BRITISH STANDARD

BS EN
954-1 : 1997

Safety of machinery — Safety related parts of control systems —

Part 1. General principles for design

The European Standard EN 954-1 : 1996 has the status of a British Standard

ICS 13.110

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee MCE/3, upon which the following bodies were represented:

Advanced Manufacturing Technology Research Institute
British Cable Makers' Confederation
British Compressed Air Society
British Robot Association
British Rubber Manufacturers' Association Ltd.
British Textile Machinery Association
Consumer Policy Committee of BSI
Electrical Installation Equipment Manufacturers Association
Health and Safety Executive
Loss Prevention Council
Machine Tool Technologies Association
Machinery Safety Equipment Manufacturers' Association
PICON
Society of Laundry Engineers and Allied Trades Limited
Trades Union Congress
Co-opted members

This British Standard, having been prepared under the direction of the Engineering Sector Board, was published under the authority of the Standards Board and comes into effect on
15 June 1997

Amendments issued since publication

Amd. No.	Date	Text affected

The following BSI references relate to the work on this standard:
Committee reference MCE/3
Draft for comment 92/86050 DC

ISBN 0 580 27466 7

Contents

National foreword

This British Standard has been prepared by Technical Committee MCE/3 and is the English language version of EN 954-1 : 1996 *Safety of machinery — Safety related parts of control systems — Part 1 : General principles for design*, published by the European Committee for Standardization (CEN). EN 954-1 was produced as a result of international discussions in which the United Kingdom took an active part.

NOTE. The remaining references to draft European Standards are still under publication. They will be published as British Standards in due course.

Cross-references

Publication referred to	Corresponding British Standard
EN 292-1 : 1991	BS EN 292-1 : 1991 *Safety of machinery. Basic concepts, general principles for design. Basic terminology, methodology*
EN 292-2 : 1991	BS EN 292-2 : 1991 *Safety of machinery. Basic concepts, general principles for design. Technical principles and specifications*
EN 418 : 1992	BS EN 418 : 1992 *Safety of machinery. Emergency stop equipment, functional aspects. Principles for design*
EN 614-1 : 1995	BS EN 614-1 : 1995 *Safety of machinery. Ergonomic design principles. Terminology and general principles*
EN 982 : 1996	BS EN 982 : 1996 *Safety of machinery. Safety requirements for fluid power systems and their components. Hydraulics*
EN 1037 : 1995	BS EN 1037 : 1996 *Safety of machinery. Prevention of unexpected start-up*
EN 60204-1 : 1993	BS EN 60204-1 : 1993 *Safety of machinery. Electrical equipment of machines. Specification for general requirements*
EN 60447 : 1993	BS EN 60447 : 1994; IEC 447 : 1993 *Man-machine interface (MMI). Actuating principles*
EN 60529 : 1991	BS EN 60529 : 1992 *Specification for degrees of protection provided by enclosures (IP code)*
EN 60721-3-0 : 1993	BS EN 60721-3-0 : 1993; IEC 721-3-0: 1984 *Classification of environmental conditions. Classification of groups of environmental parameters and their severities. Introduction*

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the EN title page, pages 2 to 22, an inside back cover and a back cover.

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 securité — 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.

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 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

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.

Contents

1) Standard in preparation.

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 role 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.

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 system 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 stopping 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 state:

– 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 predominantly 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 will 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 design 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.

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.

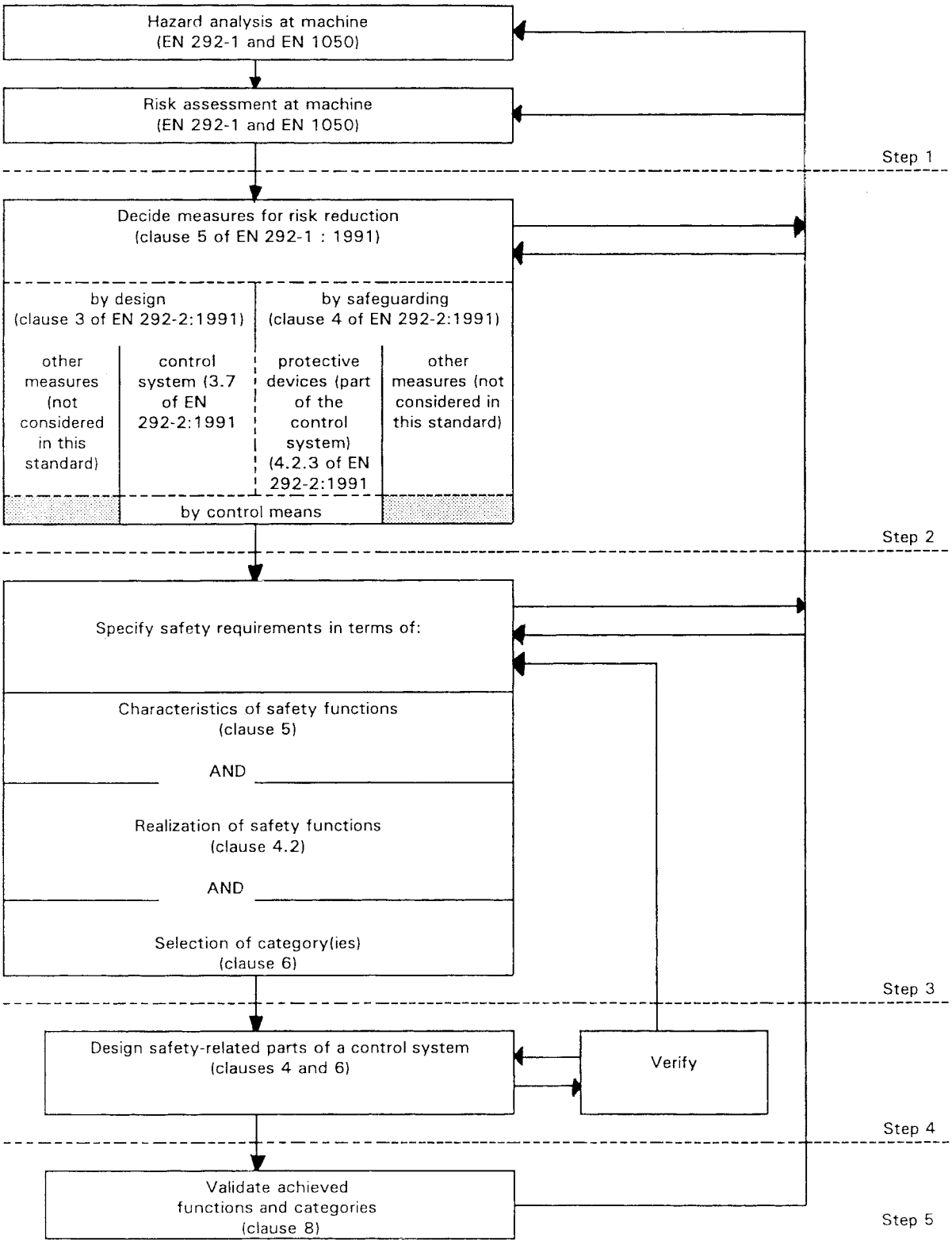


Figure 1. Iterative process for the design of safety-related parts of control systems

