

BS EN ISO 13849-2:2012



BSI Standards Publication

Safety of machinery — Safety-related parts of control systems

Part 2: Validation

bsi.

...making excellence a habit.
AVA Documents
Document Sharing Hub

National foreword

This British Standard is the UK implementation of EN ISO 13849-2:2012. It supersedes BS EN ISO 13849-2:2008 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee MCE/3, Safeguarding of machinery.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012. Published by BSI Standards Limited 2012

ISBN 978 0 580 66820 3

ICS 13.110; 29.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2012.

Amendments issued since publication

Date	Text affected
------	---------------

English Version

Safety of machinery - Safety-related parts of control systems -
Part 2: Validation (ISO 13849-2:2012)

Sécurité des machines - Parties des systèmes de
commande relatives à la sécurité - Partie 2: Validation (ISO
13849-2:2012)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von
Steuerungen - Teil 2: Validierung (ISO 13849-2:2012)

This European Standard was approved by CEN on 14 October 2012.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

This document (EN ISO 13849-2:2012) has been prepared by Technical Committee ISO/TC 199 “Safety of machinery” in collaboration with Technical Committee CEN/TC 114 “Safety of machinery” the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2013, and conflicting national standards shall be withdrawn at the latest by April 2013.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 13849-2:2008.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive.

For relationship with EU Directive, see informative Annex ZA, which is an integral part of this document.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 13849-2:2012 has been approved by CEN as a EN ISO 13849-2:2012 without any modification.

Annex ZA
(informative)
**Relationship between this European Standard and the Essential
Requirements of EU Directive 2006/42/EC**

This European Standard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association to provide a means of conforming to Essential Requirements of the New Approach Directive Machinery, 2006/42/EC.

Once this standard is cited in the Official Journal of the European Union under that Directive and has been implemented as a national standard in at least one Member State, compliance with the normative clauses of this standard confers, within the limits of the scope of this standard, a presumption of conformity with the relevant Essential Requirements 1.2.1 of that Directive and associated EFTA regulations.

WARNING — Other requirements and other EU Directives may be applicable to the product(s) falling within the scope of this standard.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Validation process	1
4.1 Validation principles	1
4.2 Validation plan	3
4.3 Generic fault lists	4
4.4 Specific fault lists	4
4.5 Information for validation	4
4.6 Validation record	6
5 Validation by analysis	6
5.1 General	6
5.2 Analysis techniques	7
6 Validation by testing	7
6.1 General	7
6.2 Measurement accuracy	8
6.3 More stringent requirements	8
6.4 Number of test samples	8
7 Validation of safety requirements specification for safety functions	9
8 Validation of safety functions	9
9 Validation of performance levels and categories	10
9.1 Analysis and testing	10
9.2 Validation of category specifications	10
9.3 Validation of MTTF _d , DC _{avg} and CCF	12
9.4 Validation of measures against systematic failures related to performance level and category of SRP/CS	13
9.5 Validation of safety-related software	13
9.6 Validation and verification of performance level	14
9.7 Validation of combination of safety-related parts	14
10 Validation of environmental requirements	15
11 Validation of maintenance requirements	15
12 Validation of technical documentation and information for use	16
Annex A (informative) Validation tools for mechanical systems	17
Annex B (informative) Validation tools for pneumatic systems	21
Annex C (informative) Validation tools for hydraulic systems	31
Annex D (informative) Validation tools for electrical systems	40
Annex E (informative) Example of validation of fault behaviour and diagnostic means	53
Bibliography	78

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.

