TECHNICAL REPORT

ISO/TR 13849-100

First edition
2000-09-01

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

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

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

Partie 100: Lignes directrices pour l'utilisation et l'application de l'ISO 13849-1

Reference number
ISO/TR 13849-100:2000(E)

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

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

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this part of ISO 13849 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 13849-100 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 100: Guidelines for the use and application of ISO 13849-1*

Introduction

ISO 13849-1 was published in 1999 and from experience gained it is clear that there have been difficulties in understanding how ISO 13849-1 is to be used. The present Technical Report gives advice on how to avoid misinterpretations.

ISO 13849-1 gives guidance on the principles to be followed in:

— designing safety-related parts of control systems (ISO 13849-1:1999, clause 4);

— the characteristics of safety functions (ISO 13849-1:1999, clause 5);

— the requirements for the categories of safety-related parts of control systems (ISO 13849-1:1999, clause 6).

Feedback from users indicates that the scope of ISO 13849-1 is not fully understood. Therefore it should be emphasised that ISO 13849-1 does not give guidance on:

— the systematic application of the risk reduction process to the selection of the categories of safety-related parts of the control system;

— the application of the risk reduction process to the overall safety requirements of the machine (see ISO 13849-1:1999, step 2 in Figure 1);

— the detailed implementation of safety-related parts utilising different technologies, and in particular when different technologies are combined within one safety function.

An amendment to/revision of ISO 13849-1:1999 is being prepared to incorporate the ideas of this Technical Report, together with some additional points. Upon its publication, this Technical Report will be withdrawn.

This Technical Report is based on CR 954-100, published by the European Committee for Standardization (CEN).

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

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

1 Scope

This Technical Report provides guidance on the appropriate use and interpretation of ISO 13849-1:1999. It also gives further information on the following topics:

— how the control system contributes to reducing risk in the machine;

— what is meant by the safety-related parts of the control system in relation to safety functions;

— the proper selection and use of categories;

— the role of annex B of ISO 13849-1:1999.

2 Correct use of ISO 13849-1:1999

The issues presented in ISO 13849-1:1999 are complex. Its clauses are interrelated and cannot be used alone. It is therefore necessary to take into account ALL clauses of ISO 13849-1:1999.

3 Explanation of the design procedures

The overall design procedure is given in ISO/TR 12100-1:1992, clause 5. Part of this process is a risk assessment, the principles of which are given in ISO 14121. This risk assessment covers the whole machine life cycle. If it is found that there are risks which must be reduced, then appropriate measures must be chosen. ISO/TR 12100-2:1992 gives guidance on the measures for risk reduction.

Part of the risk reduction process is to determine the safety functions (ISO/TR 12100-1:1992, 3.13) of the machine. This includes the safety functions of the control system, e.g. emergency stop function, start and restart (see ISO 13849-1:1999, clause 5).

A safety function may be implemented by one or more safety-related parts of the control system. The designer may use any of the technologies available, singly or in combination. A safety function can also be an operational function, e.g. a two-hand control as a means of cycle or process initiation.

A typical safety function is given in Figure 1 showing safety-related parts (SRP) for:

— input (SRP_a);

— logic/processing (SRP_b);

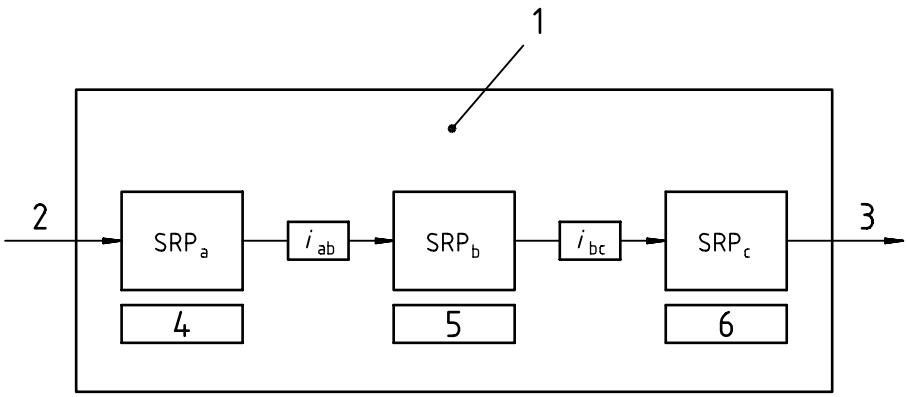
— output/power control elements (SRP_c);

— interconnecting means (i_{ab}, i_{bc}), e.g. electrical, optical.

NOTE 1 Safety-related parts consist of one or more components; components consist of one ore more elements.

NOTE 2 All interconnecting means are included in the safety-related parts.

NOTE 3 An example of a safety function is shown in Figure 2 and the associated text.



Key

1	Typical safety function
2	Initiation means, e.g. manual actuation, other signals
3	Machine actuators, disconnecting means, brakes
4	Input
5	Logic
6	Output

Figure 1 — Diagramatic presentation of a combination of safety-related parts for processing a typical safety function

Each safety-related part of the safety function may be made from different technologies. Different technologies may be used for implementing within each safety-related part, e.g. an input comprising a mechanical actuator linked to a light-activated signal converter.

