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)

COPYRIGHT PROTECTED DOCUMENT

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.

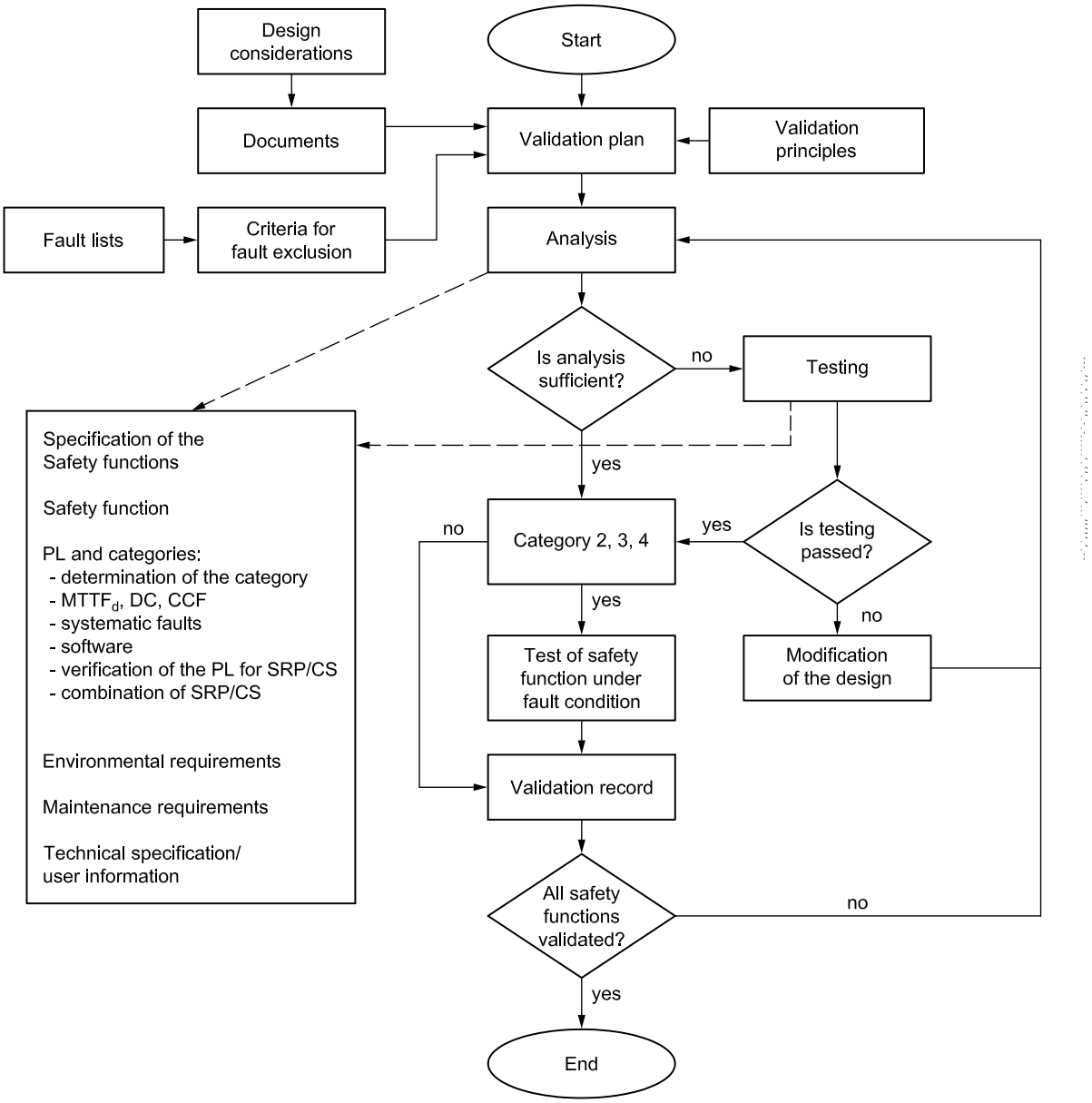


Figure 1 — Overview of the validation process

"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).

— 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 ≥ 100 × 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-tried safety principles

Well-tried 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.

Table A.2 *(continued)*

Well-tried safety principle	Remarks
Use of well-tried spring (see also Table A.3)	A well-tried spring requires — use of carefully selected materials, manufacturing methods (e.g. pre-setting and cycling before use) and treatments (e.g. rolling and shot-peening), — sufficient guidance of the spring, and — sufficient safety factor for fatigue stress (i.e. with a high probability that a fracture will not occur). Well-tried compression coil springs may also be designed, by — use of carefully selected materials, manufacturing methods (e.g. pre-setting and cycling before use) and treatments (e.g. rolling and shot-peening), — sufficient guidance of the spring, — clearance between the turns less than the wire diameter when unloaded, and — sufficient force after a fracture(s) is maintained (i.e. a fracture(s) will not lead to a dangerous condition). NOTE Compression springs are preferred.
Limited range of force and similar parameters	Determine the necessary limitation in relation to the experience and application. 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 maintaining the required level of control.**
Limited range of speed and similar parameters	Determine the necessary limitation in relation to the experience and application. Examples are centrifugal governor, safe monitoring of speed, and limited displacement.
Limited range of environmental parameters	Determine the necessary limitations. Examples are temperature, humidity, pollution at the installation. See Clause 10 and consider manufacturer's application notes.
Limited range of reaction time, limited hysteresis	Determine the necessary limitations. Consider, e.g. spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.

Table A.3 — Well-tried components

Well-tried component	Conditions for "well-tried"	Standard or specification
Screw	All factors influencing the screw connection and the application are to be considered. See Table A.2.	Mechanical jointing such as screws, nuts, washers, rivets, pins, bolts, etc. is standardized.
Spring	See Table A.2, "Use of well-tried spring".	Technical specifications for spring steels and other special applications are given in ISO 4960.

Table A.3 *(continued)*

Well-tried component	Conditions for "well-tried"	Standard or specification
Cam	All factors influencing the cam arrangement (e.g. part of an interlocking device) are to be considered. See Table A.2.	See ISO 14119 (interlocking devices).
Break-pin	All factors influencing the application are to be considered. See Table A.2.	—

Table A.4 — Faults and fault exclusions — Mechanical devices, components and elements (e.g. cam, follower, chain, clutch, brake, shaft, screw, pin, guide, bearing)

Fault considered	Fault exclusion	Remarks
Wear/corrosion	Yes, in the case of carefully selected material, (over)dimensioning, manufacturing process, treatment and proper lubrication, according to the specified lifetime (see also Table A.2).	See ISO 13849-1:2006, 7.3.
Untightening/ loosening	Yes, in the case of carefully selected material, manufacturing process, locking means and treatment, according to the specified lifetime (see also Table A.2).	
Fracture	Yes, in the case of carefully selected material, (over)dimensioning, manufacturing process, treatment and proper lubrication, according to the specified lifetime (see also Table A.2).	
Deformation by overstressing	Yes, in the case of carefully selected material, (over)dimensioning, treatment and manufacturing process, according to specified lifetime (see also Table A.2).	
Stiffness/sticking	Yes, in the case of carefully selected material, (over) dimensioning, manufacturing process, treatment and proper lubrication, according to specified lifetime (see also Table A.2).	

Table A.5 — Faults and fault exclusions — Pressure-coil springs

Fault considered	Fault exclusion	Remarks
Wear/corrosion	Yes, in case of use of well-tried springs and carefully selected fastenings (see Table A.2).	See ISO 13849-1:2006, 7.3.
Force reduction by setting and fracture		
Fracture		
Stiffness/sticking		
Loosening		
Deformation by overstressing		

Annex B
(informative)

Validation tools for pneumatic systems

When pneumatic systems are used in conjunction with other technologies, Annex B should also be taken into account. Where pneumatic components are electrically connected/controlled, the appropriate fault lists in Annex D should be considered.

NOTE Additional requirements can exist in national legislation.

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

A list of well-tried components is not given in Annex B of this edition. The status of "well-tried" is mainly application-specific. Components can be described as "well-tried" if they are in accordance with ISO 13849-1:2006, 6.2.2 and ISO 4414:2010, Clauses 5 to 7. A well-tried component for some applications could be inappropriate for other applications.

Tables B.3 to B.18 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 B.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, and manufacturing.
Proper selection, combination, arrangement, 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 release of energy to all relevant devices. 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. This principle shall not be used in some applications, e.g. where the loss of pneumatic pressure will create an additional hazard.
Proper fastening	For the application of, e.g. screw locking, fittings, gluing or clamp ring, consider manufacturer's application notes. Overloading can be avoided by applying adequate torque loading technology.
Pressure limitation	Examples are pressure-relief valve, pressure-reducing/control valve.
Speed limitation/ speed reduction	An example is the speed limitation placed on a piston by a flow valve or throttle.
Sufficient avoidance of contamination of the fluid	Consider filtration and separation of solid particles and water in the fluid.

Table B.1 *(continued)*

Basic safety principle	Remarks
Proper range of switching time	Consider, e.g. the length of pipework, pressure, exhaust capacity, force, spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, and combination of tolerances.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g. temperature, humidity, vibration, pollution. See Clause 10 and consider manufacturer's specification/application notes.
Protection against unexpected start-up	Consider unexpected start-up caused by stored energy and after power supply restoration for different modes, e.g. operation mode, maintenance mode. Special equipment for the release of stored energy can be necessary (see ISO 14118:2000, 5.3.1.3). 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.
Proper temperature range	To be considered throughout the whole system.
Separation	Separation of the safety-related functions from other functions (e.g. logical separation).

Table B.2 — Well-tried safety principles

Well-tried safety principle	Remarks
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 one of the possible positions by mechanical means (friction only is not enough). Force is needed to change the position.
Increased OFF force	One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to ON position (a safety factor).
Valve closed by load pressure	These are generally seat valves, e.g. poppet valves, ball valves. Consider how to apply the load pressure in order to keep the valve closed even if, for example, the spring closing the valve breaks.
Positive mechanical action	The positive mechanical action is used for moving parts inside pneumatic components. See also Table A.2.
Multiple parts	See Table A.2.
Use of well-tried spring	See Table A.2.
Speed limitation/speed reduction by resistance to defined flow	Examples are fixed orifices and fixed throttles.
Force limitation/force reduction	This can be achieved by a well-tried pressure relief valve which is, e.g. equipped with a well-tried spring, correctly dimensioned and selected.
Appropriate range of working conditions	The limitation of working conditions, e.g. pressure range, flow rate and temperature range, should be considered.
Proper avoidance of contamination of the fluid	Consider the need for a high degree of filtration and separation of solid particles and water in the fluid.

Table B.2 *(continued)*

Well-tried safety principle	Remarks
Sufficient positive overlapping in spool valves	The positive overlapping ensures the stopping function and prevents movements that are not allowed.
Limited hysteresis	For example, increased friction or a combination of tolerances will increase the hysteresis.

Table B.3 — Faults and fault exclusions — Directional control valves

Fault considered	Fault exclusion	Remarks
Change of switching times	Yes, in the case of positive mechanical action (see Table A.2) of the moving components, as long as the actuating force is sufficiently large.	—
Non-switching (sticking at the end or zero position) or incomplete switching (sticking at a random intermediate position)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components, as long as the actuating force is sufficiently large.	
Spontaneous change of the initial switching position (without an input signal)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components, as long as the holding force is sufficiently large, or if well-tried springs are used (see Table A.2) and normal installation and operating conditions apply (see remark), or in the case of spool valves with elastic sealing and if normal installation and operating conditions apply (see remark).	Normal installation and operating conditions apply when — the conditions laid down by the manufacturer have been taken into account, — the weight of the moving component is not acting unfavourably in terms of safety (e.g. horizontal installation), — there are no inertia forces acting adversely on moving components (e.g. direction of valve component motion takes into account magnitude and direction of inertia forces), and — no extreme vibration and shock stresses occur.
Leakage	Yes, in the case of spool-type valves with elastic seal, in so far as a sufficient positive overlap is present [see remark 1)], normal conditions of operation apply, and an adequate treatment and filtration of the compressed air is provided; or, in the case of seat valves, if normal conditions of operation apply [see remark 2)], and adequate treatment and filtration of the compressed air is provided.	1) In the case of spool-type valves with elastic seal, the effects due to leakage can usually be excluded. However, a small amount of leakage can occur over a long period of time. 2) Normal conditions of operation apply when the conditions laid down by the manufacturer are taken into account.
If the control functions are realized by a number of single-function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.		

Table B.3 *(continued)*

Fault considered	Fault exclusion	Remarks
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	
For servo and proportional valves: pneumatic faults which cause uncontrolled behaviour	Yes, in the case of servo and proportional directional valves, if these can be assessed in terms of technical safety as conventional directional control valves, owing to their design and construction.	—
If the control functions are realized by a number of single-function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.		

Table B.4 — Faults and fault exclusions — Stop (shut-off) valves/non-return (check) valves/quick-action venting valves/shuttle valves, etc.

Fault considered	Fault exclusion	Remarks
Change of switching times	None.	—
Non-opening, incomplete opening, non-closure or incomplete closure (sticking at an end position or at an arbitrary intermediate position)	Yes, if the guidance system for the moving component(s) is designed in a manner similar to that for a non-controlled ball seat valve without a damping system (see remark) and if well-tried springs are used (see Table A.2).	For a non-controlled ball seat valve without a damping system, the guidance system is generally designed such that any sticking of the moving component is unlikely.
Spontaneous change of the initial switching position (without an input signal)	Yes, for normal installation and operating conditions (see remark) and if there is sufficient closing force on the basis of the pressures and areas provided.	Normal installation and operating conditions are met when — the conditions laid down by the manufacturer are being followed, — no special inertial forces affect the moving components, e.g. direction of motion takes into account the orientation of the moving machine parts, and — no extreme vibration or shock stresses occur.
For shuttle valves: simultaneous closing of both input connections	Yes, if, on the basis of the construction and design of the moving component, simultaneous closing is unlikely.	—
Leakage	Yes, if normal conditions of operation apply (see remark) and there is adequate treatment and filtration of the compressed air.	Normal conditions of operation apply when the conditions laid down by the manufacturer are taken into account.

