INTERNATIONAL STANDARD

ISO 13849-2

First edition
2003-08-15

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

Part 2: Validation

Sécurité des machines — Parties des systèmes de commande relatifs à la sécurité —

Partie 2: Validation

Reference number
ISO 13849-2:2003(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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 the European Committee for Standardization (CEN) in collaboration with Technical Committee ISO/TC 199, *Safety of machinery*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Throughout the text of this document, read "...this European Standard..." to mean "...this International Standard...".

ISO 13849 consists of the following parts, under the general title *Safety of machinery — Safety-related parts of control systems*:

— *Part 1: General principles for design*

— *Part 2: Validation*

— *Part 100: Guidelines for the use and application of ISO 13849-1*

Contents

Page

Foreword

This document EN ISO 13849-2:2003 has been prepared by Technical Committee CEN /TC 114, "Safety of machinery", the secretariat of which is held by DIN in collaboration with Technical Committee ISO/TC 199 "Safety of machinery".

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2004, and conflicting national standards shall be withdrawn at the latest by February 2004.

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

Annexes A to D are informative and structured as given in Table 1.

Table 1 — Structure of the clauses of annexes A to D

Annex	Technology	List of basic safety principles	List of well-tried safety principles	List of well-tried components	Fault lists and fault exclusions
		Clause			
A	Mechanical	A.2	A.3	A.4	A.5
B	Pneumatic	B.2	B.3	B.4	B.5
C	Hydraulic	C.2	C.3	C.4	C.5
D	Electrical (includes electronics)	D.2	D.3	D.4	D.5

This document includes a Bibliography.

EN ISO 13849 consists of the following parts, under the general title "Safety of machinery – Safety-related parts of control systems":

Part 1: General principles for design

Part 2: Validation

Part 100: Guidelines for the use and application of EN ISO 13849-1.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and the United Kingdom.

Introduction

For the use in the European Union, this part of EN ISO 13849 has the status of a generic safety standard (type B1).

This European Standard specifies the validation process, including both analysis and testing, for the safety functions and categories for the safety–related parts of control systems. Descriptions of the safety functions and the requirements for the categories are given in EN 954-1 (ISO 13849-1) which deals with the general principles for design. Some requirements for validation are general and some are specific to the technology used. EN ISO 13849-2 also specifies the conditions under which the validation by testing of the safety-related parts of control systems should be carried out.

EN 954-1 (ISO 13849-1) specifies the safety requirements and gives guidance on the principles for the design [see EN 292-1:1991 (ISO/TR 12100:1992), 3.11] of the safety-related parts of control systems. For these parts it specifies categories and describes the characteristics of their safety functions, regardless of the type of energy used. Additional advice on EN 954-1 (ISO 13894-1) is given in CR 954-100 (ISO/TR 13849-100).

The achievement of the requirements can be validated by any combination of analysis (see clause 4) and testing (see clause 5). The analysis should be started as early as possible within the design process.

1 Scope

This European Standard specifies the procedures and conditions to be followed for the validation by analysis and testing of:

— the safety functions provided, and

— the category achieved

of the safety-related parts of the control system in compliance with EN 954-1 (ISO 13849-1), using the design rationale provided by the designer.

This European Standard does not give complete validation requirements for programmable electronic systems and therefore can require the use of other standards.

NOTE CEN/TC 114/WG 6 proposes to deal in more detail with the validation of programmable electronic systems in the elaboration of the revision to EN 954-1 (ISO 13849-1). An application standard for machinery (draft IEC 62061), based on IEC 61508, is under preparation. Requirements for programmable electronic systems, including embedded software, are given in IEC 61508.

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text, and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

EN 292-1:1991 (ISO/TR 12100:1992), *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology.*

EN 954-1:1996 (ISO 13849-1:1999), *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.*

3 Validation process

3.1 Validation principles

The purpose of the validation process is to confirm the specification and the conformity of the design of the safety-related parts of the control system within the overall safety requirements specification of the machinery.

The validation shall demonstrate that each safety-related part meets the requirements of EN 954-1 (ISO 13849-1), in particular:

— the specified safety characteristics of the safety functions provided by that part, as set out in the design rationale, and

— the requirements of the specified category [see EN 954-1:1996 (ISO 13849-1:1999), clause 6].

Validation should be carried out by persons who are independent of the design of the safety-related part(s).

NOTE Independent person does not necessarily mean that a 3rd party test is required.

The degree of independence should reflect the safety performance of the safety-related part.

Validation consists of applying analysis (see clause 4) and, if necessary, executing tests (see clause 5) in accordance with the validation plan. Figure 1 gives an overview of the validation process. The balance between the analysis and/or testing depends on the technology.

The analysis should be started as early as possible and in parallel with the design process, so that problems can be corrected early whilst they are still relatively easy to correct, i. e. during steps 3 and 4 of EN 954-1:1996 (ISO 13849-1:1999), 4.3. It can be necessary for some parts of the analysis to be delayed until the design is well developed.

For large systems, due to the size, complexity or integrated form (with the machinery) of the control system, special arrangements may be made for:

— validation of the safety-related parts of the control system separately before integration including simulation of the appropriate input and output signals;

— 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.

