INTERNATIONAL STANDARD

ISO 13849-2

Second edition
2012-10-15

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

Part 2: Validation

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —
Partie 2: Validation

Reference number
ISO 13849-2:2012(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 13849-2 was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

This second edition cancels and replaces the first edition (ISO 13849-2:2003), which has been technically revised in order to adapt to ISO 13849-1:2006. In addition, the new Annex E provides an example for the validation of fault behaviour and diagnostic means.

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*

Annexes A to D, which are informative, are structured according to Table 1.

Table 1 — Structure of Annexes A to D of this part of ISO 13849

Annex	Technology	List of basic safety principles	List of well-tried safety principles	List of well-tried components	Fault lists and fault exclusions
		Table(s)			
A	Mechanical	A.1	A.2	A.3	A.4, A.5
B	Pneumatic	B.1	B.2	—	B.3 to B.18
C	Hydraulic	C.1	C.2	—	C.3 to C.12
D	Electrical (includes electronics)	D.1	D.2	D.3	D.4 to D.21

Introduction

The structure of safety standards in the field of machinery is as follows:

a) type-A standards (basic safety standards) giving basic concepts, principles for design and general aspects that can be applied to machinery;

b) type-B standards (generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery:

   — type-B1 standards on particular safety aspects (for example safety distances, surface temperature, noise);

   — type-B2 standards on safeguards (for example two-hand controls, interlocking devices, pressure-sensitive devices, guards);

c) type-C standards (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

This document is a type-B standard as stated in ISO 12100.

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.

This part of ISO 13849 specifies the validation process for the safety functions, categories and performance levels for the safety-related parts of control systems. It recognizes that the validation of safety-related parts of control systems can be achieved by a combination of analysis (see Clause 5) and testing (see Clause 6), and specifies the particular circumstances in which testing ought to be carried out.

Most of the procedures and conditions in this part of ISO 13849 are based on the assumption that the simplified procedure for estimating the performance level (PL) described in ISO 13849-1:2006, 4.5.4, is used. This part of ISO 13849 does not provide guidance for situations when other procedures are used to estimate PL (e.g. Markov modelling), in which case some of its provisions will not apply and additional requirements can be necessary.

Guidance on the general principles for the design (see ISO 12100) of safety-related parts of control systems, regardless of the type of technology used (electrical, hydraulic, pneumatic, mechanical, etc.), is provided in ISO 13849-1. This includes descriptions of some typical safety functions, determination of their required performance levels, and general requirements of categories and performance levels.

Within this part of ISO 13849, some of the validation requirements are general, whereas others are specific to the type of technology used.

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

Part 2: Validation

1 Scope

This part of ISO 13849 specifies the procedures and conditions to be followed for the validation by analysis and testing of

— the specified safety functions,

— the category achieved, and

— the performance level achieved

by the safety-related parts of a control system (SRP/CS) designed in accordance with ISO 13849-1.

NOTE Additional requirements for programmable electronic systems, including embedded software, are given in ISO 13849-1:2006, 4.6, and IEC 61508 .

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 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and ISO 13849-1 apply.

4 Validation process

4.1 Validation principles

The purpose of the validation process is to confirm that the design of the SRP/CS supports the overall safety requirements specification for the machinery.

The validation shall demonstrate that each SRP/CS meets the requirements of ISO 13849-1 and, in particular, the following:

a) the specified safety characteristics of the safety functions provided by that part, as set out in the design rationale;

b) the requirements of the specified performance level (see ISO 13849-1:2006, 4.5):

   1) the requirements of the specified category (see ISO 13849-1:2006, 6.2),

2) the measures for control and avoidance of systematic failures (see ISO 13849-1:2006, Annex G),

3) if applicable, the requirements of the software (see ISO 13849-1:2006, 4.6), and

4) the ability to perform a safety function under expected environmental conditions;

c) the ergonomic design of the operator interface, e.g. so that the operator is not tempted to act in a hazardous manner, such as defeating the SRP/CS (see ISO 13849-1:2006, 4.8).

Validation should be carried out by persons who are independent of the design of the SRP/CS.

NOTE "Independent person" does not necessarily mean that a third-party test is required.

Validation consists of applying analysis (see Clause 5) and executing functional tests (see Clause 6) under foreseeable conditions in accordance with the validation plan. Figure 1 gives an overview of the validation process. The balance between the analysis and testing depends on the technology used for the safety-related parts and the required performance level. For Categories 2, 3 and 4 the validation of the safety function shall also include testing under fault conditions.