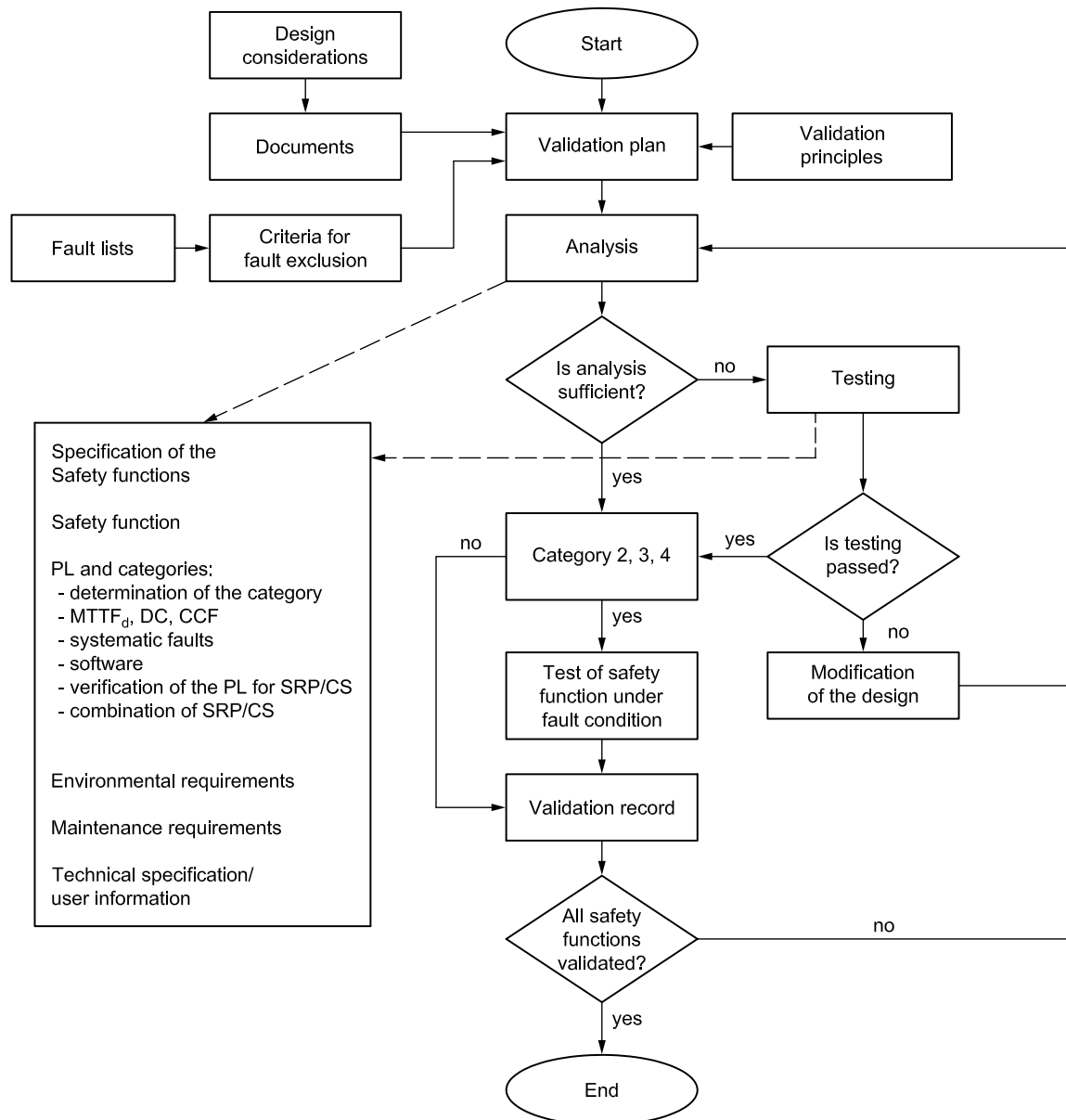


Figure 1 — Overview of the validation process

“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

- the identity of the specification documents,
- 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, hydrolysis, 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).

- Functional testing of the safety functions in all operating modes of the machine, to establish whether they meet the specified characteristics (see ISO 13849-1:2006, Clause 5, for specifications of some typical safety functions). The functional tests shall ensure that all safety-related outputs are realized over their complete ranges and respond to safety-related input signals in accordance with the specification. The test cases are normally derived from the specifications but could also include some cases derived from analysis of the schematics or software.
- Extended functional testing to check foreseeable abnormal signals or combinations of signals from any input source, including power interruption and restoration, and incorrect operations.
- Check of the operator–SRP/CS interface for the meeting of ergonomic principles (see ISO 13849-1:2006, 4.8).

NOTE 3 Other measures against systematic failures mentioned in 9.4 (e.g. diversity, failure detection by automatic tests) can also contribute in the detection of functional faults.

9 Validation of performance levels and categories

9.1 Analysis and testing

For the SRP/CS or combination of SRP/CSs that provides the safety function(s), validation shall demonstrate that the required performance levels (PL_r) and categories in the safety requirements specification are fulfilled. Principally, this will require failure analysis using circuit diagrams (see Clause 5) and, where the failure analysis is inconclusive:

- fault injection tests on the actual circuit and fault initiation on actual components, particularly in parts of the system where there is doubt regarding the results obtained from failure analysis (see Clause 6);
- a simulation of control system behaviour in the event of a fault, e.g. by means of hardware and/or software models.