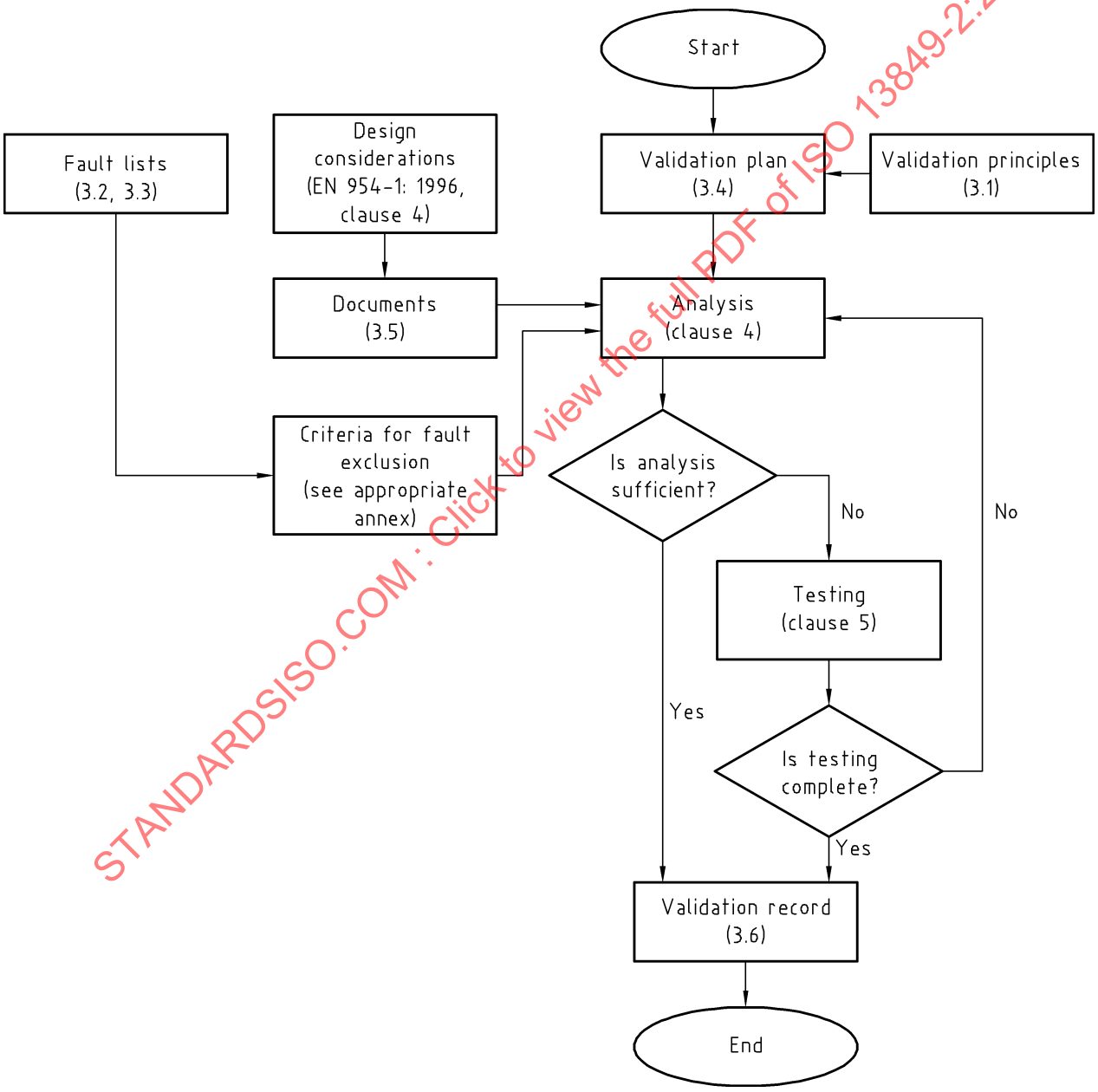

Figure 1 — Overview of the validation process

3.2 Generic fault lists

The validation process involves consideration of behaviour of the safety-related part(s) of the control system for all faults to be considered. A basis for fault consideration is given in the fault lists in the informative annexes (A.5, B.5, C.5 and D.5) which are based on experience. The generic fault lists contain:

— the components/elements to be included, e. g. conductors/cables (see D.5.2);

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

— the permitted fault exclusions;

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

Only permanent faults are taken into account.

3.3 Specific fault lists

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 annex(es).

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

— the faults taken from the generic list(s) to be included;

— any other relevant faults to be included but not given in the generic list (e. g. common mode faults);

— the faults taken from the generic list(s) which may be excluded and can meet at least the criteria given in the generic list(s) [see EN 954-1:1996 (ISO 13849-1:1999), 7.2];

and, exceptionally

— any other relevant faults, from the generic list but not permitted for exclusion by the generic list(s), together with a justification and a rationale for its exclusion [see EN 954-1:1996 (ISO 13849-1:1999), 7.2].

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

3.4 Validation plan

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

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

a) the identity of the specification documents;

b) the operational and environmental conditions;

c) the basic safety principles (see A.2, B.2, C.2 and D.2);

d) the well-tried safety principles (see A.3, B.3, C.3 and D.3);

e) the well-tried components (see A.4 and D.4);

f) the fault assumptions and fault exclusions to be considered e. g. from the informative fault lists in A.5, B.5, C.5 and D.5;

g) the analyses and tests to be applied.

