INTERNATIONAL STANDARD

ISO 13849-1

First edition
1999-11-15

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

Part 1:
General principles for design

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

Partie 1: Principes généraux de conception

Reference number
ISO 13849-1:1999(E)

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 13849-1 was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

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

— *Part 1: General principles for design*

— *Part 2: Validation, testing, fault lists*

Annexes A to D of this part of ISO 13849 are for information only.

Introduction

Certain parts of machinery control systems are frequently assigned safety functions: these are called the safety-related parts. These parts can consist of both hardware and software, and they are intended 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 classified in this part of ISO 13849 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 to:

— control systems of all kinds of machinery, from simple, e.g. small kitchen appliances, to complex manufacturing installations, e.g. packaging machinery, 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 should provide 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 of the part under consideration (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 categories as reference points and a declaration of the rationale followed during the design process is intended to allow this part of ISO 13849 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, e.g. by a third party, in-house means or an independent test house.

This part of ISO 13849 has been prepared to be a harmonized standard in the sense of the Machinery Directive of the European Union and associated regulations of the European Free Trade Association (EFTA).

International Standard ISO 13849-1 is based on EN 954-1:1996, published by the European Committee for Standardization (CEN).

Attention is drawn to the fact the working group of CEN/TC 114 responsible for the elaboration of EN 954-1:1996 has prepared a guide on the application of EN 954-1 which has been published by CEN as CR 954-100. ISO/TC 199 has agreed that this CEN Report be published as an ISO Technical Report (type 3) in order to present the same explanations for ISO 13849-1.

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

Part 1:
General principles for design

1 Scope

This part of ISO 13849 provides safety requirements and guidance on the principles for the design of safety-related parts of control systems. For these parts, it specifies categories and describes the characteristics of their safety functions, including programmable systems for all machinery and for related protective devices.

This part of ISO 13849 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.

This part of ISO 13849 applies to all machinery applications for professional and non-professional use. Where appropriate, it can also be applied to the safety-related parts of control systems used in other technical applications.

NOTE See ISO/TR 12100-1:1992, 3.11.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 13849. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 13849 are encouraged to investigate the possibility of applying the most recent edition of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 7731:1986, *Danger signals for workplaces — Auditory danger signals.*

ISO 11428:1996, *Ergonomics — Visual danger signals — General requirements, design and testing.*

ISO 11429:1996, *Ergonomics — System of auditory and visual danger and information signals.*

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

ISO/TR 12100-2:1992, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles and specifications.*

ISO 13850:1996, *Safety of machinery — Emergency stop — Principles for design.*

ISO 14118, *Safety of machinery — Prevention of unexpected start-up.*

ISO 14121, *Safety of machinery — Principles for risk assessment.*

IEC 60050 (191):1990, *International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service.*

IEC 60204-1:1992, *Safety of machinery — Electrical equipment of industrial machines — Part 1: General requirements.*

IEC 60447:1993, *Man-machine interface (MMI) — Actuating principles.*

IEC 60529:1989, *Degrees of protection provided by enclosures (IP Code).*

IEC 60721-3-0:1984 + A1:1987, *Classification of environmental conditions — Part 3: Classification of groups of environmental parameters and their severities — Introduction.*

EN 292-2:1991/A1:1995, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles and specifications.*

EN 614-1:1995, *Safety of machinery — Ergonomic design principles — Part 1: Terminology and general principles.*

EN 982:1996, *Safety of machinery — Safety requirements for fluid power systems and their components — Hydraulics.*

EN 983:1996, *Safety of machinery — Safety requirements for fluid power systems and their components — Pneumatics.*

EN 999:1998, *Safety of machinery — The positioning of protective equipment in respect of approach speeds of parts of the human body.*

3 Terms and definitions

For the purposes of this part of ISO 13849, the terms and definitions given in ISO/TR 12100-1, IEC 60050 (191) and the following apply.

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

NOTE 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 ISO/TR 12100-1:1992, annex A). 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

NOTE Such behaviour 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
state of an item characterized by inability to perform a required function, except 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 those given in IEC 60050 (191):1990, IEV 191-05-01. 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
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.

