DRAFT INTERNATIONAL STANDARD

ISO/DIS 13849-1

ISO/TC **199** Secretariat: **DIN**

Voting begins on: **2020-06-08**

Voting terminates on: **2020-08-31**

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

ICS: 13.110

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 13849-1:2020(E)

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

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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

The first edition of ISO 13849-1 was published in 1999 based on EN 954-1:1996.

The second edition of ISO 13849-1 was revised in 2006.

The third edition was amended and published in 2015.

This fourth edition cancels and replaces the third edition (ISO 13849-1:2015), which has been technically revised.

A list of all parts in the ISO 13849 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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.

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.

NOTE 1 The examples and basis for most content is based on stationary machines in factory applications. However, other machines are not excluded. This document was written with the intent of being used across many machinery industries and as a basis for type-C standards developers.

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.

Risk reduction according to ISO 12100:2010, Clause 6, is accomplished by applying, in the following sequence, inherently safe design measures, safeguarding and/or complementary risk reduction measures and information for use. A designer may reduce risks by risk reduction measures that can have safety functions. Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS). These can consist of hardware and/

or software, and can either be separate from the machine control system or an integral part of it. In addition to implementing safety functions, SRP/CS can also implement operational functions.

ISO 12100 is used for risk assessment of the machine. ISO 13849-1, Annex A, can be used for the determination of the required performance level of a safety function performed by the SRP/CS, where PL_r is not specified in the applicable type-C standard.

ISO 13849-1 is relevant for the SRP/CS safety functions that are used to address risks for cases where a risk assessment conducted according to ISO 12100 has initiated a risk reduction measure (e.g. interlocking guard) that relies on a safety-related control system. In those cases, the safety-related control system has to perform a safety function. ISO 13849-1 should be used to design and evaluate the safety-related parts of the control system. Only the part of the control system that is safety-related falls under the scope of ISO 13849-1.

Figure 1 illustrates the relationship between ISO 12100 and ISO 13849-1.

NOTE 2 See also ISO/TR 22100-2:2013 for further information.