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

3.5 Information for validation

The information required for validation will vary with the technology used, the category(ies) to be demonstrated, the design rationale of the system and the contribution of the safety-related parts of control systems to the reduction of the risk. Documents containing sufficient information from the list below shall be included in the validation process to demonstrate the category(ies) and the safety function(s) of the safety-related parts which have been achieved:

a) specification(s) of the expected performance, of the safety functions and categories;

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 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 other safety-related parts (excluding 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 for safety;

i) analysis of all relevant faults (see also 3.2) listed e. g. in A.5, B.5, C.5 and D.5, including the justification of any excluded faults;

j) an analysis of the influence of processed materials;

Category specific information in accordance with Table 2. Where software is relevant to the safety function(s), the software documentation shall include:

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

2) evidence that the software is designed to achieve the required safety performance, and

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

Table 2 — Documentation requirements for categories

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
The check procedure of the safety function(s)	–	–	x	–	–
Checking intervals, when specified	–	–	x	–	–
Foreseeable, single faults considered in the design and the detection method used	–	–	x	x	x
The common mode failures identified and how prevented	–	–	–	x	x
The foreseeable, single faults excluded	–	–	–	x	x
The faults to be detected	–	–	x	x	x
The variety of accumulations of faults considered in the design	–	–	–	–	x
How the safety function is maintained in the case of each of the fault(s)	–	–	–	x	x
How the safety function is maintained for each of the combination(s) of faults	–	–	–	–	x

NOTE The categories mentioned in Table 2 are those given in EN 954-1 (ISO 13849-1).

3.6 Validation record

Validation by analysis and testing shall be recorded. The record shall demonstrate the validation process of 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 part of the validation process, the validation record shall describe the part(s) of the validation tests and/or analysis which have been failed.

4 Validation by analysis

4.1 General

The validation of safety–related parts of control systems shall be carried out by analysis. Inputs to the analysis are:

— the hazards identified during analysis at the machine [see EN 954-1:1996 (ISO 13849-1:1999), Figure 1];

— the reliability [see EN 954-1:1996 (ISO 13849-1:1999), 4.2];

— the system structure [see EN 954-1:1996 (ISO 13849-1:1999), 4.2];

— the non–quantifiable, qualitative aspects which affect system behaviour [see EN 954-1:1996 (ISO 13849-1:1999), 4.2];

— deterministic arguments.

Validation of the safety functions by analysis rather than testing requires the formulation of deterministic arguments. 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, such as the correctness of a mechanical interlock.

NOTE A deterministic argument is an argument based on qualitative aspects (e. g. quality of manufacture, failure rates, experience of use). This consideration is depending on the application. This and other factors can affect the deterministic arguments.

4.2 Analysis techniques

The technique of analysis to be chosen depends upon the goal to be achieved. Two basic types of techniques exist:

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. Examples of top–down techniques are Fault Tree Analysis (FTA – see IEC 61025) and Event Tree Analysis (ETA);

b) Bottom–up (inductive) techniques are suitable for investigating the consequence of identified single faults. Examples of bottom–up techniques are Failure Modes and Effects Analysis (FMEA – see IEC 60812) and Failure Modes, Effects and Criticality Analysis (FMECA).

More information on analysis methods is given in EN 1050:1996 (ISO 14121:1999), annex B.

5 Validation by testing

5.1 General

When validation by analysis is not sufficient to demonstrate the achievement of specified safety functions and categories 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 prior to the starting of the test and shall include:

   1) the test specifications;

   2) the expected results of tests;

   3) the chronology of the tests.

b) Test records shall be produced that include the following:

   1) the name of the tester;

   2) the environmental conditions (see clause 8);

   3) the test procedures and equipment used;

   4) the results of the test.

c) The test records shall be compared with the test plan to give assurance 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.

Testing can be applied manually or automatically (e. g. by computer).

Where applied, validation of the safety functions by testing shall be carried out by applying inputs, in various combinations, to the safety–related part of the control system. The corresponding outputs shall be compared to the appropriate specified outputs.

It is recommended that the combination of these inputs 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 to see how the safety-related parts of the control system respond. Such combinations of input data shall take into account foreseeable incorrect operation(s).

The objectives of the test will be determined by the environmental conditions for that test. The conditions may be:

a) the environmental conditions of intended use, or

b) conditions at a particular rating, or

c) a given range of conditions if drift is expected.

NOTE 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.

5.2 Measurement uncertainty

The uncertainty of measurements during the validation by testing shall be appropriate to the test being carried out. In general, these measurement uncertainties 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 uncertainties shall be justified.

5.3 Higher requirements

If, according to the information in the accompanying documents the control system fulfils higher requirements than the requirements according to this standard, the higher requirements shall apply.

NOTE Such higher 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.

5.4 Number of test samples

Unless otherwise specified, the tests shall be made on a single production sample of the safety–related part(s) which should withstand all the relevant tests.