Table 1. List of some standards giving requirements for characteristics of safety function

Safety functions, characteristics	Requirements					Additional information[1)]
	EN 954-1 : 1996	EN 292 :		Annex A of EN 292- 2 : 1991/A1 : 1995	Further standards	
		Part 1 : 1991	Part 2 : 1991			
Definitions	**3**	**3**			clause **3** of EN 60204-1 : 1992	clause **2** of EN 60335-1 : 1994
Design principles	**4.2**		**3**	**1.2.1**, **1.2.2**, **1.2.7**, **1.5.4**	**9.4** of EN 60204-1 : 1992	clause **22** of EN 60335-1 : 1994, clauses **5** and **6** of EN 775 : 1992 + AC : 1993, clause **5** of prEN 1921 : 1995
Ergonomic principles	**4.4**	**4.9**	**3.6**, **3.7.8**a	**1.2.2**, Para 1	clause **10** of EN 60204-1 : 1992	**6.2** of EN 775 : 1992 + AC : 1993, **4.6** of prEN 1921 : 1995
Stop function	**5.2**		**3.7.1**, **3.7.8**b	**1.2.4**, **1.3.5**	**9.2.2**, **9.2.5.3** of EN 60204-1 : 1992	**7.12** of EN 60335-1 : 1994, **5.11** of prEN 1921 : 1995
Emergency stop function	**5.3**		**6.1.1**	**1.2.4**	EN 418, **9.2.5.4** of EN 60204-1 : 1992	**6.4.2**, **7.2.5** of EN 775 : 1992 + AC : 1993, **5.11.2** of prEN 1921 : 1995
Manual reset	**5.4**			**1.2.4**	**9.2.5.3**, **9.2.5.4** of EN 60204-1 : 1992	**6.4.2**, **6.4.3**, **7.6** of EN 775 : 1992 + AC : 1993, **6.4.3** of prEN 1921 : 1995
Start and restart	**5.5**		**3.7.1**, **3.7.2**	**1.2.3**, **1.3.5**	**9.2.1**, **9.2.5.1**, **9.2.5.2**, **9.2.6** of EN 60204-1 : 1992	**6.10**, **7.2.5**, **7.3.1**, **9.3.4** of EN 775 : 1992 + AC : 1993
Response time	**5.6**				**3.2**, **A.3**, **A.4** of prEN 999 : 1995	
Safety-related parameters	**5.7**		**3.7.9**e		**7.1**, **9.3.2**, **9.3.4** of EN 60204-1 : 1992	**4.2** of EN 775 : 1992 + AC : 1993, **11.8** of EN 60335-1 : 1994
Local control function	**5.8**		**3.7.9**, **3.7.10**			**3.2.9**, **7.2.6** of EN 775 : 1992 + AC : 1993, **3.13**, **4.5**, **5.9**, **6.2** of prEN 1921 : 1995
Muting	**5.9**					
Manual suspension of safety functions	**5.10**		**3.7.10**, **4.1.4**	**1.2.5**	**9.2.4** of EN 60204-1 : 1992	**6.10** of EN 775 : 1992 + AC : 1993, **5.8** of prEN 1921 : 1995
Fluctuations, loss and restoration of power sources	**5.11**		**3.7.8**e	**1.2.6**, **1.5.3**	**4.3**, **7.1**, **7.5** of EN 60204-1 : 1992	
Programmable electronic systems			**3.7.7**		**12.3** of EN 60204-1 : 1992	IEC 1508[2)]
Unexpected start-up			**3.7.2**	**1.2.3**, **1.2.6**, **1.2.7**	prEN 1037, **5.4** of EN 60204-1 : 1992	
Indications and alarms			**3.6.7**, **5.3**	**1.2.2**, Para 4, 6, **1.7.0**, **1.7.1**	EN 457, EN 842, prEN 981, **10.4**, **11.3** of EN 60204-1 : 1992, EN 60447	**5.6** of prEN 1921 : 1995
Escape and rescue of trapped persons			**6.1.2**	**1.2.2**, Para 5, 6		

Table 1. List of some standards giving requirements for characteristics of safety function *(continued)*

Safety functions, characteristics	**Requirements**					**Additional information**[1)]
	EN 954-1 : 1996	**EN 292 :**		**Annex A of EN 292- 2 : 1991/A1 : 1995**	**Further standards**	
		Part 1 : 1991	**Part 2 : 1991**			
Electrical equipment		**3.9**		**1.5.1**, **1.5.7**	EN 60204-1	
Electrical supply				**1.5.1**	**4.3** of EN 60204-1 : 1992	
Other supply				**1.5.3**	**5.1.4** of EN 982 : 1992, **5.1.4** of EN 983 : 1992	
Covers and enclosures					**13.4** of EN 60204-1 : 1992, EN 60529	
Pneumatic and hydraulic equipment			**3.8**	**1.5.3**	EN 982, EN 983	
Isolation and energy dissipation			**6.2.2**	**1.6.3**	EN 1037, **5.3**, **6.3.1** of EN 60204-1 : 1992	
Physical environment and operating conditions			**3.7.11**		**4.4** of EN 60204-1 : 1992	**6.9** of EN 775 : 1992 + AC : 1993, **4.3**, **4.5** of prEN 1921 : 1995
Control modes and mode selection			**3.7.9**, **3.7.10**	**1.2.5**	**9.2.3** of EN 60204-1 : 1992	**6.10** of EN 775 : 1992 + AC : 1993
Interfaces/connections				**1.5.4**, **1.6.1**, Para 3	**9.1.4**, **11**, **15.4** of EN 60204-1 : 1992	
Interaction between different safety-related parts of control systems			**3.7.8**e		**9.3.4** of EN 60204-1 : 1992	
Man-machine interface			**3.6.6**, **3.6.7**	**1.2.2**	clause **10** of EN 60204-1 : 1992, EN 60447	

[1)] The references in this column are to be considered as an aid to the designer but not part of the requirements of this standard.
[2)] Standard in preparation.