Having established the safety functions of the control system, it is then necessary to identify the safety-related parts of the control system (see ISO 13849-1:1999, 3.1 and clause 8) and then decide how important the contribution is to the risk reduction process. The protective measures provided by the control system depend on this contribution and not directly on the overall risk reduction for the hazard being considered.

NOTE 4 The loss of a safety function does not lead automatically to injury or damage to health if other effective protective (safety) measures have been taken.

The greater the reduction of risk is dependent on the safety-related parts of control systems, then the higher the ability of those parts to resist faults is required to be (according to ISO 13849-1:1999, 4.2). Therefore protective measures to reduce the risk are needed, principally:

— **Reducing the probability of faults at the component level.** The aim is to reduce the probability of faults or of failure modes which affect the safety function. This can be done by increasing the reliability of components, e.g. by selection of well-tried components and/or applying well-tried safety principles, in order to exclude critical faults or failure modes. ISO 13849-1:1999 does not give a systematic view on reliability requirements.

— **Improving the structure of the system.** The aim is to avoid the dangerous effect of a fault. Some faults may be detected and a redundant and/or monitored structure may be needed.

Both measures can be used separately or in combination. With some technologies, the required risk reduction can be achieved by selecting reliable components and by fault exclusions, but with other technologies, risk reduction may require a redundant and/or monitored system with two or more parts. In addition, common-cause failures should be taken into account. One way of describing these measures is to use the system of five categories established in ISO 13849-1:1999, clause 6.

4 Categories

Categories (for definition see ISO 13849-1:1999, 3.2) are intended to classify safety-related parts of the control system which carry out a safety function, on the basis of their performance in case of fault. These parts may be used singly or in combination. The categories should be considered as reference points for the performance of a safety-related part of a control system with respect to the occurrence of faults (see ISO 13849-1:1999, Introduction). Categories cannot and never should be considered as having accurately delineated limits, because the assessment of the parameters being considered can be subjective.

The common conception that the categories of ISO 13849-1:1999 always, or singly, correspond to levels of risk is not correct.

In choosing a category, the designer should also consider the safety performance to be achieved, and this depends upon both the structure and the reliability of those safety-related parts. ISO 13849-1:1999 does not fully specify reliability requirements.

Therefore all that can be said about the safety performance for a given technology is:

a) Categories 1, 2, 3 and 4 are all better than Category B;

b) In Categories B, 1 and 2, a single fault can lead to the loss of the safety function;

c) Categories 3 and 4 will not fail due to a single fault (common-mode faults are considered as a single fault);

d) Category 4 has the best performance as regards fault tolerance, because an accumulation of faults is considered.

Control systems employing certain technologies cannot always be designed to satisfy every category, e.g. a mechanical link which meets the requirements of Category 1 but which cannot meet the requirements of Categories 3 or 4. However, the expectation that the safety function will be performed can be equal to, or higher than, that of some other systems which meet Category 2, 3 or 4.

When a safety function is implemented by several safety-related parts of the control system, three possibilities can occur:

a) each of the safety-related parts has the same category and can be assigned the same overall category;

b) safety-related parts are assigned to different categories but used in combination in such a way that an overall category is assigned;

c) an overall category cannot be assigned because the technologies used cannot be designed to satisfy every category.

Detection of a fault by the control system in a Category 3 is not always necessary when a fault is self-evident, e.g. when the machine itself reveals the fault by not allowing a start or restart.

Type-C standard writers and designers should be aware of the limitations of setting out the performance of the safety function in terms of an overall category because of the limitations in the category requirements, particularly for reliability.

5 Selection of categories

When selecting categories for the safety-related parts which carry out the safety function(s) (see ISO 13849-1:1999, clause 6), faults which can occur in those parts should be considered under two aspects:

— evaluating the probability of failure or effect of a fault in those parts;

— considering the effect of failure or a fault in those parts on the safety function.

The required performance of the safety function depends upon the level of risk; if the risk is high, the required performance is high and vice versa. The relevant harmonized standards reflect the state of the art in various applications, and this information should be taken into account when selecting categories.

The probability of occurrence of faults is usually established by qualitative estimation, because there is seldom enough data to give a basis for quantitative procedures. This means that in most cases Failure Mode and Effects Analysis (FMEA - see IEC 60812) or similar methods should be used. All relevant faults and/or failure modes should be considered and the actual performance of the safety function in case of a fault should be checked against the required performance.

Some faults or failure modes can be excluded if the probability of their occurrence is very low. This probability depends upon the application conditions. One important consideration is the frequency of demands on the safety function which can vary enormously (from infrequent demands, e.g. emergency stop device, to continuous demands, e.g. control of moving machine parts). Because of this, average values or estimates of acceptable failure rates cannot usually be given.

