SLOVENSKI STANDARD

SIST EN 954-1:2000

01-junij-2000

Varnost strojev - Deli krmilnih sistemov v zvezi z varnostjo - 1. del: Splošna načela za načrtovanje

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Regeleinrichtungen - Teil 1: Allgemeine Gestaltungsleitsätze

Sécurité des machines - Parties des systèmes de commande relatives a la sécurité - Partie 1: Principes généraux de conception

Ta slovenski standard je istoveten z: **EN 954-1:1996**

ICS:

13.110

SIST EN 954-1:2000 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 954-1

December 1996

ICS 13.110

Descriptors: safety of machines, control devices, design, interfaces, hazards, generalities, defects, verification

English version

Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze

This European Standard was approved by CEN on 1996-07-11. 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 Central Secretariat or to any CEN member.

The European Standards exist 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 Central Secretariat has the same status as the official versions.

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

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Central Secretariat: rue de Stassart,36 B-1050 Brussels

Ref. No. EN 954-1:1996 E

Contents

Page

Foreword . . . 3

0 Introduction . . . 3

1 Scope . . . 4

2 Normative references . . . 4

3 Definitions . . . 5

4 General considerations . . . 5
4.1 Safety objectives in the design . . . 5
4.2 General strategy for design . . . 5
4.3 Process for the selection and design of safety measures . . . 7
4.4 Principles for ergonomic design . . . 10

5 Characteristics of safety functions . . . 10

6 Categories . . . 15
6.1 General . . . 15
6.2 Specifications for categories . . . 16
6.3 Selection and combination of safety-related parts to different categories . . . 20

7 Fault consideration . . . 21
7.1 General . . . 21
7.2 Fault exclusion . . . 21

8 Validation . . . 21
8.1 General . . . 21
8.2 Validation plan . . . 22
8.3 Validation by analysis . . . 22
8.4 Validation by testing . . . 22
8.5 Validation report . . . 22

9 Maintenance . . . 23

10 Information for use . . . 23

Annex A (informative) **Questionnaire for the design process** . . . 24

Annex B (informative) **Guidance for the selection of categories** . . . 26

Annex C (informative) **List of some significant faults and failures for various technologies** . . . 29

Annex D (informative) **Relationship between safety, reliability and availability for machinery** . . . 30

Annex E (informative) **Bibliography** . . . 31

Annex ZA (informative) **Clauses of this European Standard addressing essential requirements or other provisions of EU directives** . . . 32

Foreword

This European Standard has been prepared by Technical Committee CEN/TC 114 "Safety of machinery", the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 1997, and conflicting national standards shall be withdrawn at the latest by June 1997.

This standard has the status of an application standard (Type-B1) and is intended to give guidance during the design and assessment of control systems and to Technical Committees preparing Type-B2 or Type-C standards which are presumed to comply with the Essential Safety Requirements of Annex I of the Council directive 89/392/EEC and amending directives 91/368/EEC and 93/44/EEC (see annex A of EN 292-2 : 1991/ A1 : 1995). This standard does not give specific guidance for the compliance with other EU directives.

At the time of the submission of this Part 1 to the CEN formal vote a draft Part 2 is currently being prepared, with the following provisional title: "Safety of machinery - Safety-related parts of control systems - Part 2: Validation" (see also clauses 7 and 8 in this Part 1.)

NOTE: It is intended in the elaboration of Part 2 to take into account the requirements of IEC 1508[1]) 'Functional safety: safety-related systems' in respect of the needs of machinery safety.

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

For relationship with EU Directive(s), see informative Annex ZA, which is an integral part of this standard.

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

0 Introduction

Parts of machinery control systems are frequently assigned to provide safety functions: these are called the safety-related parts. These parts can consist of hardware and software and they provide the safety functions of control systems. They can be separate or integrated parts of the control system.

The performance of a safety-related part of a control system with respect to the occurrence of faults is allocated in this standard into five categories (B, 1, 2, 3, 4) which should be used as reference points. These categories (see 6.2) are not intended to be used in any given order or in any given hierarchy in respect of safety requirements.

The categories can be applied for:

- control systems of all kinds of machinery from simple, e.g. small kitchen-machines, up to complex manufacturing installations, e.g. packing machines, printing machines, presses;
- control systems of protective equipment, e.g. two-hand control devices, interlocking devices, electro-sensitive protective devices (e.g. photoelectric barriers) and pressure sensitive mats.