Table B.4 *(continued)*

Fault considered	Fault exclusion	Remarks
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table B.5 — Faults and fault exclusions — Flow valves

Fault considered	Fault exclusion	Remarks
Change in flow rate without any change in setting device	Yes, for flow control valves without moving parts [see remark 1)], e.g. throttle valves, if normal operating conditions apply [see remark 2)], and adequate treatment and filtration of the compressed air is provided.	1) The setting device is not considered to be a moving part. Changes in flow rate due to changes in pressure differences are physically limited in this type of valve and are not covered by this assumed fault. 2) Normal operating conditions apply when the conditions laid down by the manufacturer are taken into account.
Change in the flow rate in the case of non-adjustable, circular orifices and nozzles	Yes, if the diameter is ≥ 0,8 mm, normal operating conditions apply [see remark 2)], and if adequate treatment and filtration of the compressed air is provided.	
For proportional flow valves: change in the flow rate due to an unintended change in the set value	None.	—
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case, based upon technical safety specification(s).	
Unintended loosening (unscrewing) of the operating element(s) of the setting device	Yes, if an effective positive locking device against loosening (unscrewing) is provided.	
Bursting of the valve housing or breakage of the moving component(s) as well as the breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table B.6 — Faults and fault exclusions — Pressure valves

Fault considered	Fault exclusion	Remarks
Non-opening or insufficient opening when exceeding the set pressure (sticking or sluggish movement of the moving component) [see remark 1)]	Yes, if — the guidance system for the moving component(s) is similar to the case of a non-controlled ball seat or membrane valve [see remark 2)], e.g. for a pressure-reducing valve with secondary pressure relief, and — the installed springs are well-tried springs (see Table A.2).	1) This fault applies only when the pressure valve(s) is used for forced actions, e.g. clamping. This fault does not apply to its normal function in the pneumatic systems, e.g. pressure limitation, pressure decrease. 2) For a non-controlled ball seat valve or for a membrane valve, the guidance system is generally designed such that any sticking of the moving component is unlikely.
Non-closing or insufficient closing if pressure drops below the set value (sticking or sluggish movement of the moving component) [see remark 1)]		
Change of the pressure control behaviour without changing the setting device [see remark 1)]	Yes, for directly actuated pressure-limiting valves and pressure-switching valves if the installed spring(s) are well-tried (see Table A.2).	
For proportional pressure valves: change in the pressure control behaviour due to unintended change in the set value [see remark 1)]	None.	
Spontaneous change in the setting device	Yes, where there is effective protection of the setting device within the requirements of the application, e.g. lead seals.	—
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Leakage	Yes, for seat valves, membrane valves and spool valves with elastic sealing in normal operating conditions (see remark) and if adequate treatment and filtration of the compressed air is provided.	Normal operating conditions are met when the conditions laid down by the manufacturer are followed.
Change of the leakage flow rate, over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table B.7 — Faults and fault exclusions — Pipework

Fault considered	Fault exclusion	Remarks
Bursting and leakage	Yes, if the dimensioning, choice of materials and fixing are in accordance with good engineering practice (see remark).	When using plastic pipes, it is necessary to consider the manufacturer's data, in particular with respect to operational environmental influences, e.g. thermal influences, chemical influences or influences due to radiation. When using steel pipes that have not been treated with a corrosion-resistant medium, it is particularly important to provide sufficient drying of the compressed air.
Failure at the connector (e.g. tearing off, leakage)	Yes, if using bite-type fittings or threaded pipes (i.e. steel fittings, steel pipes) and if dimensioning, choice of materials, manufacture, configuration and fixing are in accordance with good engineering practice.	—
Clogging (blockage)	Yes, for pipework in the power circuit. Yes, for the control and measurement pipework if the nominal diameter is ≥ 2 mm.	
Kinking of plastic pipes with a small nominal diameter	Yes, if properly protected and installed, taking into account the relevant manufacturer's data, e.g. minimum bending radius.	

Table B.8 — Faults and fault exclusions — Hose assemblies

Fault considered	Fault exclusion	Remarks
Bursting, tearing off at the fitting attachment and leakage	Yes, if hose assemblies use hoses manufactured to ISO 4079-1 or similar hoses (see remark) with the corresponding hose fittings.	Fault exclusion is not considered when — the intended lifetime is expired, — fatigue behaviour of reinforcement can occur, — external damage is unavoidable.
Clogging (blockage)	Yes, for hose assemblies in the power circuit, and, in the case of the control and measurement hose assemblies, if the nominal diameter is ≥ 2 mm.	—

Table B.9 — Faults and fault exclusions — Connectors

Fault considered	Fault exclusion	Remarks
Bursting, breaking of screws or stripping of threads	Yes, if dimensioning, choice of material, manufacture, configuration and connection to the piping and/or to the pipe/hose fittings are in accordance with good engineering practice.	—
Leakage (loss of airtightness)	None.	Due to wear, ageing, deterioration of elasticity, etc. it is not possible to exclude faults over a long period. A sudden major failure of the airtightness is not assumed.
Clogging (blockage)	Yes, for applications in the power circuit and, in the case of control and measurement connectors, if the nominal diameter is ≥ 2 mm.	—

Table B.10 — Faults and fault exclusions — Pressure transmitters and pressure medium transducers

Fault considered	Fault exclusion	Remarks
Loss or change of air/oil-tightness of pressure chambers	None.	—
Bursting of the pressure chambers as well as fracture of the attachment or cover screws	Yes, if dimensioning, choice of material, configuration and attachment are in accordance with good engineering practice.	

Table B.11 — Faults and fault exclusions — Compressed air treatment — Filters

Fault considered	Fault exclusion	Remarks
Blockage of the filter element	None.	—
Rupture or partial rupture of the filter element	Yes, if the filter element is sufficiently resistant to pressure.	
Failure of the filter condition indicator or monitor	None.	
Bursting of the filter housing or fracture of the cover or connecting elements	Yes, if dimensioning, choice of material, arrangement in the system and fixing are in accordance with good engineering practice.	

Table B.12 — Faults and fault exclusions — Compressed-air treatment — Oilers

Fault considered	Fault exclusion	Remarks
Change in the set value (oil volume per unit time) without change to the setting device	None.	—
Spontaneous change in the setting device	Yes, if effective protection of the setting device is provided, adapted to the particular case.	
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Bursting of the housing or fracture of the cover, fixing or connecting elements.	Yes, if the dimensioning, choice of materials, arrangement in the system and fixing are in accordance with good engineering practice.	

Table B.13 — Faults and fault exclusions — Compressed air treatment — Silencers

Fault considered	Fault exclusion	Remarks
Blockage (clogging) of the silencer	Yes, if the design and construction of the silencer element fulfils the remark.	Clogging of the silencer element and/or an increase in the exhaust air back-pressure above a certain critical value is unlikely if the silencer has a suitably large diameter and is designed to meet the operating conditions.

Table B.14 — Faults and fault exclusions — Accumulators and pressure vessels

Fault considered	Fault exclusion	Remarks
Fracture/bursting of the accumulator/pressure vessel or connectors or stripping of the threads of the fixing screws	Yes, if construction, choice of equipment, choice of materials and arrangement in the system are in accordance with good engineering practice.	—

Table B.15 — Faults and fault exclusions — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark)	None.	Sensors in this table include signal capture, processing and output, in particular for pressure, flow rate, temperature, etc.
Change of the detection or output characteristics	None.	—

Table B.16 — Faults and fault exclusions — Information processing — Logical elements

Fault considered	Fault exclusion	Remarks
Faulty logical element (e.g. AND element, OR element, logic-storage-element) due to, e.g. change in the switching time, failing to switch or incomplete switching	For corresponding fault assumptions and fault exclusions, see Tables B.3, B.4 and B.5 and the relevant related components.	—

Table B.17 — Faults and fault exclusions — Information processing — Time-delay devices

Fault considered	Fault exclusion	Remarks
Faulty time-delay device, e.g. pneumatic and pneumatic/mechanical time and counting elements	Yes, for time-delay devices without moving components, e.g. fixed resistance, if normal operating conditions (see remark) apply and adequate treatment and filtration of the compressed air is provided.	Normal operating conditions are met when the conditions laid down by the manufacturer are followed.
Change of detection or output characteristics		
Bursting of the housing or fracture of the cover or fixing elements	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	—

Table B.18 — Faults and fault exclusions — Information processing — Converters

Fault considered	Fault exclusion	Remarks
Faulty converter [see remark 1)]	Yes, for converters without moving components, e.g. reflex nozzle, if normal operating conditions apply [see remark 2)] and adequate treatment and filtration of the compressed air is provided.	1) This covers, for example, the conversion of a pneumatic signal into an electrical one, the position detection (cylinder switch, reflex nozzle), the amplification of pneumatic signals. 2) Normal operating conditions are met when the conditions laid down by the manufacturer are followed.
Change of the detection or output characteristics		
Bursting of the housing or fracture of the cover or fixing elements	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	—

Annex C
(informative)

Validation tools for hydraulic systems

When hydraulic systems are used in conjunction with other technologies, Annex C should also be taken into account. Where hydraulic components are electrically connected/controlled, the appropriate fault lists in Annex D should be considered.

NOTE Additional requirements can exist in national legislation.

Tables C.1 and C.2 list basic and well-tried safety principles. Air bubbles and cavitation in the hydraulic fluid should be avoided because they can create additional hazards, e.g. unintended movements.

A list of well-tried components is not given in Annex C of this edition. The status of "well-tried" is mainly application-specific. Components can be described as "well-tried" if they are in accordance with ISO 13849-1:2006, 6.2.2 and ISO 4414:2010, Clauses 5 to 7. A well-tried component for some applications could be inappropriate for other applications.

Tables C.3 to C.12 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 C.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, hydraulic fluid.
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, 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 release of energy to all relevant devices. 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. This principle shall not be used in some applications, e.g. where the loss of hydraulic pressure will create an additional hazard.
Proper fastening	For the application of e.g. screw locking, fittings, gluing, clamp ring, consider manufacturers application notes. Overloading can be avoided by applying adequate torque loading technology.
Pressure limitation	Examples are pressure-relief valve, pressure-reducing/control valve.
Speed limitation/speed reduction	An example is the speed limitation of a piston by a flow valve or a throttle.

Table C.1 *(continued)*

Basic safety principle	Remarks
Sufficient avoidance of contamination of the fluid	Consider filtration/separation of solid particles/water in the fluid. Consider also an indication of the need for a filter service.
Proper range of switching time	Consider, e.g. the length of pipework, pressure, evacuation relief capacity, spring tiredness, friction, lubrication, temperature/viscosity, inertia during acceleration and deceleration, combination of tolerances.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g. temperature, humidity, vibration, pollution. See Clause 10 and consider the manufacturer's specification and application notes.
Protection against unexpected start-up	Consider unexpected start-up caused by stored energy and after power supply restoration for different modes, e.g. operation mode, maintenance mode. Special equipment for release of stored energy may 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.
Proper temperature range	To be considered throughout the whole system.
Separation	Separation of safety-related functions from other functions.

Table C.2 — Well-tried safety principles

Well-tried safety principle	Remarks
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 one of the possible positions by mechanical means (friction only is not enough). Force is needed to change the position.
Increased OFF force	One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to the ON position (a safety factor).
Valve closed by load pressure	Examples are seat and cartridge valves. Consider how to apply the load pressure in order to keep the valve closed even if, e.g. the spring closing the valve breaks.
Positive mechanical action	The positive mechanical action is used for moving parts inside hydraulic components. See also Table A.2.
Multiple parts	See Table A.2.
Use of well-tried spring	See Table A.2.
Speed limitation/speed reduction by resistance to defined flow	Examples are fixed orifices and fixed throttles.
Force limitation/force reduction	This can be achieved by a well-tried pressure-relief valve which is, e.g. equipped with a well-tried spring, correctly dimensioned and selected.
Appropriate range of working conditions	The limitation of working conditions, e.g. pressure range, flow rate and temperature range, should be considered.
Monitoring of the condition of the fluid	Consider a high degree of filtration/separation of solid particles/water in the fluid. Consider also the chemical/physical conditions of the fluid. Consider an indication of the need for a filter service.
Sufficient positive overlapping in piston valves	The positive overlapping ensures the stopping function and prevents non-permitted movements.
Limited hysteresis	For example increased friction will increase the hysteresis. A combination of tolerances will also influence the hysteresis.

Table C.3 — Faults and fault exclusions — Directional control valves

Fault considered	Fault exclusion	Remarks
Change of switching times	Yes, in the case of positive mechanical action (see Table A.2) of the moving components as long as the actuating force is sufficiently large; or, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1)].	1) A special type of cartridge seat valve is obtained if — the active area for initiating the safety-related switching movement is at least 90 % of the total area of the moving component (poppet), — the effective control pressure on the active area can be increased up to the maximum working pressure (in accordance with ISO 5598:2008, 3.2.429) in line with the behaviour of the seat valve in question, — the effective control pressure on the area opposite the active area of the moving component is vented to a very low value compared with the maximum operating pressure, e.g. return pressure in case of pressure dump valves or supply pressure in case of suction/fill valves, — the moving component (poppet) is provided with peripheral balancing grooves, and — the pilot valve(s) to this seat valve is designed together in a manifold block (i.e. without hose assemblies and pipes for the connection of these valves).
Non-switching (sticking at an end or zero position) or incomplete switching (sticking at a random intermediate position)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components as long as the actuating force is sufficiently large; or, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1)].	
Spontaneous change of the initial switching position (without an input signal)	Yes, in the case of positive mechanical action (see Table A.2) of the moving components as long as the holding force is sufficiently large; or if well-tried springs are used (see Table A.2) and normal installation and operating conditions apply [see remark 2)]; or, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1)] and if normal installation and operating conditions apply [see remark 2)].	2) Normal installation and operating conditions apply when — the conditions laid down by the manufacturer are taken into account, — the weight of the moving component does not act in an unfavourable sense in terms of safety, e.g. horizontal installation, — no special inertial forces affect the moving components, e.g. direction of motion takes into account the orientation of the moving machine parts, and — no extreme vibration and shock stresses occur.
Leakage	Yes, in the case of seat valves, if normal installation and operating conditions apply (see remark) and an adequate filtration system is provided.	Normal installation and operating conditions apply when the conditions laid down by the manufacturer are taken into account.
If the control functions are realized by a number of single-function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.		

Table C.3 *(continued)*

Fault considered	Fault exclusion	Remarks
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	
For servo and proportional valves: hydraulic faults which cause uncontrolled behaviour	Yes, in the case of servo and proportional directional valves, if these can be assessed in terms of safety as conventional directional control valves, owing to their design and construction.	
If the control functions are realized by a number of single-function valves, then a fault analysis should be carried out for each valve. The same procedure should be carried out in the case of piloted valves.		

Table C.4 — Faults and fault exclusions — Stop (shut–off) valves/non-return (check) valves/shuttle valves, etc.

Fault considered	Fault exclusion	Remarks
Change of switching times	None.	—
Non-opening, incomplete opening, non-closure or incomplete closure (sticking at an end position or at an arbitrary intermediate position)	Yes, if the guidance system for the moving component(s) is designed in a manner similar to that for a non-controlled ball seat valve without a damping system (see remark) and if well-tried springs are used (see Table A.2).	For a non-controlled ball seat valve without damping system, the guidance system is generally designed in such a manner that any sticking of the moving component is unlikely.
Spontaneous change of the initial switching position (without an input signal)	Yes, for normal installation and operating conditions (see remark) and if there is sufficient closing force on the basis of the pressures and areas provided.	Normal installation and operating conditions are met when — the conditions laid down by the manufacturer are followed and — no special inertial forces affect the moving components, e.g. direction of motion takes into account the orientation of the moving machine parts, and — no extreme vibration or shock stresses occur.
For shuttle valves: simultaneous closing of both input connections	Yes, if, on the basis of the construction and design of the moving component, this simultaneous closing is unlikely.	—
Leakage	Yes, if normal conditions of operation apply (see remark) and an adequate filtration system is provided.	Normal conditions of operation apply when the conditions laid down by the manufacturer are taken into account.