[IEC 60050(191), IEV 191-04-01]

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

3.6
safety function of a control system
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 design

The safety-related parts of a control sytem which provide the safety functions shall be designed and constructed so that the principles of ISO 14121 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 ISO 14121) of 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, 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 electrosensitive protective device on a press, or the door-locking function of a washing machine.

The key objective is that the designer ensure that the safety-related parts of a control system produce outputs which achieve the risk reduction objectives of ISO 14121. 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 ISO/TR 12100-1:1992, clause 5.

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 Introduction). 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 dependence of risk reduction upon the safety-related parts of control systems, then the higher is the required ability of those parts to resist faults. This ability — in the understanding that the required function is performed — can be partly quantified by reliability values and by a fault-resistant 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 contributions 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 part of ISO 13849 does not require the calculation of reliability values for complex structures where safety is predominantely obtained by improving the structure of the safety-related parts. For less complex structures, 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 ISO/TR 12100-2:1992, clause 3, EN 292-2:1991/A1:1995, annex A and IEC 60204-1:1992, 9.4).

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

— reliability with respect to performing the safety functions;

— structure (or architecture) of the control system;

— quality of safety-related documentation;

— completeness of the specification;

— design, manufacture and maintenance;

— quality and accuracy of software;

— extent of functional testing;

— operating characteristics of the machine or part of the machine under control.

These parameters can be grouped under three main characteristics:

a) hardware reliability: the level of reliability of the components to avoid faults;

b) system structure: the arrangement of the components in the safety-related part of a control system to avoid, tolerate or detect faults;

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

4.3 Process for selection and design of safety measures

4.3.1 General

This subclause sets out a process first 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 be 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 ISO 14121.

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 presented 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.

4.3.2 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 ISO/TR 12100-1 and ISO 14121.

Assess the risk arising from those hazards and decide the appropriate risk reduction for that application in accordance with ISO/TR 12100-1 and ISO 14121.

4.3.3 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.

4.3.4 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 met and select the category(ies) for each part and combinations of parts within the safety-related parts of the control system (see clause 6).

4.3.5 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).

4.3.6 Step 5: Validation

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

It is also necessary to validate the safety-related parts of the control system in conjunction with the entire control system and as part of the machine. The requirements of such validation are not within the scope of this part of ISO 13849, but should be specified by the machine designer or the appropriate Type C safety standard.

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 Bibliography).

NOTE 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 misoperation 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 IEC 60204-1:1992, 12.3.5).