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

Some tests can permanently change the performance of some components. Where the permanent change in the components causes the safety–related part(s) to be outside its design specification a new sample(s) shall be used for subsequent tests.

Where a particular test is destructive and equivalent results can be obtained by testing part of the safety-related part(s) of the control system providing the safety function in isolation, a sample of that 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 the safety–related part(s) is sufficient to demonstrate its safety performance of the whole safety-related part providing the safety function.

6 Validation of safety functions

An important step is the validation of the safety functions provided by the safety–related parts of the control system for complete compliance with their specified characteristics. In the validation process it is important to check for errors and particularly for omissions in the formulated specification, provided with the design rationale.

The aim of validation of the safety functions is to ascertain that the safety–related output signals are correct and logically dependent on the input signals according to the specification. The validation should cover all normal and foreseeable abnormal conditions in static and dynamic simulation.

The specified safety functions [in accordance with EN 954–1: 1996 (ISO 13849-1:1999), clause 5] shall be validated in all operating modes of the machine. This means: validation shall be carried out to demonstrate correct functionality

— in different configurations sufficient to ensure that all safety–related outputs are realised over their complete ranges. Tests (e. g. overload tests) may be necessary to validate the specified safety functions.

— in response to foreseeable abnormal signal from any input source including power interruption and restoration.

NOTE Where appropriate combinations of different configurations should be considered.

7 Validation of categories

7.1 Analysis and testing of categories

The validation of categories shall demonstrate that their requirements are fulfilled. Principally, the following methods are applicable:

— an analysis from circuit diagrams (see clause 4);

— tests on the actual circuit and fault simulation on actual components, particularly in areas of doubt, regarding performance identified during the analysis (see clause 5);

— a simulation of control system behaviour, 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 submit these groups and their interfaces to fault simulation tests.

When carrying out validation by testing, the tests can include as appropriate:

— fault injection tests into a production sample;

— fault injection tests into a hardware model;

— software simulation of faults;

— 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 should be determined by analysis and, according to this analysis, the fault should be injected at the appropriate critical time.

7.2 Validation of category specifications

7.2.1 Category B

The safety-related parts of control systems to category B shall be validated in accordance with basic safety principles (see A.2, B.2, C.2 and D.2) by demonstrating that the specification, design, construction and choice of components are in accordance with EN 954-1:1996 (ISO 13849-1:1999), 6.2.1. This shall be achieved by checking that the safety-related part(s) of control systems are in accordance with its specification as provided in the documents for validation (see 3.5). For the validation of environmental conditions see 5.1.

7.2.2 Category 1

Safety–related parts of control systems to category 1 shall be validated by demonstrating that:

a) they meet the requirements of category B;

b) components are well–tried (see A.4 and D.4) by meeting at least one of the following conditions:

   1) they have been widely used with successful results in similar applications;

   2) they have been made using principles which demonstrate their suitability and reliability for safety-related applications;

c) well-tried safety principles (where applicable see A.3, B.3, C.3 and D.3) have been implemented correctly. Where newly developed principles have been used then the following shall be validated:

   1) how the expected modes of failure have been avoided;

   2) how faults have been avoided or their probability has been reduced.

Relevant component standards may be used to demonstrate compliance with this subclause (see A.4 and D.4).

7.2.3 Category 2

Safety-related parts of control systems to category 2 shall be validated by demonstrating that:

a) they meet the requirements of category B;

b) the well–tried safety principles used (if applicable) meet the requirements of 7.2.2c);

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 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 an hazardous situation, and

   2) periodically during operation if the risk assessment and the kind of operations show that it is necessary.

7.2.4 Category 3

Safety-related parts of control systems to category 3 shall be validated by demonstrating that:

a) they meet the requirements of category B;

b) the well–tried safety principles (if applicable) meet the requirements of 7.2.2 c);

c) a single fault does not lead to the loss of the safety function;

d) single faults (including common mode faults) are detected in accordance with the design rationale.

7.2.5 Category 4

Safety-related parts of control systems to category 4 shall be validated by demonstrating that:

a) they meet the requirements of category B;

b) the well–tried safety principles (if applicable) meet the requirements of 7.2.2 c);

c) a single fault (including common mode faults) does not lead to the loss of the safety function;

d) the single faults are detected at or before the next demand on the safety function.

e) if d) is not possible, an accumulation of faults does not lead to the loss of the safety function(s). The extent of the accumulation of faults considered shall be in accordance with the design rationale.

7.3 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 specified in the design. Existing recorded validation results of safety-related parts can be taken into account.

8 Validation of environmental requirements

The performance specified in the design for the safety-related parts of the control system 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) which is 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) may 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);

— electromagnetic compatibility (immunity).

When testing is necessary 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 safety-related parts of the control system shall provide output(s) for a safe state.

9 Validation of maintenance requirements

The validation process shall demonstrate that the maintenance requirements as specified in EN 954-1:1996 (ISO 13849-1:1999), clause 9, paragraph 2, have been implemented.

Annex A
(informative)

Validation tools for mechanical systems

Contents

A.1 Introduction

When mechanical systems are used in conjunction with other technologies, then relevant tables for basic safety and well–tried safety principles should also be taken into account. For further fault exclusions see 3.3.