The category selected will depend upon the machine and the extent to which control means are used for the protective measures.

When selecting a category and designing a safety-related part of a control system the designer will need to declare at least the following information about the safety-related part:

- the category(ies) selected;
- the functional characteristics;
- the precise rôle it plays in the machinery protective measure(s);
- the exact limits (see 3.1);
- all safety-relevant faults considered;
- those safety-relevant faults not considered by fault exclusion and the measures employed to allow their exclusion;
- the parameters relevant to the reliability such as environmental conditions;
- the technology(ies) used.

[1]) Standard in preparation

The use of the categories as reference points and this declaration of the rationale followed during the design process is intended to allow the standard to be used flexibly. It is intended to provide a clear basis upon which the design and performance of any application of the safety-related part of a control system (and the machine) can be assessed by e.g. a third party, or in-house or an independent test house.

1 Scope

This European Standard provides safety requirements and guidance on the principles for the design (see 3.11 of EN 292-1 : 1991) of safety-related parts of control systems. For these parts it specifies categories and describes the characteristics of their safety functions. This includes programmable systems for all machinery and for related protective devices. It applies to all safety-related parts of control systems, regardless of the type of energy used, e.g. electrical, hydraulic, pneumatic, mechanical. It does not specify which safety functions and which categories shall be used in a particular case.

It applies to all machinery applications for professional and non-professional use. Also, where appropriate, this standard can be applied to the safety-related parts of control systems used in other technical applications.

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.

EN 292-1 : 1991	Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology
EN 292-2 : 1991/A1 : 1995	Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles and specifications
EN 418	Safety of machinery – Emergency stop equipment, functional aspects – Principles for design
EN 457	Safety of machinery – Auditory danger signals – General requirements, design and testing (ISO 7731 : 1986 modified)
EN 614-1	Safety of machinery – Ergonomic design principles – Part 1: Terminology and general principles
EN 842	Safety of machinery – Visual danger signals – General requirements, design and testing
EN 981	Safety of machinery – System of auditory and visual danger and information signals
EN 982	Safety of machinery – Safety requirements for fluid power systems and their components – Hydraulics
EN 983	Safety of machinery – Safety requirements for fluid power systems and their components – Pneumatics
prEN 999 : 1995	Safety of machinery - The positioning of protective equipment in respect of approach speeds of parts of the human body
EN 1037	Safety of machinery – Prevention of unexpected start-up
EN 1050 : 1996	Safety of machinery – Principles for risk assessment
EN 60204-1 : 1992	Safety of machinery – Electrical equipment of machines – Part 1: General requirements (IEC 204-1 : 1992, modified)
EN 60447 : 1993	Man-machine interface (MMI) – Actuating principles (IEC 447 : 1993)
EN 60529	Degrees of protection provided by enclosures (IP Code) (IEC 529 : 1989)
EN 60721-3-0	Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Introduction (IEC 721-3-0 : 1984 + A1 : 1987)
IEC 50 (191) : 1990	International Electrotechnical Vocabulary, Chapter 191: Dependability and quality of service

3 Definitions

For the purposes of this standard the following definitions apply in addition to the definitions given in EN 292-1 and IEC 50 (191):

3.1 Safety-related part of a control system: Part or subpart(s) of a control system which responds to input signals and generates safety-related output signals. The combined safety-related parts of a control system start at the points where the safety-related signals are initiated and end at the output of the power control elements (see also annex A of EN 292-1 : 1991). This also includes monitoring systems.

3.2 Category: Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts and/or by their reliability.

3.3 Safety of control systems: Ability of safety-related parts of a control system to perform their safety function(s) for a given time according to their specified category.

3.4 Fault: The state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

NOTE 1: A fault is often the result of a failure of the item itself, but may exist without prior failure.

NOTE 2: In English the term "fault" and its definition are identical with these given in IEV 191-05-01 of IEC 50 (191) : 1990. In the field of machinery, the French term "défaut" and the German term "Fehler" are used rather than the terms "panne" and "Fehlzustand" that appear with this definition.

3.5 Failure: The termination of the ability of an item to perform a required function.

NOTE 1: After a failure the item has a fault.

NOTE 2: "Failure" is an event, as distinguished from "fault" which is a state.

NOTE 3: This concept as defined does not apply to items consisting of software only.

