

This is a preview of "ISO 13849-1:2015". [Click here to purchase the full version from the ANSI store.](#)

Third edition
2015-12-15

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 13849-1:2015(E)

© ISO 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

This is a preview of "ISO 13849-1:2015". [Click here to purchase the full version from the ANSI store.](#)

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	2
3.1 Terms and definitions.....	2
3.2 Symbols and abbreviated terms.....	7
4 Design considerations	9
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).....	13
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).....	16
4.5.3 Diagnostic coverage (DC).....	17
4.5.4 Simplified procedure for estimating the quantifiable aspects of PL.....	17
4.5.5 Description of the output part of the SRP/CS by category.....	19
4.6 Software safety requirements.....	20
4.6.1 General.....	20
4.6.2 Safety-related embedded software (SRESW).....	21
4.6.3 Safety-related application software (SRASW).....	22
4.6.4 Software-based parameterization.....	24
4.7 Verification that achieved PL meets PL _r	25
4.8 Ergonomic aspects of design.....	26
5 Safety functions	26
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.....	30
6 Categories and their relation to MTTF_D of each channel, DC_{avg} and CCF	31
6.1 General.....	31
6.2 Specifications of categories.....	31
6.2.1 General.....	31
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.....	38
7 Fault consideration, fault exclusion	40
7.1 General.....	40
7.2 Fault consideration.....	40

This is a preview of "ISO 13849-1:2015". Click here to purchase the full version from the ANSI store.

7.3	Fault exclusion.....	40
8	Validation.....	40
9	Maintenance.....	40
10	Technical documentation.....	41
11	Information for use.....	41
Annex A (informative)	Determination of required performance level (PL_r).....	43
Annex B (informative)	Block method and safety-related block diagram.....	47
Annex C (informative)	Calculating or evaluating MTTF_D values for single components.....	49
Annex D (informative)	Simplified method for estimating MTTF_D for each channel.....	56
Annex E (informative)	Estimates for diagnostic coverage (DC) for functions and modules.....	58
Annex F (informative)	Estimates for common cause failure (CCF).....	61
Annex G (informative)	Systematic failure.....	63
Annex H (informative)	Example of combination of several safety-related parts of the control system.....	66
Annex I (informative)	Examples.....	69
Annex J (informative)	Software.....	76
Annex K (informative)	Numerical representation of Figure 5.....	79
Bibliography	84

This is a preview of "ISO 13849-1:2015". [Click here to purchase the full version from the ANSI store.](#)

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.

This is a preview of "ISO 13849-1:2015". [Click here to purchase the full version from the ANSI store.](#)

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.