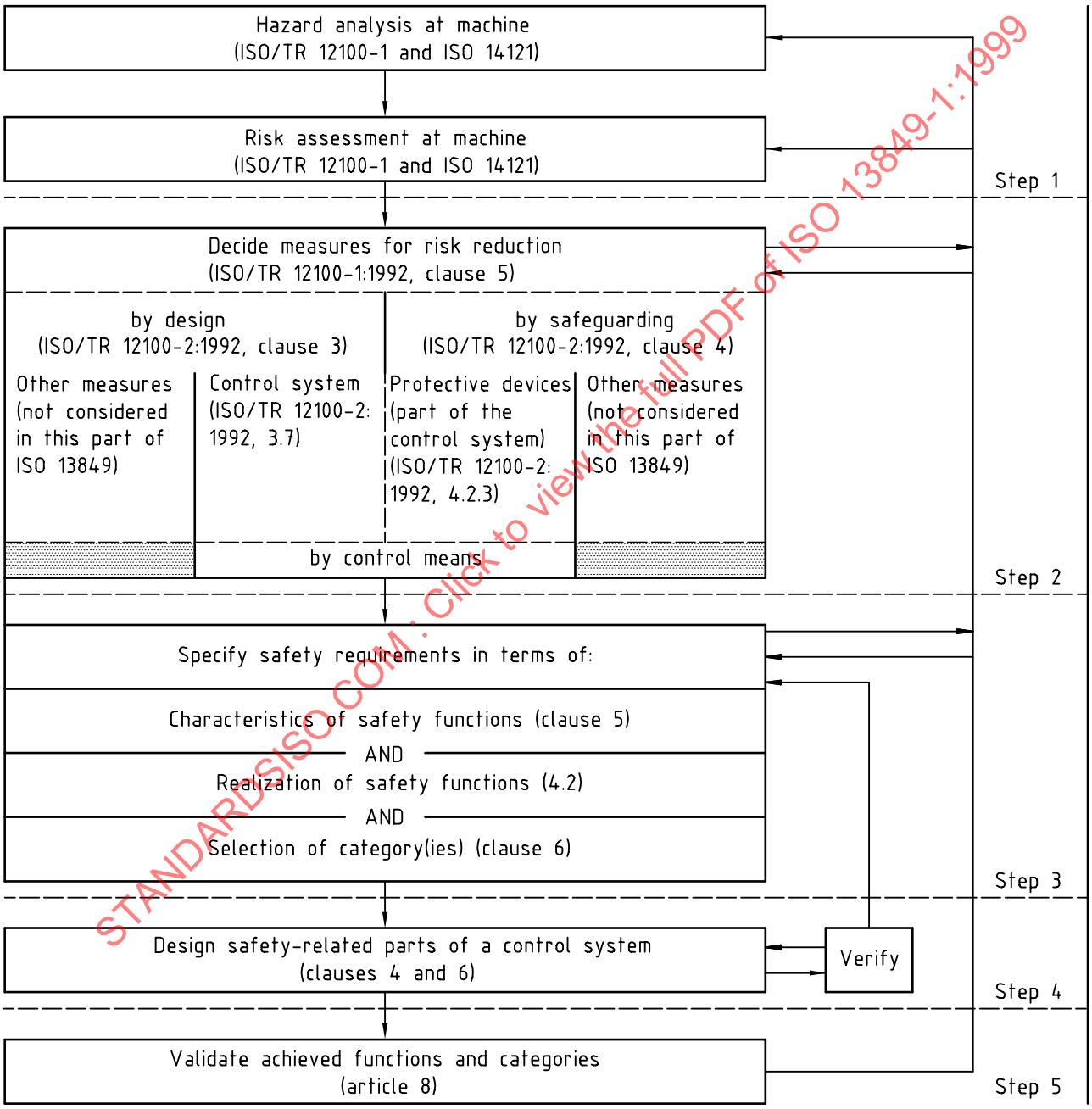

Figure 1 — Iterative process for the design of safety-related parts of control systems

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 (for information see also ISO/TR 12100-2; IEC 60204-1:1992, clause 10; IEC 60447:1993, clause 2; EN 614-1; EN 894-1; EN 894-2; prEN 894-3 and prEN 1005-3).

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 ISO/TR 12100-2:1992, 3.6, should apply.

5 Characteristics of safety functions

5.1 General

This clause provides a list of typical safety functions (see ISO/TR 12100-1:1992, 3.13) 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 International Standards (see also clause 2). The designer (or Type-C standard maker) shall ensure that the requirements of all these International 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.

5.2 Stop function

In addition to the requirements of the reference given in Table 1, the following shall apply.

a) 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.

b) When a group of machines are working together in a coordinated 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 apply.

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

b) Where sections of the coordinated 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.

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

5.4 Manual reset

In addition to the requirements of the reference given in Table 1, the following shall apply.

a) 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.

b) 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).

c) 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.

d) 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.

e) 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 apply.

a) A restart shall take place automatically only if a hazardous situation cannot exist. In particular, for control guards, see ISO/TR 12100-2:1992, 4.2.2.5.

b) 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 apply.

a) 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 parts, 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 apply.

a) 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.

b) 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 or pendant, the following requirements shall apply in addition to the requirements of the reference given in Table 1.

a) The means for selecting local control shall be situated outside the danger zone.

b) It shall not be possible to initiate hazardous conditions from outside the zone of local control.

c) 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.

In some applications, a signal indicating muting is required.

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 apply in addition to the requirements of the reference given in Table 1.

a) Effective and secure means shall be provided to prevent manual suspension in those operating modes where it is not allowed.

b) Safety functions of the safety-related parts of the control system shall be reinstated before normal operations can be continued.

c) Safety-related parts of the control system which are responsible for the manual suspension shall be selected so that the principles of ISO 14121 are fully taken into account.