[IEV 191-04-01 of IEC 50(191): 1990]

NOTE 4: In practice the terms fault and failure are often used synonymously.

3.6 Safety function of control systems: Function initiated by an input signal and processed by the safety-related parts of the control system to enable the machine (as a system) to achieve a safe state.

3.7 Muting: Temporary automatic suspension of a safety function(s) by safety-related parts of the control system.

3.8 Manual reset: Function within the safety-related parts of the control system to manually restore given safety functions before the re-starting of a machine.

4 General considerations

4.1 Safety objectives in the design

The safety-related parts of a control sytem which provide the safety functions shall be designed and constructed so that the principles of EN 1050 are fully taken into account:

- during all intended use and foreseeable misuse;
- when faults occur;
- when foreseeable human mistakes are made during the intended use of the machine as a whole.

4.2 General strategy for design

From the risk assessment (see EN 1050) at the machine, the designer shall decide the contribution to the reduction of risk which needs to be provided by each safety-related part of the control system (see annex B). This contribution does not cover the overall risk of the machinery under control, e.g. not the overall risk of a mechanical press, or washing machine is considered, but that part of risk reduced by the application of particular safety functions. Examples of such functions are the stop function initiated by using an electro-sensitive protective device on a press or the door-locking function of a washing machine.

The key objective is that the designer shall ensure that the safety-related parts of a control system produce outputs which achieve the risk reduction objectives of EN 1050. This is not always achievable and in such cases the designer shall provide other safety measures. The hierarchy for the strategy in reducing risk is given in clause 5 of EN 292-1 : 1991.

The category and other features, e.g. physical position of parts, isolation, selected by the designer for the safety-related parts will depend upon the contribution made by those parts to the reduction of risk, the design and the technology (see clause 0). The designer shall declare:

- which category(ies) is being used as the reference point for the design;
- the exact points at which the safety-related part(s) start and at which it ends;
- the design rationale, e.g. the faults considered, the faults excluded, within the design to achieve that category(ies).

The greater the reduction of risk is dependent upon the safety-related parts of control systems, then the ability of those parts to resist faults is required to be higher. This ability - in the understanding that the required function is performed - can be partly quantified by reliability values and by a fault resistance structure. Both reliability and structure contribute to this ability of safety-related parts to resist faults. A specified resistance to faults can be achieved by specifying levels of reliability of components and/or with improved structures for the safety-related parts. The contribution of reliability and of structure can vary with the technology used. For example, it is possible for a single channel of safety-related parts of high reliability in one technology to provide the same or higher resistance to faults as a fault tolerant structure of lower reliability in a different technology.

NOTE: The higher the resistance to faults of the safety-related parts, the lower the probability that the safety-related parts will fail to carry out the required safety functions.

Reliability and safety are not the same (see annex D). For example, it is possible that the safety of a system with relatively unreliable components, in a redundant structure, is higher than the safety of a system with a simpler structure but with more reliable components. This concept is important because in some applications safety requires the highest priority regardless of the reliability achieved, e.g. when the consequences of failure are always serious and normally irreversible. In such applications a fault detection (one cycle fault tolerant) structure which provides the required safety function after one or two or more faults shall be provided in accordance with the risk assessment.

This standard does not require the calculation of reliability values for structures which are complex where safety is predominantely obtained by improving the structure of the safety-related parts. For structures which are less complex, where component reliability is important to safety, the calculation of reliability values is a useful indicator of the contribution to the overall risk reduction by the safety-related parts.

In the case of applications with lower risk measures to avoid faults may be appropriate; for higher risk applications improving the structure of the safety-related parts of a control system can provide measures to avoid, detect or tolerate faults. Practical measures include redundancy, diversity, monitoring (see also clause 3 of EN 292-2 : 1991,annex A of EN 292-2 : 1991/A1 : 1995 and 9.4 of EN 60204-1 : 1992).

The achieved behaviour for fault resistance of the safety-related parts of the control system is a function of many parameters including, e.g.:

- the reliability with respect to performing the safety functions;
- the structure (or architecture) of the control system;
- the quality of safety-related documentation;
- the completeness of the specification;
- the design, manufacture and maintenance;
- the quality and accuracy of software;
- the extent of functional testing;
- the operating characteristics of the machine or part of the machine under control.