Table C.4 *(continued)*

Fault considered	Fault exclusion	Remarks
Change in the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table C.5 — Faults and fault exclusions — Flow valves

Fault considered	Fault exclusion	Remarks
Change in the flow rate without change in the setting device	Yes, in the case of flow valves without moving parts [see remark 1)], e.g. throttle valves, if normal operating conditions apply [see remark 2)] and an adequate filtration system is provided [see remark 3)].	1) The setting device is not considered to be a moving part. Changes in flow rate due to changes in the pressure differences and viscosity are physically limited in this type of valve and are not covered by this assumed fault. 2) Normal operating conditions are met when the conditions laid down by the manufacturer are followed. 3) Where a non-return valve is integrated into the flow valve, then, in addition, the fault assumptions for non-return valves have to be taken into account.
Change in the flow rate in the case of non-adjustable, circular orifices and nozzles	Yes, if the diameter is > 0,8 mm, normal operating conditions apply [see remark 2)] and an adequate filtration system is provided.	
For proportional flow valves: change in the flow rate due to an unintended change in the set value	None.	—
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case, based upon technical safety specification(s).	
Unintended loosening (unscrewing) of the operating element(s) of the setting device	Yes, if an effective positive locking device against loosening (unscrewing) is provided.	
Bursting of the valve housing or breakage of the moving component(s) as well as the breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table C.6 — Faults and fault exclusions — Pressure valves

Fault considered	Fault exclusion	Remarks
Non-opening or insufficient opening (spatially and temporarily) when exceeding the set pressure (sticking or sluggish movement of the moving component) [see remark 1)]	Yes, in respect of the non-opening of a special type of cartridge seat valve, when used with at least one other valve, to control the main flow of the fluid [see remark 1)] of Table C.3); or if the guidance system for the moving component(s) is similar to the case of a non-controlled ball seat valve without a damping device [see remark 2)] and if the installed springs are well-tried (see Table A.2).	1) This fault applies only when the pressure valve(s) is (are) used for forced actions, e.g. clamping, and for the control of hazardous movement, e.g. suspension of loads. This fault does not apply to its normal function in hydraulic systems, e.g. pressure limitation, pressure decrease. 2) For a non-controlled ball seat valve without a damping device, the guidance system is generally designed in such a manner that any sticking of the moving component is unlikely.
Non-closing or insufficient closing (spatially and temporarily) if the pressure drops below the set value (sticking or sluggish movement of the moving component) [see remark 1)]		
Change of the pressure control behaviour without changing the setting device [see remark 1)]	Yes, in the case of directly actuated pressure-relief valves, if the installed spring(s) are well-tried (see Table A.2).	
For proportional pressure valves: change in the pressure control behaviour due to unintended change in the set value [see remark 1)]	None.	
Spontaneous change in the setting device	Yes, where there is an effective protection of the setting device adapted to the particular case in relation to technical safety specifications (e.g. lead seals).	—
Unintended unscrewing of the operating element of the setting device	Yes, if an effective positive locking device against unscrewing is provided.	
Leakage	Yes for seat valves if normal operating conditions apply (see remark) and if an adequate filtration system is provided.	Normal operating conditions apply when the conditions laid down by the manufacturer are taken into account.
Change of the leakage flow rate over a long period of use	None.	—
Bursting of the valve housing or breakage of the moving component(s) as well as breakage/fracture of the mounting or housing screws	Yes, if construction, dimensioning and installation are in accordance with good engineering practice.	

Table C.7 — Faults and fault exclusions — Metal pipework

Fault considered	Fault exclusion	Remarks
Bursting and leakage	Yes, if the dimensioning, choice of materials and fixing are in accordance with good engineering practice.	—
Failure at the connector (e.g. tearing off, leakage)	Yes, if welded fittings or welded flanges or flared fittings are used, and dimensioning, choice of materials, manufacture, configuration and fixing are in accordance with good engineering practice.	—
Clogging (blockage)	Yes, for pipework in the power circuit, and for control and measurement pipework if the nominal diameter is ≥ 3 mm.	

Table C.8 — Faults and fault exclusions — Hose assemblies

Fault considered	Fault exclusion	Remarks
Bursting, tearing off at the fitting attachment and leakage	None.	—
Clogging (blockage)	Yes, for hose assemblies in the power circuit, and for control and measurement hose assemblies if the nominal diameter is ≥ 3 mm.	

Table C.9 — Faults and fault exclusions — Connectors

Fault considered	Fault exclusion	Remarks
Bursting, breaking of screws or stripping of threads	Yes, if dimensioning, choice of material, manufacture, configuration and connection to the piping and/or to the fluid technology component are in accordance with good engineering practice.	—
Leakage (loss of the leak-tightness)	None (see remark).	Due to wear, ageing, deterioration of elasticity, etc., it is not possible to exclude faults over a long period. A sudden major failure of the leak-tightness is not assumed.
Clogging (blockage)	Yes, for applications in the power circuit, and for control and measurement connectors if the nominal diameter is ≥ 3 mm.	—

Table C.10 — Faults and fault exclusions — Filters

Fault considered	Fault exclusion	Remarks
Blockage of the filter element	None.	—
Rupture of the filter element	Yes, if the filter element is sufficiently resistant to pressure and an effective bypass valve or an effective monitoring of dirt is provided.	
Failure of the bypass valve	Yes, if the guidance system of the bypass valve is designed similarly to that for a non-controlled ball seat valve without a damping device (see Table C.4) and if well-tried springs are used (see Table A.2).	
Failure of the dirt indicator or dirt monitor	None.	
Bursting of the filter housing or fracture of the cover or connecting elements	Yes, if dimensioning, choice of material, arrangement in the system and fixing are in accordance with good engineering practice.	

Table C.11 —Faults and fault exclusions — Energy storage

Fault considered	Fault exclusion	Remarks
Fracture/bursting of the energy storage vessel or connectors or cover screws as well as stripping of the screw threads	Yes, if construction, choice of equipment, choice of materials and arrangement in the system are in accordance with good engineering practice.	—
Leakage at the separating element between the gas and the operating fluid	None.	
Failure/breakage of the separating element between the gas and the operating fluid	Yes, in the case of cylinder/piston storage (see remark).	A sudden major leakage is not to be considered.
Failure of the filling valve on the gas side	Yes, if the filling valve is installed in accordance with good engineering practice and if adequate protection against external influences is provided.	—

Table C.12 — Faults and fault exclusions — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark)	None.	Types of sensors include signal capture, processing and output, in particular for pressure, flow rate and temperature.
Change of the detection or output characteristics	None.	—

Annex D
(informative)

Validation tools for electrical systems

D.1 General

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

The environmental conditions of IEC 60204-1 apply to the validation process. If other environmental conditions are specified, they should also be taken into account.

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

The components listed in Table D.3 are considered to be "well-tried" when they comply with the description given in ISO 13849-1:2006, 6.2.4. The standards listed in Table D.3 can be used to demonstrate their suitability and reliability for a particular application. A well-tried component for some applications could be inappropriate for other applications.

NOTE Complex electronic components, such as programmable logic controllers (PLCs), microprocessors and application-specific integrated circuits, cannot be considered equivalent to the "well-tried" components.

Clause D.2 and Tables D.4 to D.18 list fault exclusions and their rationale. For further exclusions, see 4.4.

For validation, both permanent faults and transient disturbances should be considered.

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

Table D.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, conductivity, dielectric rigidity.
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, 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.
Correct protective bonding	One side of the control circuit, one terminal of the operating coil of each electromagnetic operated device, or one terminal of another electrical device is connected to the protective bonding circuit (see IEC 60204-1:2005, 9.4.3.1).
Insulation monitoring	Use of an insulation monitoring device which either indicates an earth fault or interrupts the circuit automatically after an earth fault (see IEC 60204-1:2005, 6.3.3).

Table D.1 *(continued)*

Basic safety principle	Remarks
Use of de-energization	A safe state is obtained by de-energizing all relevant devices, e.g. by use of normally closed (NC) contact for inputs (push-buttons and position switches) and normally open (NO) contact for relays (see also ISO 12100:2010, 6.2.11.3). Exceptions can exist in some applications, e.g. where the loss of the electrical supply will create an additional hazard. Time-delay functions may be necessary to achieve a system safe state (see IEC 60204-1:2005, 9.2.2).
Transient suppression	Use of a suppression device (RC, diode, varistor) parallel to the load, but not parallel to the contacts. NOTE A diode increases the switch-off time.
Reduction of response time	Minimize delay in de-energizing of switching components.
Compatibility	Use components compatible with the voltages and currents used.
Withstanding environmental conditions	Design the equipment so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g. temperature, humidity, vibration and electromagnetic interference (EMI) (see Clause 10).
Secure fixing of input devices	Secure input devices, e.g. interlocking switches, position switches, limit switches, proximity switches, so that position, alignment and switching tolerance is maintained under all expected conditions, e.g. vibration, normal wear, ingress of foreign bodies, temperature. See ISO 14119:1998, Clause 5.
Protection against unexpected start-up	Prevent unexpected start-up, e.g. after power supply restoration (see ISO 12100:2010, 6.2.11.4, ISO 14118, IEC 60204-1).
Protection of the control circuit	The control circuit should be protected in accordance with IEC 60204-1:2005, 7.2 and 9.1.1.
Sequential switching for circuit of serial contacts of redundant signals	To avoid common mode failure by the welding of both contacts, switching on and off does not happen simultaneously, so that one contact always switches without current.

Table D.2 — Well-tried safety principles

Well-tried safety principle	Remarks
Positively mechanically linked contacts	Use of positively mechanically linked contacts for, e.g. monitoring function in Category 2, 3, and 4 systems (see EN 50205, IEC 60947-4-1:2001, Annex F, IEC 60947-5-1:2003 + A1:2009, Annex L).
Fault avoidance in cables	To avoid short circuits between two adjacent conductors, either — use cable with shielding connected to the protective bonding circuit on each separate conductor, or — in flat cables, use one earthed conductor between each signal conductor.
Separation distance	Use of sufficient distance between position terminals, components and wiring to avoid unintended connections.
Energy limitation	Use of a capacitor for supplying a finite amount of energy, e.g. in a timer application.
Limitation of electrical parameters	Limiting voltage, current, energy or frequency to restrict movement, e.g. torque limitation, hold-to-run with displacement/time limited, reduced speed, to avoid an unsafe state.

Table D.2 *(continued)*

Well-tried safety principle	Remarks
No undefined states	Avoid undefined states in the control system. Design and construct the control system so that, during normal operation and all expected operating conditions, its state, e.g. its output(s), can be predicted.
Positive mode actuation	Direct action is transmitted by the shape (and not the strength) with no elastic elements, e.g. spring between actuator and the contacts (see ISO 14119:1998, 5.1, ISO 12100:2010, 6.2.5).
Failure mode orientation	Wherever possible, the device/circuit should fail to the safe state or condition.
Oriented failure mode	Oriented failure mode components or systems should be used wherever practicable (see ISO 12100:2010, 6.2.12.3).
Overdimensioning	De-rate components when used in safety circuits, e.g. by the following means: — the current passed through switched contacts should be less than half their rated current; — the switching frequency of components should be less than half their rated value; — the total number of expected switching operations should be no more than 10 % of the device's electrical durability. NOTE De-rating can depend on the design rationale.
Minimizing possibility of faults	Separate safety-related functions from the other functions.
Balance complexity/simplicity	Balance should be made between — complexity to reach a better control, and — simplification in order to have better reliability.

Table D.3 — Well-tried components

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Switch with positive mode actuation (direct opening action), e.g.: — push-button; — position switch; — cam-operated selector switch, e.g. for mode of operation	—	IEC 60947-5-1:2003, Annex K
Emergency stop device	—	ISO 13850 IEC 60947-5-5
Fuse	—	IEC 60269-1
Circuit-breaker	—	IEC 60947-2
Switches, disconnectors	—	IEC 60947-3
Differential circuit-breaker/RCD (residual current device)	—	IEC 60947-2:2006, Annex B

Table D.3 *(continued)*

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Main contactor	Only well-tried if a) other influences are taken into account, e.g. vibration, b) failure is avoided by appropriate methods, e.g. overdimensioning (see Table D.2), c) the current to the load is limited by the thermal protection device, and d) the circuits are protected by a protection device against overload. NOTE Fault exclusion is not possible.	IEC 60947-4-1
Control and protective switching device or equipment (CPS)	—	IEC 60947-6-2
Auxiliary contactor (e.g. contactor relay)	Only well-tried if a) other influences are taken into account, e.g. vibration, b) there is positively energized action, c) failure is avoided by appropriate methods, e.g. overdimensioning (see Table D.2), d) the current in the contacts is limited by a fuse or circuit-breaker to avoid the welding of the contacts, and e) contacts are positively mechanically guided when used for monitoring. NOTE Fault exclusion is not possible.	EN 50205 IEC 60947-5-1 IEC 60947-4-1:2001, Annex F
Relay	Only well-tried if a) other influences are taken into account, e.g. vibration, b) positively energized action, c) failure avoided by appropriate methods, e.g. overdimensioning (see Table D.2), and d) the current in the contacts is limited by fuse or circuit-breaker to avoid the welding of the contacts. NOTE Fault exclusion is not possible.	IEC 61810-1 IEC 61810-2
Transformer	—	IEC 61558
Cable	Cabling external to enclosure should be protected against mechanical damage (including, e.g. vibration or bending).	IEC 60204-1:2005, Clause 12
Plug and socket	—	According to an electrical standard relevant for the intended application. For interlocking, see also ISO 14119.
Temperature switch	—	For the electrical side, see EN 60730-1

Table D.3 *(continued)*

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Pressure switch	—	For the electrical side, see IEC 60947-5-1 For the pressure side, see Annexes B and C.
Solenoid for valve	—	—

D.2 Fault exclusion

D.2.1 General

A fault exclusion is valid only if the parts operate within their specified ratings.

D.2.2 "Tin whiskers"

If lead-free processes and products are applied, electrical short circuits due to the growth of "tin whiskers" can occur. This possibility should be evaluated and considered when applying the fault exclusion "short circuit…" of any component. For example, if the risk of tin whisker growth is considered high, the fault exclusion "short circuit of a resistor" is useless, since a short between the contacts of this component has to be considered.

NOTE 1 Tin whisker growth is a phenomenon related mainly to pure bright tin finishes. The needle-like protrusions can grow to several hundred micrometres in length and can cause electrical short circuits. The prevailing theory is that the whiskers are caused by compressive stress build-up in tin plating.

NOTE 2 References [34] and [35] can be helpful for evaluation of the phenomenon.

NOTE 3 Whiskers on printed circuit boards have not so far been reported. Tracks usually consist of copper without tin coating. Pads can be coated with tin alloy, but the production process seems not to stimulate the susceptibility to whisker growing.

D.2.3 Short circuits on PCB-mounted parts

Short circuits for parts which are mounted on a printed circuit board (PCB) can only be excluded if the fault exclusion "short circuit between two adjacent tracks/pads", described in Table D.5, is made.

D.2.4 Fault exclusions and integrated circuits

As it is not possible to exclude faults that can cause the malfunction of an integrated circuit (see Tables D.20 and D.21), a single fault can lead to loss of a safety function (including its check/test) implemented in a single integrated circuit. Consequently, it is highly unlikely that the multi-channel functionality necessary for the fault tolerance and/or detection requirements of category 2, 3 or 4 can be achieved using a single integrated circuit, unless it satisfies the special architecture requirements of IEC 61508-2:2010, Annex E.

