SLOVENSKI STANDARD
SIST EN ISO 13849-2:2004

01-junij-2004

Varnost strojev - Z varnostjo povezani deli krmilnih sistemov - 2. del: Potrjevanje (ISO 13849-2:2003)

Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2003)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung (ISO 13849-2:2003)

Sécurité des machines - Parties des systèmes de commande relatives a la sécurité - Partie 2: Validation (ISO 13849-2:2003)

Ta slovenski standard je istoveten z: **EN ISO 13849-2:2003**

ICS:

13.110	Varnost strojev	Safety of machinery

SIST EN ISO 13849-2:2004 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 13849-2

August 2003

ICS 13.110

English version

Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2003)

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 2: Validation (ISO 13849-2:2003)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung (ISO 13849-2:2003)

This European Standard was approved by CEN on 10 April 2003.

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

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

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.

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

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN ISO 13849-2:2003 E

Contents

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).

For relationship with EC Directives, see informative annex ZA, which is an integral part of this document.

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.

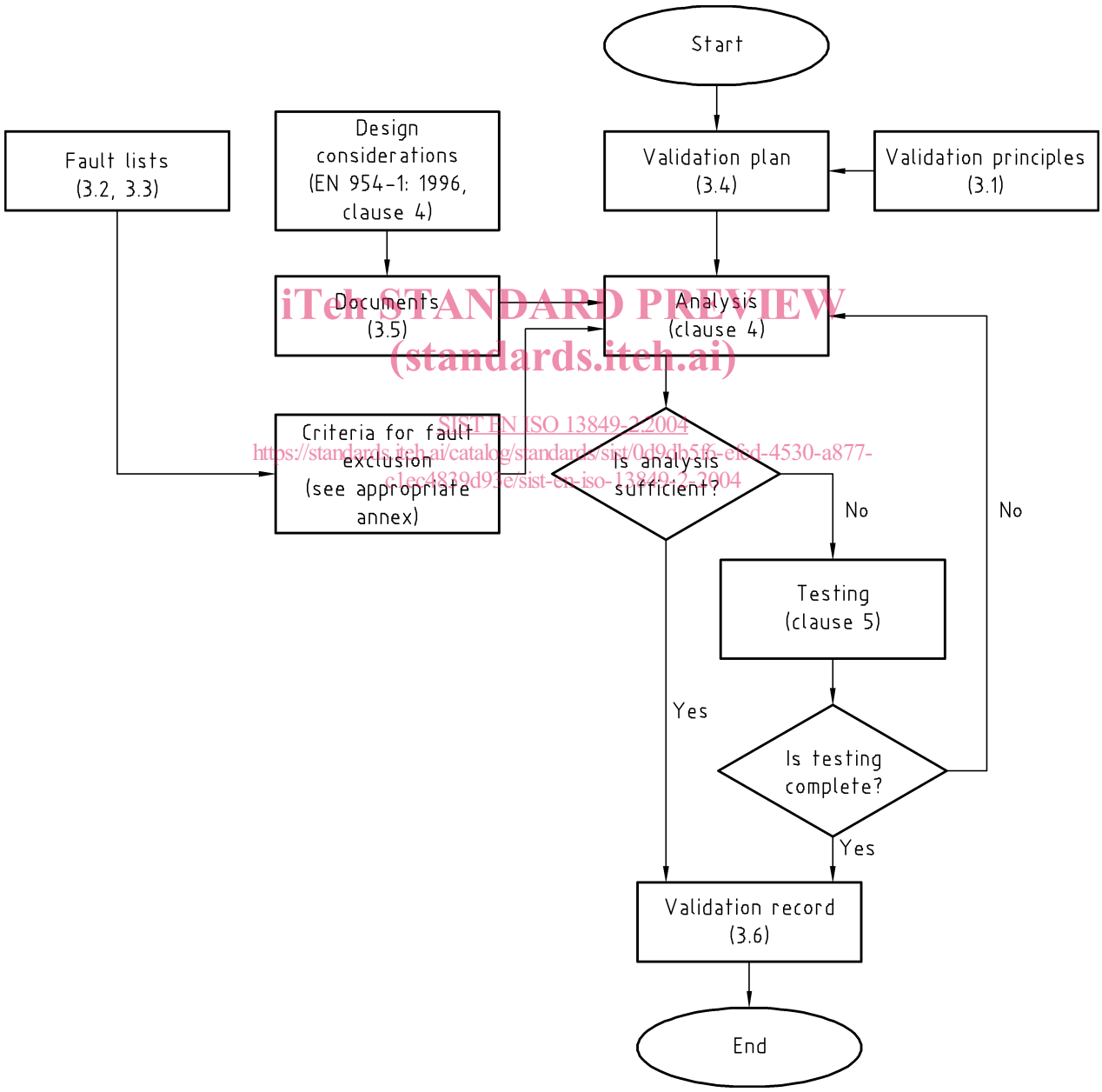

Figure 1 — Overview of the validation process

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;