In some applications it may be necessary to divide the connected safety-related parts into several functional groups and to subject these groups and their interfaces to fault simulation tests.

When validating by testing, the tests should include, as appropriate,

- fault injection tests into a production sample,
- fault injection tests into a hardware model,
- software simulation of faults, and
- subsystem failure, e.g. power supplies.

The precise instant at which a fault is injected into a system can be critical. The worst-case effect of a fault injection shall be determined by analysis and by injecting the fault at this appropriate critical time.

9.2 Validation of category specifications

9.2.1 Category B

SRP/CSs to Category B shall be validated in accordance with basic safety principles (see Tables A.1, B.1, C.1 and D.1) by demonstrating that the specification, design, construction and choice of components are in accordance with ISO 13849-1:2006, 6.2.3. The $MTTF_d$ of the channel shall be demonstrated to be at least 3 years. This shall be achieved by checking that the SRP/CS is in accordance with its specification as provided in the documents for validation (see 4.5). For the validation of environmental conditions, see 6.1.

NOTE In particular cases, higher values of $MTTF_d$ can be required — for example, when $PL_r = b$.

9.2.2 Category 1

SRP/CSs to Category 1 shall be validated by demonstrating the following:

- a) they meet the requirements of Category B;
- b) components are well-tried (see Tables A.3 and D.3), meeting at least one of the following conditions:
 - 1) they have been widely used in the past with successful results in similar applications;
 - 2) they have been made and verified using principles which demonstrate their suitability and reliability for safety-related applications;
- c) well-tried safety principles (where applicable, see Tables A.2, B.2, C.2 and D.2) have been implemented correctly, and, where newly developed principles have been used, validation has been made of
 - 1) how the expected modes of failure have been avoided, and
 - 2) how faults have been avoided or their probability reduced to a suitable level.

Relevant component standards may be used to demonstrate compliance with this subclause (see Tables A.3 and D.3). The $MTTF_d$ of the channel shall be demonstrated to be at least 30 years.

9.2.3 Category 2

SRP/CSs to Category 2 shall be validated by demonstrating the following:

- a) they meet the requirements of Category B;
 - b) the well-tried safety principles used (if applicable) are in accordance with 9.2.2 c);
 - c) the checking equipment detects all relevant faults applied, one at a time, during the checking process and generates an appropriate control action which
 - 1) initiates a safe state or, when this is not possible,
 - 2) provides a warning of the hazard;
 - d) the check(s) provided by the checking equipment do not introduce an unsafe state;
 - e) the initiation of the check is carried out
 - 1) at the machine start-up and prior to the initiation of a hazardous situation, and
 - 2) periodically, during operation in accordance with the design specification and if the risk assessment and kind of operations show that it is necessary;
- NOTE 1 The need for, and extent of, checks during operation are determined by the designer's risk assessment and the kind of operation necessary.
- f) the $MTTF_d$ of the functional channel ($MTTF_{d,L}$) is at least 3 years;
 - g) the $MTTF_{d,TE}$ is larger than half of $MTTF_{d,L}$;
 - h) the test rate $\geq 100 \times$ expected demand rate;
 - i) the DC_{avg} is at least 60 %;
 - j) common-cause failures are sufficiently reduced (see ISO 13849-1:2006, Annex F).

NOTE 2 In particular cases, higher values of $MTTF_d$ and/or DC_{avg} can be required — for example, owing to high PL_r .

9.2.4 Category 3

SRP/CSs to Category 3 shall be validated by demonstrating the following:

- a) they meet the requirements of Category B;
- b) the well-tried safety principles (if applicable) meet the requirements of 9.2.2 c);
- c) a single fault does not lead to the loss of the safety function;
- d) single faults (including common cause faults) are detected in accordance with the design rationale and the technology applied;
- e) the $MTTF_d$ of each channel is at least 3 years;
- f) the DC_{avg} is at least 60 %;
- g) common-cause failures are sufficiently reduced (see ISO 13849-1:2006, Annex F).

NOTE In particular cases, higher values of $MTTF_d$ and/or DC_{avg} can be required — for example, due to high PL_r .