A.2 List of basic safety principles

Table A.1 — Basic safety principles

Basic safety principles	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–energisation principle	The safe state is obtained by release of energy. See primary action for stopping in EN 292–2:1991 (ISO/TR 12100-2:1992), 3.7.1. Energy is supplied for starting the movement of a mechanism. See primary action for starting in EN 292–2:1991 (ISO/TR 12100-2:1992), 3.7.1. Consider different modes, e. g. operation mode, maintenance mode. This principle shall not be used in special applications, e. g. to keep energy for clamping devices.
Proper fastening	For the application of screw locking consider manufacturer's application notes. Overloading can be avoided by applying adequate torque loading technology

Table A.1 — Basic safety principles (continued)

Basic safety principles	Remarks
Limitation of the generation and/or transmission of force and similar parameters	Examples are break pin, break plate, torque limiting clutch.
Limitation of range of environmental parameters	Examples of parameters are temperature, humidity, pollution at the installation place. See clause 8 and consider manufacturer's application notes.
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 as operation mode, maintenance mode etc. 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	Reduce the number of components in the safety-related system.
Separation	Separation of safety-related functions from other functions.
Proper lubrication	—
Proper prevention of the ingress of fluids and dust	Consider IP rating [see EN 60529 (IEC 60529)]

A.3 List of well-tried safety principles

Table A.2 — Well–tried safety principles

Well–tried safety principles	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 always the same, see EN 292-2:1991, (ISO/TR 12100-2:1992), 3.7.4.
Over–dimensioning/safety factor	The safety factors are 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 for changing the position.
Increased OFF force	A safe position/state is obtained by an increased OFF force in relation to ON force.
Carefully selection, combination, arrangement, assembly and installation of components/system related to the application	—
Carefully selection of fastening related to the application	Avoid relying only on friction.

Table A.2 — Well–tried safety principles (continued)

Well–tried safety principles	Remarks
Positive mechanical action	Dependent operation (e. g. parallel operation) between parts is obtained by positive mechanical link(s). Springs and similar "flexible" elements should not be part of the link(s) [see EN 292-2:1991 (ISO/TR 12100-2:1992), 3.5].
Multiple parts	Reducing the effect of faults by multiplying parts, e. g. where a fault of one spring (of many springs) does not lead to a dangerous condition.
Use of well–tried spring (see also Table A.3)	A well–tried spring requires: — use of carefully selected materials, manufacturing methods (e. g. presetting 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 high probability a fracture will not occur). Well–tried pressure coil springs may also be designed by: — use of carefully selected materials, manufacturing methods (e. g. presetting and cycling before use) and treatments (e. g. rolling and shot-peening), — sufficient guidance of the spring, and — 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).
Limited range of force and similar parameters	Decide the necessary limitation in relation to the experience and application. Examples for limitations are break pin, break plate, torque limiting clutch.
Limited range of speed and similar parameters	Decide the necessary limitation in relation to the experience and application. Examples for limitations are centrifugal governor; safe monitoring of speed or limited displacement.
Limited range of environmental parameters	Decide the necessary limitations. Examples on parameters are temperature, humidity, pollution at the installation. See clause 8 and consider manufacturer's application notes.
Limited range of reaction time, limited hysteresis	Decide the necessary limitations. Consider e. g. spring tiredness, friction, lubrication, temperature, inertia during acceleration and deceleration, combination of tolerances.

A.4 List of well–tried components

Well–tried components for a safety–related application in the following list are based on the application of well–tried safety principles and/or a standard for their particular applications.

A well–tried component for some applications can be inappropriate for other applications.

Table A.3 — Well–tried components

Well-tried components	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 "List of well–tried safety principles".	Mechanical jointing such as screws, nuts, washers, rivets, pins, bolts etc. are standardised.
Spring	See Table A.2 "Use of a well–tried spring".	Technical specifications for spring steels and other special applications are given in ISO 4960.
Cam	All factors influencing the cam arrangement (e. g. part of an interlocking device) are to be considered. See Table A.2 "List of well–tried safety principles".	See EN 1088 (ISO 14119) (Interlocking devices).
Break–pin	All factors influencing the application are to be considered. See Table A.2 "List of well-tried safety principles".	—

A.5 Fault lists and fault exclusions

A.5.1 Introduction

The lists express some fault exclusions and their rationale. For further exclusions see 3.3.

The precise instant that the fault occurs can be critical (see 7.1).

A.5.2 Various mechanical devices, components and elements

Table A.4 — 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 life-time (see also Table A.2).	See EN 954-1:1996 (ISO 13849-1:1999), 7.2
Untightening/ loosening	Yes, in the case of carefully selected material, manufacturing process, locking means and treatment, according to the specified life-time (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 life-time (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 life-time (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 life-time (see also Table A.2).	

A.5.3 Pressure coil springs

Table A.5 — Pressure coil springs

Fault considered	Fault exclusion	Remarks
Wear/corrosion	Yes, in the case of the use of well-tried spring(s) and carefully selected fastening(s) (see Table A.2).	See EN 954-1:1996 (ISO 13849-1:1999), 7.2
Force reduction by setting and fracture		
Fracture		
Stiffness/sticking		
Loosening		
Deformation by overstressing		

Annex B
(informative)

Validation tools for pneumatic systems

Contents

B.1 Introduction

When pneumatic systems are used in conjunction with other technologies, then relevant tables for basic safety and well-tried safety principles should also be taken into account. Where pneumatic components are electrically connected/controlled the appropriate fault lists in annex D should be considered.