Table D.4 — Faults and fault exclusions — Conductors/cables

Fault considered	Fault exclusion	Remarks
Short circuit between any two conductors	Short circuits between conductors which are — permanently connected (fixed) and protected against external damage, e.g. by cable ducting, armouring, — separate multicore cables, — within an electrical enclosure (see remark), or — individually shielded with earth connection.	Provided both the conductors and enclosure meet the appropriate requirements (see IEC 60204-1).
Short circuit of any conductor to an exposed conductive part or to earth or to the protective bonding conductor	Short circuits between conductor and any exposed conductive part within an electrical enclosure (see remark).	
Open circuit of any conductor	None.	—

Table D.5 — Faults and fault exclusions — Printed circuit boards/assemblies

Fault considered	Fault exclusion	Remarks
Short circuit between two adjacent tracks/pads	Short circuits between adjacent conductors in accordance with remarks.	As base material, EP GC according to IEC 60893-1 is used as a minimum. The clearances and creepage distances are dimensioned to at least IEC 60664-5 (IEC 60664-1 for distances greater than 2 mm) with pollution degree 2/ overvoltage category III; if both tracks are powered by a SELV/PELV power supply, pollution degree 2/ overvoltage category II applies, with a minimum clearance of 0,1 mm. The assembled board is mounted in an enclosure giving protection against conductive contamination, e.g. an enclosure with a protection of at least IP54, and the printed side(s) is (are) coated with an ageing-resistant varnish or protective layer covering all conductor paths. NOTE 1 Experience has shown that solder masks are satisfactory as a protective layer. NOTE 2 A further protective layer covering according to IEC 60664-3 can reduce the creepage distances and clearances dimensions.
Open circuit of any track	None.	—

Table D.6 — Faults and fault exclusions — Terminal block

Fault considered	Fault exclusion	Remarks
Short circuit between adjacent terminals	Short circuit between adjacent terminals in accordance with remarks 1) or 2).	1) The terminals and connections used are in accordance with IEC 60947-7-1 or IEC 60947-7-2 and the requirements of IEC 60204-1:2006, 13.1.1, are satisfied. 2) The design in itself ensures that a short circuit is avoided, e.g. by shaping shrink-down plastic tubing over connection point.
Open circuit of individual terminals	None.	—

Table D.7 — Faults and fault exclusions — Multi–pin connector

Fault considered	Fault exclusion	Remarks
Short circuit between any two adjacent pins	Short circuit between adjacent pins in accordance with remark. If the connector is mounted on a PCB, the fault exclusion considerations of Table D.5 apply.	By using ferrules or other suitable means for multi-stranded wires. Creepage distances and clearances and all gaps should be dimensioned to at least IEC 60664-1 with overvoltage category III.
Interchanged or incorrectly inserted connector when not prevented by mechanical means	None.	—
Short circuit of any conductor (see remark) to earth or a conductive part or to the protective conductor	None.	The core of the cable is considered a part of the multi-pin connector.
Open circuit of individual connector pins	None.	—

Table D.8 — Faults and fault exclusions — Switches — Electromechanical position switches, manually operated switches (e.g. push-button, reset actuator, DIP switch, magnetically operated contacts, reed switch, pressure switch, temperature switch)

Fault considered	Fault exclusion	Remarks
Contact will not close	Pressure-sensitive devices in accordance with ISO 13856	—
Contact will not open	Contacts in accordance with IEC 60947-5-1:2003, Annex K, are expected to open.	—
For PL e, a fault exclusion for mechanical (e.g. the mechanical link between an actuator and a contact element) and electrical aspects is not allowed. In this case redundancy is necessary. For emergency stop devices in accordance with IEC 60947-5-5, a fault exclusion for mechanical aspects is allowed if a maximum number of operations is considered.		
NOTE The fault lists for the mechanical aspects are considered in Annex A.		

Table D.8 *(continued)*

Fault considered	Fault exclusion	Remarks
Short circuit between adjacent contacts insulated from each other	Short circuit can be excluded for switches in accordance with IEC 60947-5-1 (see remark).	Conductive parts which become loose should not be able to bridge the insulation between contacts.
Simultaneous short circuit between three terminals of change-over contacts	Simultaneous short circuits can be excluded for switches in accordance with IEC 60947-5-1 (see remark).	
For PL e, a fault exclusion for mechanical (e.g. the mechanical link between an actuator and a contact element) and electrical aspects is not allowed. In this case redundancy is necessary. For emergency stop devices in accordance with IEC 60947-5-5, a fault exclusion for mechanical aspects is allowed if a maximum number of operations is considered.		
NOTE The fault lists for the mechanical aspects are considered in Annex A.		

Table D.9 — Faults and fault exclusions — Switches — Electromechanical devices (e.g. relay, contactor relays)

Fault considered	Fault exclusion	Remarks
All contacts remain in the energized position when the coil is de-energized (e.g. due to mechanical fault)	None.	—
All contacts remain in the de-energized position when power is applied (e.g. due to mechanical fault, open circuit of coil)	None.	
Contact will not open	None.	
Contact will not close	None.	
Simultaneous short circuit between the three terminals of a change-over contact	Simultaneous short circuit can be excluded if remarks are taken into account.	The creepage and clearance distances are dimensioned to at least IEC 60664-1 with at least pollution degree 2/overvoltage category III. Conductive parts which become loose cannot bridge the insulation between contacts and the coil.
Short circuit between two pairs of contacts and/or between contacts and coil terminal	Short circuit can be excluded if remarks are taken into account.	
Simultaneous closing of normally open and normally closed contacts	Simultaneous closing of contacts can be excluded if remark is taken into account.	Positively driven (or mechanically linked) contacts are used (see IEC 60947-5-1:2003, Annex L).

Table D.10 — Faults and fault exclusions — Switches — Proximity switches

Fault considered	Fault exclusion	Remarks
Permanently low resistance at output	None (see remark).	See IEC 60947-5-3.
Permanently high resistance at output	None (see remark).	Fault prevention measures should be described.
Interruption in power supply	None.	—
No operation of switch due to mechanical failure	No operation due to mechanical failure when remark is taken into account.	All parts of the switch should be sufficiently well fixed. For mechanical aspects, see Annex A.
Short circuit between the three connections of a change-over switch	None.	—

Table D.11 — Faults and fault exclusions — Switches — Solenoid valves

Fault considered	Fault exclusion	Remarks
Does not energize	None.	—
Does not de-energize	None.	
NOTE The fault lists for the mechanical aspects of pneumatic and hydraulic valves are considered in Annexes B and C respectively.		

Table D.12 — Faults and fault exclusions — Discrete electrical components — Transformers

Fault considered	Fault exclusion	Remarks
Open circuit of individual winding	None.	—
Short circuit between different windings	Short circuit between different windings can be excluded if remarks 1) and 2) are taken into account.	1) The requirements of the relevant parts of IEC 61558 should be met. 2) Between different windings, doubled or reinforced insulation or a protective screen applies. Testing according to IEC 61558-1:2005, Clause 18, applies. Appropriate test voltages are given in IEC 61558-1:2005, Table 8 a). Short circuits in coils and windings need to be avoided by taking appropriate steps, e.g. — impregnating the coils so as to fill all the cavities between individual coils and the body of the coil and the core, and — using winding conductors well within their insulation and high-temperature ratings. 3) In the event of a secondary short circuit, heating above a specified operating temperature should not occur.
Short circuit in one winding	A short circuit in one winding can be excluded if remark 1) is taken into account.	
Change in effective turns ratio	Change in effective turns ratio can be excluded if remark 1) is taken into account. See also remark 3).	

Table D.13 — Faults and fault exclusions — Discrete electrical components — Inductances

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit	Short circuit can be excluded if remark is taken into account.	Coil is single-layered, enamelled or potted, with axial wire connections and axial-mounted.
Random change of value $0{,}5\ L_N < L < L_N$ + tolerance, where L_N is the nominal value of the inductors	None.	Depending upon the type of construction, other ranges can be considered.

Table D.14 — Faults and fault exclusions — Discrete electrical components — Resistors

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit	Short circuit can be excluded if remark 1) or 2) is taken into account.	1) The resistor is of the film type, or wire-wound single-layer type with protection to prevent unwinding of wire in the event of breakage, with axial wire connections, axial-mounted and varnished. 2) Resistors in surface-mount technology must be of the thin film metal type in package types MELF, mini MELF or μMELF. 3) For example, if the risk of tin-whisker growth is considered high, the fault exclusion "short circuit of a resistor" is useless, since a short between the contacts of this component has to be considered.
Random change of value $0{,}5\ R_N < R < 2\ R_N$, where R_N is the nominal value of resistance [see also remark 3)]	None.	Depending upon the type of construction, other ranges can be considered.

Table D.15 — Faults and fault exclusions — Discrete electrical components — Resistor networks

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit between any two connections	None.	
Short circuit between any connections.	None.	
Random change of value $0{,}5\ R_N < R < 2\ R_N$, where R_N is the nominal value of resistance	None.	Depending upon the type of construction, other ranges can be considered.

Table D.16 — Faults and fault exclusions — Discrete electrical components — Potentiometers

Fault considered	Fault exclusion	Remarks
Open circuit of individual connection	None.	—
Short circuit between all connections	None.	
Short circuit between any two connections	None.	
Random change of value $0{,}5\ R_p < R < 2\ R_p$, where R_p is the nominal value of resistance	None.	Depending upon the type of construction, other ranges can be considered.

Table D.17 — Faults and fault exclusions — Discrete electrical components — Capacitors

Fault considered	Fault exclusion	Remarks
Open circuit	None.	—
Short circuit	None.	
Random change of value $0{,}5\ C_N < C < C_N$ + tolerance, where C_N is the nominal value of capacitance	None.	Depending upon the type of construction, other ranges can be considered.
Changing value tan, δ	None.	—

Table D.18 — Faults and fault exclusions — Electronic components — Discrete semiconductors (e.g. diodes, Zener diodes, transistors, triacs, thyristors, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs])

Fault considered	Fault exclusion	Remarks
Open circuit of any connection	None.	—
Short circuit between any two connections	None.	
Short circuit between all connections	None.	
Change in characteristics	None.	

Table D.19 — Faults and fault exclusions — Electronic components — Optocouplers

Fault considered	Fault exclusion	Remarks
Open circuit of individual connection	None.	—
Short circuit between any two input connections	None.	
Short circuit between any two output connections	None.	
Short circuit between any two connections of input and output	Short circuit between input and output can be excluded if the remarks are taken into account.	The optocoupler is built in accordance with overvoltage category III according to IEC 60664-1. If a SELV/PELV power supply is used, pollution degree 2/overvoltage category II applies. NOTE See Table D.5. Measures are taken to ensure that an internal failure of the optocoupler cannot result in excessive temperature of its insulating material.

Table D.20 — Faults and fault exclusions — Electronic components — Non–programmable integrated circuits

Fault considered	Fault exclusions	Remarks
Open circuit of each individual connection	None.	—
Short circuit between any two connections	None.	
Stuck-at-fault (i.e. short circuit to 1 and 0 with isolated input or disconnected output). Static "0" and "1" signal at all inputs and outputs, either individually or simultaneously	None.	
Parasitic oscillation of outputs	None.	
Changing values (e.g. input/output voltage of analogue devices)	None.	
NOTE In this part of ISO 13849, ICs with less than 1 000 gates and/or less than 24 pins, operational amplifiers, shift registers and hybrid modules are considered non-complex. This definition is arbitrary.		

Table D.21 — Faults and fault exclusions — Electronic components — Programmable and/or complex integrated circuits

Fault considered	Fault exclusions	Remarks
Faults in all or part of the function including software faults	None.	—
Open circuit of each individual connection	None.	
Short circuit between any two connections	None.	
Stuck-at-fault (i.e. short circuit to 1 and 0 with isolated input or disconnected output). Static "0" and "1" signal at all inputs and outputs, either individually or simultaneously	None.	
Parasitic oscillation of outputs	None.	
Changing value, e.g. input/output voltage of analogue devices	None.	
Undetected faults in the hardware which go unnoticed because of the complexity of the integrated circuit	None.	
The analysis should identify additional faults, which should be considered if they influence the operation of the safety function.		
NOTE In this part of ISO 13849, an IC is considered complex if it consists of more than 1 000 gates and/or more than 24 pins. This definition is arbitrary.		

Annex E
(informative)

Example of validation of fault behaviour and diagnostic means

E.1 General

This example considers the validation of the PL of a safety function (SF 1), with the exception of requirements relating to the following aspects of the PL:

— $MTTF_d$ values;

— common-cause failures (CCFs);

— software analysis;

— systematic failures.

The example does not cover the validation of

— safety requirements specification (see Clause 7),

— characteristics of safety functions (see Clause 8),

— environmental requirements (see Clause 10),

— maintenance requirements (see Clause 11),

— documentation requirements (see Clause 12).

Three safety functions, SF 1, SF 2 and SF 3, are considered in the example.

SF 1 is a safety-related stopping function of four individual machine actuators initiated by the opening of one interlocking guard, and this is treated as a separate safety function for each actuator (SF 1.0, SF 1.1, SF 1.2 and SF 1.3). In order to reduce the extent of the example, the validation has been limited to SF 1.0 and SF 1.3.

Annex A provides guidance on how to examine the fault behaviour and diagnostic coverage of a given circuit is provided. The methods used for determination of the diagnostic coverage are based on failure mode and effects analysis (FMEA), taking into account ISO 13849-1:2006, Annex E.

NOTE This example does not cover the complete validation process of SRP/CS. In particular, the necessary validation of the PLC software has not been considered. For the validation of safety-related software, see 9.5.

E.2 Description of machine

The example is based upon an automatic assembly machine, with manual loading and unloading of workpieces. The machine is intended to perform two sequential operations: ball insertion and screw fixing on each workpiece.

There are four stations on the machine: the loading and unloading stations and two workstations (see Figure E.1). The first workstation is the pneumatically driven ball-insertion stage, and the second the pneumatically driven screw-fixing stage.

An electrically-driven rotary table moves workpieces around each of the four stations. The workpieces are manually placed on, and removed from, workpiece holders mounted on the rotary table. An inverter-controlled electric motor drives a planetary gear and drive-belt system which moves the rotary table.

At the first workstation a ball is inserted into the workpiece by a horizontally mounted pneumatic cylinder, which is controlled by a monostable 5/2 port directional control valve (1V1, see Figure E.3). The basic position (valve de-energized) of this cylinder is the retracted position. The depth of the inserted ball is checked by monitoring a limit switch at the fully extended position of the cylinder, and the applied pressing pressure is monitored by a pressure sensor in the air supply line for cylinder extension.

The screw-fixing workstation consists of a vertically mounted, rodless pneumatic cylinder carrying a pneumatically driven rotary screwdriver unit. The screwdriver unit is raised and lowered by the pneumatic cylinder, which is controlled by a monostable 5/2 port directional control valve (2V1). The basic position (valve de-energized) of this cylinder is the upper position, with the screwdriver unit raised. Additionally, a pilot-controlled check valve (2V2) is provided in the lower connection of the pneumatic cylinder.

Rotary motion of the screwdriver unit is provided by a pneumatic motor, controlled by a monostable 5/2 port directional control valve (3V1). The basic position (valve de-energized) of this pneumatic motor is the OFF state. The torque provided by the screwdriver unit is monitored by a pressure sensor in its air supply line.