The analysis should be started as early as possible in, and in parallel with, the design process. Problems can then be corrected early while they are still relatively easy to correct, i.e. during steps "design and technical realization of the safety function" and "evaluate the performance level PL" [the fourth and fifth boxes down in in ISO 13849-1:2006, Figure 3]. It can be necessary for some parts of the analysis to be delayed until the design is well developed.

Where necessary due to the system's size, complexity or the effects of integrating it with the control system (of the machinery), special arrangements should be made for

— validation of the SRP/CS separately before integration, including simulation of the appropriate input and output signals, and

— validation of the effects of integrating safety-related parts into the remainder of the control system within the context of its use in the machine.

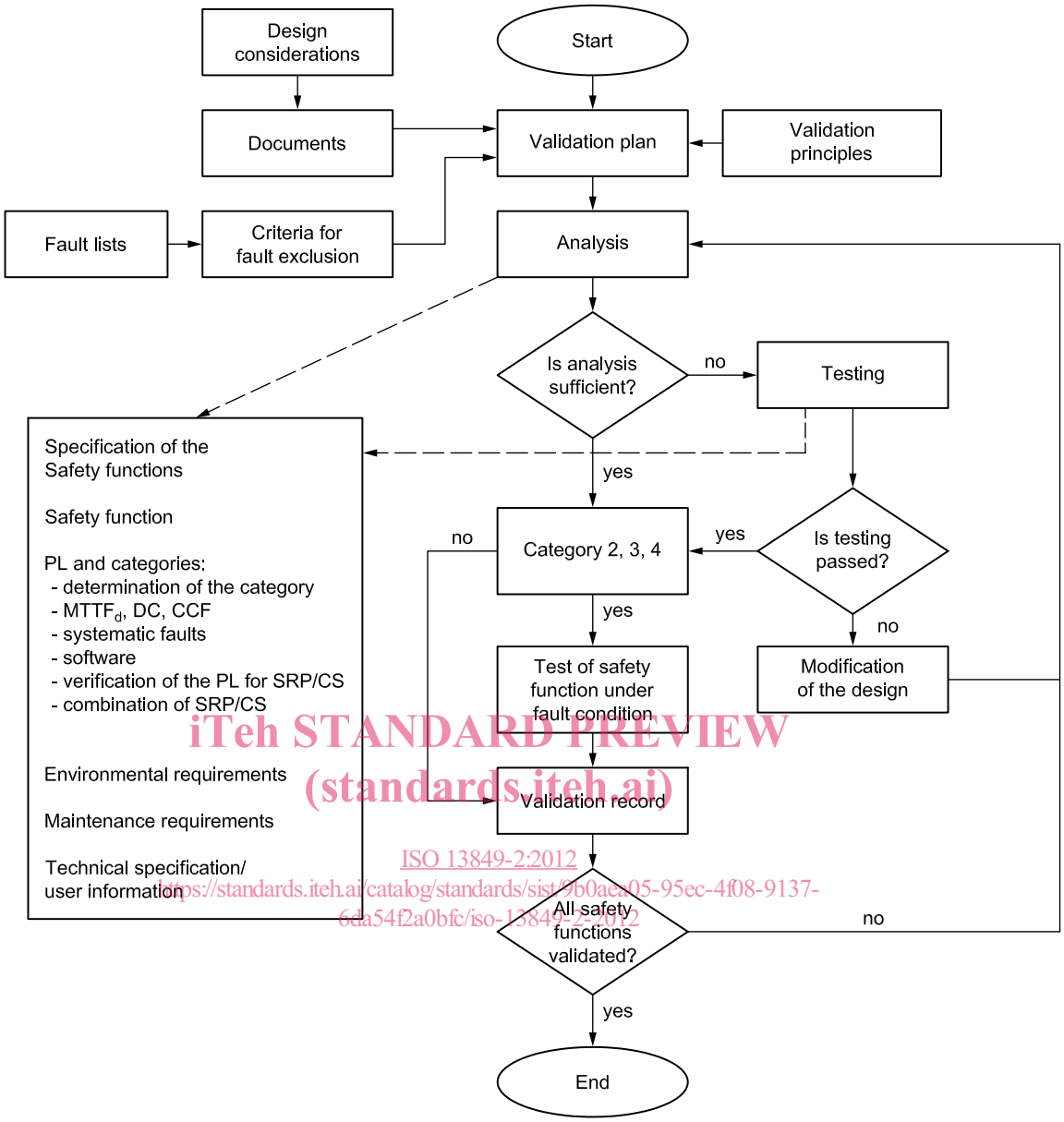

Figure 1 — Overview of the validation process

"Modification of the design" in Figure 1 refers to the design process. If the validation cannot be successfully completed, changes in the design are necessary. The validation of the modified safety-related parts should then be repeated. This process should be iterated until all safety-related parts of the safety functions are successfully validated.