NOTE Requirements of specific directives could apply such as simple pressure vessels, pressure equipment.

B.2 List of basic safety principles

Table B.1 — Basic safety principles

Basic safety principles	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, 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.

Table B.1 — Basic safety principles (continued)

Basic safety principles	Remarks
Use of de–energisation principle	The safe state is obtained by release of energy to all relevant devices. See primary action for stopping in EN 292-2:1991 (ISO/TR 12100-2:1992), 3.7.1. Energy is supplied for starting the movement of a mechanism. See primary action for starting in EN 292-2:1991 (ISO/TR 12100-2:1992), 3.7.1. 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, 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 of a piston by a flow valve or a throttle.
Sufficient avoidance of contamination of the fluid	Consider filtration and separation of solid particles and water in the fluid.
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, 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 8 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 release of stored energy may be necessary [see EN 1037:1995 (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	Reduce the number of 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.

B.3 List of well–tried safety principles

Table B.2 — Well–tried safety principles

Well–tried safety principles	Remarks
Over–dimensioning/safety factor	The safety factor is 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.

Table B.2 — Well–tried safety principles (continued)

Well–tried safety principles	Remarks
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 e. g. 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 orifice, fixed throttle.
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 high degree of filtration and separation of solid particles and water in the fluid.
Sufficient positive overlapping in piston valves	The positive overlapping ensures the stopping function and prevents un-allowed movements.
Limited hysteresis	For example increased friction will increase the hysteresis. Combination of tolerances will also influence the hysteresis.

B.4 List of well–tried components

At the present time no list of well-tried components is given. The status of being well-tried is mainly application specific. Components can be stated as being well-tried if they comply with the description given in EN 954-1:1996 (ISO 13849-1:1999), 6.2.2 and in EN 983:1996, clauses 5 to 7.

A well-tried component for some applications can be inappropriate for other applications.

B.5 Fault lists and fault exclusions

B.5.1 Introduction

The lists express some fault exclusions and their rationale. For further exclusions see 3.3.

The precise instant that the fault occurs can be critical (see 7.1).

B.5.2 Valves

Table B.3 — 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 Yes, if well–tried springs are used (see Table A.2) and if normal installation and operating conditions apply (see remark 1)), or Yes, in the case of spool valves with elastic sealing and if normal installation and operating conditions apply (see remark 1)).	1) Normal installation and operating conditions apply when: — the conditions laid down by the manufacturer have been observed and — the weight of the moving component is not acting in an unfavorable sense in terms of safety (e. g. horizontal installation) 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 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 2)) and if normal conditions of operation apply and an adequate treatment and filtration of the compressed air is provided, or Yes, in the case of seat valves if normal conditions of operation apply (see remark 3)) and adequate treatment and filtration of the compressed air is provided.	2) 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 may occur over a long period of time. 3) Normal conditions of operation apply when the conditions laid down by the manufacturer are being observed.
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.3 — Directional control valves (continued)

Fault considered	Fault exclusion	Remarks
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 due to their design and construction.	
NOTE If the control functions are realised 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 — 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 1)) and if well-tried springs are used (see Table A.2).	1) For a non–controlled ball seat valve without damping system, the guidance system is generally designed in a manner 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 2)) and if there is sufficient closing force on the basis of the pressures and areas provided.	2) Normal installation and operating conditions are being met when: — the conditions laid down by the manufacturer are being 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, simultaneous closing is unlikely.	—
Leakage	Yes, if normal conditions of operation apply (see remark 3)) and there is adequate treatment and filtration of the compressed air.	3) Normal conditions of operation apply when the conditions laid down by the manufacturer are being observed.
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 — 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 being observed.
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 — 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, 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 in such a manner that any sticking of the moving component is unlikely.
Non–closing or insufficient closing (spatially and temporarily) 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	

Table B.6 — Pressure valves (continued)

Fault considered	Fault exclusion	Remarks
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 3)) and if adequate treatment and filtration of the compressed air is provided.	3) Normal operating conditions are being met when the conditions laid down by the manufacturer are being 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.	

B.5.3 Pipework, hose assemblies and connectors

Table B.7 — 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 1)).	1) 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, 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 the 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 — Hose assemblies

Fault considered	Fault exclusion	Remarks
Bursting, tearing off at the fitting attachment and leakage	Yes, if hose assemblies using hoses manufactured to EN 854 (ISO 4079-1) or similar hoses (see remark 1)) with the corresponding hose fittings.	1) Fault exclusion is not considered when: - the intended life time is expired, - fatigue behaviour of reinforcement can occur, - external damage is unavoidable.
Clogging (blockage)	Yes, for hose assemblies in the power circuit. Yes, for the control and measurement hose assemblies if the nominal diameter is ≥ 2mm.	—

Table B.9 — 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 components are in accordance with good engineering practice.	—
Leakage (loss of airtightness)	None (see remark 1))	1) 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. Yes, in the case of the control and measurement connectors if the nominal diameter is ≥ 2 mm.	—

B.5.4 Pressure transmitters and pressure medium transducers

Table B.10 — 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.	