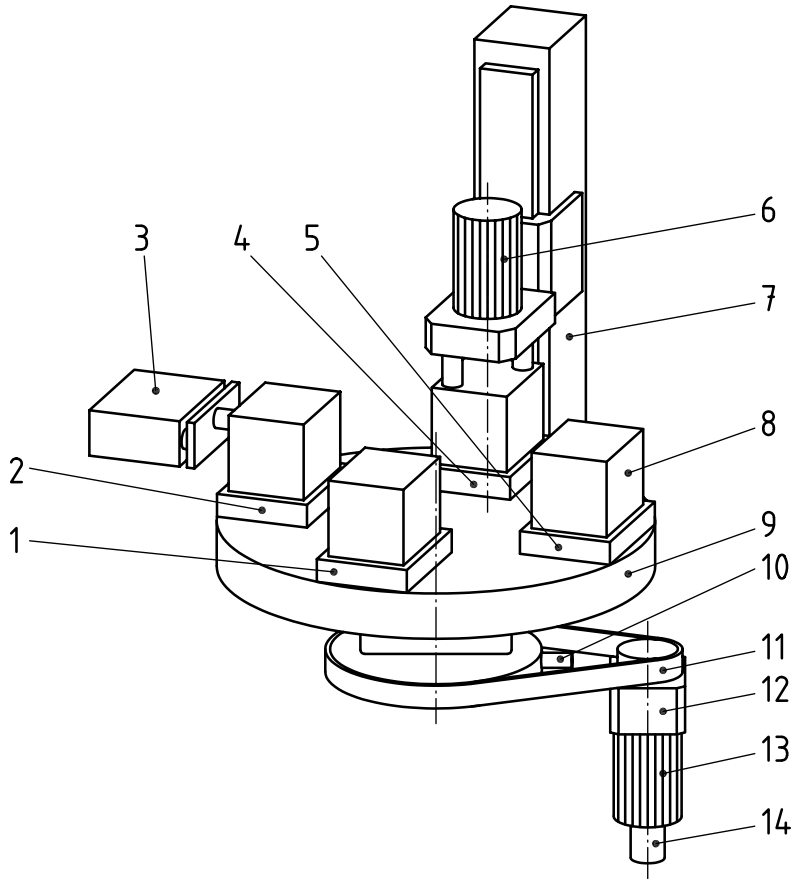
A single cycle of the machine in automatic mode of operation is initiated by actuating the start push-button. At the beginning of a cycle, the rotary table holds three workpieces: (i) a newly loaded workpiece, (ii) a partially finished workpiece (ball inserted), and (iii) a finished workpiece (ball inserted and screw fixed). Each cycle of the machine consists of the rotary table moving through 90°, followed by simultaneous ball-insertion and screw-fixing operations on the newly loaded and partially finished workpieces. The machine then comes to an operational stop, after which the operator opens the interlocking guard to unload the finished workpiece and load a new workpiece. The completion of a workpiece requires three machine cycles to rotate the workpiece by 270° from the loading station through to the unloading station.

The following modes of operation are provided:

— automatic mode with manual loading and unloading (full motion of the machine with the interlocking guard closed);

— set-up mode for the rotary table (motion of the rotary table with hold-to-run control and the interlocking guard open).

The machine presents mechanical hazards arising out of movements of the pneumatically driven machine actuators (at the ball-insertion and screw-fixing workstations) and the electrically driven rotary table. It is for this reason protected by mechanical guards, all of which are fixed, except for an interlocking guard that provides access to the loading and unloading stations (the hazard zone).



Key

1	loading station	8	workpiece
2	ball-insertion workstation	9	rotary table
3	ball-insertion cylinder (A1)	10	pulse sensor (G2)
4	screw-fixing workstation	11	drive belt
5	unloading station	12	planetary gear
6	screwdriver unit (A3)	13	electric motor (M1)
7	screw insertion (vertical-drive) cylinder (A2)	14	rotation sensor (G1)

Figure E.1 — Machine used in example: automatic assembly machine

E.3 Specification of safety function requirements

In the automatic mode of operation, protection against hazardous movements is provided by the following safety function:

SF 1 safety-related stopping initiated by the opening of the interlocking guard and prevention of unexpected start-up whenever the interlocking guard is open.

For the purposes of the example, this can be considered a separate safety function for each of the four individual machine actuators:

SF 1.0 electric motor of the rotary table (M1);

SF 1.1 ball-insertion cylinder (A1);

SF 1.2 screw-insertion cylinder (A2);

SF 1.3 pneumatic motor of the screwdriver unit (A3).

NOTE 1 For the example, safety-related stop and protection against unexpected start-up are considered a single safety function because they are implemented in the same combination of SRP/CS.

During the set-up mode for the rotary table with the interlocking guard open (pneumatically driven machine actuators disabled by SF 1.1, SF 1.2 and SF 1.3), the safe condition of the rotary table movement is achieved by a combination of the following safety functions:

SF 2: safely-limited speed;

SF 3: hold-to-run mode.

Table E.1 — Active safety functions according to mode of operation

Mode of operation	Safety function					
	SF 1.0	SF 1.1	SF 1.2	SF 1.3	SF 2	SF 3
Automatic mode (interlocking guard closed)	X	X	X	X		
Set-up mode (interlocking guard open)		X	X	X	X	X
X: safety function active						

After performing a risk assessment, the following values of PL_r were assigned to the safety functions:

PL_r d for SF 1 (safety-related stopping and prevention of unexpected start-up);

PL_r d for SF 2 (safely-limited speed);

PL_r c for SF 3 (hold-to-run mode).

NOTE 2 The selection of PL_r c for SF 3 takes account of its use in combination with SF 2, for which PL d is achieved.

When SF 1 is demanded, it initiates the following actions:

— the rotary table performs a controlled stop in accordance with Stop Category 2 of IEC 60204-1;

— the horizontally mounted pneumatic cylinder (A1) of the ball-insertion workstation and the vertically mounted pneumatic cylinder (A2) of the screw-fixing workstation return to and/or remain in their basic positions (i.e. retracted and upper respectively);

— the screwdriver unit (A3) stops immediately.

NOTE 3 For the example, the risk assessment determined that loss of controlled deceleration of the rotary table as a result of an inverter malfunction was acceptable, and movement of pneumatic cylinders A1 and A2 to their basic positions non-hazardous.

The minimum distance between the interlocking guard and these moving parts of the machine was determined according to ISO 13855, based on the machine stopping performance.

The machine is provided with other safety functions, such as an emergency stop, restart interlock, reset, and selection of modes for operation, but these are not considered in the example and, consequently, relevant components are not shown in the circuit diagrams of Figures E.2 and E.3.

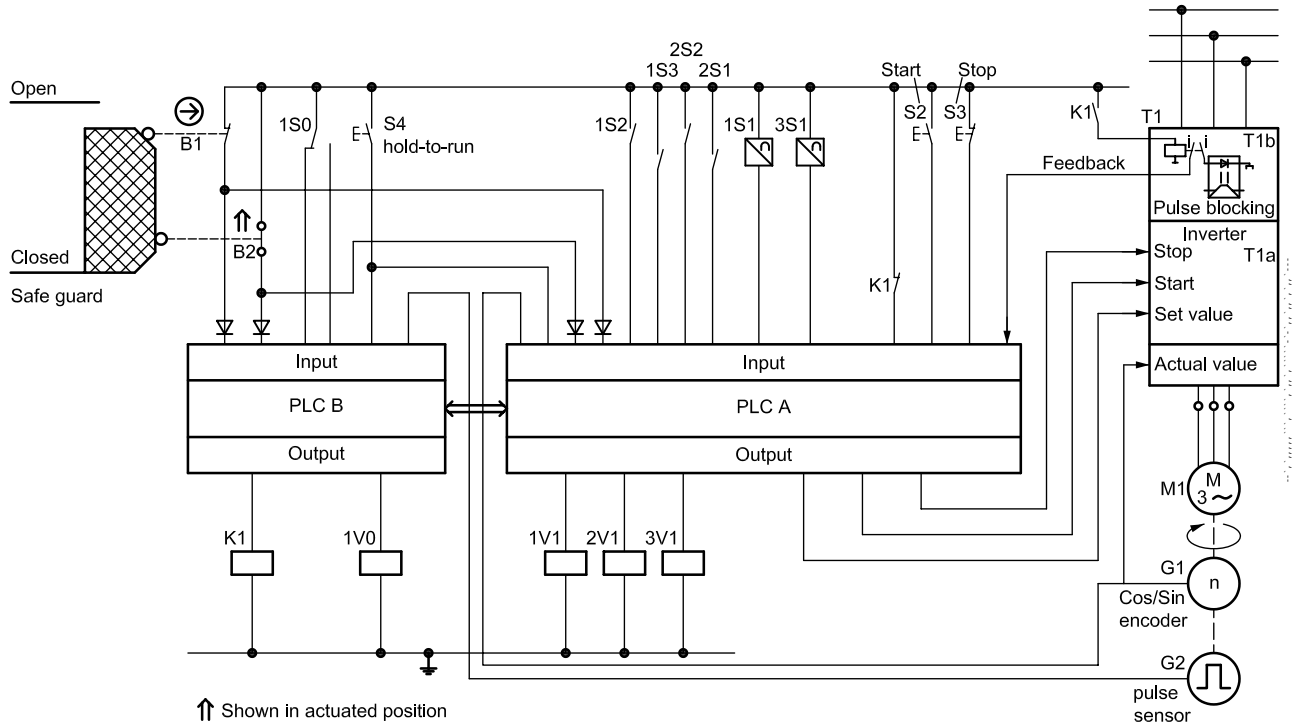


Figure E.2 — Automatic assembly machine — Electrical circuit diagram

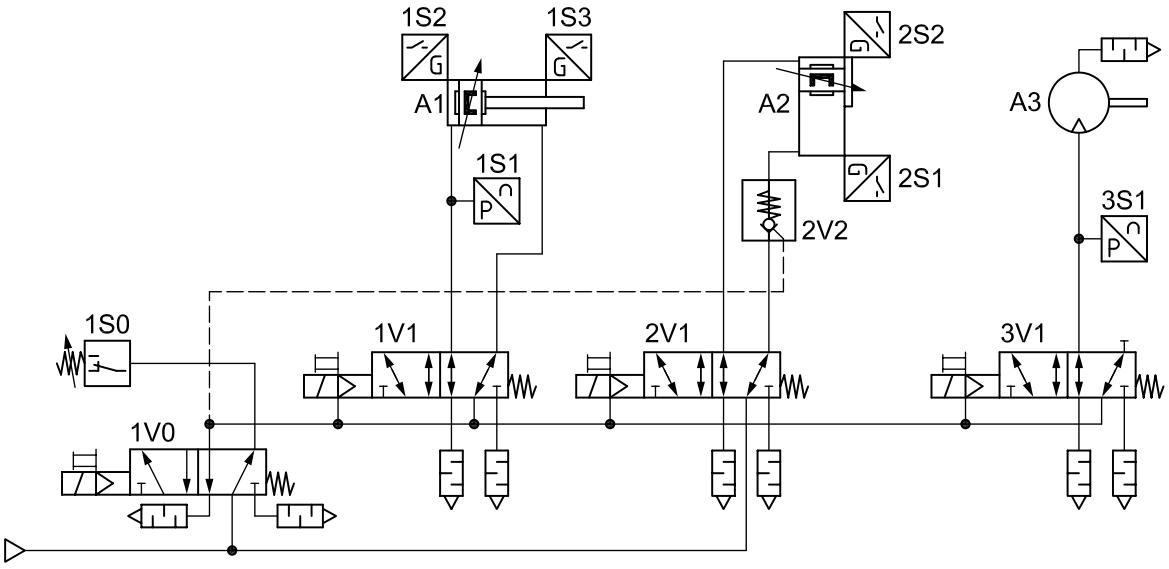


Figure E.3 — Automatic assembly machine — Pneumatic circuit diagram

E.4 Design of SRP/CS

E.4.1 General

The control system for the example has been implemented using a combination of electromechanical, electronic and pneumatic technologies.

In order to achieve the PL_r for SF 1 and SF 2, Category 3 has been selected. A diverse redundant and monitored structure has therefore been adopted for all electrical and pneumatic parts associated with these safety functions (see Figures E.2 and E.3).

To achieve the PL_r for SF 3, a combination of Category 2 and Category 3 has been selected.

The signals from the sensors and control actuators (interlocking guard position switches, hold-to-run push-button) have been duplicated and connected into two diverse PLCs (different types of hardware for PLC A and PLC B), which process them using specific software function blocks (SRASW). Each PLC also controls both the rotary table inverter and the pneumatically driven machine actuators via switching paths that are independent of the other PLCs' switching paths.

For diagnostic (cross-monitoring) and synchronization purposes, the two PLCs communicate with each other via a standard data-bus.

The particular inverter in this example has an additional facility (internal relay) to disable its power semiconductor control signals (pulse-blocking), which can be considered a second shutdown path [Safe Torque Off (STO) according to IEC 61800-5-2].

This pulse-blocking feature will not bring a rotating motor to a rapid stop, because disabling the inverter control of the motor causes an uncontrolled deceleration. However, in this example pulse-blocking would still cause the rotary table to stop before an operator can access the hazard zone, and so the controlled deceleration to a standstill that normally precedes pulse-blocking is not a required characteristic of SF 1.0.

In the pneumatic circuit, the supply of air to each of the machine actuators (A1, A2 and A3) is controlled by a monostable 5/2 port directional control valve (1V1, 2V1 and 3V1) of the pilot-controlled solenoid type. The control air for all three valves is switched by an additional valve (1V0) of the same type, which provides a redundant channel of control. The status of this release valve is monitored by a pressure switch (1S0).The air supply for A2 is taken from the main air supply, whereas for A1 and A3 it is taken from the control air supply (1V0).

De-energizing of the driving chamber from moving cylinder A1 during penetration of the workspace is provided by two channels too:

— air bleeding through 1V1 by switching in normal position, and

— de-energizing through 1V0 by switching in normal position.

The status of 1V1 is monitored by a limit switch (1S2).

A pilot-controlled check valve (2V2), which also takes its control air from 1V0, is provided in the lower connection of A2 (vertically mounted rodless pneumatic cylinder). This provides a redundant channel for stopping the downward motion and retaining the machine actuator in its basic (upper) position.

The status of 2V1 is monitored by a limit switch (2S2).

The air supply for pneumatic motor A3 (screwdriver unit) is taken from the control air supply (1V0) rather than the main air supply. This use of 1V0 in addition to 3V1 to switch off the air supply to A3 provides a redundant channel of control, which ensures that A3 will not continue to rotate if 3V1 were to fail in the energized position. The status of 3V1 is monitored by a pressure sensor (3S1) that provides an analogue output signal.

In accordance with Category 3, basic and well-tried safety principles are taken into account, and the requirements of Category B are also satisfied. In particular, the requirements of the standards IEC 60204-1 and ISO 4414 have been applied.

The attributes of components implementing SRP/CS are explained in detail in Table E.2.

Table E.2 — Attributes of components implementing SRP/CS (parts list of Figures E.2 and E.3)

Component label	Function	Element	Attribute	Well-tried safety principle[a]	Possible fault exclusion
B1	Monitoring position of interlocking guard	Interlocking switch	IEC 60947-5-1:2003, including direct opening action in accordance with IEC 60947-5-1:2003, Annex K	Positive mode actuation	Failure of switch contacts to open when operated can be excluded. Electrical faults because B1 possesses positive mode of actuation.
B2	Monitoring position of interlocking guard	Interlocking switch	IEC 60947-5-1	None.	None.
S4	Generates hold-to-run motion during set-up mode	Normally open push-button	—	None.	None.
PLC A PLC B	Processing safety-related and non safety-related signals	Programmable logic controller (PLC)	IEC 61131-1 and IEC 61131-2	None.	None.
K1	Generates redundant STOP signal for inverter in case of failure in PLC A path	Relay contactor	IEC 60947-5-1, including mechanically linked contact elements in accordance with IEC 60947-5-1:2003, Annex L, and EN 50205	Mechanically-linked contacts	None.
T1	Drives rotary table electric motor	Inverter	Inverter has additional shut-down path using pulse blocking.	Blocking relay with positively mechanically linked contacts	None.
G1	Measures speed of electric motor for rotary table	Rotation sensor (cos/sin encoder)	—	None.	None.
G2	Monitors motion of rotary table	Pulse sensor	—	None.	None.
1V0	Control of pilot air for directional control valves 1V1, 2V1, 3V1, and for check valve 2V2	Directional-control solenoid valve	Spring-biased valve, 5/2-function, pilot-operated, internal pilot air supply, spool valve with overlap	Table B.2 overdimensioning/ safety factor, safe position (use of well-tried spring), sufficient positive overlapping in piston valves	Pressure build-up at port 4 with exhausted port 5 in normal position, failure of the sealing through extrusion, moving of valve spool without operating power.

