
**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

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 13849-1:2015

<https://standards.iteh.ai/catalog/standards/iso/102c8872-3b48-445c-a20d-f2a203deca14/iso-13849-1-2015>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 13849-1:2015

<https://standards.iteh.ai/catalog/standards/iso/102c8872-3b48-445c-a20d-f2a203deca14/iso-13849-1-2015>



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

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

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

iteh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 13849-1:2015

<https://standards.iteh.ai/catalog/standards/iso/102c8872-3b48-445c-a20d-f2a203deca14/iso-13849-1-2015>

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](https://standards.iso.org/standards.html?csd=622007236837700d-f2a203deca14/iso-13849-1-2015).

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.]

3.1.5**dangerous failure**

failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

Note 1 to entry: Whether or not the potential is realized can depend on the channel architecture of the system; in redundant systems a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

Note 2 to entry: [SOURCE: IEC 61508-4, 3.6.7, modified.]

3.1.6**common cause failure****CCF**

failures of different items, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: Common cause failures should not be confused with common mode failures (see ISO 12100:2010, 3.36).

[SOURCE: IEC 60050-191-am1:1999, 04-23.]

3.1.7**systematic failure**

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in

- the safety requirements specification,
- the design, manufacture, installation, operation of the hardware, and
- the design, implementation, etc., of the software.

[SOURCE: IEC 60050-191:1990, 04-19.]

3.1.8**muting**

temporary automatic suspension of a safety function(s) by the SRP/CS

3.1.9**manual reset**

function within the SRP/CS used to restore manually one or more safety functions before re-starting a machine

3.1.10**harm**

physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5.]

3.1.11**hazard**

potential source of harm

Note 1 to entry: A hazard can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard, fire hazard).

Note 2 to entry: The hazard envisaged in this definition:

- either is permanently present during the intended use of the machine (e.g. motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature);
- or may appear unexpectedly (e.g. explosion, crushing hazard as a consequence of an unintended/unexpected start-up, ejection as a consequence of a breakage, fall as a consequence of acceleration/deceleration).

[SOURCE: ISO 12100:2010, 3.6, modified.]

3.1.12

hazardous situation

circumstance in which a person is exposed to at least one hazard

Note 1 to entry: The exposure can result in harm immediately or over a period of time.

[SOURCE: ISO 12100:2010, 3.10.]

3.1.13

risk

combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12.]

3.1.14

residual risk

risk remaining after protective measures have been taken

Note 1 to entry: See [Figure 2](#).

[SOURCE: ISO 12100:2010, 3.13, modified.]

3.1.15

risk assessment

overall process comprising risk analysis and risk evaluation

[SOURCE: ISO 12100:2010, 3.17.]

3.1.16

risk analysis

combination of the specification of the limits of the machine, hazard identification and risk estimation

[SOURCE: ISO 12100:2010, 3.15.]

3.1.17

risk evaluation

judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

[SOURCE: ISO 12100:2010, 3.16.]

3.1.18

intended use of a machine

use of the machine in accordance with the information provided in the instructions for use

[SOURCE: ISO 12100:2010, 3.23.]

3.1.19

reasonably foreseeable misuse

use of a machine in a way not intended by the designer, but which may result from readily predictable human behaviour

[SOURCE: ISO 12100:2010, 3.24.]

3.1.20**safety function**

function of the machine whose failure can result in an immediate increase of the risk(s)

[SOURCE: ISO 12100:2010, 3.30.]

3.1.21**monitoring**

safety function which ensures that a protective measure is initiated if the ability of a component or an element to perform its function is diminished or if the process conditions are changed in such a way that a decrease of the amount of risk reduction is generated

3.1.22**programmable electronic system****PES**

system for control, protection or monitoring dependent for its operation on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, contactors and other output devices

[SOURCE: IEC 61508-4:1998, 3.3.2, modified.]

3.1.23**performance level****PL**

discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

Note 1 to entry: See [4.5.1](#).

3.1.24**required performance level****PL_r**

performance level (PL) applied in order to achieve the required risk reduction for each safety function

Note 1 to entry: See [Figures 2](#) and [A.1](#).

3.1.25**mean time to dangerous failure****MTTF_D**

expectation of the mean time to dangerous failure

[SOURCE: IEC 62061:2005, 3.2.34, modified.]

3.1.26**diagnostic coverage****DC**

measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures

Note 1 to entry: Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or final elements.

[SOURCE: IEC 61508-4:1998, 3.8.6, modified.]

3.1.27**protective measure**

measure intended to achieve risk reduction

EXAMPLE 1 Implemented by the designer: inherent design, safeguarding and complementary protective measures, information for use.

EXAMPLE 2 Implemented by the user: organization (safe working procedures, supervision, permit-to-work systems), provision and use of additional safeguards, personal protective equipment, training.

[SOURCE: ISO 12100:2010, 3.19, modified.]

3.1.28
mission time

T_M
period of time covering the intended use of an SRP/CS

3.1.29
test rate

r_t
frequency of automatic tests to detect faults in a SRP/CS, reciprocal value of diagnostic test interval

3.1.30
demand rate

r_D
frequency of demands for a safety-related action of the SRP/CS

3.1.31
repair rate

r_r
reciprocal value of the period of time between detection of a dangerous failure by either an online test or obvious malfunction of the system and the restart of operation after repair or system/component replacement

Note 1 to entry: The repair time does not include the span of time needed for failure-detection.

3.1.32
machine control system

system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

Note 1 to entry: The machine control system can use any technology or any combination of different technologies (e.g. electrical/electronic, hydraulic, pneumatic, mechanical).

3.1.33
safety integrity level

SIL
discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

[SOURCE: IEC 61508-4:1998, 3.5.6.]

3.1.34
limited variability language

LVL
type of language that provides the capability of combining predefined, application-specific library functions to implement the safety requirements specifications

Note 1 to entry: Typical examples of LVL (ladder logic, function block diagram) are given in IEC 61131-3.

Note 2 to entry: A typical example of a system using LVL: PLC.

[SOURCE: IEC 61511-1:2003, 3.2.80.1.2, modified.]