B.5.5 Compressed air treatment

Table B.11 — 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 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 B.12 — 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 — Silencer

Fault considered	Fault exclusion	Remarks
Blockage (clogging) of the silencer	Yes, if the design and construction of the silencer element fulfils remark 1).	1) 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.

B.5.6 Accumulators and pressure vessels

Table B.14 — 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.	—

B.5.7 Sensors

Table B.15 — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark 1))	None	1) 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	—

B.5.8 Information processing

Table B.16 — 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.	—

Table B.17 — 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 1)) apply and adequate treatment and filtration of the compressed air is provided.	1) Normal operating conditions are being met when the conditions laid down by the manufacturer are being 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 — 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 e. g. 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 being met when the conditions laid down by the manufacturer are being 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

Contents

C.1 Introduction

When hydraulic systems are used in conjunction with other technologies, then relevant tables for basic safety and well-tried safety principles should also be taken into account. Where hydraulic components are electrically connected/controlled the appropriate fault lists in annex D should be considered.

NOTE Requirements of specific directives could apply such as pressure equipment.

C.2 List of basic safety principles

NOTE Air bubbles and cavitation in the hydraulic fluid should be avoided because they can create additional hazards, e. g. unintended movements.

Table C.1 — Basic safety principles

Basic safety principles	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.

Table C.1 — Basic safety principles (continued)

Basic safety principles	Remarks
Use of de–energisation principle	The safe state is obtained by release of energy to all relevant devices. See primary action for stopping in EN 292-2:1991 (ISO/TR 12100-2:1992), 3.7.1. Energy is supplied for starting the movement of a mechanism. See primary action for starting in EN 292-2:1991 (ISO/TR 12100-2:1992), 3.7.1. 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 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 of a piston by a flow valve or a throttle.
Sufficient avoidance of contamination of the fluid	Consider filtration/separation of solid particles/water in the fluid. Consider also an indication of the need of 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 8 and consider 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. keep energy for clamping devices or ensure a position) need to be considered separately.
Simplification	Reduce the number of 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.

C.3 List of well–tried safety principles

Table C.2 — Well–tried safety principles

Well–tried safety principles	Remarks
Over–dimensioning/safety factor	The safety factor is 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	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 orifice, fixed throttle.
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 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 of filter–service.
Sufficient positive overlapping in piston valves	The positive overlapping ensures the stopping function and prevents un-allowed movements.
Limited hysteresis	For example increased friction will increase the hysteresis. Combination of tolerances will also influence the hysteresis.

C.4 List of well–tried components

At the time no list of well–tried components is given. The status of being well–tried is mainly application specific. Components can be stated as being well–tried if they comply with the description given in EN 954-1:1996 (ISO 13849-1:1999), 6.2.2 and in EN 982:1996, clauses 5 to 7.

A well–tried component for some applications can be inappropriate for other applications.

C.5 Fault lists and fault exclusions

C.5.1 Introduction

The lists express some fault exclusions and their rationale. For further exclusions see 3.3.

The precise instant that the fault occurs can be critical (see 7.1).

C.5.2 Valves

Table C.3 — 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 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)).	1) Special type of cartridge seat valve is achieved if: — the active area for initiating the safety–related switching movement is at least 90 % of the total area of the moving component (poppet) and — the effective control pressure on the active area, can be increased up to the maximum operating pressure (in accordance with EN 982:1996, 3.5) in line with the behaviour of the seat valve in question and — the effective control pressure on the area opposite to 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, and — 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 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)).	
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 Yes, if well–tried springs are used (see Table A.2) and if normal installation and operating conditions apply (see remark 2)), or 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)) 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 being observed and — the weight of the moving component is not acting in an unfavourable sense in terms of safety, e. g. horizontal installation 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 and shock stresses occur.

Table C.3 — Directional control valves (continued)

Fault considered	Fault exclusion	Remarks
Leakage	Yes, in the case of seat valves, if normal installation and operating conditions apply (see remark 3)) and an adequate filtration system is provided.	3) Normal installation and operating conditions apply when the conditions laid down by the manufacturer are being observed.
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 due to their design and construction.	
NOTE If the control functions are realised 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 — 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 1)) and if well–tried springs are used (see Table A.2).	1) For a non–controlled ball seat valve without damping system, the guidance system is generally designed in a manner 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 2)) and if there is sufficient closing force on the basis of the pressures and areas provided.	2) Normal installation and operating conditions are being met when: — the conditions laid down by the manufacturer are being 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.	—

Table C.4 — Stop (shut–off) valves/non–return (check) valves/shuttle valves, etc. (continued)

Fault considered	Fault exclusion	Remarks
Leakage	Yes, if normal conditions of operation apply (see remark 3)) and an adequate filtration system is provided.	3) Normal conditions of operation apply when the conditions laid down by the manufacturer are being observed.
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 — 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 being met when the conditions laid down by the manufacturer are being 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 observed.
Change in the flow rate in the case of non–adjustable, circular orifices and nozzles	Yes, if the diameter is $\geq$ 0,8 mm, normal operating conditions apply (see remark 2)) and if 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 — 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 cartride 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 Yes, 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 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 3)) and if an adequate filtration system is provided.	3) Normal operating conditions apply when the conditions laid down by the manufacturer are being observed.
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.	

