INTERNATIONAL STANDARD

ISO 13849-2

Second edition
2012-10-15

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

Part 2: Validation

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

Partie 2: Validation

Reference number
ISO 13849-2:2012(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.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Validation process ... **1**
4.1 Validation principles ... 1
4.2 Validation plan ... 3
4.3 Generic fault lists ... 4
4.4 Specific fault lists ... 4
4.5 Information for validation ... 4
4.6 Validation record ... 6
5 Validation by analysis ... **6**
5.1 General ... 6
5.2 Analysis techniques ... 7
6 Validation by testing ... **7**
6.1 General ... 7
6.2 Measurement accuracy ... 8
6.3 More stringent requirements ... 8
6.4 Number of test samples ... 8
7 Validation of safety requirements specification for safety functions ... **9**
8 Validation of safety functions ... **9**
9 Validation of performance levels and categories ... **10**
9.1 Analysis and testing ... 10
9.2 Validation of category specifications ... 10
9.3 Validation of $MTTF_d$, DC_{avg} and CCF ... 12
9.4 Validation of measures against systematic failures related to performance level and category of SRP/CS ... 13
9.5 Validation of safety-related software ... 13
9.6 Validation and verification of performance level ... 14
9.7 Validation of combination of safety-related parts ... 14
10 Validation of environmental requirements ... **15**
11 Validation of maintenance requirements ... **15**
12 Validation of technical documentation and information for use ... **16**
Annex A (informative) **Validation tools for mechanical systems** ... **17**
Annex B (informative) **Validation tools for pneumatic systems** ... **21**
Annex C (informative) **Validation tools for hydraulic systems** ... **31**
Annex D (informative) **Validation tools for electrical systems** ... **40**
Annex E (informative) **Example of validation of fault behaviour and diagnostic means** ... **53**
Bibliography ... **78**

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 2.

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.

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

ISO 13849-2 was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

This second edition cancels and replaces the first edition (ISO 13849-2:2003), which has been technically revised in order to adapt to ISO 13849-1:2006. In addition, the new Annex E provides an example for the validation of fault behaviour and diagnostic means.

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*

Annexes A to D, which are informative, are structured according to Table 1.

Table 1 — Structure of Annexes A to D of this part of ISO 13849

Annex	Technology	List of basic safety principles	List of well-tried safety principles	List of well-tried components	Fault lists and fault exclusions
		Table(s)			
A	Mechanical	A.1	A.2	A.3	A.4, A.5
B	Pneumatic	B.1	B.2	—	B.3 to B.18
C	Hydraulic	C.1	C.2	—	C.3 to C.12
D	Electrical (includes electronics)	D.1	D.2	D.3	D.4 to D.21

Introduction

The structure of safety standards in the field of machinery is as follows:

a) type-A standards (basic safety standards) giving basic concepts, principles for design and general aspects that can be applied to machinery;

b) type-B standards (generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery:

   — type-B1 standards on particular safety aspects (for example safety distances, surface temperature, noise);

   — type-B2 standards on safeguards (for example two-hand controls, interlocking devices, pressure-sensitive devices, guards);

c) type-C standards (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

This document is a type-B standard as stated in ISO 12100.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

This part of ISO 13849 specifies the validation process for the safety functions, categories and performance levels for the safety-related parts of control systems. It recognizes that the validation of safety-related parts of control systems can be achieved by a combination of analysis (see Clause 5) and testing (see Clause 6), and specifies the particular circumstances in which testing ought to be carried out.

Most of the procedures and conditions in this part of ISO 13849 are based on the assumption that the simplified procedure for estimating the performance level (PL) described in ISO 13849-1:2006, 4.5.4, is used. This part of ISO 13849 does not provide guidance for situations when other procedures are used to estimate PL (e.g. Markov modelling), in which case some of its provisions will not apply and additional requirements can be necessary.

Guidance on the general principles for the design (see ISO 12100) of safety-related parts of control systems, regardless of the type of technology used (electrical, hydraulic, pneumatic, mechanical, etc.), is provided in ISO 13849-1. This includes descriptions of some typical safety functions, determination of their required performance levels, and general requirements of categories and performance levels.

Within this part of ISO 13849, some of the validation requirements are general, whereas others are specific to the type of technology used.

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

Part 2: Validation

1 Scope

This part of ISO 13849 specifies the procedures and conditions to be followed for the validation by analysis and testing of

— the specified safety functions,

— the category achieved, and

— the performance level achieved

by the safety-related parts of a control system (SRP/CS) designed in accordance with ISO 13849-1.

NOTE Additional requirements for programmable electronic systems, including embedded software, are given in ISO 13849-1:2006, 4.6, and IEC 61508 .

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100 and ISO 13849-1 apply.

4 Validation process

4.1 Validation principles

The purpose of the validation process is to confirm that the design of the SRP/CS supports the overall safety requirements specification for the machinery.

The validation shall demonstrate that each SRP/CS meets the requirements of ISO 13849-1 and, in particular, the following:

a) the specified safety characteristics of the safety functions provided by that part, as set out in the design rationale;

b) the requirements of the specified performance level (see ISO 13849-1:2006, 4.5):

   1) the requirements of the specified category (see ISO 13849-1:2006, 6.2),

2) the measures for control and avoidance of systematic failures (see ISO 13849-1:2006, Annex G),

3) if applicable, the requirements of the software (see ISO 13849-1:2006, 4.6), and

4) the ability to perform a safety function under expected environmental conditions;

c) the ergonomic design of the operator interface, e.g. so that the operator is not tempted to act in a hazardous manner, such as defeating the SRP/CS (see ISO 13849-1:2006, 4.8).