In some applications, a signal indicating manual suspension is required.

5.11 Fluctuations, loss and restoration of power sources

In addition to the requirements of the reference given in Table 1, the following shall 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.

Table 1 — Some International Standards giving requirements for characteristics of safety function

Safety functions, Characteristics	Requirements				Further standards	Additional information[a]
	ISO 13849-1:1999	ISO/TR 12100		EN 292- 2: 1991/A 1:1995, annex A		
		Part 1: 1992	Part 2: 1992			
Definitions	3	3			IEC 60204-1:1992, clause 3	IEC 60335-1:1994, clause 2
Design principles	4.2		3	1.2.1 1.2.2 1.2.7 1.5.4	IEC 60204-1:1992, 9.4	IEC 60335-1:1994, clause 22; ISO 10218:1992, clauses 5 and 6; ISO 11161:1994, clause 5
Ergonomic principles	4.4	4.9	3.6 3.7.8a	1.2.2 Para 1	IEC 60204-1:1992, clause 10	ISO 10218:1992, 6.2; ISO 11161:1994, 4.6
Stop function	5.2		3.7.1 3.7.8b	1.2.4 1.3.5	IEC 60204-1:1992, 9.2.2, 9.2.5.3	IEC 60335-1:1994, 7.12; ISO 11161:1994, 5.11
Emergency stop function	5.3		6.1.1	1.2.4	ISO 13850, IEC 60204-1:1992, 9.2.5.4	ISO 10218:1992, 6.4.2, 7.2.5; ISO 11161:1994, 5.11.2
Manual reset	5.4			1.2.4	IEC 60204-1:1992, 9.2.5.3, 9.2.5.4	ISO 10218:1992, 6.4.2, 6.4.3, 7.6; ISO 11161:1994, 6.4.3
Start and restart	5.5		3.7.1 3.7.2	1.2.3 1.3.5	IEC 60204-1:1992, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6	ISO 10218:1992, 6.10, 7.2.5, 7.3.1, 9.3.4
Response time	5.6				EN 999:1998, 3.2, A.3, A.4	
Safety-related parameters	5.7		3.7.9e		IEC 60204-1:1992, 7.1, 9.3.2, 9.3.4	ISO 10218:1992, 4.2; IEC 60335-1:1994, 11.8
Local control function	5.8		3.7.9 3.7.10			ISO 10218:1992, 3.2.9, 7.2.6; ISO 11161:1994, 3.13, 4.5, 5.9, 6.2
Muting	5.9					
Manual suspension of safety functions	5.10		3.7.10 4.1.4	1.2.5	IEC 60204-1:1992, 9.2.4	ISO 10218:1992, 6.10; ISO 11161:1994, 5.8
Fluctuations, loss and restoration of power sources	5.11		3.7.8e	1.2.6 1.5.3	IEC 60204-1:1992, 4.3, 7.1, 7.5	
Programmable electronic systems			3.7.7		IEC 60204-1:1992, 12.3	IEC 61508[b]

Safety functions, Characteristics	Requirements				Further standards	Additional information[a]
	ISO 13849-1:1999	ISO/TR 12100		EN 292- 2: 1991/A 1:1995, annex A		
		Part 1: 1992	Part 2: 1992			
Unexpected start-up			3.7.2	1.2.3 1.2.6 1.2.7	ISO 14118; IEC 60204-1:1992, 5.4	
Indications and alarms			3.6.7 5.3	1.2.2 Para 4, 6 1.7.0 1.7.1	ISO 7731; ISO 11428; ISO 11429; IEC 60204-1:1992, 10.4, 11.3; IEC 60447	ISO 11161:1994, 5.6
Escape and rescue of trapped persons			6.1.2	1.2.2 Para 5, 6		
Electrical equipment		3.9		1.5.1 1.5.7	IEC 60204-1	
Electrical supply				1.5.1	IEC 60204-1:1992, 4.3	
Other supply				1.5.3	EN 982:1992, 5.1.4; EN 983:1992, 5.1.4	
Covers and enclosures					IEC 60204-1:1992, 13.4; IEC 60529	
Pneumatic and hydraulic equipment			3.8	1.5.3	EN 982 EN 983	
Isolation and energy dissipation			6.2.2	1.6.3	ISO 14118; IEC 60204-1:1992, 5.3, 6.3.1	
Physical environment and operating conditions			3.7.11		IEC 60204-1:1992, 4.4	ISO 10218:1992, 6.9; ISO 11161:1994, 4.3, 4.5
Control modes and mode selection			3.7.9 3.7.10	1.2.5	IEC 60204-1:1992, 9.2.3	ISO 10218:1992, 6.10
Interfaces/ connections				1.5.4 1.6.1 Para 3	IEC 60204-1:1992, 9.1.4, 11, 15.4	
Interaction between different safety-related parts of control systems			3.7.8e		IEC 60204-1:1992, 9.3.4	
Man-machine interface			3.6.6 3.6.7	1.2.2	IEC 60204-1:1992, clause 10; IEC 60447	