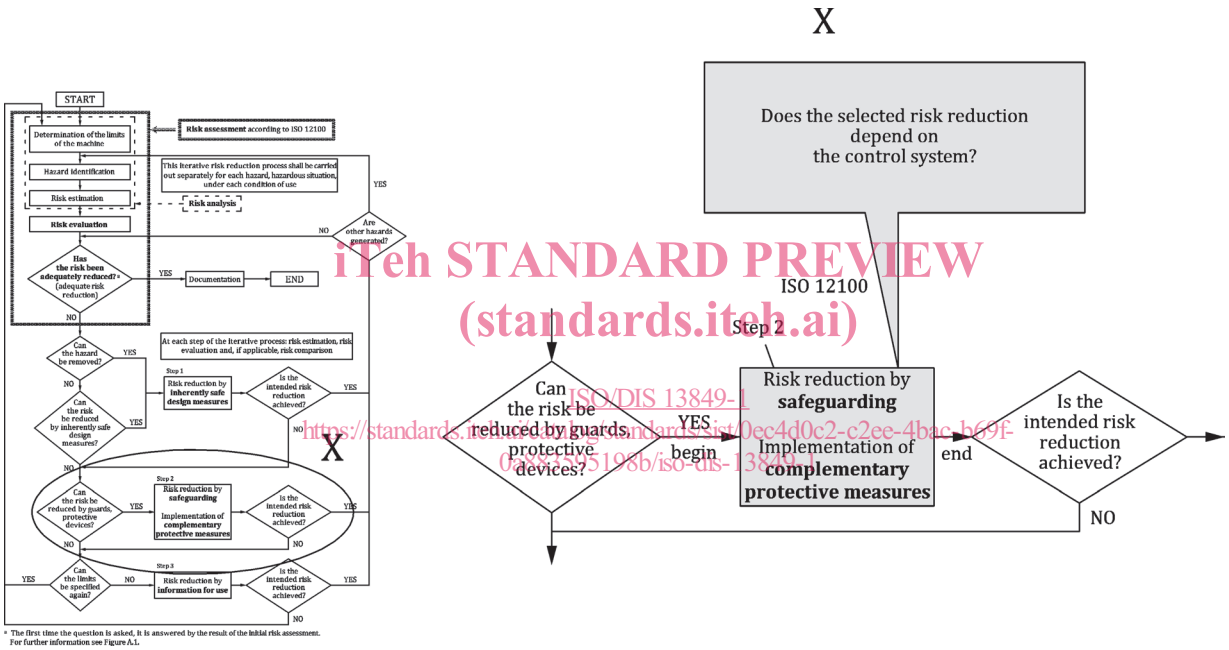

Figure 1 — Integration of ISO 13849-1 within the risk reduction process of ISO 12100

NOTE 3 Figure 1 shows where the SRP/CS contributes to the risk reduction process of ISO 12100: Step 2. The SRP/CS supports the combined risk reduction measures by the implementation of safety functions.

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). The required performance level (PLr) for a particular safety function will be determined by risk estimation.

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.

Functional safety includes a categorization of architecture according to specific design and specified behaviours under fault conditions. This architecture is allocated one of five categories B, 1, 2, 3 and 4.

Functional safety considers the failure characteristics of elements/components performing a safety function. For each safety function, this failure characteristic is expressed as the probability of dangerous failure per hour (PFH_D).

Risk estimation will show a variance because of the subjective nature of the evaluation criteria. Type-C standards can have more specific risk estimation methods for specific machine applications, which can be less subjective in nature. Therefore, using the methodology in this document should be considered as valuable guidance for the design of the safety-related parts of the control system rather than a strict requirement. The performance levels and categories can be applied to safety-related parts of control systems, such as

— control units (e.g. a logic unit for control functions, data processing, monitoring, etc.) and

— electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices.

The performance levels can be calculated, and categories determined for

— SRP/CS performing safety functions for machinery,

— subsystems of SRP/CS using safety parts (components) such as

— protective devices (e.g. two-hand control devices, interlocking devices);

— power control elements (e.g. relays, valves);

— Sensors and HMI elements (position sensors, enable switches).

Machinery considered by this standard can range from simple (e.g., small kitchen machines, or automatic doors and gates) to complex (e.g., packaging machines, printing machines, presses).

IEC 62061 and this part of ISO 13849 both specify a methodology and provide related guidance for the design and implementation of safety-related control systems of machinery.

NOTE ISO/TR 23849 gives guidance on the relation between both standards, how they complement each other.

The requirements of Clause 10 of ISO 13849-1 supersede the requirements of ISO 13849-2:2012 with the exception of the informative annexes. An SRP/CS that meets the requirements of Clause 10 is considered to meet the requirements of ISO 13849-2:2012.

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

Part 1: General principles for design

1 Scope

This part of ISO 13849 specifies a methodology and provides related guidance for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. This document specifies the characteristics needed to determine the performance level required of safety functions. This document applies to SRP/CS for high demand and continuous mode including their subsystems, regardless of the type of technology and energy (e.g. electrical, hydraulic, pneumatic, mechanical), for many kinds of machinery. The standard does not apply to low demand mode.

This document does not specify the safety functions or required performance levels that are to be used in particular applications.

This document does not give specific requirements for the design of products that are parts of SRP/CS.

This document does not provide specific measures for security (e.g. physical, IT-security, cyber security) aspects.

NOTE 1 This document specifies a methodology for SRP/CS design without considering if certain machinery (e.g. mobile machinery) requires specific requirements. These specific requirements can be considered in a Type-C standard.

NOTE 2 See IEC 61508 for low demand mode.

NOTE 3 See also ISO/TR 22100-4 for IT-security aspects and IEC/TR 63074 for security aspects.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 13849-2:2013, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

IEC 60204-1:2016, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 62046:2018, *Safety of machinery — Application of protective equipment to detect the presence of persons*

ISO 62061:2015, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1 Terms and definitions

3.1.1
safety–related part of a control system
SRP/CS
part of a control system that performs a safety function, starting from safety-related input(s) to generating safety-related output(s)

Note 1 to entry: The safety-related parts of a control system starts at the point where the safety-related inputs 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).