5.2 Stop function

In addition to the requirements of the reference given in table 1 the following shall also apply.

A stop function initiated by a protective device shall, as soon as necessary after actuation, put the machine in a safe state. Such a stop shall have priority over a stop for operational reasons.

When a group of machines are working together in a co-ordinated manner, provision shall be made to signal to the supervisory control and/or the other machines that such a stop condition exists.

NOTE. Such a stop can cause operational problems and a difficult restart, e.g. in arc welding. In some applications this function can be combined with a stop for operational reasons to reduce the temptation to defeat the safety function.

5.3 Emergency stop function

In addition to the requirements of the reference given in table 1 the following shall also apply.

When a group of machines are working together in a co-ordinated manner the safety-related parts shall have the facility to signal an emergency stop condition to all parts of the co-ordinated system.

Where sections of the co-ordinated system are clearly separated, e.g. by safeguards or physical position, it is not always necessary to apply an emergency stop to the whole system but only to particular section(s) as identified by the risk assessment.

After an emergency stop has become effective for a section a hazard shall not be present at the interfaces of this section to other sections.

5.4 Manual reset

In addition to the requirements of the reference given in table 1 the following shall also apply.

After a stop command has been initiated by a protective device, the stop condition shall be maintained until the manual reset device is actuated and safe conditions for restarting exist.

The re-establishment of the safety function by resetting the protective device cancels the stop command. If indicated by the risk assessment this cancellation of the stop command shall be confirmed by a manual, separate and deliberate action (manual reset).

The manual reset function:

– shall be provided through a separate and manually operated device within the safety-related parts of the control system;

– shall only be achieved if all safety functions and protective devices are operative. If this is not possible the reset shall not be achieved;

– shall not initiate motion or a hazardous situation by itself;

– shall be by deliberate action;

– shall prepare the control system for accepting a separate start command;

– shall only be accepted by actuation of the actuator from its released (off) position.

The category of safety-related parts providing the manual reset shall be selected so that the inclusion of the manual reset does not diminish the safety required of the relevant safety function.

The reset actuator shall be situated outside the danger zone and in a safe position from which there is a good visibility for checking that no person is within the danger zone.

5.5 Start and restart

In addition to the requirements of the reference given in table 1 the following shall also apply.

A restart shall take place automatically only if a hazardous situation cannot exist. In particular, for control guards, see **4.2.2.5** of EN 292-2 : 1991.

These requirements for start and restart shall also apply to machines which can be controlled remotely.

5.6 Response time

In addition to the requirements of the reference given in table 1 the following shall also apply.

The designer or supplier shall declare the response time when the risk assessment of the safety-related parts of the control system indicates that this is necessary (see also clause **10**).

NOTE. The response time of the control system is part of the overall response time of the machine. The required overall response time of the machine can influence the design of the safety-related part, e.g. the need to provide a braking system.

5.7 Safety-related parameters

In addition to the requirements of the reference given in table 1 the following shall also apply.

When safety-related parameters, e.g. position, speed, temperature, pressure, deviate from preset limits the control system shall initiate appropriate measures, e.g. actuation of stopping, warning signal, alarm.

If errors in manual inputting of safety-related data in programmable electronic systems can lead to a hazardous situation, then a data checking system within the safety-related control system shall be provided, e.g. check of limits, format and/or logic input values.

5.8 Local control function

When a machine is controlled locally, e.g. by a portable control device, pendant, the following requirements shall also apply in addition to the requirements of the reference given in table 1:

– the means for selecting local control shall be situated outside the danger zone;

– it shall not be possible to initiate hazardous conditions from outside the zone of local control;

– switching between local and external, e.g. remote, control shall not create a hazardous situation.

5.9 Muting

Muting shall not result in any person being exposed to hazardous situations.

During muting safe conditions shall be provided by other means.

At the end of muting all safety functions of the safety-related parts of the control system shall be reinstated.

The category of safety-related parts providing the muting function shall be selected so that the inclusion of the muting function does not diminish the safety required of the relevant safety function.

NOTE. In some applications an indication signal of muting is necessary.

5.10 Manual suspension of safety functions

If it is necessary to manually suspend safety functions, e.g. for set up, adjustments, maintenance, repair, the following requirements shall also apply in addition to the requirements of the reference given in table 1:

– effective and secure means to prevent manual suspension in those operating modes where it is not allowed;

– reinstatement of the safety functions of the safety-related parts of the control system before normal operations can be continued;

– selection of the safety-related parts of the control system which are responsible for the manual suspension so that the principles of EN 1050 are fully taken into account.

NOTE. In some applications an indication signal of manual suspension is necessary.

5.11 Fluctuations, loss and restoration of power sources

In addition to the requirements of the reference given in table 1 the following shall also apply.

When fluctuations in energy levels outside the design operating range occur, including loss of energy supply, the safety-related parts of the control system shall continue to provide or initiate output signal(s) which will enable other parts of the machine system to maintain a safe state.

6 Categories

6.1 General

The safety-related parts of control systems shall be in accordance with the requirements of one or more of the 5 categories specified in **6.2**. These categories are not intended to be used in any given order or in any given hierarchy in respect of safety requirements.

The categories state the required behaviour of safety-related parts of a control system in respect of its resistance to faults based on the strategy described in **4.2**.

Category B is the basic category. The occurrence of a fault can lead to the loss of the safety function. In category 1 improved resistance to faults is achieved predominantly by selection and application of components. In categories 2, 3 and 4, improved performance in respect to a specified safety function is achieved predominantly by improving the structure of the safety-related part of the control system. In category 2 this is provided by periodically checking that the specified safety function is being performed. In categories 3 and 4 this is provided by ensuring that the single fault will not lead to the loss of the safety function. In category 4, and whenever reasonably practicable in category 3, such faults will be detected. In category 4 the resistance to the accumulation of faults will be specified.

Direct comparison of behaviour to resist faults, between categories, can only be made if one parameter (see **4.2**) at a time is changed. Higher numbered categories can only be interpreted as providing a greater resistance to faults in comparable circumstances, e.g. when using similar technology, components of comparable reliability, similar maintenance regimes and in comparable applications.