Table E.2 *(continued)*

Component label	Function	Element	Attribute	Well-tried safety principle[a]	Possible fault exclusion
1V1 2V1 3V1	Control of ball-insertion cylinder A1 Control of screw-insertion cylinder A2 Control of screwdriver unit (pneumatic motor) A3	See 1V0.	See 1V0.	See 1V0.	See 1V0.
2V2	Anti-fall device for vertically mounted screw-insertion cylinder (A2) of the screwdriver unit	Check valve	Pilot-operated non-return valve, spring-loaded poppet valve	Table B.2 valve closed by load pressure	Opening without pilot air
1S0	Monitors status of valve 1V0	Pressure switch	Fixed switch point	Basic safety principles are not required for monitoring (no safety function).	None.
1S1 3S1	Monitors pressure applied during ball insertion process Monitors torque (pressure) applied during screwdriving process	Pressure sensor	Analogue output signal	Basic safety principles are not required for monitoring (no safety function).	None.
1S2, 1S3 2S1, 2S2	Limit switches for ball-insertion cylinder A1 Limit switches for screw-insertion cylinder A2	Proximity sensor	Magnetic measuring principle	Basic safety principles are not required for monitoring (no safety function).	None.
A1	Ball-insertion cylinder	Pneumatic cylinder	Not in scope of this standard according to ISO 13849-1:2006, 3.1.1.		
A2	Screw-insertion cylinder	Rodless pneumatic cylinder with external guide	Not in scope of this standard according to ISO 13849-1:2006, 3.1.1.		
A3	Screwdriver unit	Pneumatic motor	Not in scope of this standard according to ISO 13849-1:2006, 3.1.1.		

[a] Basic safety principles have also been taken into account in the design of components (see Table D.1 for electrical components and Table B.1 for pneumatic components).

E.4.2 Safety function SF 1 — Safety-related stopping initiated by the opening of the interlocking guard and prevention of unexpected start-up whenever the interlocking guard is open

According to the machine specification, opening of the interlocking guard has to initiate the stopping of four machine actuators: (i) the rotary table (driven by inverter-controlled motor), (ii) the ball-insertion cylinder, (iii) the screw-insertion cylinder, and (iv) the screwdriver unit. This function can therefore be represented as shown in Figure E.4.

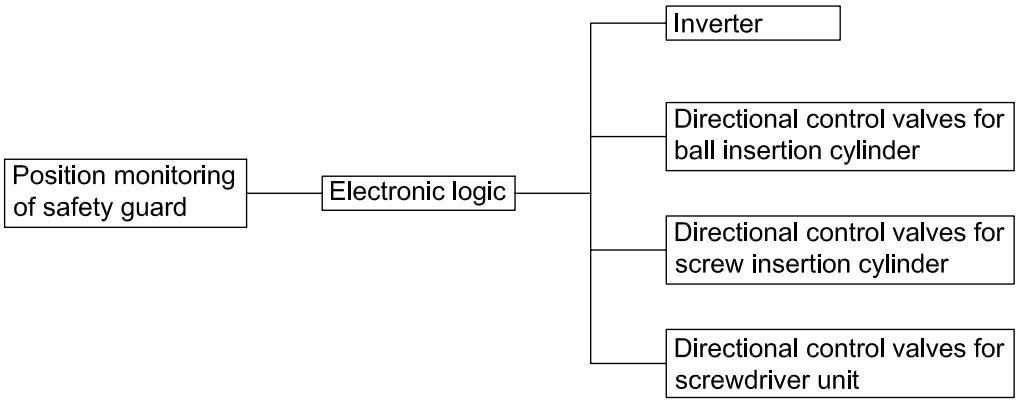


Figure E.4 — Function blocks — SF 1.0, SF 1.1, SF 1.2 and SF 1.3

When the interlocking guard is opened, PLC A initiates a stop of the rotary table by providing a stop signal to the inverter (T1a). PLC B monitors the resulting deceleration of the rotary table via G2, and when it detects that this has reached a standstill it de-energizes K1 to initiate pulse-blocking at the inverter (T1b). If the rotary table does not stop due to a fault in T1a or PLC A, then PLC B will detect this fault and still provide its own stop signal to the inverter (T1b). This is the second independent channel for the stopping function. The part of the safety function relating to prevention of unexpected start-up is performed in the same way.

Opening the interlocking guard also causes PLC A to initiate a first stop of the ball-insertion cylinder, the screw-insertion cylinder and the screwdriver unit by de-energizing 1V1, 2V1 and 3V1. PLC B initiates a second stop of these three actuators by de-energizing 1V0.

If the rotary table is already stopped, but the ball-insertion and screw-fixing workstations are in operation when the interlocking guard is opened, then PLC A will immediately de-energize 1V1, 2V1 and 3V1, and PLC B will immediately de-energize K1. PLC B will also de-energize 1V0 after a delay, to allow for the ball-insertion cylinder (A1) to complete its travel to the retracted position.

While the interlocking guard is in the open position, it needs to be ensured that a fault in the enabling path of PLC A does not lead to an uncontrolled start-up. This is achieved by the action of PLC B de-energizing K1 as soon as the rotary table motor has reached a standstill, and also de-energizing 1V0 to prevent a start-up of the ball-insertion cylinder or the screw-insertion cylinder.

The evaluation of the PL for the SRP/CS performing SF 1 has been carried out as follows:

a) **Identification of safety-related parts**

The safety-related parts of stopping function SF 1.0 and their division into channels can be illustrated by the safety-related block diagram shown in Figure E.5.

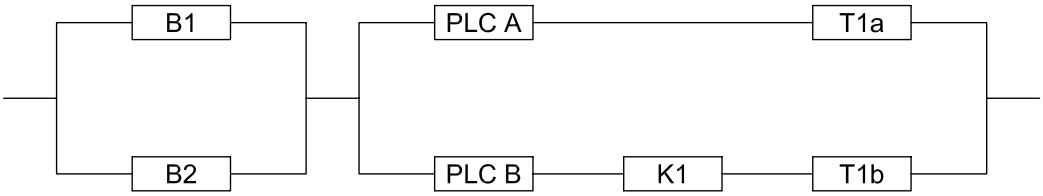
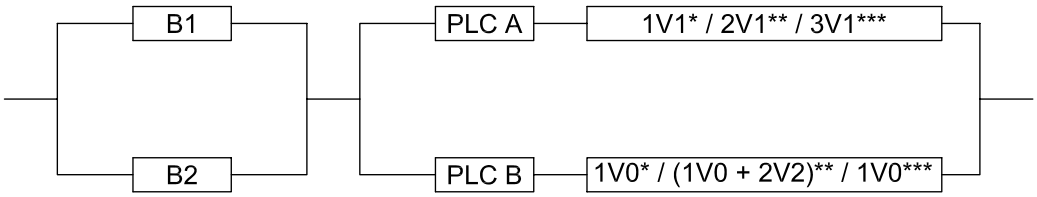


Figure E.5 — Safety-related block diagram — SF 1.0

Similarly, the safety-related parts of stopping functions SF 1.1, SF 1.2 and SF 1.3 and their division into channels can be illustrated by the safety-related block diagram shown in Figure E.6.



* SF 1.1 ** SF 1.2 *** SF 1.3

Figure E.6 — Safety-related block diagram — SF 1.1, SF 1.2 and SF 1.3

The two parts of the diagrams in Figures E.5 and E.6 can each be mapped to the designated architecture for Category 3, so the diagrams can be simplified as the two SRP/CS (input, logic/output) shown in Figure E.7.

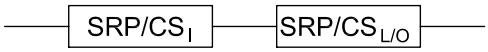


Figure E.7 — Combination of SRP/CS performing safety functions

For each SRP/CS, a PL has been estimated by applying the simplified procedure from ISO 13849-1:2006, 4.5.4.

b) **Estimation of $MTTF_d$ of each channel**

For the estimation of component $MTTF_d$ values, reliability data provided by the manufacturers has been used.

For the estimation of the $MTTF_d$ of a channel, the parts count method has been applied (see ISO 13849-1:2006; Annex D). The diverse redundant structure leads to dissimilar $MTTF_d$ values for each channel, so that application of the symmetrisation equation provides an average result of 25 years (medium) for the $MTTF_d$ of each channel of both SRP/CS_I and $SRP/CS_{L/O}$ of SF 1.0, SF 1.1, SF 1.2, and SF 1.3 (see ISO 13849-1:2006, D.2).

c) **Estimation of DC_{avg}**

The DC_{avg} has been calculated for both SRP/CS from the DC of the internal test and monitoring measures applied to the different components.

A plausibility check of the guard interlocking switches B1 and B2 by PLC A and PLC B according to ISO 13849-1:2006, Annex E, results in a DC_{avg} high (99 %) for the SRP/CS_I of SF 1.0, SF 1.1, SF 1.2 and SF 1.3.

The following diagnostic measures are provided in the $SRP/CS_{L/O}$ of SF 1.0, SF 1.1, SF 1.2 and SF 1.3:

— monitoring of the relay contactor, K1, by PLC A through the position of K1 contacts;

- cross-monitoring between PLC A and PLC B;
- indirect monitoring of T1a and PLC A by PLC B through G2;
- indirect monitoring of the PLC A output card by itself through 1S2, 2S2, 3S1 and G1;
- program sequence monitoring by an internal watchdog in PLC A and in PLC B;
- indirect monitoring of T1a by PLC A through G1;
- monitoring of T1b by PLC A through the position of pulse-blocking relay contact;
- indirect monitoring of the PLC B by PLC A through the position of K1 contacts;
- indirect monitoring of the PLC B output card by itself through 1S0;
- indirect monitoring of 1V1 by the PLC A through 1S2;
- indirect monitoring of 2V1 by the PLC A through 2S2;
- indirect monitoring of 3V1 by the PLC A through 3S1;
- indirect monitoring of 1V0 by the PLC B through 1S0;
- fault detection of PLC A, T1a and 1V1, 2V1 and 3V1 through process observation.

According to ISO 13849-1:2006, Annex E, these diagnostic measures provide a DC_{avg} result of medium (90 %) for the $SRP/CS_{L/O}$ of SF 1.0, SF 1.1, SF 1.2 and SF 1.3.

d) **Estimation of measures against common-cause failure (CCF)**

It is estimated that adequate measures against common-cause failure (separation, diversity, protection against over-pressure, environmental) have been taken for both SRP/CS of SF 1.0, SF 1.1, SF 1.2 and SF 1.3, which, according to ISO 13849-1:2006, Annex F, results in a score of 75 points for each SRP/CS.

e) **Determination of PL for each SRP/CS**

The PL for each SRP/CS is determined as follows:

- SRP/CS_I of SF 1.0, SF 1.1, SF 1.2 and SF 1.3:
  - Category 3;
  - medium $MTTF_d$ of each channel;
  - high DC_{avg};
  - 75 points for measures against CCF.

Applying these values to ISO 13849-1:2006, Figure 5, but with DC_{avg} restricted to medium (Category 3), gives a result of PL d.

- $SRP/CS_{L/O}$ of SF 1.0, SF 1.1, SF 1.2 and SF 1.3:
  - Category 3;
  - medium $MTTF_d$ of each channel;
  - medium DC_{avg};
  - 75 points for measures against CCF.

Applying these values to ISO 13849-1:2006, Figure 5, gives a result of PL d.

f) **Determination of the PL for the combination of SRP/CS performing SF 1.0, SF 1.1, SF 1.2 and SF 1.3**

According to ISO 13849-1:2006, 6.3, and taking into account that the individual SRP/CS for SF 1.0, SF 1.1, SF 1.2 and SF 1.3 have the same values of PL, the PL of the overall combination of SRP/CS for SF 1.0, SF 1.1, SF 1.2 and SF 1.3 is determined as follows:

— PL_{low} = d

— N_{low} = 2

The PL for the combination of SRP/CS for each of SF 1.0, SF 1.1, SF 1.2 and SF 1.3 is therefore PL d.

NOTE Calculation of the resulting PL by adding the PFH values of all subsystems will lead to a more precise result.

g) **Systematic failures**

It is estimated that the adequate measures against systematic failure have been applied to the SRP/CS for SF 1.0, SF 1.1, SF 1.2 and SF 1.3 according to ISO 13849-1:2006, Annex G.

E.4.3 Safety function SF 2 — Safely-limited speed (SLS)

When the machine is in the set-up mode and the interlocking guard is in the open position, the rotary table can only move at a safely limited speed (SLS), which is measured by both G1 and G2. PLC A monitors the signal from G1 and PLC B monitors the signal from G2, with both PLCs performing the desired/actual speed comparisons independently. If the speed is not successfully reduced to the limited value by the inverter T1a, then PLC A can react by providing a stop signal to the inverter (T1a), and PLC B can react by activating a delayed pulse-blocking on the inverter (T1b) via K1.

a) **Identification of safety-related parts**

The safety-related parts of safety function SF 2 and its division into channels can be illustrated by the safety-related block diagram shown in Figure E.8.

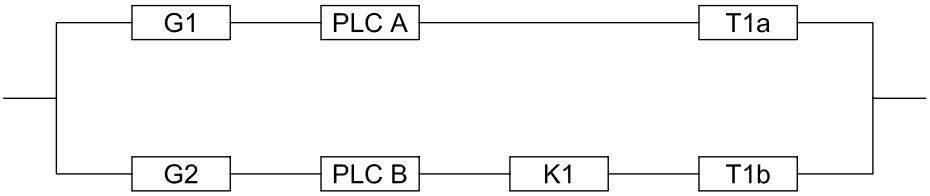


Figure E.8 — Safety-related block diagram — SF 2

For the SRP/CS, a PL has been estimated by applying the simplified procedure in ISO 13849-1:2006, 4.5.4.

The diagram can be mapped to the designated architecture for Category 3, so the safety function is performed by one SRP/CS, as shown in Figure E.9.

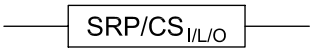


Figure E.9 — SRP/CS performing the safety function SF 2

For the SRP/CS, a PL has been estimated by applying the simplified procedure in ISO 13849-1:2006, 4.5.4.

b) **Estimation of MTTFd of each channel**

For the estimation of component $MTTF_d$ values, reliability data provided by the manufacturers has been used.

For the estimation of the $MTTF_d$ of a channel, the parts count method has been applied (see ISO 13849-1:2006; Annex D). The diverse redundant structure leads to dissimilar $MTTF_d$ values for each channel, so application of the symmetrisation equation provides an average result of medium $MTTF_d$ (more than 25 years) for each channel of the SRP/CS.

c) **Estimation of DC_{avg}**

The DC_{avg} has been calculated for the SRP/CS from the DC of the internal test and monitoring measures applied to the different components.