Validation should be carried out by persons who are independent of the design of the SRP/CS.

NOTE "Independent person" does not necessarily mean that a third-party test is required.

Validation consists of applying analysis (see Clause 5) and executing functional tests (see Clause 6) under foreseeable conditions in accordance with the validation plan. Figure 1 gives an overview of the validation process. The balance between the analysis and testing depends on the technology used for the safety-related parts and the required performance level. For Categories 2, 3 and 4 the validation of the safety function shall also include testing under fault conditions.

The analysis should be started as early as possible in, and in parallel with, the design process. Problems can then be corrected early while they are still relatively easy to correct, i.e. during steps "design and technical realization of the safety function" and "evaluate the performance level PL" [the fourth and fifth boxes down in in ISO 13849-1:2006, Figure 3]. It can be necessary for some parts of the analysis to be delayed until the design is well developed.

Where necessary due to the system's size, complexity or the effects of integrating it with the control system (of the machinery), special arrangements should be made for

— validation of the SRP/CS separately before integration, including simulation of the appropriate input and output signals, and

— validation of the effects of integrating safety-related parts into the remainder of the control system within the context of its use in the machine.

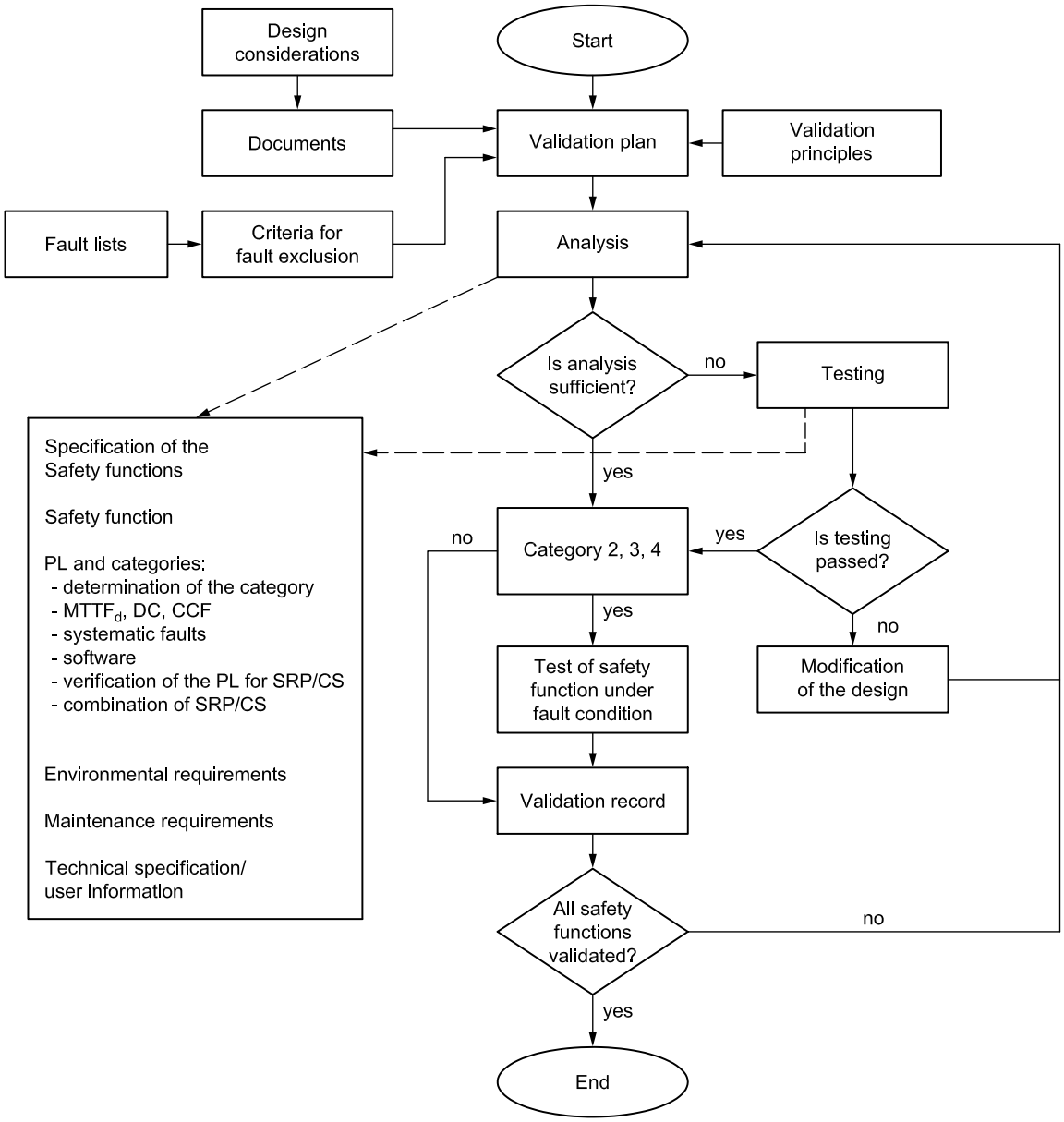

Figure 1 — Overview of the validation process

"Modification of the design" in Figure 1 refers to the design process. If the validation cannot be successfully completed, changes in the design are necessary. The validation of the modified safety-related parts should then be repeated. This process should be iterated until all safety-related parts of the safety functions are successfully validated.

4.2 Validation plan

The validation plan shall identify and describe the requirements for carrying out the validation process for the specified safety functions, their categories and performance levels.

The validation plan shall also identify the means to be employed to validate the specified safety functions, categories and performance levels. It shall set out, where appropriate

a) the identity of the specification documents,

b) the operational and environmental conditions during testing,