
**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



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS

© ISO 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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	8
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).....	14
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 ($MTTF_d$)	17
4.5.3 Diagnostic coverage (DC)	18
4.5.4 Simplified procedure for estimating PL	18
4.6 Software safety requirements	21
4.6.1 General.....	21
4.6.2 Safety-related embedded software (SRESW).....	21
4.6.3 Safety-related application software (SRASW).....	22
4.6.4 Software-based parameterization	25
4.7 Verification that achieved PL meets PL_r	26
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	31
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	32
6.2.1 General.....	32
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	39

7	Fault consideration, fault exclusion.....	40
7.1	General	40
7.2	Fault consideration	40
7.3	Fault exclusion	41
8	Validation	41
9	Maintenance.....	41
10	Technical documentation.....	41
11	Information for use	42
Annex A (informative)	Determination of required performance level (PL_r)	44
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	57
Annex E (informative)	Estimates for diagnostic coverage (DC) for functions and modules.....	59
Annex F (informative)	Estimates for common cause failure (CCF)	62
Annex G (informative)	Systematic failure	64
Annex H (informative)	Example of combination of several safety-related parts of the control system	67
Annex I (informative)	Examples	70
Annex J (informative)	Software	77
Annex K (informative)	Numerical representation of Figure 5	80
Bibliography	83

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 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.			

This document is a preview generated by EVS

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*

ISO 14121¹⁾, *Safety of machinery — Principles of risk assessment*

IEC 60050-191:1990, *International electrotechnical vocabulary — Chapter 191: Dependability and quality of service*, and IEC 60050-191-am1:1999 and IEC 60050-191-am2:2002:1999, *Amendment 1 and Amendment 2, International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service*

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements*, and IEC 61508-3 Corr.1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*, and IEC 61508-4 Corr.1:1999, *Corrigendum 1 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

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 12100-1 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 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 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 A fault is often the result of a failure of the item itself, but may exist without prior failure.

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

NOTE 2 In this part of ISO 13849, "fault" means *random fault*.

1) To be published. (Revision of ISO 14121:1999)