These parameters can be grouped under three main characteristics:

- hardware reliability - the level of reliability of the components to avoid faults;
- system structure - the arrangement of the components in the safety-related part of a control system to avoid, tolerate or detect faults;

– the non-quantifiable, qualitative aspects which affect the behaviour of the safety-related part of a control system .

4.3 Process for the selection and design of safety measures

This subclause sets out a process for the selection of the safety measures to be provided and then for the design of the safety-related parts of the control system. It is important that the interfaces between the safety-related parts of the control system, the non-safety-related parts of the control system and all other parts of the machine are identified. Then the contribution to risk reduction provided by the safety-related parts, can be specified within the risk assessment of the machine according to EN 1050.

Because there are many ways in which the risk at a machine can be reduced and because there are many ways in which the safety-related parts of the control system can be designed this process is iterative. Decisions and/or assumptions made at any step in the procedure may affect decisions and/or assumptions made at an earlier step. This aspect can be checked by looping back through the procedure at any step. Such checking in the validation step is essential to ensure that the safety performance which is achieved is the same as that set out in the specification.

The process is illustrated in figure 1. Important aspects which should be considered during the design process are given as questions in annex A to prompt the designer.These questions illustrate the philosophy which should be followed in the design of the safety-related parts. Not all questions apply to every application. Some applications require additional questions.

Step 1: Hazard analysis and risk assessment

– Identify the hazards present at the machine during all modes of operation and at each stage in the life of the machine by following the guidance in EN 292-1 and EN 1050.

– Assess the risk arising from those hazards and decide the appropriate risk reduction for that application in accordance with EN 292-1 and EN 1050.

Step 2: Decide measures for risk reduction by control means

– Decide the design measures at the machine and/or the provision of safeguards to provide the risk reduction. Those parts of the control system which contribute as an integral part of the design measures and/or in the control of the safeguards shall be considered safety-related parts.

Step 3: Specify safety requirements for the safety-related parts of the control system

– Specify the safety functions (see clause 5 and other referenced documents), to be provided in the control system. Table 1 lists the source reference of the more common safety functions and the characteristics which shall be included if a particular safety function is selected.

– Specify how the safety functions will be realized and select the category(ies) for each part and combinations of parts within the safety-related parts of the control system (see clause 6).

Step 4: Design

– Design the safety-related parts of the control system according to the specification developed in step 3 and to the general strategy for design in 4.2. List the features included in the design which provide the rationale for the category(ies) achieved.

– Verify the design at each stage to ensure that the safety-related parts fulfil the requirements from the previous stage in the context of the specified safety function(s) and category(ies).

Step 5: Validation

– Validate the achieved safety functions and category(ies) against the specification in step 3. Re-design as necessary (see clause 8).

– When programmable electronics are used in the design of safety-related parts of the control systems other detailed procedures are required (see 8.4.2). These procedures are under consideration (see also annex E).

NOTE 1: It is believed at present that it is difficult to determine with any degree of certainty in situations when a significant hazard can occur due to the maloperation of the control system that reliance on correct operation of a single channel of programmable electronic equipment can be assured. Until such time that this situation can be resolved, it is inadvisable to rely on the correct operation of such a single channel device (according to 12.3.5 of EN 60204-1 : 1992).

NOTE 2: It will also be necessary to validate the safety-related parts of the control system in conjunction with all the control system and as part of the machine. The requirements of such validation are not part of this European Standard but should be specified by the machine designer or the appropriate Type-C standard.