9.2.5 Category 4

SRP/CSs to Category 4 shall be validated by demonstrating the following:

- a) they meet the requirements of Category B;
- b) the well-tried safety principles (if applicable) are in accordance with 9.2.2 c);
- c) a single fault (including common-mode faults) does not lead to the loss of the safety function;
- d) single faults are detected at or before the next demand on the safety function, this being achieved with a DC_{avg} of at least 99 %;
- e) if a single fault is not detected with a DC_{avg} of at least 99 %, an accumulation of faults does not lead to the loss of the safety function(s), and the extent of the accumulation of faults considered is in accordance with the design rationale;
- f) the $MTTF_d$ of each channel is at least 30 years;
- g) common-cause failures are sufficiently reduced (see ISO 13849-1:2006, Annex F).

9.3 Validation of $MTTF_d$, DC_{avg} and CCF

The validation of $MTTF_d$, DC_{avg} and CCF is typically performed by analysis and visual inspection.

The $MTTF_d$ values for components (including B_{10d} , T_{10d} and n_{op} values) shall be checked for plausibility (e.g. against ISO 13849-1:2006, Annex C). For example, the value given on the supplier datasheet is to be compared with ISO 13849-1:2006, Annex C. Where fault exclusion claims mean that particular components do not contribute to the channel $MTTF_d$, the plausibility of the fault exclusion shall be checked.

NOTE 1 A fault exclusion implies infinite $MTTF_d$; therefore, the component will not contribute to the calculation of channel $MTTF_d$.

NOTE 2 For the determination of the B_{10d} value, see e.g. IEC 60947-4-1:2010, Annex K.

The $MTTF_d$ of each channel of the SRP/CS, including application of the symmetrisation formula (see ISO 13849-1:2006, Annex D) to dissimilar redundant channels, shall be checked for correct calculation. It shall be ensured that the $MTTF_d$ of individual channels has been restricted to no greater than 100 years before the symmetrisation formula is applied.

The DC values for components and/or logic blocks shall be checked for plausibility (e.g. against measures in ISO 13849-1:2006, Annex E). The correct implementation (hardware and software) of

checks and diagnostics, including appropriate fault reaction, shall be validated by testing under typical environmental conditions in use.

The DC_{avg} of the SRP/CS shall be checked for correct calculation.

The correct implementation of sufficient measures against common-cause failures shall be validated (e.g. against ISO 13849-1:2006, Annex F). Typical validation measures are static hardware analysis and functional testing under environmental conditions.

NOTE 3 For the calculation of the $MTTF_d$ values of electronic components, an ambient temperature of +40 °C is taken as a basis. During validation, it is important to ensure that, for $MTTF_d$ values, the environmental and functional conditions (in particular temperature) taken as basis are met. Where a device, or component, is operated significantly above (e.g. more than 15 °C) the specified temperature of +40 °C, it will be necessary to use $MTTF_d$ values for the increased ambient temperature.

9.4 Validation of measures against systematic failures related to performance level and category of SRP/CS

The validation of measures against systematic failures (defined in ISO 13849-1:2006, 3.1.7) related to performance levels and categories of each SRP/CS can typically be provided by

- a) inspections of design documents which confirm the application of
 - 1) basic and well-tried safety principles (see Annexes A to D),
 - 2) further measures for avoidance of systematic failures (see ISO 13849-1:2006, G.3), and
 - 3) further measures for the control of systematic failures such as hardware diversity (see ISO 13849-1:2006, Annex G), modification protection or failure assertion programming;
- b) failure analysis (e.g. FMEA);
- c) fault injection tests/fault initiation;
- d) inspection and testing of data communication, where used;
- e) checking that a quality management system avoids the causes of systematic failures in the manufacturing process.

9.5 Validation of safety-related software

The validation of both safety-related embedded software (SRESW) and safety-related application software (SRASW) shall include

- the specified functional behaviour and performance criteria (e.g. timing performance) of the software when executed on the target hardware,
- verification that the software measures are sufficient for the specified PL_r of the safety function, and
- measures and activities taken during software development to avoid systematic software faults.

As a first step, check that there is documentation for the specification and design of the safety-related software. This documentation shall be reviewed for completeness and absence of erroneous interpretations, omissions or inconsistencies.

NOTE In the case of small programs, an analysis of the program by means of reviews or walk-through of control flow, procedures, etc. using the software documentation (control flow chart, source code of modules or blocks, I/O and variable allocation lists, cross-reference lists) can be sufficient.

In general, software can be considered a “black box” or “grey box” (see ISO 13849-1:2006, 4.6.2), and validated by the black- or grey-box test, respectively.