Table 2 gives an overview of categories of safety-related parts of control systems, the requirements and the system behaviour in case of faults.

When considering the causes of failures in some components it is possible to exclude certain faults (see clause **7**).

6.2 Specifications of categories

6.2.1 *Category B*

The safety-related parts of control systems shall, as a minimum, be designed, constructed, selected, assembled and combined, in accordance with the relevant standards, using basic safety principles for the specific application so that they can withstand:

– the expected operating stresses, e.g. the reliability with respect to breaking capacity and frequency;

– the influence of the processed material, e.g. detergents in a washing machine;

– other relevant external influences, e.g. mechanical vibration, external fields, power supply interruptions or disturbances.

NOTE 1. No special measures for safety are applied to parts complying with category B.

NOTE 2. When a fault occurs it can lead to the loss of the safety function. To fulfil the requirements of annex A of EN 292-2 : 1991/A1 : 1995 additional measures, which are not provided by the safety-related parts of the control system can be necessary.

Table 2. Summary of requirements for categories (For full requirements see clause **6**)

Category[1)]	**Summary of requirements**	**System behaviour**[2)]	**Principles to achieve safety**
B (see **6.2.1**)	Safety-related parts of control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence.	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components.
1 (see **6.2.2**)	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B.	
2 (see **6.2.3**)	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.	– The occurrence of a fault can lead to the loss of the safety function between the checks. – The loss of safety function is detected by the check.	Mainly characterized by structure.
3 (see **6.2.4**)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that: – a single fault in any of these parts does not lead to the loss of the safety function; and – whenever reasonably practicable the single fault is detected.	– When the single fault occurs the safety function is always performed. – Some but not all faults will be detected. – Accumulation of undetected faults can lead to the loss of the safety function.	
4 (see **6.2.5**)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that: – a single fault in any of these parts does not lead to a loss of the safety function; and – the single fault is detected at or before the next demand upon the safety function. If this is not possible, then an accummulation of faults shall not lead to a loss of the safety function.	– When the faults occur the safety function is always performed. – The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure.

[1)] The categories are not intended to be used in any given order or in any given hierarchy in respect of safety requirements.
[2)] The risk assessment will indicate whether the total or partial loss of the safety function(s) arising from faults is acceptable.

6.2.2 ***Category 1***

The requirements of category B and of this subclause shall apply.

Safety-related parts of control systems to category 1 shall be designed and constructed using well-tried components and well-tried safety principles.

A well-tried component for a safety-related application is a component which has been:

– widely used in the past with successful results in similar applications; or

– made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

In some well-tried components certain faults can also be excluded because the fault rate is known to be very low.

The decision to accept a particular component as a well-tried one, can depend on the application.

NOTE 1. On the level of single electronic components alone, it is not normally possible to realize category 1.

Well-tried safety principles are, for example:

– avoidance of certain faults, e.g. avoidance of short circuit by separation;

– reducing the probability of faults, e.g. over-dimensioning or underrating of components;

– by orientating the mode of fault, e.g. by ensuring an open circuit when it is vital to remove power in the event of fault;

– detect faults very early;

– restrict the consequences of a fault, e.g. earthing of equipment.

Newly developed components and safety principles may be considered as equivalent to 'well-tried' if they fulfil the above mentioned conditions.

NOTE 2. The probability of failure in category 1 is lower than in category B. Consequently the loss of the safety function is less likely.

NOTE 3. When a fault occurs it can lead to the loss of the safety function. To fulfil the requirements of annex A of EN 292-2 : 1991/A1 : 1995 additional measures, which are not provided by the safety-related parts of the control system can be necessary.

6.2.3 ***Category 2***

The requirements of category B, the use of well-tried safety principles and the requirements in this subclause shall apply.

Safety-related parts of control systems to category 2 shall be designed so that their function(s) are checked at suitable intervals by the machine control system. The check of the safety function(s) shall be performed:

– at the machine start-up and prior to the initiation of any hazardous situation; and

– periodically during operation if the risk assessment and the kind of operation shows that it is necessary.

The initiation of this check may be automatic or manual. Any check of the safety function(s) shall either:

– allow operation if no faults have been detected; or

– generate an output which initiates appropriate control action, if a fault is detected. Whenever possible this output shall initiate a safe state. When it is not possible to initiate a safe state (e.g. welding of the contact in the final switching device) the output shall provide a warning of the hazard.

The check itself shall not lead to a hazardous situation. The checking equipment may be integral with, or separate from, the safety-related part(s) providing the safety function.

After the detection of a fault a safe state shall be maintained until the fault is cleared.

NOTE 1. In some cases category 2 is not applicable because the checking of the safety function cannot be applied to all components, e.g. pressure switch or temperature sensor.

NOTE 2. In general category 2 can be realised with electronic techniques, e. g. in protective equipment and particular control systems.

NOTE 3. Category 2 system behaviour allows that:

– the occurrence of a fault can lead to the loss of the safety function between checks;

– the loss of safety function is detected by the check.

6.2.4 ***Category 3***

The requirements of category B, the use of well-tried safety principles and the requirements in this subclause shall apply.

Safety-related parts of control systems to category 3 shall be designed so that a single fault in any of these parts does not lead to the loss of the safety function. Common mode faults shall be taken into account when the probability of such a fault occurring is significant. Whenever reasonably practicable the single fault shall be detected at or before the next demand upon the safety function.

NOTE 1. This requirement of single fault detection does not mean that all faults will be detected. Consequently, the accumulation of undetected faults can lead to an unintended output signal and a hazardous situation at the machine. Typical examples of practicable measures for fault detection are the connected movement of relay contacts or monitoring of redundant electrical outputs.

NOTE 2. If it is necessary, because of technology and application, Type-C standard makers should give further details on the detection of faults.

NOTE 3. Category 3 system behaviour allows that:

– when the single fault occurs the safety function is always performed;

– some but not all faults will be detected;

– accumulation of undetected faults can lead to the loss of the safety function.

NOTE 4. 'Whenever reasonably practicable' means that the required measures for fault detection and the extent to which they are implemented depends mainly upon the consequence of a failure and the probability of the occurrence of this failure within the application. The technology used will influence the possibilities for the implementation of fault detection.

6.2.5 *Category 4*

The requirements of category B, the use of well-tried safety principles and the requirements in this subclause shall apply.