3.1.2
safety requirement specification
SRS
specification containing the requirements for the safety functions that have to be performed by the safety related control system in terms of characteristics of the safety functions (functional requirements) and required performance levels

[SOURCE: IEC 61508-4:2010, 3.5.11 and 3.5.12, modified, NOTE added]

3.1.3
category
classification of the subsystem in respect of the resistance to faults and the subsequent behaviour in the fault condition which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

3.1.4
fault
state of a device 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 can exist without prior failure.

Note 2 to entry: In this part of ISO 13849-1, “fault” means random fault or fault caused by a systematic failure.

[SOURCE: IEC 60050-192:2015; modified: NOTE 2 to entry amended]

3.1.5
fault exclusion
exclusion of certain faults within an SRP/CS, if this can be justified due to their improbability and their negligible contribution to the reliability of the SRP/CS

3.1.6
failure
termination of the ability of a device to perform a required function

Note 1 to entry: After a failure, the device has a fault.

Note 2 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

Note 3 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 60050-192:2015; modified: NOTE 4 to entry amended]

3.1.7
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.

[SOURCE: IEC 61508-4:2010, 3.6.7]

3.1.8
common cause failure
CCF
failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel subystem, leading to failure of a safety function

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

[SOURCE: IEC 61508-4:2010]

3.1.9
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 60050-192:2015]

3.1.10
muting
temporary automatic suspension of a safety function(s) by the SRP/CS

3.1.11
manual reset
safety function within the SRP/CS used to restore manually one or more safety functions before re-starting a machine

3.1.12
harm
physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5]

3.1.13
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 and 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 can 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, Note 3 deleted]

3.1.14
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]

3.1.15
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 12100:2010, 3.12]

3.1.16
residual risk
risk remaining after risk reduction measures (protective measures) have been taken

Note 1 to entry: See Figure 2.

[SOURCE: ISO 12100:2010, 3.13, Note 1 modified]

3.1.17
risk assessment
overall process comprising risk analysis and risk evaluation

[SOURCE: ISO 12100:2010, 3.17]

3.1.18
risk analysis
combination of the specification of the limits of the machine, hazard identification and risk estimation

[SOURCE: ISO 12100:2010, 3.15]

3.1.19
risk evaluation
judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved

[SOURCE: ISO 12100:2010, 3.16]

3.1.20
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]

3.1.21
reasonably foreseeable misuse
use of a machine in a way not intended by the designer, but which can result from readily predictable human behaviour

[SOURCE: ISO 12100:2010, 3.24]

3.1.22
safety function
function of the machine whose failure can result in an immediate increase of the risk(s)

Note 1 to entry: A safety function is a function to be implemented by a safety-related part of a control system, which is needed to achieve or maintain a safe state for the machine, in respect of a specific hazardous event.

[SOURCE: ISO 12100:2010, 3.30]

3.1.23
monitoring
diagnostic measure which detects a state and compares it to the expected value

Note 1 to entry: Monitoring is realised by following methods: plausibility check (direct or indirect monitoring), cyclic test stimulus or cross monitoring

3.1.24
cross monitoring
diagnostic measure which checks plausibility of redundant signals in both channels of a redundant logic unit

3.1.25
programmable electronic system
PE system
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices

[SOURCE: IEC 61508-4:2010, 3.3.1]

3.1.26
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 6.1.

3.1.27
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 Figure 2 and Figure A.1.

3.1.28
mean time to dangerous failure
$MTTF_D$
expected value of time to dangerous failure

Note 1 to entry: In the case of items with an exponential distribution of operating times to dangerous failure (i.e. a constant failure rate) the MTTF D is numerically equal to the reciprocal of the dangerous failure rate".

[SOURCE: IEC 62061:2005, 3.2.34, NOTE 1 to entry modified]

3.1.29
mean time between failure
MTBF
expected value of the operating time between consecutive failures