[a] The references in this column are to be considered as an aid to the designer but not part of the requirements of this part of ISO 13849.

[b] To be published.

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 five 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 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 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 fault-resistance behaviour 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 failure 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 International Standards, using basic safety principles for the specific application so that they can withstand:

— expected operating stresses, e.g. force and frequency of braking;

— influence of the processed material, e.g. resistance of a washing machine to detergents;

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

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

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

6.2.2 Category 1

6.2.2.1 General

The requirements of category B and the following requirement shall apply.

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

Table 2 — Summary of requirements for categories
(for full requirements see clause 6)

Category[a]	Summary of requirements	System behaviour[b]	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 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 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 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 loss of the safety function, and — whenever reasonably practicable the single fault is detected.	— When a single fault occurs, the safety function is always performed. — Some but not all faults will be detected. — Accumulation of undetected faults can lead to 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 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 accumulation of faults shall not lead to loss of the safety function.	— When the faults occur the safety function is always performed. — The faults will be detected in time to prevent loss of the safety function.	

[a] The categories are not intended to be used in any given order or in any given hierarchy in respect of safety requirements.

[b] The risk assessment will indicate whether the total or partial loss of the safety function(s) arising from faults is acceptable.

6.2.2.2 Well-tried components

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 well-tried one can depend on the application.

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

6.2.2.3 Well-tried safety principles

Well-tried safety principles are, for example:

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

— reduction of the probability of faults, e.g. over-dimensioning or underrating of components;

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

— very early detection of faults ;

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

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

6.2.3 Category 2

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

a) 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.

b) 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.

c) 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.

d) 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 achieved with electronic techniques, e.g. in protective equipment and particular control systems.

Category 2 system behaviour allows that:

— the occurrence of a fault can lead to 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 following requirements shall apply.

a) Safety-related parts of control systems to category 3 requirements shall be designed so that a single fault in any of these parts does not lead to loss of the safety function.

b) Common-mode faults shall be taken into account when the probability of such a fault occurring is significant.

c) 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 necessary because of technology and application, Type-C standard makers should give further details on the detection of faults.

NOTE 3 "Whenever reasonably practicable" means that the required measures for fault detection and the extent to which they are implemented depends mainly upon the consequences 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.

Category 3 system behaviour allows that:

— when a single fault occurs, the safety function is always performed;

— some but not all faults will be detected;

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

6.2.5 Category 4

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

a) 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.

b) 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 loss of the safety function.

c) 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 electrohydraulic 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.

d) 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.

e) 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 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.

Category 4 system behaviour allows that:

— when faults occur, the safety function is always performed;

— faults will be detected in time to prevent 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 carried out 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 carried out by several safety-related parts, e.g. sensors, control unit, power control elements, these parts may be assigned to one category and/or to different categories in combination.

When safety-related parts assigned 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 for information in ISO 13849-2. The lists of faults given in annex C and in ISO 13849-2 are not exclusive and, if necessary, additional faults should be considered and listed. In such cases, the method of validation should also be clearly described.

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 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 IEC 61496-1.

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:

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

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

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

NOTE Guidance on validation procedures is given in IEC 61508.