After the whole procedure of risk reduction, a validation (see ISO 13849-1:1999, clause 8) should be made. This validation is part of the validation of the whole machine system.

Figure 2 is a schematic diagram of the safety-related parts which provide one of the functions to control a machine actuator. **This is not a functional/working diagram and is included only to demonstrate the principle of combining categories and technologies in this one function.**

The control is provided through an electronic control logic and a fluidic directional valve, checked at suitable intervals (see ISO 13849-1:1999, 6.2.3). The risk is reduced by an interlocking guard which prevents access to the hazardous situation when the guard is closed and prevents start-up of the fluidic actuator when the guard is open.

For this example, the combined safety-related parts of the control system begin at point 7 and end at point 1 (see Figure 2).

The safety-related parts which provide the safety function are: guard cam, position device, electronic control logic, fluidic directional valve and the interconnecting means.

These combined safety-related parts provide a stop function (see ISO 13849-1:1999, 5.2) as a safety function (for definition see ISO 13849-1:1999, 3.6). As the guard opens, the contacts in the position device open and the electronic control logic provides a signal to the fluidic directional valve to stop the fluidic flow as the output of the safety-related parts of the control system. At the machine, this stops the hazardous movement of the actuator.

This combination of safety-related parts creates a safety function to demonstrate the categorization based on the requirements of ISO 13849-1:1999, clause 6. It considers the possibility and the probability of the faults that can occur which may affect the ability of those combined parts to perform the safety function. Using these principles, the safety-related parts shown in Figure 2 can be categorized as follows:

— Category 1 for the electromechanical position device.

  To reduce the probability of faults, this device is comprised of well-tried components applied using well-tried safety principles, e.g. positive-opening operation, over-dimensioning (see ISO 13849-1:1999, clause 3 and 6.2.2);

— Category 3 for the electronic control logic.

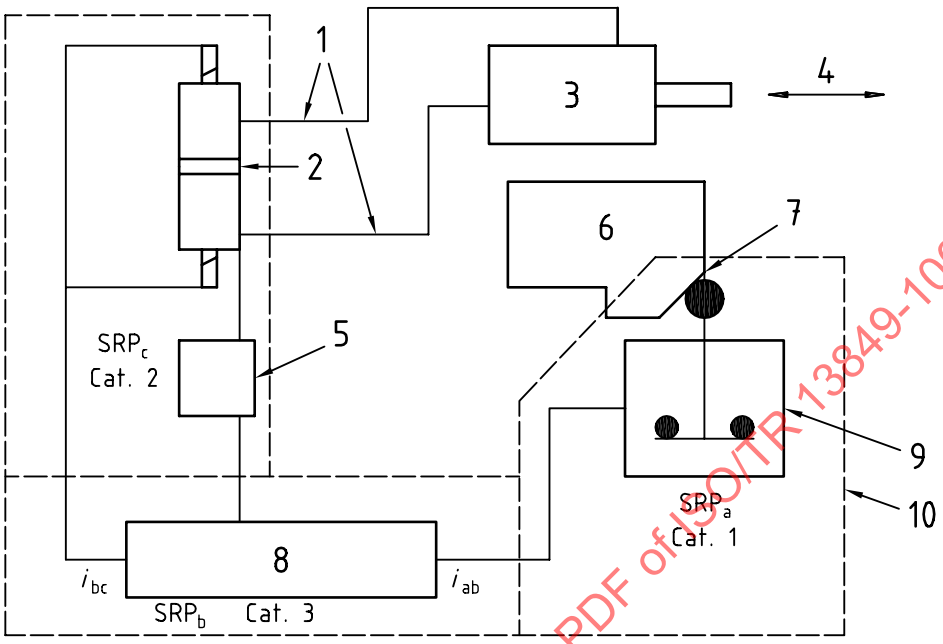
  To increase the level of safety performance of this electronic control logic, the structure of this safety-related part of the control system is designed so that it is able to detect most single faults, e.g. redundancy (see ISO 13849-1:1999, 6.2.4);

— Category 2 for the checked fluidic directional valve.

  To achieve the required level of safety performance, this safety-related part uses components which are periodically checked, e.g. monitoring, in order to detect the faults which have not been avoided using well-tried safety principles (see ISO 13849-1:1999, 6.2.3).

The position, size and layout of the interconnecting means should also be taken into account.

The overall objective is that each of the safety-related parts achieves a similar level of safety performance so that the contribution of the safety-related parts of the control system provides the required reduction in risk. Therefore both the reliability and the structure within the safety-related parts of the control system need to be considered.



Key

1	Output signal
2	Fluidic directional valve
3	Fluidic actuators
4	Hazardous movement
5	Checking function
6	Guard
7	Input signal
8	Electronic control logic
9	Position device
10	Scope of ISO 13849-1:1999

NOTE The stop and start functions have been omitted to keep the example simple.

Figure 2 — Example to explain the use of categories

6 The role of annex B in ISO 13849-1

When evaluating risks, the procedures given in ISO 14121 should be followed. The advice given in ISO 13849-1:1999, annex B is for information only.