4.2 Validation plan

The validation plan shall identify and describe the requirements for carrying out the validation process for the specified safety functions, their categories and performance levels.

The validation plan shall also identify the means to be employed to validate the specified safety functions, categories and performance levels. It shall set out, where appropriate

a) the identity of the specification documents,

b) the operational and environmental conditions during testing,

c) the analyses and tests to be applied,

d) the reference to test standards to be applied, and

e) the persons or parties responsible for each step in the validation process.

Safety-related parts which have previously been validated to the same specification need only a reference to that previous validation.

4.3 Generic fault lists

The validation process involves consideration of the behaviour of the SRP/CS for all faults to be considered. A basis for fault consideration is given in the tables of fault lists in Annexes A to D, which are based on experience and which contain

— the components/elements to be included, e.g. conductors/cables (see Annex D),

— the faults to be taken into account, e.g. short circuits between conductors,

— the permitted fault exclusions, taking into account environmental, operating and application aspects, and

— a remarks section giving the reasons for the fault exclusions.

Only permanent faults are taken into account in the fault lists.

4.4 Specific fault lists

If necessary, a specific product-related fault list shall be generated as a reference document for the validation process of the safety-related part(s). The list can be based on the appropriate generic list(s) found in the annexes.

Where the specific product-related fault list is based on the generic list(s) it shall state

a) the faults taken from the generic list(s) to be included,

b) any other relevant faults to be included but not given in the generic list (e.g. common-cause failures),

c) the faults taken from the generic list(s) which may be excluded on the basis that the criteria given in the generic list(s) (see ISO 13849-1:2006, 7.3) are satisfied, and

exceptionally

d) any other faults for which the generic list(s) do not permit an exclusion, but for which justification and rationale for an exclusion is presented (see ISO 13849-1:2006, 7.3).

Where this list is not based on the generic list(s), the designer shall give the rationale for fault exclusions.

4.5 Information for validation

The information required for validation will vary with the technology used, the category or categories and performance level(s) to be demonstrated, the design rationale of the system, and the contribution of the SRP/CS to the reduction of the risk. Documents containing sufficient information from the following list shall be included in the validation process to demonstrate that the safety-related parts perform the specified safety functions to the required performance level or levels and category or categories:

a) specification of the required characteristics of each safety function, and its required category and performance level;

b) drawings and specifications, e.g. for mechanical, hydraulic and pneumatic parts, printed circuit boards, assembled boards, internal wiring, enclosure, materials, mounting;

c) block diagram(s) with a functional description of the blocks;

d) circuit diagram(s), including interfaces/connections;

e) functional description of the circuit diagram(s);

f) time sequence diagram(s) for switching components, signals relevant for safety;

g) description of the relevant characteristics of components previously validated;

h) for safety-related parts other than those listed in g), component lists with item designations, rated values, tolerances, relevant operating stresses, type designation, failure-rate data and component manufacturer, and any other data relevant to safety;

i) analysis of all relevant faults (see also 4.3 and 4.4), such as those listed in the tables of Annexes A to D, including the justification of any excluded faults;

j) an analysis of the influence of processed materials;

k) information for use, e.g. installation and operation manual/instruction handbook.

Where software is relevant to the safety function(s), the software documentation shall include

— a specification which is clear and unambiguous and which states the safety performance the software is required to achieve,

— evidence that the software is designed to achieve the required performance level (see 9.5), and

— details of tests (in particular test reports) carried out to prove that the required safety performance is achieved.

NOTE See ISO 13849-1:2006, 4.6.2 and 4.6.3, for requirements.

Information is required on how the performance level and average probability of a dangerous failure per hour is determined. The documentation of the quantifiable aspects shall include

— the safety-related block diagram (see ISO 13849-1:2006, Annex B) or designated architecture (see ISO 13849-1:2006, 6.2),

— the determination of $MTTF_d$, DC_{avg} and CCF, and

— the determination of the category (see Table 2).