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:

1) test of the specified safety functions;

2) test of the specified categories;

3) test of dimensioning and compliance to environmental parameters.

8.3 Validation by analysis

In general, analysis 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 effects analysis, critically 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 dependent 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.

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 in which 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 the Bibliography.

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 tests 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. IEC 60068, IEC 60204-1, IEC 60529, IEC 60721-3-0:1984 + A1:1987, IEC 61000-4-1.

8.5 Validation report

At the conclusion of the validation process, a safety validation report shall be made summarizing the tests and analyses which were carried out, 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;

— analyses and tests carried out;

— problems encountered and how these problems were resolved;

— 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 ISO/TR 12100-2:1992, 6.2.1 and EN 292-2:1991/A1:1995, annex A, 1.6. All information for maintenance shall comply with ISO/TR 12100-2:1992, 5.5.1 e).

10 Information to be provided to the user

The principles of ISO/TR 12100-2:1992, clause 5 and other relevant documents, e.g. IEC 60204-1:1992, clauses 18 und 19, 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 provided 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;

  When fault exclusions are essential in maintaining the selected category(ies) and safety performance, appropriate information, e.g. for modification, maintenance and repair, is 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 checklists;

— 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, the categories shall be referred to in the following way:

ISO/TR 12100 Category B;

ISO/TR 12100 Category 1;

ISO/TR 12100 Category 2;

ISO/TR 12100 Category 3;

ISO/TR 12100 Category 4.

Annex A
(informative)

Questionnaire for use during the design process

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

❑ No special action required.

❑ Safe reaction required within a certain time.

❑ Safe reaction immediately required.

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

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

❑ In auxiliary parts.

❑ In all safety-related parts.

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

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

❑ Faults only in components which are not well-tried.

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

❑ Faults in all components.

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

❑ Normal requirements for fault detection.

NOTE 1 This means that all faults which can be detected with relatively simple methods should be detected.

❑ Stringent requirements for fault detection.

NOTE 2 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 should the next action of the control system be if a fault has been detected?

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

- ❑ Further operation of the machine can be permitted until the fault is rectified.
- ❑ 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?

- ❑ Information on the effects of deviation from design specifications.
- ❑ Automatic indication of the need for maintenance.
- ❑ Setting of maintenance intervals.
- ❑ Setting of component lifetimes.
- ❑ Provision of diagnostic facilities and test points.
- ❑ Special precautions for safety during maintenance.

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

- ❑ Automatic fault detection, as far as appropriate.
- ❑ Manual fault detection, e.g. by periodic inspection.
- ❑ Provision of more than one method.

A.9 Has the risk reduction been achieved?

- ❑ Can the risk reduction be achieved more easily with a different combination of risk reduction measures?
- ❑ 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.
- ❑ Are the solutions valid for all operating conditions and for all procedures?
- ❑ Are these solutions compatible with each other?
- ❑ Is the safety specification correct?

A.10 Have ergonomic principles being considered?

- ❑ Are the safety-related parts of the control system, including the protective devices, easy to use?
- ❑ Is there safe and easy access to the control system?
- ❑ Are warning signals given priority (e.g. highlighted)?

A.11 Have the relationships between safety, reliability, availability and ergonomics been optimized in such a way that the safety measures will be maintained during the lifetime of the system, and do 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 ISO 14121 (particularly in respect to a simplification of the elements of risks as described in ISO 14121:1997, 7.1) 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 ISO 14121, 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 ISO 14121 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, for example component reliability, the technology used or 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:

a) frequency and duration of exposure to the hazard (F);

b) 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. Categories other than preferred can be used (see 6.3), but the intended system behaviour in case of fault(s) should be maintained. Reasons for deviating from the preferred categories should be given. These reasons can be the use of different technologies, e.g. well-tried hydraulic or electromechanical 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;

— 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 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 selection, 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 duration of exposure to hazard F1 and F2

A generally valid time period during which parameter F1 or F2 should be selected cannot be specified. However, the following explanation can facilitate 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. the use of lifts.

The duration 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 workpieces, 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 nonprofessionals;

— 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.