BRITISH STANDARD

BS EN ISO
13849-1:2006

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

## Part 1: General principles for design

The European Standard EN ISO 13849-1:2006 has the status of a British Standard

ICS 13.110



BSI
British Standards

# National foreword

This British Standard was published by BSI. It is the UK implementation of EN ISO 13849-1:2006. It is identical to ISO 13849-1:2006. It supersedes BS EN 954-1:1997 which will be withdrawn by November 2009. ISO 13849-1:2006 supersedes ISO 13849-1:1999.

The UK participation in its preparation was entrusted to Technical Committee MCE/3, Safety of Machinery.

A list of organizations represented on this committee can be obtained on request to its secretary.

The date of applicability of EN ISO 13849-1:2006 as a "harmonized" European Standard is subject to an announcement in the *Official Journal of the European Communities*. After this date this EN ISO 13849-1:2006 may be used for CE marking purposes for items within its scope.

The UK as a member of CEN is obliged to publish EN ISO 13849-1:2006 as a British Standard. Attention is drawn to the fact that during the development of this European standard, the UK voted against its approval as a European standard because in the opinion of the UK committee the document might lead to design of complex electronic systems including programmable systems with associated software[1] that have inappropriate safety performance for their intended application.

EN ISO 13849-1:2006 is intended to provide users with a means of transition from categories given in BS EN 954-1:1997 to performance levels, which are a more comprehensive indicator of functional safety.

There is an overlap in scope with EN 62061:2005 and therefore joint work is in progress between ISO and IEC to publish a technical report that will explain the relationship between the requirements of EN ISO 13849-1:2006 and EN 62061:2005.

It is recommended that EN ISO 13849-1:2006 is used primarily for the design of low complexity[2] SRP/CS.

[1] This includes software that is developed separately for use with programmable electronic systems.
[2] It is recommended that EN 62061 be used for the design of complex electrical/electronic/ programmable electronic safety-related control systems for machinery until the technical report is published.

Users of EN ISO 13849-1:2006 in the UK can obtain further support in its interpretation and application, and propose future modifications, by contacting the secretary of Technical Committee MCE/3.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2007



ISBN 978 0 580 50882 0

**Amendments issued since publication**

| Amd. No. | Date | Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN ISO 13849-1

November 2006

ICS 13.110

Supersedes EN 954-1:1996

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 2 October 2006.

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 Central Secretariat 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 Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, 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**



Ref. No. EN ISO 13849-1:2006: E

## Foreword

This document (EN ISO 13849-1:2006) has been prepared by Technical Committee CEN/TC 114 "Safety of machinery", the secretariat of which is held by DIN, in collaboration with Technical Committee ISO/TC 199 "Safety of machinery".

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 May 2007, and conflicting national standards shall be withdrawn at the latest by November 2009.

This document supersedes EN 954-1:1996.

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, 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.

EN ISO 13849-1:2006

INTERNATIONAL STANDARD

**ISO 13849-1**

Second edition
2006-11-01

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

## Part 1: General principles for design

*Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —*

*Partie 1: Principes généraux de conception*

Reference number
ISO 13849-1:2006(E)

# 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 13849-1 was prepared by the European Committee for Standardization (CEN) Technical Committee CEN/TC 114, *Safety of machinery*, in collaboration with Technical Committee ISO/TC 199, *Safety of machinery*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO ISO 13849-1:1999), which has been technically revised.

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*

— *Part 100: Guidelines for the use and application of ISO 13849-1* [Technical Report]

# 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 ($MTTF_d$), 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 [a] and up to PL = e | All architectures and up to SIL 3 |
| C | Complex electronics, e.g. programmable | Restricted to designated architectures [a] and up to PL = d | All architectures and up to SIL 3 |
| D | A combined with B | Restricted to designated architectures [a] and up to PL = e | X [c] |
| 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 [b] | X [c] |

X indicates that this item is dealt with by the International Standard shown in the column heading.

[a] Designated architectures are defined in 6.2 in order to give a simplified approach for quantification of performance level.

[b] For complex electronics: use designated architectures according to this part of ISO 13849 up to PL = d or any architecture according to IEC 62061.

[c] For non-electrical technology, use parts in accordance with this part of ISO 13849 as subsystems.

*blank*

# 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*