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

iTeh STANDARD PREVIEW

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

(standards.iteh.ai)

Partie 1: Principes généraux de conception

ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-db60630bcee6/iso-13849-1-1999

Reference number
ISO 13849-1:1999(E)

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-db60630baae6/iso-13849-1-1999

© ISO 1999

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

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

Printed in Switzerland

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-db60630bcee6/iso-13849-1-1999

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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:

ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-db60620baae6/iso-13849-1-1999

— 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-db60630bcee6/iso-13849-1-1999

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-db60630bcee6/iso-13849-1-1999

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

iTeh STANDARD PREVIEW

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.

(standards.iteh.ai)

ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4 General considerations

ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-db60630bcee6/iso-13849-1-1999

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 predominantly 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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).

ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0baee-d5c0-4774-9fa4-db60630bcee6/iso-13849-1-1999

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.

iTeh STANDARD PREVIEW

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.

(standards.iteh.ai)

4.3.3 Step 2: Decide measures for risk reduction by control means

ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-0b60b30bc6e6/iso-13849-1-1999

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).

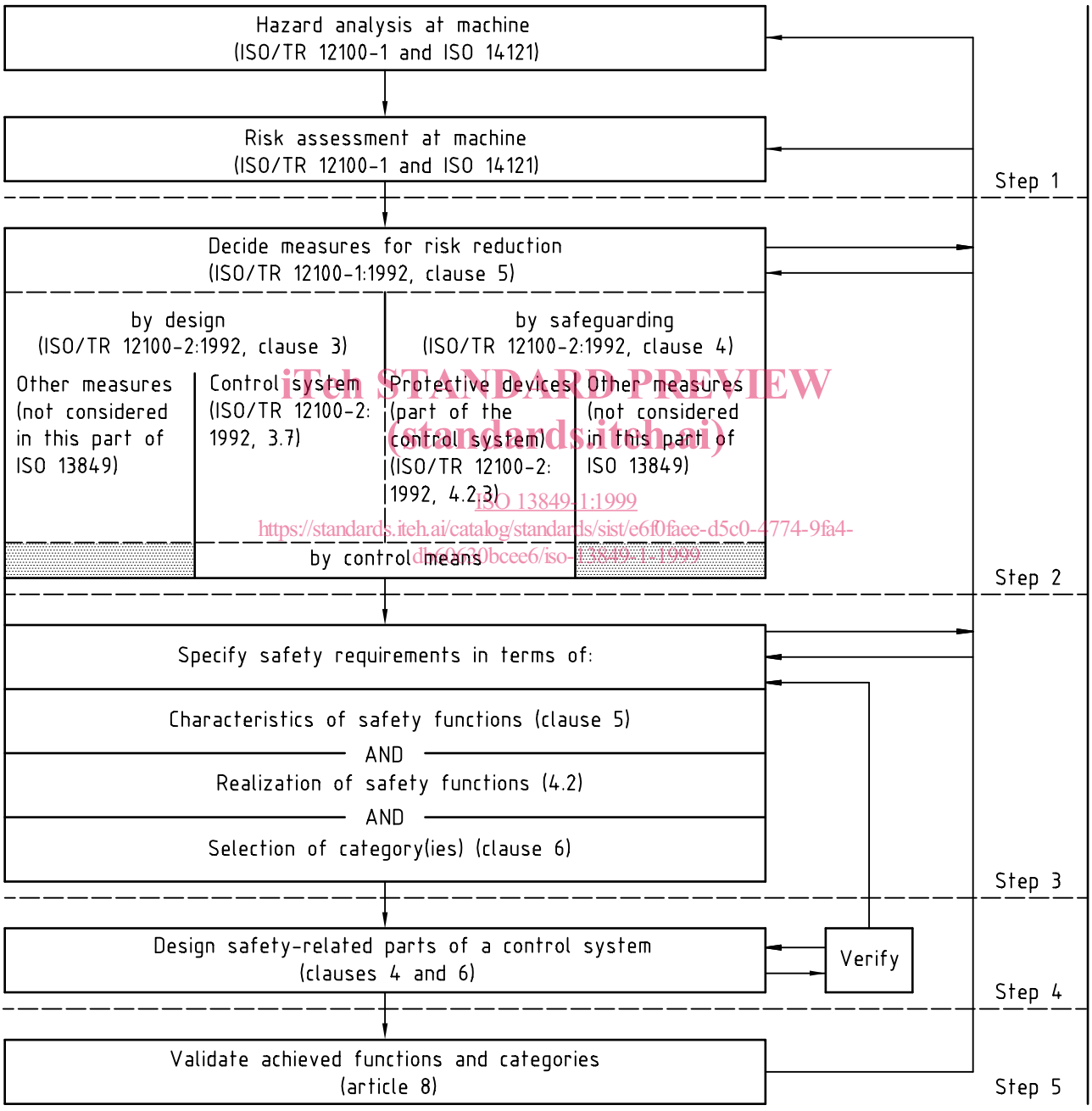
4.3.6 Step 5: Validation

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).



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-1:1999
https://standards.iteh.ai/catalog/standards/sist/e6f0faee-d5c0-4774-9fa4-d6063b0bcee6/iso-13849-1-1999

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