Information is required for documentation on systematic aspects of the SRP/CS.

Information is required as to how the combination of several SRP/CS achieves a performance level in accordance with the performance level required.

Table 2 — Documentation requirements for categories in respect of performance levels

Documentation requirement	Category for which documentation is required				
	B	1	2	3	4
Basic safety principles	X	X	X	X	X
Expected operating stresses	X	X	X	X	X
Influences of processed material	X	X	X	X	X
Performance during other relevant external influences	X	X	X	X	X
Well-tried components	—	X	—	—	—
Well-tried safety principles	—	X	X	X	X

Table 2 *(continued)*

Documentation requirement	Category for which documentation is required				
	B	1	2	3	4
Mean time to dangerous failure ($MTTF_d$) of each channel	X	X	X	X	X
The check procedure of the safety function(s)	—	—	X	—	—
Diagnostic measures performed, including fault reaction	—	—	X	X	X
Checking intervals, when specified	—	—	X	X	X
Diagnostic coverage (DC_{avg})	—	—	X	X	X
Foreseeable single faults considered in the design and the detection method used	—	—	X	X	X
Common-cause failures (CCF) identified and how to prevent them	—	—	X	X	X
Foreseeable single faults excluded	—	—	—	X	X
Faults to be detected	—	—	X	X	X
How the safety function is maintained in the case of each of the faults	—	—	—	X	X
How the safety function is maintained for each of the combinations of faults	—	—	—	—	X
Measures against systematic faults	X	X	X	X	X
Measures against software faults	X	—	X	X	X
X documentation required — documentation not required					
NOTE The categories are those given in ISO 13849-1:2006.					

4.6 Validation record

Validation by analysis and testing shall be recorded. The record shall demonstrate the validation process for each of the safety requirements. Cross-reference may be made to previous validation records, provided they are properly identified.

For any safety-related part which has failed an element of the validation process, the validation record shall describe which elements in the validation analysis/testing have been failed. It shall be ensured that all safety-related parts are successfully re-validated after modification.

5 Validation by analysis

5.1 General

Validation of the SRP/CS shall be carried out by analysis. Inputs to the analysis include the following:

— the safety function(s), their characteristics and the required performance level(s) identified during the risk analysis (see ISO 13849-1:2006, Figures 1 and 3);

— the quantifiable aspects ($MTTF_d$, DC_{avg} and CCF);

— the system structure (e.g. designated architectures) (see ISO 13849-1:2006, Clause 6);

— the non-quantifiable, qualitative aspects which affect system behaviour (if applicable, software aspects);

— deterministic arguments.

Validation of the safety functions by analysis rather than testing requires the formulation of deterministic arguments.

NOTE 1 A deterministic argument is an argument based on qualitative aspects (e.g. quality of manufacture, experience of use). This consideration depends on the application, which, together with other factors, can affect the deterministic arguments.

NOTE 2 Deterministic arguments differ from other evidence in that they show that the required properties of the system follow logically from a model of the system. Such arguments can be constructed on the basis of simple, well-understood concepts.

5.2 Analysis techniques

The selection of an analysis technique depends upon the particular object. Two basic techniques exist, as follows.

a) Top-down (deductive) techniques are suitable for determining the initiating events that can lead to identified top events, and calculating the probability of top events from the probability of the initiating events. They can also be used to investigate the consequences of identified multiple faults.

   EXAMPLE Fault tree analysis (FTA, see IEC 61025), event tree analysis (ETA).

b) Bottom-up (inductive) techniques are suitable for investigating the consequence of identified single faults.

   EXAMPLE Failure modes and effects analysis (FMEA, see IEC 60812) and failure modes, effects and criticality analysis (FMECA).

6 Validation by testing

6.1 General

When validation by analysis is not conclusive, testing shall be carried out to complete the validation. Testing is always complementary to analysis and is often necessary.

Validation tests shall be planned and implemented in a logical manner. In particular:

a) a test plan shall be produced before testing begins that shall include

   1) the test specifications,

   2) the required outcome of the tests for compliance, and

   3) the chronology of the tests;

b) test records shall be produced that include

   1) the name of the person carrying out the test,

   2) the environmental conditions (see Clause 10),

   3) the test procedures and equipment used,

   4) the date of the test, and

   5) the results of the test;

c) the test records shall be compared with the test plan to ensure that the specified functional and performance targets are achieved.

The test sample shall be operated as near as possible to its final operating configuration, i.e. with all peripheral devices and covers attached.

