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)

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

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.

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 14121[1)], *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)

3.1.4
failure
termination of the ability of an item to perform a required function

NOTE 1 After a failure, the item has a fault.

NOTE 2 “Failure” is an event, as distinguished from “fault”, which is a state.

NOTE 3 The concept as defined does not apply to items consisting of software only.

[IEC 60050–191:1990, 04-01]

NOTE 4 Failures which only affect the availability of the process under control are outside of the scope of this part of ISO 13849.

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 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 Adapted from IEC 61508-4:1998, definition 3.6.7.

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

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

NOTE Common cause failures should not be confused with common mode failures (see ISO 12100-1:2003, 3.34).

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 Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

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

NOTE 3 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.

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

[ISO 12100-1:2003, 3.5]

3.1.11
hazard
potential source of harm

NOTE 1 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 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).

[ISO 12100-1:2003, 3.6]

3.1.12
hazardous situation
circumstance in which a person is exposed to at least one hazard, the exposure having immediately or over a long period of time the potential to result in harm

[ISO 12100-1:2003, 3.9]

3.1.13
risk
combination of the probability of occurrence of harm and the severity of that harm

[ISO 12100-1:2003, 3.11]

3.1.14
residual risk
risk remaining after protective measures have been taken

See Figure 2.

NOTE Adapted from ISO 12100-1:2003, definition 3.12.

3.1.15
risk assessment
overall process comprising risk analysis and risk evaluation

[ISO 12100-1:2003, 3.13]

3.1.16
risk analysis
combination of the specification of the limits of the machine, hazard identification and risk estimation

[ISO 12100-1:2003, 3.14]

3.1.17
risk evaluation
judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

[ISO 12100-1:2003, 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

[ISO 12100-1:2003, 3.22]

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

[ISO 12100-1:2003, 3.23]

3.1.20
safety function
function of the machine whose failure can result in an immediate increase of the risk(s)

[ISO 12100-1:2003, 3.28]

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

NOTE Adapted from IEC 61508-4:1998, definition 3.3.2.

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 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

See Figures 2 and A.1.

3.1.25
mean time to dangerous failure
$MTTF_d$
expectation of the mean time to dangerous failure

NOTE Adapted from IEC 62061:2005, definition 3.2.34.

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 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.

NOTE 2 Adapted from IEC 61508-4:1998, definition 3.8.6.

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.

NOTE Adapted from ISO 12100-1:2003, definition 3.18.

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 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 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

[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 Adapted from IEC 61511-1:2003, definition 3.2.80.1.2.

NOTE 2 Typical examples of LVL (ladder logic, function block diagram) are given in IEC 61131-3.

NOTE 3 A typical example of a system using LVL: PLC.

3.1.35
full variability language
FVL
type of language that provides the capability of implementing a wide variety of functions and applications

EXAMPLE C, C++, Assembler.

NOTE 1 Adapted from IEC 61511-1:2003, definition 3.2.80.1.3.

NOTE 2 A typical example of systems using FVL: embedded systems.

NOTE 3 In the field of machinery, FVL is found in embedded software and rarely in application software.

3.1.36
application software
software specific to the application, implemented by the machine manufacturer, and generally containing logic sequences, limits and expressions that control the appropriate inputs, outputs, calculations and decisions necessary to meet the SRP/CS requirements

3.1.37
embedded software
firmware
system software
software that is part of the system supplied by the control manufacturer and which is not accessible for modification by the user of the machinery.

NOTE Embedded software is usually written in FVL.