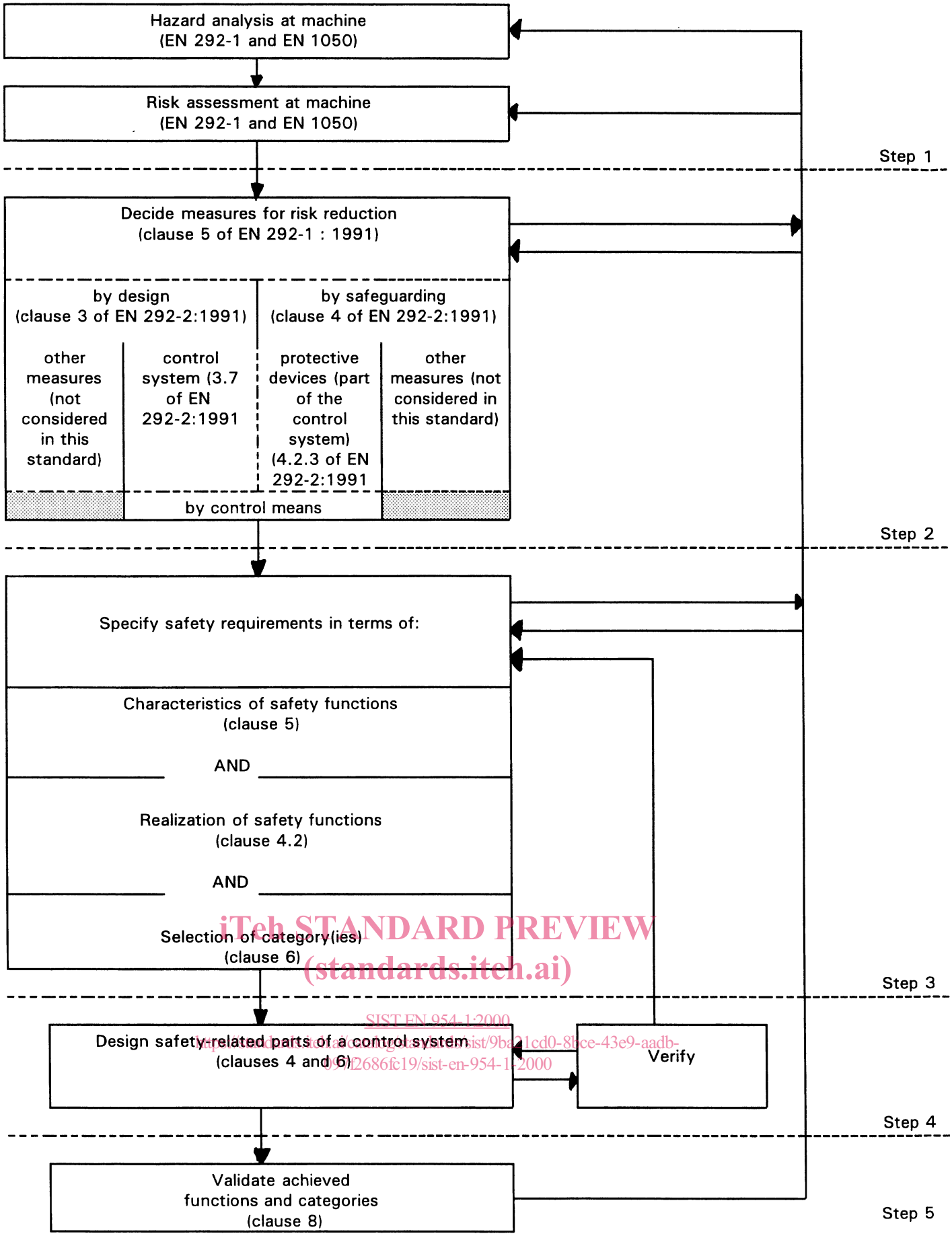

Figure 1: Iterative process for the design of safety-related parts of control systems

4.4 Principles for ergonomic design

The interface between persons and the safety-related parts of control systems shall be designed and installed, so that no one is endangered during all intended use and foreseeable misuse of the machine (see also EN 292-2, EN 614-1, prEN 894-1, prEN 894-2, prEN 894-3, prEN 1005-3, clause 10 of EN 60204-1 : 1992 and clause 2 of EN 60447 : 1993).

Ergonomic principles should be used so that the machine and the control system, including the safety-related parts, are easy to use, and so that the operator is not tempted to act in a hazardous manner. The safety requirements for observing ergonomic principles given in 3.6 of EN 292-2 : 1991 should apply.

5 Characteristics of safety functions

5.1 General

This clause provides a list of typical safety functions (see 3.13 of EN 292-1 : 1991) which can be provided by the safety-related parts of control systems. The designer (or Type-C standard maker) shall include the necessary safety functions from this list to achieve the measures of safety required of the control system for the specific application.

Table 1 lists typical safety functions and some of their characteristics. It makes reference to details which are clearly set out in the normative references. For each safety function, reference is made to the relevant parts of these standards (see also clause 2). The designer (or Type-C standard maker) shall ensure that the requirements of all these standards are satisfied for the selected safety functions. Additional detailed requirements are also set out in this clause for some characteristics. These shall be included.

Where necessary the characteristics shall be adapted for use with different energy sources.