The following diagnostic measures are provided:

— monitoring of the relay contactor, K1, by PLC A through the position of K1 contacts;

— cross-monitoring between PLC A and PLC B;

— indirect monitoring of G1, T1a and PLC A by PLC B through G2;

— monitoring of T1b by PLC A through the position of pulse-blocking relay contact;

— program sequence monitoring by an internal watchdog in PLC A and in PLC B;

— indirect monitoring of G2 and PLC B by PLC A through the position of K1 contacts;

— monitoring of G1 by PLC A;

— monitoring of G1 and T1a (plausibility of sin/cos information);

— monitoring of G2 by PLC B (after pushing S4, PLC B checks for pulses from G2; if there are none, PLC B stops T1b).

According to ISO 13849-1:2006, Annex E, these diagnostic measures provide a DC_{avg} result of medium (90 %) for the SRP/CS.

d) **Estimation of measures against common-cause failure (CCF)**

It is estimated that the adequate measures against common-cause failure (separation, diversity, protection against over-pressure, environmental) have been taken for the SRP/CS, which according to ISO 13849-1:2006, Annex F, results in a score of 75 points for the SRP/CS.

e) **Determination of the PL for the SRP/CS**

The PL for the SRP/CS is determined as follows:

— Category 3;

— medium $MTTF_d$ of each channel;

— medium DC_{avg};

— 75 points for measures against CCF.

Applying these values to ISO 13849-1:2006, Figure 5, but with DC_{avg} restricted to medium (Category 3), gives a result of PL d.

f) **Systematic failures**

It is estimated that adequate measures against systematic failures have been applied to the SRP/CS according to ISO 13849-1:2006, Annex G.

E.4.4 Safety function SF 3 — Hold-to-run mode

Movement of the rotary table (at a safely limited speed) with the interlocking guard open is initiated and continues while the push-button S4 is actuated, and stops when the push-button is released. When the push-button is in the released position, unexpected start-up has to be prevented. The signal from the push-button S4 is processed by both PLCs.

a) **Identification of safety-related parts**

The safety-related parts of safety function SF 3 and their division into channels can be illustrated by the safety-related block diagram shown in Figure E.10.

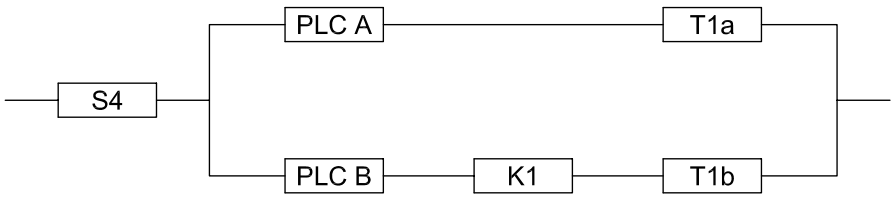


Figure E.10 — Safety-related block diagram — SF 3

The two parts of the diagram can each be mapped to the designated architecture for Category 1 and Category 3, so the diagram can be simplified as the two SRP/CS (input, logic/output) shown in Figure E.11.

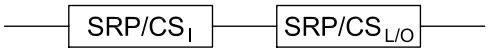


Figure E.11 — Combination of SRP/CS performing the safety function SF 3

For each SRP/CS, a PL has been estimated by applying the simplified procedure in ISO 13849-1:2006, 4.5.4.

b) **Estimation of $MTTF_d$ of each channel**

The $MTTF_d$ for the SRP/CS_I (hold-to-run push-button) is calculated using the manufacturer's B_{10d} value to give a result of high $MTTF_d$.

The estimation of the $MTTF_d$ of $SRP/CS_{L/O}$ provides, as in $SRP/CS_{L/O}$ of SF 1.0, an average result of 25 years (medium) for the $MTTF_d$ (more than 25 years) of each channel.

c) **Estimation of DC_{avg}**

The DC_{avg} has been calculated for both SRP/CS from the DC of the internal test and monitoring measures executed on the different components.

Time monitoring of hold-to-run push-button S4 (low-high alternation in a time frame window) by PLC A and PLC B according to ISO 13849-1:2006, Annex E, results in a DC_{avg} low (75 %) for the SRP/CS_I.

The monitoring measures as per $SRP/CS_{L/O}$ of SF 1.0 are provided in the $SRP/CS_{L/O}$ of SF 3, resulting in a DC_{avg} medium (90 %) for the $SRP/CS_{L/O}$.

d) **Estimation of measures against common-cause failure (CCF)**

It is estimated that adequate measures against common-cause failure (separation, diversity, protection against over-voltage, environmental) have been taken for each SRP/CS, which, according to ISO 13849-1:2006, Annex F, results in a score of 75 points for both SRP/CS.

e) **Determination of PL for each SRP/CS**

The PL for each SRP/CS is determined as follows.

— SRP/CS_I:

  — Category 1;

  — High $MTTF_d$ of the channel.

Applying these values to ISO 13849-1:2006, Figure 5, gives a result of PL c.

— $SRP/CS_{L/O}$:

  — Category 3;

  — Medium $MTTF_d$ of each channel;

  — Medium DC_{avg};

  — 75 points for measures against CCF.

Applying these values to ISO 13849-1:2006, Figure 5, gives a result of PL d.

f) **Determination of the PL of the combination of SRP/CS performing SF 3**

According to ISO 13849-1:2006, 6.3, and taking into account both SRP/CS of SF 3, the PL of the overall combination of SRP/CS is determined as follows:

— PL_{low} = c;

— N_{low} = 1.

The PL for the combination of SRP/CS of SF 3 is therefore PL c.

g) **Systematic failures**

It is estimated that the adequate measures against systematic failures have been taken for both SRP/CS of SF 3 according to ISO 13849-1:2006, Annex G.

E.5 Validation

E.5.1 General

As stated in E.1, the example has been reduced to the validation of fault behaviour and diagnostic means of safety functions SF 1.0 and SF 1.3.

According to 9.2 and 9.3, validation of fault behaviour and diagnostic means are performed by a review of design documentation, a failure analysis and complementary fault injection tests.

The following steps are carried out.

a) Identify the diagnostic measures and the units (components, blocks) that they test/monitor.

b) Verify the DC value assigned to each diagnostic measure (DC) for a particular unit.

c) Analyse the fault behaviour of the system and define the test cases.

d) Check for correct calculation of the DC_{avg} for each SRP/CS.

e) Carry out required tests to confirm the DC values.

E.5.2 Validation of fault behaviour and DC_{avg}

A check of the design documentation (safety-related block diagram and list of diagnostic measures for the SRP/CS) confirms that

— blocks (components) related to each SRP/CS and the combination of SRP/CS, in the safety-related block diagrams, and

— diagnostic measures and monitored units

assumed in the design rationale are correct for all safety functions.

A FMEA is used to check the values of DC assigned to each monitored unit of each SRP/CS, and also the fault behaviour of the system.

As safety function SF 1 has to fulfil both safety-related stopping and subsequent prevention of unexpected start-up, the failure analysis for each associated component is considered in a separate row for each of these requirements.

For the analysis, the appropriate fault lists given in Annexes A, B, C and D have been used.

The FMEA for safety functions SF 1.0 and SF 1.3, including test cases, are now considered.

E.5.3 FMEA and DC_{avg} for SF 1.0 and SF 1.3

E.5.3.1 SF 1.0

In order to facilitate the analysis of SF 1.0, its safety-related block diagram is reproduced in Figure E.12.

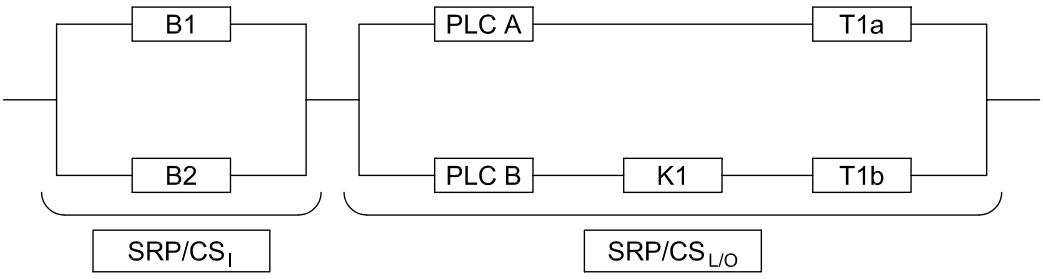


Figure E.12 — Safety-related block diagram — SF 1.0

See Tables E.3 and E.4.

Table E.3 — FMEA and estimation of DC for components of SRP/CS_I of SF 1.0

	Component/ unit	Potential fault	Fault detection	Effect/reaction	Tests for confirmation
F1	Interlocking switch B1	Contact does not open when the guard is opened (mechanical faults).[a]	Fault is recognized independently by PLC A and PLC B through signal change in B2 when the safety function is demanded (opening of the safety guard, plausibility check).	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs before the guard is opened.
F2		No dangerous fault while the guard is open (fault exclusion).	—	—	—
A plausibility check of B1 and B2 by PLC A and PLC B gives a DC of 99 % for B1 (see ISO 13849-1:2006, Table E.1).					
F3	Interlocking switch B2	Contact does not open when the guard is opened (electrical or mechanical faults)	Fault is recognized independently by PLC A and PLC B through signal change in B1 when the safety function is demanded (opening of the safety guard, plausibility check).	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs before the guard is opened.
F4		Spontaneous contact closure while the guard is open (mechanical faults).	Fault is recognized independently and immediately by PLC A and PLC B as a result of there being no corresponding signal change in B1.	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs while the guard is open.
A plausibility check of B1 and B2 by PLC A and PLC B gives a DC of 99 % for B2 (see ISO 13849-1:2006, Table E.1).					
NOTE Conductors are not included in the fault analysis because it is considered that they only fail due to systematic causes.					
[a] Electrical faults can be excluded because B1 posses a direct mode of actuation (see IEC 60947-5-1:2003, Annex K).					

From the analysis it can be deduced that any single faults in the SRP/CS_I will be detected either immediately, or at the next demand upon the safety function. When a single fault occurs, the safety function is always performed and re-start is prevented.

As a result of the analysis, it is considered that the assumed values of DC (high) during the design for B1 and B2 are adequate. As the DC of both components is equal (99 %), the DC_{avg} of SRP/CS_I is high (99 %), as was estimated during the design.

These characteristics are typical for Category 3, selected in the design (see E.4.1) in order to comply with the safety requirement specification given in E.3 (PL_r).

In order to check the correct implementation of the diagnostic measures, the tests described in the final column of Table E.3 could be applied.

Table E.4 — FMEA and estimation of DC of components for SRP/$CS_{L/O}$ of SF 1.0

	Component/ unit	Potential faults	Fault detection	Effect/reaction	Tests for confirmation
F1	PLC A	Stuck-at-fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which prevents PLC A from sending a stop command to T1a before or when the guard is opened.	Fault is recognized by PLC B through reading of G2 to compare its time-related signal with the expected change in the number of revolutions. Some faults (e.g. output cards) are recognized by PLC A through reading of G1 at an operational stop of the electric motor M1 or when the safety function is demanded. Other faults can be detected early by the internal watchdog (WD[a]) function of PLC A.	Electric motor M1 is stopped by PLC B via K1 and T1b after a time delay when the guard is opened, and re-start is prevented. In the case of faults detected by PLC A through reading of G1 during the operational stop, PLC A informs PLC B. As a result of reporting PLC B, the electric motor M1 is stopped and re-start is prevented by PLC B. In the case of faults detected by WD, PLC A tries to stop electric motor M1 and prevent the re-start via T1a before the safety function is demanded or before electrical motor M1 comes to an operational stop, and then to inform PLC B.	Apply a static high level at the stop output of PLC A before the guard is open.
F2		Stuck-at-fault at the input/ output cards, or stuck-at or wrong coding or no execution in the CPU, which removes the PLC A stop command from T1a while the guard is open.	Faults cannot be recognized by PLC B through reading of G2 because the motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. Some faults (e.g. output cards) are recognized by PLC A through reading of G1 on closing the guard. The above and additional faults are detected by operator through process observation on closing the guard, or by PLC B when the safety function is next demanded (opening of the guard). Other faults can be detected early by WD[a] function of PLC A.	Electric motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. In the case of faults detected by PLC A through reading of G1 on closing the guard, PLC A informs PLC B. As a result of reporting PLC B, the unintended start-up of electric motor M1 is prevented by PLC B. In the case of faults detected by WD, PLC A tries to keep electric motor M1 stopped and to prevent the re-start via T1a, and to inform PLC B.	Transfer the start signal to the inverter while the guard is open.

[a] Some internal faults of PLCs that, *a priori*, do not cause a failure of the safety function (e.g. inability of PLCs to send a stop command to the drive or to a valve, or inability to keep a stop command on the drive or on a valve) can be detected by the WD function.

Table E.4 *(continued)*

	Component/ unit	Potential faults	Fault detection	Effect/reaction	Tests for confirmation
As a result of the indirect monitoring of PLC A by PLC B through G2, PLC A's indirect monitoring of its own output card through G1, program sequence monitoring by the internal watchdog, and fault detection through process observation, PLC A is considered to have a DC of 90 % (see ISO 13849-1:2006, Table E.1). The above measures can be considered as being in relation to ISO 13849-1:2006, Table E.1, NOTE 2.					
NOTE It is considered that most PLC faults occur at the input/output cards and are of the stuck-at type (90 % of all faults in a PLC), but the WD function of a PLC can only detect some faults that affect program sequencing.					
F3	Inverter T1a	Stuck-at-fault and other complex internal faults in control and power electronics of the inverter, which prevent T1a from stopping the motor before or when the guard is opened.	Fault is recognized by PLC B through reading of G2 when the safety function is demanded. Fault is recognized also by PLC A through reading of G1 at an operational stop of the electric motor M1 or when the safety function is demanded.	Electric motor M1 is stopped by PLC B via K1 and T1b after a time delay when the guard is opened, and re-start is prevented. PLC A informs PLC B when a fault is recognized during the operational stop. As a result of reporting PLC B, the electric motor M1 is stopped and re-start is prevented by PLC B.	Set the stop-input of the inverter to high before or when the guard is opened.
F4		Stuck-at-fault and other complex internal faults in control and power electronics of the inverter, which provides gate signals to power semiconductors of T1a, while the guard is open.	Fault cannot be recognized by PLC B through reading of G2 because the motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. Fault will be detected by the operator through process observation on closing the guard. Fault is also recognized by PLC A through reading of G1 on closing the guard.	Electric motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. On closing the guard, an unintended start-up of the motor occurs (non-hazardous). PLC A informs PLC B when a fault is recognized. As a result of reporting PLC B, the unintended start-up of electric motor M1 is prevented and re-start is prevented by PLC B.	Transfer the start signal to the inverter while the guard is open.
As a result of the indirect monitoring of T1a by PLC B through G2, indirect monitoring of T1a by PLC A through G1 and fault detection through process observation, T1a is considered to have a DC of 99 %.					
[a] Some internal faults of PLCs that, *a priori*, do not cause a failure of the safety function (e.g. inability of PLCs to send a stop command to the drive or to a valve, or inability to keep a stop command on the drive or on a valve) can be detected by the WD function.					