Safety-related parts of control systems to category 4 shall be designed so that:

– a single fault in any of these safety-related parts does not lead to a loss of the safety function; and

– the single fault is detected at or before the next demand upon the safety functions, e.g. immediately, at switch on, at end of a machine operating cycle. If this detection is not possible, then an accumulation of faults shall not lead to a loss of the safety function.

If the detection of certain faults is not possible, at least during the next check-up after the occurrence of the fault, for reasons of technology or circuit engineering, the occurrence of further faults shall be assumed. In this situation the accumulation of faults shall not lead to the loss of the safety function. Fault review may be stopped when the probability of occurrence of further faults is considered to be sufficiently low. In this case the number of faults in combination, which need to be taken into consideration, will depend upon the technology, structure and application but shall be sufficient to meet the detection criteria.

NOTE 1. In practice, the number of faults which need to be considered will vary considerably, for example, in the case of complex microprocessor circuits, a large number of faults can exist but in an electro-hydraulic circuit, the consideration of three (or even two) faults can be sufficient.

This fault review may be limited to two faults in combination, when:

– the fault rates of the components are low; and

– the faults in combination are largely independent of each other; and

– the interruption of the safety function occurs only when the faults appear in a certain order.

If further faults occur as a result of the first single fault the first and all consequent faults shall be considered as a single fault.

Common mode faults shall be taken into account, e.g. by using diversity, special procedures to identify such faults.

NOTE 2. In the case of the complex circuit structures, e.g. microprocessors, complete redundancies, the review of faults is generally carried out at the structural level, i.e., based on assembly groups.

NOTE 3. Category 4 system behaviour allows that:

– when the faults occur the safety function is always performed;

– the faults will be detected in time to prevent the loss of the safety function.

6.3 Selection and combination of safety-related parts to different categories

The safety functions (see **3.6** and clause **5**) are specified by the procedure described in **4.3** (figure 1, step 3). Categories according to **6.2** should be selected for all safety-related parts of the control system. The design and selection of safety-related parts of the control system shall be done according to clauses **4** and **5**. A single safety function may be processed by one or more safety-related parts. Similarly several safety functions may be processed by one or more safety-related parts. In practice it can be necessary to implement one or more safety functions to achieve the reduction in risk.

When a safety function is realized by several safety-related parts, e.g. sensors, control units, power control elements, these parts may be to one category and/or to different categories in combination.

When safety-related parts to the same or different categories are used in combination to fulfil a safety function an analysis of the combination shall be included in the overall validation required in step 5 of **4.3**. This analysis is simpler if the categories of some or all of the safety-related parts used are already known.

The selection of a category for a particular safety-related part of the control system depends mainly upon:

– the reduction in risk to be achieved by the safety function to which the part contributes;

– the probability of occurrence of a fault(s) in that part;

– the risk arising in the case of a fault(s) in that part;

– the possibilities to avoid a fault(s) in that part;

– the technologies used.

Additional information for the selection of categories is given in annex B.

7 Fault consideration

7.1 General

In accordance with the category required, safety-related parts shall be selected on their ability to resist faults (see **4.2**). To assess their ability to resist faults the various modes of failure shall be considered. Also, certain faults may be excluded (see **7.2**).

Annex C lists some of the significant faults and failures for the various technologies. These lists and the ways in which they shall be validated are further elaborated in Part 2 of this standard. The lists of faults given in annex C and in Part 2 are not exclusive and, if necessary, additional faults should be considered and listed. In such cases the method of validation should also be clearly elaborated.

In general, the following fault criteria shall be taken into account:

– if as consequence of a fault further components fail, the first fault and all these following faults shall be considered to be a single fault;

– common mode faults are regarded as a single fault;

– the occurrence at the same time of two independent faults is not considered.

For detailed information see also EN 982, EN 983 and prEN 50100-1[2)]

7.2 Fault exclusion

It is impracticable to assess safety-related parts of control systems without assuming that certain faults can be excluded. The faults which can be excluded are a compromise between the technical requirements for safety and the theoretical possibilities of occurrence. This will be influenced by the design, dimensioning, installation and arrangement of components in the safety-related parts. The designer shall declare, justify and list all fault exclusions.

Fault exclusion can be based on:

– the improbability of occurrence of certain fault(s);

– generally accepted technical experience which can be applied independently of the application under consideration;

– technical requirements deriving from the application and the specific risk under consideration.

8 Validation

8.1 General

This clause explains the requirements of step 5 in **4.3**.

The purpose of validation is to determine the level of conformity of the safety-related parts of the control system to their specification within the overall safety requirements specification of the machinery. Validation consists of executing tests and applying analysis in accordance with the validation plan (see **8.2**).

The design of the safety-related parts of the control system shall be validated. The validation shall demonstrate that each safety-related part meets:

– all the requirements of the specified category (see clause **6**); and

– the specified safety characteristics for that part, as set out in the design rationale.

The validation of the safety-related parts of control systems should contain the following elements:

– selection of the validation strategy (a validation plan);

– management and execution of validation activities (test specifications, testing procedures, analysis procedures);

– documentation (auditable reports of all validation activities and decisions).

NOTE. Guidance on validation procedures is given in IEC 1508[3)].

8.2 Validation plan

The validation plan shall identify the requirements for carrying out all stages of the validation process. The plan should be developed concurrently with the design of the safety-related parts of the control system or can be specified by the relevant Type-C standard. The plan should include a description of all the requirements for:

– validation by analysis;

– validation by testing, including:

a) test of the specified safety functions;

b) test of the specified categories;

c) test of dimensioning and compliance to environmental parameters.

8.3 Validation by analysis

In general analysis it is necessary to validate that the reduction in risk has been achieved. Examples of analysis tools include fault lists (see clause **7**), fault tree analysis, failure mode and effect analysis, criticality analysis, check lists for systematic faults.

8.4 Validation by testing

8.4.1 *Test of the specified safety functions*

An important step is the testing of the safety functions (of the safety-related parts of the control system) for complete compliance with their specified characteristics. It is important to check for errors and particularly for omissions when formulating the specification, and during development, of the machine.

The aim of testing of the safety functions is to ascertain that the safety-related output signals are correct and logically dependant on the input signals. The tests should cover all normal and foreseeable abnormal conditions in static and dynamic simulation, as necessary from the risk assessment, to validate the system.

---

2) Will be replaced by prEN 61496-1.
3) Standard in preparation.