C.5.3 Metal pipework, hose assemblies and connectors

Table C.7 — 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.	—

Table C.7 — Metal pipework (continued)

Fault considered	Fault exclusion	Remarks
Failure at the connector (e. g. tearing off, leakage)	Yes, if using welded fittings or welded flanges or flared fittings 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 ≥ 3 mm.	

Table C.8 — 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. Yes, for the control and measurement hose assemblies if the nominal diameter is ≥ 3 mm.	

Table C.9 — 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 1))	1) 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 leaktightness is not assumed.
Clogging (blockage)	Yes, for applications in the power circuit. Yes, in the case of the control and measurement connectors if the nominal diameter is ≥ 3 mm.	—

C.5.4 Filters

Table C.10 — 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 in a manner similar 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.	

C.5.5 Energy storage

Table C.11 — 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 1)).	1) 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.	—

C.5.6 Sensors

Table C.12 — Sensors

Fault considered	Fault exclusion	Remarks
Faulty sensor (see remark 1))	None	1) 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	—

Annex D
(informative)

Validation tools for electrical systems

Contents

D.1 Introduction

When electrical systems are used in conjunction with other technologies, then relevant tables for basic safety and well–tried safety principles should also be taken into account.

NOTE 1 Electronic components cannot be considered as well-tried.

NOTE 2 The environmental conditions of EN 60204-1 (IEC 60204-1) do not apply to the validation process if other environmental conditions are specified.

D.2 List of basic safety principles

Table D.1 — Basic safety principles

Basic safety principles	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 other electrical device is connected to the protective bonding circuit [for full text see EN 60204-1:1997 (IEC 60204-1:1997), 9.1.4].
Insulation monitoring	Use of isolation monitoring device which either indicates an earth fault or interrupts the circuit automatically after an earth fault [see EN 60204-1:1997 (IEC 60204-1:1997), 9.4.3.1].

Table D.1 — Basic safety principles (continued)

Basic safety principles	Remarks
Use of de–energisation principle	A safe state is obtained by de–energising all relevant devices, e. g. by using of normally closed (NC) contact for inputs (push–buttons and position switches) and normally open (NO) contact for relays [see also EN 292–2:1991 (ISO/TR 12100-2:1992), 3.7.1]. Exceptions may 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 EN 60204–1:1997 (IEC 60204-1:1997), 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	Minimise delay in de–energising 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 8).
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 EN 1088:1995 (ISO 14119:1998), clause 5.
Protection against unexpected start–up	Prevent unexpected start–up, e. g. after power supply restoration [see EN 292–2:1991 (ISO/TR 12100-2:1992), 3.7.2, EN 1037 (ISO 14118), EN 60204–1 (IEC 60204-1)].
Protection of the control circuit	The control circuit should be protected in accordance with EN 60204-1:1997 (IEC 60204:-1:1997), 7.2 and 9.1.1.
Sequential switching for circuit of serial contacts of redundant signals	To avoid the common mode failure of the welding of both contacts, the switching on and off does not happen simultaneously, so that one contact always switches without current.

D.3 List of well–tried safety principles

Table D.2 — Well–tried safety principles

Well–tried safety principles	Remarks
Positive mechanically linked contacts	Use of positively mechanically linked contacts for, e. g. monitoring function [see EN 292–2:1991 (ISO/TR 12100-2:1992), 3.5].
Fault avoidance in cables	To avoid short circuit between two adjacent conductors: — use cable with shield connected to the protective bonding circuit on each separate conductor, or — in flat cables, use of one earthed conductor between each signal conductors.
Separation distance	Use of sufficient distance between position terminals, components and wiring to avoid unintended connections.

Table D.2 — Well–tried safety principles (continued)

Well–tried safety principles	Remarks
Energy limitation	Use of a capacitor for supplying a finite amount of energy, e. g. in timer application.
Limitation of electrical parameters	Limitation in voltage, current, energy or frequency resulting, e. g. in torque limitation, hold–to–run with displacement/time limited, reduced speed, to avoid leading to an unsafe state.
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 by the strength) with no elastic elements, e. g. spring between actuator and the contacts, [see EN 1088:1995 (ISO 14119:1998), 5.1].
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 EN 292–2:1991 (ISO/TR 12100-2:1992), 3.7.4].
Over–dimensioning	Derate components when used in safety circuits, e. g. by : — 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, and — total number of expected switching operation shall be ten times less than the device's electrical durability. NOTE Derating can depend on the design rationale.
Minimise 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 — simplify to have a better reliability.

D.4 List of well–tried components

The components listed in Table D.3 are considered to be well–tried if they comply with the description given in EN 954-1:1996 (ISO 13849-1:1999), 6.2.2. The standards listed in this table can demonstrate their suitability and reliability for a particular application.

A well–tried component for some applications can be inappropriate for other applications.

Table D.3 — Well–tried components

Well–tried components	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 operation	—	EN 60947–5–1:1997 (IEC 60947-5-1:1997), annex K