Table E.4 *(continued)*

	Component/ unit	Potential faults	Fault detection	Effect/reaction	Tests for confirmation
F5	PLC B	Stuck-at-fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which prevents PLC B from switching off K1 before or when the guard is opened.	Fault is recognized by PLC A monitoring of K1 mechanically linked feedback contact when the safety function is demanded. Some faults can be detected early by the WD[a] function of PLC B.	Electric motor M1 is immediately stopped by PLC A via T1a when the guard is opened and re-start is prevented. In the case of faults detected by WD, PLC B tries to inform PLC A and then to stop the electric motor M1 and prevent the re-start via T1b before the safety function is demanded.	Keep K1 in the energized position when the guard is opened.
F6		Stuck-at-fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which removes the PLC B stop command from K1 while the guard is open.	Fault is immediately recognized by PLC A monitoring of K1 mechanically linked feedback contact. Some faults can be detected early by the WD[a] function of PLC B.	Electric motor M1 is kept stopped by PLC A via T1a while the guard is open, and re-start is prevented. In the case of faults detected by WD, PLC B tries to keep stopped the electric motor M1 and prevent the re-start via T1b, and to inform PLC A.	Switch K1 to its energized position while the guard is open.
As a result of the indirect monitoring of PLC B by PLC A through the position of K1 feedback contact and program sequence monitoring by the internal watchdog, PLC B is considered to have a DC of 90 %.					
NOTE It is considered that most PLC faults occur at input/output cards and are of the stuck-at type (90 % of all faults in a PLC), but the WD function of a PLC can only detect some faults that affect program sequencing.					
F7	Relay contactor K1	The contact does not open when the guard is opened (electrical fault, e.g. welded contacts).	Fault is recognized by PLC A monitoring of K1 mechanically linked feedback contact when the safety function is demanded.	Electric motor M1 is immediately stopped by PLC A via T1a when the guard is opened and re-start is prevented.	Keep K1 contact in the ON position when the guard is opened.
F8		No dangerous fault while the guard is open (fault exclusion).	—	—	—
Monitoring of relay contactor K1 by PLC A through the position of K1 mechanically linked feedback contact gives a DC of 99 % for K1.					
[a] Some internal faults of PLCs that, *a priori*, do not cause a failure of the safety function (e.g. inability of PLCs to send a stop command to the drive or to a valve, or inability to keep a stop command on the drive or on a valve) can be detected by the WD function.					

Table E.4 *(continued)*

	Component/ unit	Potential faults	Fault detection	Effect/reaction	Tests for confirmation
F9	Inverter T1b	Non-opening of internal relay contact when the guard is opened.	Fault is recognized by PLC A monitoring of mechanically linked feedback contact for T1b internal relay when the safety function is demanded.	Electric motor M1 is immediately stopped by PLC A via T1a when the guard is opened and re-start is prevented.	Keep the input of the coil of the blocking relay in T1b to high level when the guard is opened.
F10		No dangerous fault while the guard is open (fault exclusion).	—	—	—
Monitoring of the T1b internal (pulse-blocking) relay by PLC A gives a DC of 99 % for T1b.					
[a] Some internal faults of PLCs that, *a priori*, do not cause a failure of the safety function (e.g. inability of PLCs to send a stop command to the drive or to a valve, or inability to keep a stop command on the drive or on a valve) can be detected by the WD function.					

From the analysis, it can be deduced that single faults in the SRP/CS will be detected either immediately, or at an operational stop of electric motor M1, or at the next demand upon the safety function. When a single fault occurs, the safety function is always performed. Re-start is possible with only one channel in the case of undetected faults in PLC A and PLC B.

The analysis determines that values of DC assumed during the design of the $SRP/CS_{L/O}$ are adequate. Taking into account the estimated $MTTF_d$ values and the DC values for the various components used in $SRP/CS_{L/O}$, a DC_{avg} result of medium (90 %) is achieved, as was estimated during the design.

These characteristics are typical for Category 3, selected in the design (see E.4.1) in order to comply with the safety requirement specification given in E.3 (PL_r).

To check the correct implementation of the diagnostic measures, the tests described in the final column of Table E.4 could be applied.

E.5.3.2 SF 1.3

In order to facilitate the analysis of SF 1.3, its safety-related block diagram is reproduced in Figure E.13.

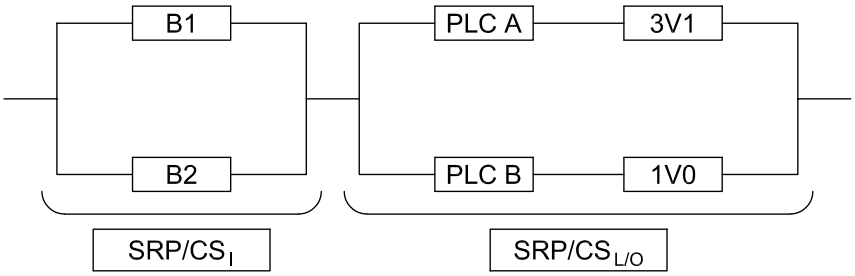


Figure E.13 — Safety-related block diagram for SF 1.3

For SRP/CS_I of SF 1.3, the diagnostic measures and the tested/monitored units are identical to those for SF 1.0 and therefore the DC_{avg} of SRP/CS_I is also high (99 %).

See Table E.5.

Table E.5 — FMEA of SRP/$CS_{L/O}$ of SF 1.3

	Component/ unit	Potential faults/ failure	Fault detection	Effect/reaction	Tests for confirmation
F1	PLC A	Stuck-at-fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which prevents PLC A from switching off 3V1 before or when the guard is opened.	Some faults (e.g. output cards) are recognized by PLC A through reading of pressure sensor 3S1 at an operational stop of the pneumatic motor A3 or when the safety function is demanded. Other faults can be detected early by the WD[a] function of PLC A.	Pneumatic motor A3 is stopped by PLC B via 1V0 after a time delay when the guard is opened. In the case of faults detected by PLC A through reading of 3S1 during the operational stop, PLC A informs PLC B. As a result of reporting PLC B, the pneumatic motor A3 is stopped via 3V1 and re-start is prevented by PLC B. For faults detected by the WD, PLC A tries to stop the pneumatic motor A3 and to prevent the re-start via 3V1 before the safety function is demanded or before the pneumatic motor A3 comes to an operational stop and then to inform PLC B.	Apply a static high level at the 3V1 output of PLC A before the guard is opened.
F2		Stuck-at-fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which causes PLC A to switch on 3V1 while the guard is open.	Some faults (e.g. output cards) are recognized by PLC A through reading of pressure sensor 3S1 on closing the guard. Other faults can be detected early by the WD[a] function of the PLC A.	Pneumatic motor A3 is kept stopped by PLC B via 1V0 while the guard is open. On closing the guard, PLC B energizes 1V0 and pneumatic motor A3 will restart-up (non hazardous). In the case of faults detected by PLC A through reading of 3S1 on closing the guard, PLC A informs PLC B. As a result of reporting PLC B, the unintended start-up of pneumatic motor A3 is prevented and re-start is prevented by PLC B. For faults detected by the WD, PLC A tries to keep stopped the pneumatic motor A3 and to prevent the re-start via 3V1, and to inform PLC B.	Change the 3V1 output of PLC A to a high level while the guard is open.

Table E.5 *(continued)*

	Component/ unit	Potential faults/ failure	Fault detection	Effect/reaction	Tests for confirmation
As a result of PLC A's indirect monitoring of its own output card through 3S1 and program sequence monitoring by the internal watchdog, PLC A is considered to have a DC of 90 %.					
NOTE It is considered that most PLC faults occur at input/output cards and are of the stuck-at type (90 % of all faults in a PLC), but the WD function of a PLC can only detect some faults that affect to program sequencing.					
F3	Directional-control solenoid valve 3V1	Non-switching (sticking at the end position) or incomplete switching (sticking at a random intermediate position) or change of switching times, before or when the guard is opened.	Fault is recognized by PLC A through reading of pressure sensor 3S1 at an operational stop of the pneumatic motor A3 or when the safety function is demanded. Faults are also detected by the operator through process observation.	Pneumatic motor A3 is stopped by PLC B via 1V0 after a time delay when the guard is opened. PLC A informs PLC B when a fault is recognized. As a result of this reporting, PLC B stops via 1V0 the pneumatic motor A3 and any re-start is prevented.	Keep the electrical and pneumatic control signals for 3V1 at a high level as the guard is opened.
F4		Spontaneous change of the initial switching position (without an input signal) while the guard is open. NOTE This fault can be excluded because 3V1 has well-tried springs, and normal installation and operating conditions are applied.	—	—	—
As a result of indirect monitoring of 3V1 by PLC A through 3S1 and fault detection through process observation, 3V1 is considered to have a DC of 99 %.					

Table E.5 *(continued)*

	Component/ unit	Potential faults/ failure	Fault detection	Effect/reaction	Tests for confirmation
F5	PLC B	Stuck-at-fault at the input/output cards, or stuck-at or wrong coding or no execution in the CPU, which prevents PLC B from switching off 1V0 before or when the guard is opened.	Some faults (e.g. output cards) are recognized by PLC B through reading the pressure switch 1S0 when the safety function is demanded. Others can be detected early by WD[a] function of PLC B.	Pneumatic motor A3 is immediately stopped by PLC A via 3V1 when the guard is opened. In the case of faults detected by PLC B through reading the pressure switch 1S0, PLC B informs PLC A and keeps K1 deactivated. As a result of reporting, PLC A prevents the re-start. For faults detected by the WD, PLC B tries to inform PLC A and then to stop the pneumatic motor A3 via 1V0 and to prevent the re-start before the safety function is demanded.	Apply a static high level at the 1V0 output of PLC B before the guard is opened.
F6		Stuck-at-fault at the input/output cards, or stuck-at or wrong coding or no execution at the CPU, which causes PLC B to switch on 1V0 while the guard is open.	Some faults (e.g. output cards) are immediately recognized by PLC B through reading the pressure switch 1S0. Others can be detected early by WD[a] function of PLC B.	Pneumatic motor A3 is kept stopped by PLC A via 3V1 while the guard is open. In the case of faults detected by PLC B through reading the pressure switch 1S0, PLC B informs PLC A and keeps K1 deactivated. As a result of reporting, PLC A prevents the re-start. In the case of faults detected by WD, PLC B tries to inform PLC A and then to keep stopped the pneumatic motor A3 via 1V0 and prevent the re-start.	Change the 1V0 output of PLC B to a high level while the guard is open.
As a result of the indirect monitoring by PLC B of its own output card through 1S0, indirect monitoring of PLC B by PLC A through the position of K1 feedback contact and program sequence monitoring by the internal watchdog, PLC B is considered to have a DC of 90 %.					
NOTE It is considered that most PLC faults occur at input/output cards and are of the stuck-at type (90 % of all faults in a PLC), but the WD function of a PLC can only detect some faults that affect program sequencing.					

Table E.5 *(continued)*

	Component/ unit	Potential faults/ failure	Fault detection	Effect/reaction	Tests for confirmation
F7	Directional-control solenoid valve 1V0	Non-switching (sticking at the end position) or incomplete switching (sticking at a random intermediate position) or change of switching times, before or when the guard is opened.	Fault is recognized by PLC B through reading of pressure switch 1S0 when the safety function is demanded.	Pneumatic motor A3 is immediately stopped by PLC A via 3V1 when the guard is opened. In the case of faults detected by PLC B through reading the pressure switch 1S0, PLC B informs PLC A and keeps K1 de-energized. As a result of reporting, PLC A prevents the re-start.	Apply a static high level at the 1V0 output of PLC B before the guard is opened.
F8	Magnetic valve 1V0	Spontaneous change of the initial switching position (without an input signal) while the guard is open. NOTE This fault can be excluded because 1V0 possesses well-tried springs and normal installation and operating conditions are applied.	—	—	—
Indirect monitoring of 1V0 by PLC B through 1S0 gives a DC of 99 % for 1V0.					
a Some internal faults of PLCs that, *a priori*, do not cause a failure of the safety function (e.g. inability of PLCs to send a stop command to the drive or to a valve, or inability to keep a stop command on the drive or on a valve) can be detected by the WD function.					

From the analysis, it can be deduced that most single faults in the SRP/CS will be detected either immediately, or at an operational stop of the pneumatic motor, A3, or at the next demand upon the safety function. When a single fault occurs, the safety function is always performed. Re-start is possible with only one channel in the case of undetected faults in PLC A and PLC B.

The analysis determines that values of DC assumed during the design of the $SRP/CS_{L/O}$ are adequate. Taking into account the estimated $MTTF_d$ values and the DC values for the various components used in $SRP/CS_{L/O}$, a DC_{avg} result of medium (90 %) is achieved, as was estimated during the design.

These characteristics are typical for Category 3, selected in the design (see E.4.1) in order to comply with the safety requirement specification given in E.3 (PL_r).

To check the correct implementation of the diagnostic measures, the tests described in the final column of Table E.5 could be applied.

Bibliography

[1] ISO 4079-1, *Rubber hoses and hose assemblies — Textile-reinforced hydraulic types — Specification — Part 1: Oil-based fluid applications*

[2] ISO 4413:2010, *Hydraulic fluid power — General rules and safety requirements for systems and their components*

[3] ISO 4414:2010, *Pneumatic fluid power — General rules and safety requirements for systems and their components*

[4] ISO 4960, *Cold-reduced carbon steel strip with a mass fraction of carbon over 0,25 %*

[5] ISO 5598:2008, *Fluid power systems and components — Vocabulary*

[6] ISO 11161, *Safety of machinery — Integrated manufacturing systems — Basic requirements*

[7] ISO 13850, *Safety of machinery — Emergency stop — Principles for design*

[8] ISO 13851, *Safety of machinery — Two-hand control devices — Functional aspects and design principles*

[9] ISO 13855, *Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body*

[10] ISO 13856 (all parts), *Safety of machinery — Pressure-sensitive protective devices*

[11] ISO 14118:2000, *Safety of machinery — Prevention of unexpected start-up*

[12] ISO 14119:1998, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

[13] IEC 60204-1:2005, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[14] IEC 60269-1, *Low-voltage fuses — Part 1: General requirements*

[15] IEC 60529, *Degrees of protection provided by enclosures (IP code)*

[16] IEC 60664 (all parts), *Insulation coordination for equipment within low-voltage systems*

[17] IEC 60812, *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[18] IEC 60893-1, *Insulating materials — Industrial rigid laminated sheets based on thermosetting resins for electrical purposes — Part 1: Definitions, designations and general requirements*

[19] IEC 60947 (all parts), *Low-voltage switchgear and controlgear*

[20] IEC 61025, *Fault tree analysis (FTA)*

[21] IEC 61078, *Analysis techniques for dependability — Reliability block diagram and boolean methods*

[22] IEC 61131-1, *Programmable controllers — Part 1: General information*

[23] IEC 61131-2, *Programmable controllers — Part 2: Equipment requirements and tests*

[24] IEC 61165, *Application of Markov techniques*

[25] IEC 61249 (all parts), *Materials for printed boards and other interconnecting structures*

[26] IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[27] IEC 61558 (all parts), *Safety of power transformers, power supplies, reactors and similar products*

[28] IEC 61800-5-2, *Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional*

[29] IEC 61810 (all parts), *Electromechanical elementary relays*

[30] EN 952:1996, *Safety of machinery — Safety requirements for fluid power systems and their components — Hydraulics*

[31] EN 953:1996, *Safety of machinery — Safety requirements for fluid power systems and their components — Pneumatics*

[32] EN 50205, *Relays with forcibly guided (mechanically linked) contacts*

[33] EN 60730 (all parts), *Automatic electric controls for household and similar use*

[34] JESD22A121.01,*Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes*[1)]

[35] JESD201, *Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Alloy Surface Finishes*[1)]

1) JEDEC Solid State Technology Association, 2500 Wilson Boulevard, Arlington, VA 22201-3834, www.jedec.org/download/search/22a1121-01.pdf

ICS 13.110

Price based on 79 pages