Depending on the PL_r [ISO 13849-1:2006, 4.6.2 (for SRESW) and 4.6.3 (for SRASW)], the tests should include

- black-box testing of functional behaviour and performance (e.g. timing performance),
- additional extended test cases based upon limit value analyses, recommended for PL d or e,
- I/O tests to ensure that the safety-related input and output signals are used properly, and
- test cases which simulate faults determined analytically beforehand, together with the expected response, in order to evaluate the adequacy of the software-based measures for control of failures.

Individual software functions which have already been validated do not need to be validated again. Where a number of such safety function blocks are combined for a specific project, however, the resulting total safety function shall be validated.

Software documentation shall be checked to confirm that sufficient measures and activities have been implemented against systematic software faults in accordance with the simplified V-model (ISO 13849-1:2006, Figure 6).

The measures for software implementation according to ISO 13849-1:2006, 4.6.2 (for SRESW) and 4.6.3 (for SRASW), which depend on the PL to be attained, shall be examined with regard to their proper implementation.

Should the safety-related software be subsequently modified, it shall be revalidated on an appropriate scale.

9.6 Validation and verification of performance level

For the simplified procedure for estimating PL of the SRP/CS according to ISO 13849-1:2006, 4.5.4, and ISO 13849-1:2006, Annexes B to F and Annex K, the following verification and validation steps shall be performed:

- checking for correct evaluation of PL based on the category, DC_{avg} and $MTTF_d$ (according to ISO 13849-1:2006, 4.5.4 and Annex K);
- verification that the PL achieved by the SRP/CS satisfies the required performance level PL_r in the safety requirements specification for the machinery: $PL \geq PL_r$.

Where other methods are used to evaluate the achieved PL, based on the estimated average probability of a dangerous failure per hour, validation shall consider

- the $MTTF_d$ value for each component,
- the DC,
- the CCF,
- the structure, and
- the documentation, application and calculation, which shall be checked for correctness.

9.7 Validation of combination of safety-related parts

Where the safety function is implemented by two or more safety-related parts, validation of the combination — by analysis and, if necessary, by testing — shall be undertaken to establish that the combination achieves the performance level specified in the design. Existing recorded validation results of safety-related parts can be taken into account. The following validation steps shall be performed:

- inspection of design documents describing the overall safety function(s);
- a check that the overall PL of the SRP/CS combination has been correctly evaluated, based on the PL of each individual safety-related part (according to ISO 13849-1:2006, 6.3);

NOTE A summation of the average probability of dangerous failures per hour of all combined SRP/CS can be used as an alternative to ISO 13849-1:2006, Table 11. It is important to check the non-quantifiable restrictions of systematic, architectural and CCF aspects which can limit the overall performance level to lower values.

- consideration of the characteristics of the interfaces, e.g. voltage, current, pressure, data format of information, signal level;
- failure analysis relating to combination/integration, e.g. by FMEA;
- for redundant systems, fault injection tests relating to combination/integration.

10 Validation of environmental requirements

The performance specified in the design of the SRP/CS shall be validated with respect to the environmental conditions specified for the control system.

Validation shall be carried out by analysis and, if necessary, by testing. The extent of the analysis and of the testing will depend upon the safety-related parts, the system in which they are installed, the technology used, and the environmental condition(s) being validated. The use of operational reliability data on the system or its components, or the confirmation of compliance to appropriate environmental standards (e.g. for waterproofing, vibration protection) can assist this validation process.

Where applicable, validation shall address

- expected mechanical stresses from shock, vibration, ingress of contaminants,
- mechanical durability,
- electrical ratings and power supplies,
- climatic conditions (temperature and humidity), and
- electromagnetic compatibility (immunity).

When testing is needed to determine compliance with the environmental requirements, the procedures outlined in the relevant standards shall be followed as far as required for the application.

After the completion of validation by testing, the safety functions shall continue to be in accordance with the specifications for the safety requirements, or the SRP/CS shall provide output(s) for a safe state.

11 Validation of maintenance requirements

The validation process shall demonstrate that the provisions for maintenance requirements specified in ISO 13849-1:2006, Clause 9, Paragraph 2, have been implemented.

