MASINATE OHUTUS. JUHTIMISSÜSTEEMIDE OHUTUSEGA SEOTUD OSAD. OSA 1: KAVANDAMISE PÕHIMÕTTED

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2015)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO 13849-1:2015 sisaldab Euroopa standardi EN ISO 13849-1:2015 ingliskeelset teksti.	This Estonian standard EVS-EN ISO 13849-1:2015 consists of the English text of the European standard EN ISO 13849-1:2015.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 23.12.2015.	Date of Availability of the European standard is 23.12.2015.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 13.110

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 13849-1

December 2015

ICS 13.110

Supersedes EN ISO 13849-1:2008

English Version

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2015)

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception (ISO 13849-1:2015)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015)

This European Standard was approved by CEN on 20 June 2015.

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-CENELEC 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-CENELEC Management Centre has the same status as the official versions.

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO 13849-1:2015 E

European foreword

This document (EN ISO 13849-1:2015) has been prepared by Technical Committee ISO/TC 199 “Safety of machinery” in collaboration with 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 June 2016, and conflicting national standards shall be withdrawn at the latest by June 2016.

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 13849-1:2008.

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 EU Directive(s).

For relationship with EU Directive(s), see informative Annex ZA, which is an 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, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 13849-1:2015 has been approved by CEN as EN ISO 13849-1:2015 without any modification.

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 199, *Safety of machinery*.

This third edition cancels and replaces the second edition (ISO 13849-1:2006), which has been technically revised. It also incorporates Technical Corrigendum ISO 13849-1:2006/Cor 1:2009. Changes from the previous edition include

— deletion of the former Table 1 from the Introduction,

— updating and addition of normative references,

— modification of the definitions of terms *hazardous situation* and *high demand or continuous mode*,

— addition of a new term and definition, *proven in use*,

— editorial, but not technical, modification of Figure 1,

— a new subclause, 4.5.5, as well as modifications to existing sections including the annexes, substantial modification of Annex C and an entirely new Annex I.

ISO 13849 consists of the following parts, under the general title *Safety of machinery — Safety-related parts of control systems*:

— *Part 1: General principles for design*

— *Part 2: Validation*

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.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organisations, market surveillance etc.).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions, organizations for people with special needs);

— service providers, e. g. for maintenance (small, medium and large enterprises);

— consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

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 Directive 2006/42/EC on machinery. 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 2).

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 ($MTTF_D$), common cause failure (CCF)], design process, operating stress, environmental conditions and operation procedures.

In order to assist the designer and 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. ISO/TR 23849 gives guidance on the application of this part of ISO 13849 and IEC 62061 in the design of safety-related control systems for machinery.

As with ISO/TR 23849, ISO/TR 22100-2 has been added to the list of normative references given in Clause 2 — the latter owing to its importance for an understanding of the relationship between this part of ISO 13849 and ISO 12100.

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 for high demand and continuous mode, 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.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-2:2012, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

IEC 60050-191:1990, *International electrotechnical vocabulary — Chapter 191: Dependability and quality of service.* Amended by IEC 60050-191-am1:1999 and IEC 60050-191-am2:2002:1999

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements.* Corrected by IEC 61508-3/Cor.1:1999

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations.* Corrected by IEC 61508-4/Cor.1:1999

IEC 62061:2012, *Safety of machinery — Functional safety of safety–related electrical, electronic and programmable electronic control systems*

ISO/TR 22100-2:2013, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*

ISO/TR 23849, *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*

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 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 to entry: 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 to entry: 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 to entry: A fault is often the result of a failure of the item itself, but may exist without prior failure.

Note 2 to entry: In this part of ISO 13849, "fault" means *random fault*.

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

3.1.4
failure
termination of the ability of an item to perform a required function

Note 1 to entry: After a failure, the item has a fault.

Note 2 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

Note 3 to entry: The concept as defined does not apply to items consisting of software only.

Note 4 to entry: Failures which only affect the availability of the process under control are outside of the scope of this part of ISO 13849.

[SOURCE: IEC 60050–191:1990, 04-01.]