This testing may be applied manually or automatically, e.g. by computer.

Where applied, validation of the safety functions by testing shall be carried out by applying input signals, in various combinations, to the SRP/CS. The resultant response at the outputs shall be compared to the appropriate specified outputs.

It is recommended that the combination of these input signals be applied systematically to the control system and the machine. An example of this logic is power-on, start-up, operation, directional changes, restart-up. Where necessary, an expanded range of input data shall be applied to take into account anomalous or unusual situations, in order to see how the SRP/CS responds. Such combinations of input data shall take into account foreseeable incorrect operation(s).

The objectives of the test will determine the environmental condition for that test, which can be one or another of the following:

— the environmental conditions of intended use;

— the conditions at a particular rating;

— a given range of conditions if drift is expected.

The range of conditions which is considered stable and over which the tests are valid should be agreed between the designer and the person(s) responsible for carrying out the tests and should be recorded.

6.2 Measurement accuracy

The accuracy of measurements during the validation by testing shall be appropriate for the test carried out. In general, these measurement accuracies shall be within 5 K for temperature measurements and 5 % for the following:

a) time measurements;

b) pressure measurements;

c) force measurements;

d) electrical measurements;

e) relative humidity measurements;

f) linear measurements.

Deviations from these measurement accuracies shall be justified.

6.3 More stringent requirements

If, according to its accompanying documentation, the requirements for the SRP/CS exceed those within this part of ISO 13849, the more stringent requirements shall apply.

NOTE More stringent requirements can apply if the control system has to withstand particularly adverse service conditions, e.g. rough handling, humidity effects, hydrolysation, ambient temperature variations, effects of chemical agents, corrosion, high strength of electromagnetic fields — for example, due to close proximity of transmitters.

6.4 Number of test samples

Unless otherwise specified, the tests shall be made on a single production sample of the safety-related part being tested.

Safety-related part(s) under test shall not be modified during the course of the tests.

Certain tests can permanently change the performance of some components. Where a permanent change in a component causes the safety-related part to be incapable of meeting the requirements of further tests, a new sample or samples shall be used for subsequent tests.

Where a particular test is destructive and equivalent results can be obtained by testing part of the SRP/CS in isolation, a sample of that safety-related part may be used instead of the whole safety-related part(s) for the purpose of obtaining the results of the test. This approach shall only be applied where it has been shown by analysis that testing of a safety-related part(s) is sufficient to demonstrate the safety performance of the whole safety-related part that performs the safety function.

7 Validation of safety requirements specification for safety functions

Prior to the validation of the design of the SRP/CS, or the combination of SRP/CS providing the safety function, the requirements specification for the safety function shall be verified to ensure consistency and completeness for its intended use.

The safety requirements specification should be analysed before starting the design, since every other activity is based on these requirements.

It shall be ensured that requirements for all safety functions of the machine control system are documented.

In order to validate the specification, appropriate measures to detect systematic faults (errors, omissions or inconsistencies) shall be applied.

Validation may be performed by reviews and inspections of the SRP/CS safety requirements and design specification(s), in particular to prove that all aspects of

— the intended application requirements and safety needs, and

— the operational and environmental conditions and possible human errors (e.g. misuse)

have been considered.

Where a product standard specifies the safety requirements for the design of a SRP/CS (e.g. ISO 11161 for integrated manufacturing systems or ISO 13851 for two-hand control devices), these shall be taken into account.

8 Validation of safety functions

The validation of safety functions shall demonstrate that the SRP/CS, or combination of SRP/CSs, provides the safety function(s) in accordance with their specified characteristics.

NOTE 1 A loss of the safety function in the absence of a hardware fault is due to a systematic fault, which can be caused by errors made during the design and integration stages (a misinterpretation of the safety function characteristics, an error in the logic design, an error in hardware assembly, an error in typing the code of software, etc.). Some of these systematic faults will be revealed during the design process, while others will be revealed during the validation process or will remain unnoticed. In addition, it is also possible for an error to be made (e.g. failure to check a characteristic) during the validation process.

Validation of the specified characteristics of the safety functions shall be achieved by the application of appropriate measures from the following list.

— Functional analysis of schematics, reviews of the software (see 9.5).

NOTE 2 Where a machine has complex or a large number of safety functions, an analysis can reduce the number of functional tests required.

— Simulation.

— Check of the hardware components installed in the machine and details of the associated software to confirm their correspondence with the documentation (e.g. manufacture, type, version).