8.4.2 *Test of the specified categories*

The categories are based on behaviour in the event of a fault. The tests shall demonstrate that this requirement is fulfilled. The test procedures shall be chosen on the basis of two criteria: technology and complexity of the control system. Principally, the following methods are applicable:

– a theoretical check and behaviour analysis based on circuit diagrams;

– practical tests on the actual circuit and fault simulation on actual components, particularly in areas of doubt, of behaviour identified during the theoretical check and analysis;

– a simulation of control system behaviour, e.g. by means of hardware and/or software models.

In some applications when the safety-related parts of the control system are connected in a complex manner, it is usually necessary to divide the connected safety-related parts into several functional groups and to exclusively submit the interfaces to fault simulation tests.

Guidance for assessing programmable electronic systems is given in annex E.

8.4.3 *Test of dimensioning and compliance to environmental parameters*

These tests shall demonstrate that the specified design performance is achieved during all specified operating modes and all specified environmental conditions. The test should include, e.g., tests for expected mechanical structure, electrical ratings, temperature, humidity, vibration, shock loading, electromagnetic compatibility, influence of processed materials.

For these tests the relevant standards should be taken into account, e.g. EN 60204-1, EN 60529, EN 60721-3-0, EN 61000-4-1, IEC 68.

8.5 Validation report

At the conclusion of the validation process, a safety validation report shall be made summarising the tests and analyses indicating which were accomplished, including the results. The report should specifically identify:

– all items under test;

– personnel responsible for testing;

– test equipment (including details of calibration) and simulation tools;

– the analyses and tests carried out;

– the problems encountered and how these problems were resolved;

– the results.

The results shall be documented and retained in an auditable form.

NOTE. Compliance with **8.5** will assist the manufacturer in the completion of the technical construction file in respect of the safety-related parts of the control system.

9 Maintenance

Preventive or corrective maintenance is usually necessary to maintain the specified performance of the safety-related parts. Deviations with time from the specified performance can lead to a deterioration in safety or can even lead to a hazardous situation. To identify such deviations manual periodic inspections are sometimes necessary.

The provisions for the maintainability of the safety-related part(s) of a control system shall follow the principles of **6.2.1** of EN 292-2 : 1991 and **1.6** of annex A of EN 292-2 : 1991/A1 : 1995. All information for maintenance shall comply with **5.5.1**e of EN 292-2 : 1991.

10 Information for use

The principles of clause **5** of EN 292-2 : 1991 and other relevant documents, e.g. clauses **18** and **19** of EN 60204-1 : 1992, shall be applied. In particular that information which is important for the safe use of the safety-related parts of the control system shall be given to the user. This includes but is not limited to:

– the limits of the safety-related parts to the category(ies) selected and any fault exclusions;

NOTE. When fault exclusions are essential in maintaining the selected category(ies) and safety performance, appropriate information, e.g. for modification, maintenance and repair, will be needed to ensure the continued justification of that fault exclusion(s).

– the effects of deviations from the specified performance on the safety function(s);

– clear descriptions of the interfaces to the safety-related parts of control systems and protective devices;

– response time;

– operating limits (including environmental conditions);

– indications and alarms;

– muting and suspension of safety functions;

– control modes;

– maintenance (see clause **9**);

– maintenance check lists;

– ease of accessibility and replacing of internal parts;

– means for easy and safe trouble shooting.

Whenever information is provided about the category(ies) of the safety-related parts of the control system they shall be referred to in the following way:

– EN 954 Category B;

– EN 954 Category 1;

– EN 954 Category 2;

– EN 954 Category 3;

– EN 954 Category 4.

Annex A (informative)

Questionnaire for the design process

This annex lists some important aspects to be taken into consideration during the design process (see **4.3**).

A.1 What reaction is required from the safety-related parts of the control system(s) when faults occur?

a) No special action required.

b) Safe reaction required within a certain time.

c) Safe reaction immediately required.

A.2 In which safety-related part(s) of the control system should faults be assumed?

a) Only in those parts in which (by experience) faults occur relatively often, e.g. in the peripheral sensors and wiring.

b) In auxiliary parts.

c) In all safety-related parts.

A.3 Have both random and systematic faults to be considered?

A.4 Which faults should be assumed in the components of the safety-related parts of the control system?

a) Faults only in components which are not well-tried.

NOTE. 'Well-tried' not in the sense of reliability, but from the view of safety (see **6.2.2**).

b) Faults in all components.

A.5 Has the correct reference category been selected in respect of the requirement for detecting faults?

a) Normal requirements for fault detection.

NOTE. This means, that all faults which can be detected with relatively simple methods, should be detected.

b) Strong requirements for fault detection.

NOTE. This means that techniques should be used which enable most of the faults to be detected. If this is not reasonably practicable, combinations of faults should be assumed (fault accumulation, see **6.2.5**).

A.6 What shall be the next action of the control system if a fault has been detected?

a) The machine should be brought to a predetermined state as required by the risk assessment.

b) Further operation of the machine can be permitted until the fault is rectified.

c) The indication of the fault(s) is sufficient (e.g. warning signal by visual display units (VDU).

A.7 What is necessary to meet the maintenance requirement?

a) Provision of information about the effects of deviations from design specifications.

b) Automatic indication of the need of maintenance.

c) Setting of maintenance intervals.

d) Setting of components life.

e) Provision of diagnostic facilities and test points.

f) Special precautions for safety during maintenance.

A.8 What methods should be used for fault detection?

a) Automatic fault detection, as far as it is appropriate.

b) Manual fault detection, e.g. by periodic inspection.

c) By more than one method.

A.9 Has the risk reduction been achieved?

a) Can the risk reduction be achieved more easily with a different combination of risk reduction measures?

b) Check that the measures taken:

– do not reduce the ability of the machine to perform its function,

– do not generate new, unexpected hazards or problems.

c) Are the solutions valid for all operating conditions and for all procedures?

d) Are these solutions compatible with each other?

e) Is the safety specification correct?

A.10 Have ergonomic principles been considered?

a) Are the safety-related parts of the control system, including the protective devices, easy to use?

b) Is there safe and easy access to the control system?

c) Are warning signals given priority (e.g. highlighted)?

A.11 Have the relationships between safety, reliablity, availability and ergonomics been optimised in such a way that the safety measures will be maintained during the lifetime of the system, and does not tempt personnel to defeat the safety functions?

Annex B (informative)
Guidance for the selection of categories

B.1 General

This annex describes a simplified method based on EN 1050 (particularly in respect to a simplification of the elements of risks in **7.1** of EN 1050 : 1996) to select the appropriate categories as reference points for the design of the various safety-related parts of a control system. The guidance given in this annex should be considered as part of the risk assessment given in EN 1050 and not a substitute for it.

