Examples.....</b>	<b>70</b>
<b>Annex J (informative)</b>	<b>Software.....</b>	<b>77</b>
<b>Annex K (informative)</b>	<b>Numerical representation of Figure 5.....</b>	<b>80</b>
<b>Bibliography</b>	<b>.....</b>	<b>83</b>



## Introduction

The structure of safety standards in the field of machinery is as follows.

- a) Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.
- b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:
  - type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);
  - type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).
- c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This part of ISO 13849 is a type-B-1 standard as stated in ISO 12100-1.

When provisions of a type-C standard are different from those which are stated in type-A or type-B standards, the provisions of the type-C standard take precedence over the provisions of the other standards for machines that have been designed and built according to the provisions of the type-C standard.

This part of ISO 13849 is intended to give guidance to those involved in the design and assessment of control systems, and to Technical Committees preparing Type-B2 or Type-C standards which are presumed to comply with the Essential Safety Requirements of Annex I of the Council Directive 98/37/EC, The Machinery Directive. It does not give specific guidance for compliance with other EC directives.

As part of the overall risk reduction strategy at a machine, a designer will often choose to achieve some measure of risk reduction through the application of safeguards employing one or more safety functions.

Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS) and these can consist of hardware and software and can either be separate from the machine control system or an integral part of it. In addition to providing safety functions, SRP/CS can also provide operational functions (e.g. two-handed controls as a means of process initiation).

The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). These performance levels are defined in terms of probability of dangerous failure per hour (see Table 3).

The probability of dangerous failure of the safety function depends on several factors, including hardware and software structure, the extent of fault detection mechanisms [diagnostic coverage (DC)], reliability of components [mean time to dangerous failure (MTTF<sub>d</sub>), common cause failure (CCF)], design process, operating stress, environmental conditions and operation procedures.

In order to assist the designer and help facilitate the assessment of achieved PL, this document employs a methodology based on the categorization of structures according to specific design criteria and specified behaviours under fault conditions. These categories are allocated one of five levels, termed Categories B, 1, 2, 3 and 4.

The performance levels and categories can be applied to safety-related parts of control systems, such as

- protective devices (e.g. two-hand control devices, interlocking devices), electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices,
- control units (e.g. a logic unit for control functions, data processing, monitoring, etc.), and
- power control elements (e.g. relays, valves, etc),

as well as to control systems carrying out safety functions at all kinds of machinery — from simple (e.g. small kitchen machines, or automatic doors and gates) to manufacturing installations (e.g. packaging machines, printing machines, presses).

This part of ISO 13849 is intended to provide a clear basis upon which the design and performance of any application of the SRP/CS (and the machine) can be assessed, for example, by a third party, in-house or by an independent test house.

### Information on the recommended application of IEC 62061 and this part of ISO 13849

IEC 62061 and this part of ISO 13849 specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these International Standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. The following table summarizes the scopes of IEC 62061 and this part of ISO 13849.

**Table 1 — Recommended application of IEC 62061 and ISO 13849-1**

	Technology implementing the safety-related control function(s)	ISO 13849-1	IEC 62061
A	Non-electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, and/or non complex electronics	Restricted to designated architectures <sup>a</sup> and up to PL = e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures <sup>a</sup> and up to PL = d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures <sup>a</sup> and up to PL = e	X <sup>c</sup>
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 <sup>b</sup>	X <sup>c</sup>
X indicates that this item is dealt with by the International Standard shown in the column heading.			
<sup>a</sup> Designated architectures are defined in 6.2 in order to give a simplified approach for quantification of performance level.			
<sup>b</sup> For complex electronics: use designated architectures according to this part of ISO 13849 up to PL = d or any architecture according to IEC 62061.			
<sup>c</sup> For non-electrical technology, use parts in accordance with this part of ISO 13849 as subsystems.			

# Safety of machinery — Safety-related parts of control systems —

## Part 1: General principles for design

### 1 Scope

This part of ISO 13849 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. For these parts of SRP/CS, it specifies characteristics that include the performance level required for carrying out safety functions. It applies to SRP/CS, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery.

It does not specify the safety functions or performance levels that are to be used in a particular case.

This part of ISO 13849 provides specific requirements for SRP/CS using programmable electronic system(s).

It does not give specific requirements for the design of products which are parts of SRP/CS. Nevertheless, the principles given, such as categories or performance levels, can be used.

NOTE 1 Examples of products which are parts of SRP/CS: relays, solenoid valves, position switches, PLCs, motor control units, two-hand control devices, pressure sensitive equipment. For the design of such products, it is important to refer to the specifically applicable International Standards, e.g. ISO 13851, ISO 13856-1 and ISO 13856-2.

NOTE 2 For the definition of *required performance level*, see 3.1.24.

NOTE 3 The requirements provided in this part of ISO 13849 for programmable electronic systems are compatible with the methodology for the design and development of safety-related electrical, electronic and programmable electronic control systems for machinery given in IEC 62061.

NOTE 4 For safety-related embedded software for components with  $PL_r = e$  see IEC 61508-3:1998, Clause 7.

NOTE 5 See also Table 1.

### 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.

ISO 12100-1:2003, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

ISO 12100-2:2003, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles*

ISO 13849-2:2003, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

ISO 14121<sup>1)</sup>, *Safety of machinery — Principles of risk assessment*

IEC 60050-191:1990, *International electrotechnical vocabulary — Chapter 191: Dependability and quality of service*, and IEC 60050-191-am1:1999 and IEC 60050-191-am2:2002:1999, *Amendment 1 and Amendment 2, International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service*

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements*, and IEC 61508-3 Corr.1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*, and IEC 61508-4 Corr.1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

### 3 Terms, definitions, symbols and abbreviated terms

#### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100-1 and IEC 60050-191 and the following apply.

##### 3.1.1

##### **safety-related part of a control system**

##### **SRP/CS**

part of a control system that responds to safety-related input signals and generates safety-related output signals

NOTE 1 The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

NOTE 2 If monitoring systems are used for diagnostics, they are also considered as SRP/CS.

##### 3.1.2

##### **category**

classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

##### 3.1.3

##### **fault**

state of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

NOTE 1 A fault is often the result of a failure of the item itself, but may exist without prior failure.

[IEC 60050-191:1990, 05-01]

NOTE 2 In this part of ISO 13849, "fault" means *random fault*.

---

1) To be published. (Revision of ISO 14121:1999)