INTERNATIONAL STANDARD

ISO 13849-2

First edition
2003-08-15

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

Part 2: Validation

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

Partie 2: Validation

Reference number
ISO 13849-2:2003(E)

© ISO 2003

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO 2003

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 either ISO at the address below or ISO's member body in the country of the requester.

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

 © ISO 2003 – All rights reserved

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 the European Committee for Standardization (CEN) in collaboration with Technical Committee ISO/TC 199, *Safety of machinery*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Throughout the text of this document, read "...this European Standard..." to mean "...this International Standard...".

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*

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

© ISO 2003 – All rights reserved

Contents

Page

Foreword v
Introduction vi
1 Scope 1
2 Normative references 1
3 Validation process 1
3.1 Validation principles 1
3.2 Generic fault lists 3
3.3 Specific fault lists 3
3.4 Validation plan 3
3.5 Information for validation 4
3.6 Validation record 5
4 Validation by analysis 5
4.1 General 5
4.2 Analysis techniques 6
5 Validation by testing 6
5.1 General 6
5.2 Measurement uncertainty 7
5.3 Higher requirements 7
5.4 Number of test samples 7
6 Validation of safety functions 8
7 Validation of categories 8
7.1 Analysis and testing of categories 8
7.2 Validation of category specifications 9
7.3 Validation of combination of safety–related parts 10
8 Validation of environmental requirements 10
9 Validation of maintenance requirements 11
Annex A (informative) **Validation tools for mechanical systems** 12
Annex B (informative) **Validation tools for pneumatic systems** 17
Annex C (informative) **Validation tools for hydraulic systems** 28
Annex D (informative) **Validation tools for electrical systems** 38
Bibliography 49

© ISO 2003 – All rights reserved

Foreword

This document EN ISO 13849-2:2003 has been prepared by Technical Committee CEN /TC 114, "Safety of machinery", the secretariat of which is held by DIN in collaboration with Technical Committee ISO/TC 199 "Safety of machinery".

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2004, and conflicting national standards shall be withdrawn at the latest by February 2004.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association and supports essential requirements of EC Directive(s).

Annexes A to D are informative and structured as given in Table 1.

Table 1 — Structure of the clauses of annexes A to D

Annex	Technology	List of basic safety principles	List of well-tried safety principles	List of well-tried components	Fault lists and fault exclusions
		Clause			
A	Mechanical	A.2	A.3	A.4	A.5
B	Pneumatic	B.2	B.3	B.4	B.5
C	Hydraulic	C.2	C.3	C.4	C.5
D	Electrical (includes electronics)	D.2	D.3	D.4	D.5

This document includes a Bibliography.

EN 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

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

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and the United Kingdom.

© ISO 2003 – All rights reserved

Introduction

For the use in the European Union, this part of EN ISO 13849 has the status of a generic safety standard (type B1).

This European Standard specifies the validation process, including both analysis and testing, for the safety functions and categories for the safety–related parts of control systems. Descriptions of the safety functions and the requirements for the categories are given in EN 954-1 (ISO 13849-1) which deals with the general principles for design. Some requirements for validation are general and some are specific to the technology used. EN ISO 13849-2 also specifies the conditions under which the validation by testing of the safety-related parts of control systems should be carried out.

EN 954-1 (ISO 13849-1) specifies the safety requirements and gives guidance on the principles for the design [see EN 292-1:1991 (ISO/TR 12100:1992), 3.11] of the safety-related parts of control systems. For these parts it specifies categories and describes the characteristics of their safety functions, regardless of the type of energy used. Additional advice on EN 954-1 (ISO 13894-1) is given in CR 954-100 (ISO/TR 13849-100).

The achievement of the requirements can be validated by any combination of analysis (see clause 4) and testing (see clause 5). The analysis should be started as early as possible within the design process.

© ISO 2003 – All rights reserved

1 Scope

This European Standard specifies the procedures and conditions to be followed for the validation by analysis and testing of:

— the safety functions provided, and

— the category achieved

of the safety-related parts of the control system in compliance with EN 954-1 (ISO 13849-1), using the design rationale provided by the designer.

This European Standard does not give complete validation requirements for programmable electronic systems and therefore can require the use of other standards.

NOTE CEN/TC 114/WG 6 proposes to deal in more detail with the validation of programmable electronic systems in the elaboration of the revision to EN 954-1 (ISO 13849-1). An application standard for machinery (draft IEC 62061), based on IEC 61508, is under preparation. Requirements for programmable electronic systems, including embedded software, are given in IEC 61508.

2 Normative references

This European Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text, and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

EN 292-1:1991 (ISO/TR 12100:1992), *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology.*

EN 954-1:1996 (ISO 13849-1:1999), *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.*

3 Validation process

3.1 Validation principles

The purpose of the validation process is to confirm the specification and the conformity of the design of the safety-related parts of the control system within the overall safety requirements specification of the machinery.

The validation shall demonstrate that each safety-related part meets the requirements of EN 954-1 (ISO 13849-1), in particular:

— the specified safety characteristics of the safety functions provided by that part, as set out in the design rationale, and

— the requirements of the specified category [see EN 954-1:1996 (ISO 13849-1:1999), clause 6].

Validation should be carried out by persons who are independent of the design of the safety-related part(s).

NOTE Independent person does not necessarily mean that a 3rd party test is required.

The degree of independence should reflect the safety performance of the safety-related part.

Validation consists of applying analysis (see clause 4) and, if necessary, executing tests (see clause 5) in accordance with the validation plan. Figure 1 gives an overview of the validation process. The balance between the analysis and/or testing depends on the technology.

© ISO 2003 – All rights reserved