Validation of maintenance requirements shall include the following, as applicable:

- a) a review of the information for use confirming that
 - 1) maintenance instructions are complete [including procedures, required tools, frequency of inspections, time interval for changing components subjected to wear (T_{10d}) etc.] and understandable,
 - 2) if appropriate, there are provisions for the maintenance to be performed only by skilled maintenance personnel;
- b) a check that measures for ease of maintainability (e.g. provision of diagnostic tools to aid fault-finding and repair) have been applied.

In addition, the following measures shall be included when applied:

- measures against mistakes during maintenance (e.g. detection of wrong input data via plausibility checks);
- measures against modification (e.g. password protection to prevent access to the program by unauthorized persons).

12 Validation of technical documentation and information for use

The validation process shall demonstrate that the requirements for technical documentation specified in ISO 13849-1:2006, Clause 10, and for information for use specified in ISO 13849-1:2006, Clause 11, have been implemented.

Annex A (informative)

Validation tools for mechanical systems

When mechanical systems are used in conjunction with other technologies, Annex A should also be taken into account.

Tables A.1 and A.2 list basic and well-tried safety principles.

Table A.3 lists well-tried components for a safety-related application based on the application of well-tried safety principles and/or a standard for their particular applications. A well-tried component for some applications could be inappropriate for others.

Tables A.4 and A.5 list fault exclusions and their rationale. For further exclusions, see 4.4.

The precise instant at which the fault occurs can be critical (see 9.1).

Table A.1 — Basic safety principles

Basic safety principle	Remarks
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature.
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, sticking, manufacturing.
Proper selection, combination, arrangements, assembly and installation of components/system	Apply manufacturer's application notes, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components/systems.
Use of de-energization principle	The safe state is obtained by a release of energy. See primary action for stopping in ISO 12100:2010, 6.2.11.3. Energy is supplied for starting the movement of a mechanism. See primary action for starting in ISO 12100:2010, 6.2.11.3. Consider different modes, e.g. operation mode, maintenance mode. IMPORTANT — This principle is not to be followed when loss of energy would create a hazard, e.g. release of workpiece caused by loss of clamping force.
Proper fastening	For the application of screw locking, consider manufacturer's application notes. Overloading can be avoided and adequate resistance to release can be achieved by applying adequate torque loading technology.
Limitation of the generation and/or transmission of force and similar parameters	Examples are break pin, break plate, and torque-limiting clutch. IMPORTANT — This principle is not to be followed when the continued integrity of components is essential to maintain the required level of control.
Limitation of range of environmental parameters	Examples are temperature, humidity and pollution at the installation place. See Clause 10 and consider manufacturer's application notes.

Table A.1 (continued)

Basic safety principle	Remarks
Limitation of speed and similar parameters	Consider, e.g. the speed, acceleration, deceleration required by the application.
Proper reaction time	Consider, e.g. spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.
Protection against unexpected start-up	Consider unexpected start-up caused by stored energy and after power supply restoration for different modes (operation mode, maintenance mode, etc.). Special equipment for release of stored energy can be necessary. Special applications, e.g. to keep energy for clamping devices or ensure a position, need to be considered separately.
Simplification	Avoid unnecessary components in the safety-related system.
Separation	Separation of safety-related functions from other functions.
Proper lubrication	Consider the need for lubrication devices, information on lubricants and lubrication intervals.
Proper prevention of the ingress of fluids and dust	Consider IP rating (see IEC 60529).

Table A.2 — Well-trying safety principles

Well-trying safety principle	Remarks
Use of carefully selected materials and manufacturing	Selection of suitable material, adequate manufacturing methods and treatments related to the application.
Use of components with oriented failure mode	The predominant failure mode of a component is known in advance and is always the same. See ISO 12100:2010, 6.2.12.3.
Overdimensioning/safety factor	Safety factors are as given in standards or by good experience in safety-related applications.
Safe position	The moving part of the component is held in a safe position, by mechanical means (friction alone is not sufficient). Force is required to move from the safe position.
Increased OFF force	A safe position/state is obtained by an increased OFF force in relation to the ON force.
Careful selection, combination, arrangement, assembly and installation of components/system related to the application	—
Careful selection of fastening related to the application	Avoid relying only on friction.
Positive mechanical action	To achieve positive mechanical action, all moving mechanical components required to perform the safety function shall inevitably move connected components, e.g. a cam directly opens the contacts of an electrical switch rather than relying on a spring. See ISO 12100:2010, 6.2.5.
Multiple parts	Reducing the effect of faults by providing multiple parts acting in parallel, e.g. where a failure of one of several springs does not lead to a dangerous condition.