

BS EN ISO 13849-2:2012



BSI Standards Publication

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

## Part 2: Validation

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

*raising standards worldwide™*



**National foreword**

This British Standard is the UK implementation of EN ISO 13849-2:2012. It supersedes BS EN ISO 13849-2:2008 which is withdrawn.

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

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

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

© The British Standards Institution 2012. Published by BSI Standards Limited 2012

ISBN 978 0 580 66820 3

ICS 13.110; 29.020

**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 October 2012.

**Amendments issued since publication**

Date	Text affected
------	---------------

---

English Version

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

Sécurité des machines - Parties des systèmes de  
commande relatives à la sécurité - Partie 2: Validation (ISO  
13849-2:2012)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von  
Steuerungen - Teil 2: Validierung (ISO 13849-2:2012)

This European Standard was approved by CEN on 14 October 2012.

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

**Management Centre: Avenue Marnix 17, B-1000 Brussels**

## Foreword

This document (EN ISO 13849-2:2012) 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 April 2013, and conflicting national standards shall be withdrawn at the latest by April 2013.

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 13849-2:2008.

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.

For relationship with EU Directive, see informative Annex ZA, which is an integral part of this document.

According to the CEN/CENELEC Internal Regulations, the national standards organisations 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 13849-2:2012 has been approved by CEN as a EN ISO 13849-2:2012 without any modification.

**Annex ZA**  
(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 Union 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 the relevant Essential Requirements 1.2.1 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
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Validation process</b> .....	<b>1</b>
4.1 Validation principles.....	1
4.2 Validation plan.....	3
4.3 Generic fault lists.....	4
4.4 Specific fault lists.....	4
4.5 Information for validation.....	4
4.6 Validation record.....	6
<b>5 Validation by analysis</b> .....	<b>6</b>
5.1 General.....	6
5.2 Analysis techniques.....	7
<b>6 Validation by testing</b> .....	<b>7</b>
6.1 General.....	7
6.2 Measurement accuracy.....	8
6.3 More stringent requirements.....	8
6.4 Number of test samples.....	8
<b>7 Validation of safety requirements specification for safety functions</b> .....	<b>9</b>
<b>8 Validation of safety functions</b> .....	<b>9</b>
<b>9 Validation of performance levels and categories</b> .....	<b>10</b>
9.1 Analysis and testing.....	10
9.2 Validation of category specifications.....	10
9.3 Validation of MTTF <sub>d</sub> , DC <sub>avg</sub> and CCF.....	12
9.4 Validation of measures against systematic failures related to performance level and category of SRP/CS.....	13
9.5 Validation of safety-related software.....	13
9.6 Validation and verification of performance level.....	14
9.7 Validation of combination of safety-related parts.....	14
<b>10 Validation of environmental requirements</b> .....	<b>15</b>
<b>11 Validation of maintenance requirements</b> .....	<b>15</b>
<b>12 Validation of technical documentation and information for use</b> .....	<b>16</b>
<b>Annex A (informative) Validation tools for mechanical systems</b> .....	<b>17</b>
<b>Annex B (informative) Validation tools for pneumatic systems</b> .....	<b>21</b>
<b>Annex C (informative) Validation tools for hydraulic systems</b> .....	<b>31</b>
<b>Annex D (informative) Validation tools for electrical systems</b> .....	<b>40</b>
<b>Annex E (informative) Example of validation of fault behaviour and diagnostic means</b> .....	<b>53</b>
<b>Bibliography</b> .....	<b>78</b>

## 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 13849-2 was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

This second edition cancels and replaces the first edition (ISO 13849-2:2003), which has been technically revised in order to adapt to ISO 13849-1:2006. In addition, the new Annex E provides an example for the validation of fault behaviour and diagnostic means.

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*

Annexes A to D, which are informative, are structured according to Table 1.

**Table 1 — Structure of Annexes A to D of this part of ISO 13849**

Annex	Technology	List of basic safety principles	List of well-tried safety principles	List of well-tried components	Fault lists and fault exclusions
		Table(s)			
A	Mechanical	A.1	A.2	A.3	A.4, A.5
B	Pneumatic	B.1	B.2	—	B.3 to B.18
C	Hydraulic	C.1	C.2	—	C.3 to C.12
D	Electrical (includes electronics)	D.1	D.2	D.3	D.4 to D.21

## Introduction

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

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

This document is a type-B standard as stated in ISO 12100.

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.

This part of ISO 13849 specifies the validation process for the safety functions, categories and performance levels for the safety-related parts of control systems. It recognizes that the validation of safety-related parts of control systems can be achieved by a combination of analysis (see Clause 5) and testing (see Clause 6), and specifies the particular circumstances in which testing ought to be carried out.

Most of the procedures and conditions in this part of ISO 13849 are based on the assumption that the simplified procedure for estimating the performance level (PL) described in ISO 13849-1:2006, 4.5.4, is used. This part of ISO 13849 does not provide guidance for situations when other procedures are used to estimate PL (e.g. Markov modelling), in which case some of its provisions will not apply and additional requirements can be necessary.

Guidance on the general principles for the design (see ISO 12100) of safety-related parts of control systems, regardless of the type of technology used (electrical, hydraulic, pneumatic, mechanical, etc.), is provided in ISO 13849-1. This includes descriptions of some typical safety functions, determination of their required performance levels, and general requirements of categories and performance levels.

Within this part of ISO 13849, some of the validation requirements are general, whereas others are specific to the type of technology used.





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

## Part 2: Validation

### 1 Scope

This part of ISO 13849 specifies the procedures and conditions to be followed for the validation by analysis and testing of

- the specified safety functions,
- the category achieved, and
- the performance level achieved

by the safety-related parts of a control system (SRP/CS) designed in accordance with ISO 13849-1.

NOTE Additional requirements for programmable electronic systems, including embedded software, are given in ISO 13849-1:2006, 4.6, and IEC 61508.

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

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

### 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and ISO 13849-1 apply.

### 4 Validation process

#### 4.1 Validation principles

The purpose of the validation process is to confirm that the design of the SRP/CS supports the overall safety requirements specification for the machinery.

The validation shall demonstrate that each SRP/CS meets the requirements of ISO 13849-1 and, in particular, the following:

- a) the specified safety characteristics of the safety functions provided by that part, as set out in the design rationale;
- b) the requirements of the specified performance level (see ISO 13849-1:2006, 4.5):
  - 1) the requirements of the specified category (see ISO 13849-1:2006, 6.2),