It is important that the design of safety-related parts of control systems including the selection of categories, as described in clause **4** should be based on a risk assessment using the principles given in EN 1050 and be part of the overall risk assessment for the machine.

To quantify risk is usually very difficult or impossible and this method is only concerned with the contribution to the reduction in risk made by the safety-related parts of the control system. This method provides only an estimation of risk reduction and is intended to guide the designer and standard maker to a choice of category based on its behaviour in case of a fault. However this is only one aspect and other influences will also contribute to the assessment that adequate safety has been achieved. These include, e.g. component reliability, the technology used, the particular application, and they can indicate a deviation from the expected choice of category.

The method is as follows:

The severity of injury (denoted by S) is relatively easy to estimate, for example, laceration, amputation, fatality.

For the frequency of occurrence, auxiliary parameters are used to improve the estimation. These parameters are:

– frequency and exposure time to the hazard (F);

– possibility of avoiding the hazard (P).

Experience has shown that these parameters can be combined as in figure B.1 to give a gradation of risk from low to high. It is emphasized that this is a qualitative process which gives only an estimation of risk.

In figure B.1 the preferred category(ies) is indicated by a large filled circle. In some applications the designer or Type-C standard maker can deviate to another category indicated by either a small circle or a large unfilled circle. Other than preferred categories can be used (see **6.3**), but the intended system behaviour in case of fault(s) should be maintained. Reasons for deviating should be given. These reasons, to select other than the preferred categories, can be the use of different technologies, e.g. well-tried hydraulic or electro-mechanical components (category 1) in combination with electrical or electronic systems (category 3 or 4). When categories indicated with a small circle in figure B.1 are selected, additional measures can be required, e.g.:

– over dimensioning or the use of techniques leading to fault exclusion;

– the use of dynamic monitoring.

For example, a risk estimation with the parameter S1 (see **B.2.1**) gives the category for the safety-related part of the control system as a category 1. In some applications the designer or the Type-C standard maker can choose category B by using other safeguarding measures.

B.2 Guidance for selecting parameters S, F and P for the risk estimation

B.2.1 *Severity of injury S1 and S2*

In estimating the risk arising from a fault(s) in the safety-related parts of a control system only slight injuries (normally reversible) and serious injuries (normally irreversible including death) are considered.

To make a decision the usual consequences of accidents and normal healing processes should be taken into account in determining S1 and S2, e.g. bruising and/or lacerations without complications would be classified as S1 whereas an amputation or death would be classified as S2.

B.2.2 *Frequency and/or exposure time to the hazard F1 and F2*

A generally valid time period when parameter F1 or when parameter F2 should be selected cannot be specified. However, the following explanation can facilitate making the right decision in cases of doubt.

F2 should be selected if a person is frequently or continuously exposed to the hazard. It is irrelevant whether the same or different persons are exposed to the hazard on successive exposures, e.g. for the use of lifts.

The period of exposure to the hazard should be evaluated on the basis of an average value which can be seen in relation to the total period of time in which the equipment is used. For example, if it is necessary to reach regularly between the tools of the machine during cyclic operation in order to feed and move work pieces, then F2 should be selected. If access is only required from time to time, then F1 can be selected.

B.2.3 Possibility of avoiding the hazard P

When a hazard arises it is important to know if it can be recognized and whether it can be avoided before it leads to an accident. For example, an important consideration is whether the hazard can be directly identified by its physical characteristics, or whether it can only be recognized by technical means, e.g. indicators. Other important aspects which influence the selection of parameter P include, e.g.:

– operation with or without supervision;

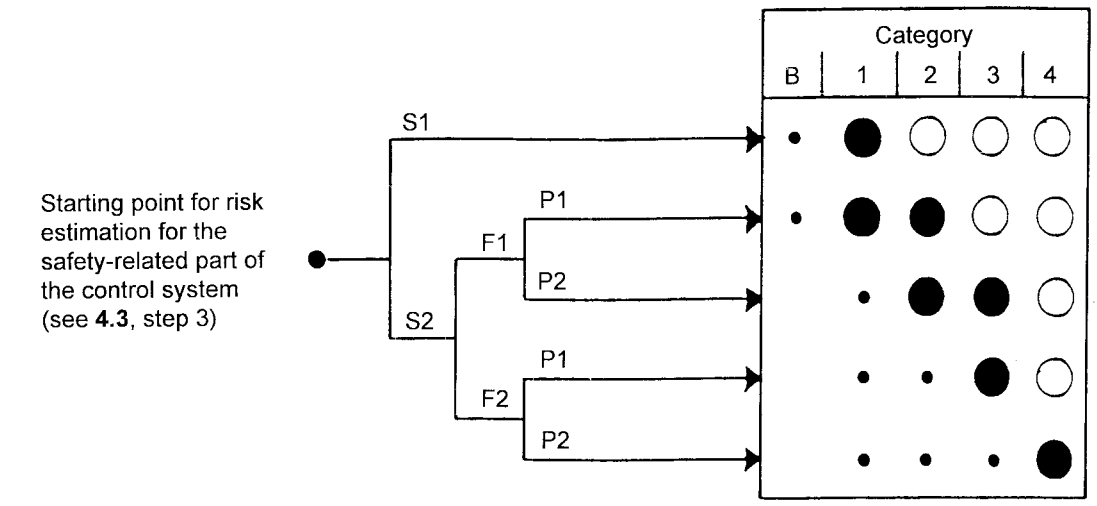
– operation by experts or non-professionals;

– speed with which the hazard arises, e.g. quickly or slowly;

– possibilities for hazard avoidance, e.g. by taking flight or by intervention of a third party;

– practical safety experiences relating to the process.

When a hazardous situation occurs P1 should only be selected if there is a realistic chance of avoiding an accident or of significantly reducing its effect. P2 should be selected if there is almost no chance of avoiding the hazard.



Key

S Severity of injury

S1 Slight (normally reversible) injury

S2 Serious (normally irreversible) injury including death

F Frequency and/or exposure time to the hazard

F1 Seldom to quite often and/or the exposure time is short

F2 Frequent to continuous and/or the exposure time is long

P Possibility of avoiding the hazard

P1 Possible under specific conditions

P2 Scarcely possible

Category selection

B, 1 to 4 Categories for safety-related parts of control systems

● Preferred categories for reference points (see **4.2**)

• Possible categories which can require additional measures (see **B.1**)

○ Measures which can be over dimensioned for the relevant risk

Figure B.1 Possible selection of categories

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

C.1 Electrical/electronic components

Some faults and failures to be considered are:

– short circuit or open circuit, e.g. earth faults (short circuit to the protective conductor or a conductive part), open circuit of any conductor;

– short circuit or open circuit occurring in single components, e.g. in position switches, control and regulation equipment, machine actuators, relays;

– non drop-out or non pick-up of electromagnetic elements, e.g. contactors, relays solenoids;

– non-starting or non-stopping of motors, e.g. servomotors;

– mechanical blocking of moving elements, loosening or displacing of fixed elements, e.g. position switches;

– drift beyond the tolerance values for analogue elements, e.g. resistors, capacitors, transistors;

– oscillation of (unstable) output signals in integrated components;

– loss of entire function or of partial functions (worst-case-behaviour) in complex integrated components, e.g. microprocessors, programmable electronic systems, application specific integrated circuits.

C.2 Hydraulic and pneumatic components

Some faults and failures to be considered are:

– no switching or incomplete switching of the moving element, e.g. sticking of a valve piston;

– drift in the original control position of the moving element, e.g. directional control valves;

– leakage and modification of the leakage volume flow, e.g. directional control valves;

– unstable control characteristics in servo-valves and proportional valves;

– loss of pressure or bursting of lines, e.g. of hose pipes and at the hose coupling;

– clogging of the filter element (in particular caused by solid substances);

– abnormal pressure and/or volume flow, e.g. hydraulic pumps, hydraulic motors, compressors, cylinders;

– failure or abnormal modification of the input or output signal characteristics in sensors, e.g. pressure switches.

C.3 Mechanical components

Some faults and failures to be considered are:

– spring fracture;

– stiffness or sticking of guide moving components;

– loosening of fixtures, e.g. by vibration;

– wear, e.g. runners, latches, rollers;

– misalignment of parts;

– environmental influences, e.g. corrosion, temperature.

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

The concepts of safety, reliability and availability can be described in the following way:

– Safety of a machine is the ability of a machine to perform its function, to be transported, installed, adjusted, maintained, dismantled and disposed of under conditions of intended use specified in the instruction handbook (and, in some cases, within a given period of time indicated in the instruction handbook) without causing injury or damage to health. (According to **3.4** of EN 292-1 : 1991.)

– Reliability is the ability of a machine or components, or equipment, to perform a required function without failing under specified conditions and for a given period of time. (According to **3.2** of EN 292-1 : 1991.)

– Availability is the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided. (According to IEC 50(191) : 1990.)

Safety looks at the causes and consequences of possible accidents (injury or damage to health). Safety requirements are concerned with making a system which does not cause accidents. The safety requirements ensure that the system does not reach a hazardous or unsafe state, when an event(s) could cause an accident. The safety requirements should indicate what actions ought to be taken if an unforeseen event in the environment leads to an unsafe state.

From that point of safety it does not matter if the system does not service its purpose, as long as the safety requirements are not violated. On the other hand it is possible that the system is highly reliable, but unsafe, e.g. a system with formally verified software but where a safety-related situation had not been properly specified.

Availability influences the safety. The availability of a system implies that the safety-related reliability is performed, otherwise the protective device can be defeated.

The designer has the responsibility to decide, for each application, the relationship between availability, reliability and safety to ensure that the reduction in risk is achieved.

Annex E (informative)

Bibliography

The following is a list of national, European and international publications giving additional information on safety-related parts of control systems.

E.1 Publications on programmable electronic systems

– EN 61000-4-1 *Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 1: Overview of immunity tests — Basic EMC publication* (IEC 1000-4-1 : 1992);

– prEN 50100-1[4] *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests*;

– IEC 1508[5] *Functional safety: safety-related systems* (provisional title),

– DIN V VDE 0801 *Principles for computers in safety-related computer systems*, January 1990;

– HSE Guidelines *Programmable Electronic Systems in Safety-related Applications Part 1* (ISBN 0 11 883906 6) and *Part 2* (ISBN 0 11 883906 3);

– *Personal Safety in Microprocessor Control Systems* (CECR-184, Elektronikcentralen, Denmark).

E.2 Further Publications

EN 775 : 1992 + AC : 1993	*Manipulating industrial robots — Safety* (ISO 10218 : 1992 modified) (includes AC : 1993)
prEN 894-1	*Safety of machinery — Ergonomics requirements for the design of displays and control actuators — Part 1: General principles for human interactions with displays and control actuators*
prEN 894-2	*Safety of machinery — Ergonomics requirements for the design of displays and control actuators — Part 2: Displays*
prEN 894-3	*Safety of machinery — Ergonomics requirements for the design of displays and control actuators — Part 3: Control actuators*
prEN 1005-3	*Safety of machinery — Human physical performance — Part 3: Recommended force limits for machinery operation*
prEN 1921 : 1995	*Industrial automation systems — Safety of integrated manufacturing systems — Basic requirements* (ISO 11161 : 1994 modified)
EN 60335-1 : 1994	*Safety of household and similar electrical appliances — Part 1: General requirements* (IEC 335-1: 1991 modified)
IEC 68	*Basic environmental testing procedures*

[4] Will be replaced by prEN 61496-1.
[5] Standard in preparation.

Annex ZA (informative)

Clauses of this European Standard addressing essential requirements or other provisions of EU directives

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 directives:

Council Directive of 14 June 1989 on the approximation of the laws of the Member States relating to Machinery (89/392/EEC);

Council Directive of 20 June 1991 amending Directive 89/392/EEC on the approximation of the laws of the Member States relating to machinery (91/368/EEC);

Council Directive of 14 June 1993 amending Directive 89/392/EEC on the approximation of the laws of the Member States relating to machinery (93/44/EEC).

WARNING. Other requirements and other EU directives may be applicable to the products falling within the scope of this standard.

The clauses of this standard are likely to support requirements of the three directives mentioned above.

Compliance with this standard provides one means of conforming with the specific essential requirements of the directives concerned and associated EFTA regulations.

List of references

See national foreword.

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: 020 8996 9000. Fax: 020 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: 020 8996 9001. Fax: 020 8996 7001.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: 020 8996 7111. Fax: 020 8996 7048.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: 020 8996 7002. Fax: 020 8996 7001.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL