SLOVENSKI STANDARD
oSIST prEN ISO 13849-2:2010

01-september-2010

Varnost strojev - Z varnostjo povezani deli krmilnih sistemov - 2. del: Potrjevanje (ISO/DIS 13849-2:2010)

Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO/DIS 13849-2:2010)

Sicherheit von Maschinen und Geräten - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung (ISO/DIS 13849-2:2010)

Sécurité des machines - Parties des systèmes de commande relatifs à la sécurité - Partie 2: Validation (ISO/DIS 13849-2:2010)

Ta slovenski standard je istoveten z: **prEN ISO 13849-2**

ICS:

13.110	Varnost strojev	Safety of machinery

oSIST prEN ISO 13849-2:2010 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN ISO 13849-2

May 2010

ICS 13.110

Will supersede EN ISO 13849-2:2008

English Version

Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO/DIS 13849-2:2010)

Sécurité des machines - Parties des systèmes de commande relatifs à la sécurité - Partie 2: Validation (ISO/DIS 13849-2:2010)

Sicherheit von Maschinen und Geräten - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung (ISO/DIS 13849-2:2010)

This draft European Standard is submitted to CEN members for parallel enquiry. It has been drawn up by the Technical Committee CEN/TC 114.

If this draft becomes a European Standard, CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. prEN ISO 13849-2:2010: E

Contents

Page

Foreword

This document (prEN ISO 13849-2:2010) has been prepared by Technical Committee ISO/TC 199 “Safety of machinery” in collaboration with Technical Committee CEN/TC 114 “Safety of machinery” the secretariat of which is held by DIN.

This document is currently submitted to the parallel Enquiry.

This document will supersede EN ISO 13849-2:2008.

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 EU Directive(s).

Endorsement notice

The text of ISO/DIS 13849-2:2010 has been approved by CEN as a prEN ISO 13849-2:2010 without any modification.

DRAFT INTERNATIONAL STANDARD ISO/DIS 13849-2

ISO/TC **199** Secretariat: **DIN**

Voting begins on: **2010-05-27** Voting terminates on: **2010-10-27**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

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

[Revision of first edition (ISO 13849-2:2003)]

ICS 13.110

ISO/CEN PARALLEL PROCESSING

This draft has been developed within the International Organization for Standardization (ISO), and processed under the **ISO-lead** mode of collaboration as defined in the Vienna Agreement.

This draft is hereby submitted to the ISO member bodies and to the CEN member bodies for a parallel five-month enquiry.

Should this draft be accepted, a final draft, established on the basis of comments received, will be submitted to a parallel two-month approval vote in ISO and formal vote in CEN.

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

Contents

Page

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 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.

Introduction

This document is a type-B standard as stated in ISO 12100-1.

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 International Standard specifies the validation process, including both analysis and testing, for the safety functions, categories and performance levels for the safety–related parts of control systems. Most of the procedures and conditions in this International Standard are based on the assumption that the Simplified Procedure described in ISO 13849-1:2006, 4.5.4 is used for the estimation of Performance Level (PL). When a different procedure is used (e.g. Markov modelling), then some parts of this standard can not be applicable and additional requirements can be necessary. This standard does not provide guidance specifically for the case when other procedures are used to estimate PL.

Descriptions of the safety functions and the requirements for the categories and performance levels are given in 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. 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.

ISO 13849-1 specifies the safety requirements and gives guidance on the principles for the design (see ISO 12100-1) of the safety-related parts of control systems. For these parts it specifies categories and performance levels and describes the characteristics of their safety functions, regardless of the type of energy used.

The achievement of the requirements can be validated by any combination of analysis (see Clause 5) and testing (see Clause 6). The analysis should be started as early as possible within the design process.

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

Part 2: Validation

1 Scope

This International 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, and

— the performance level achieved

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

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

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 12100-1, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

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 13849-1 apply.

4 Validation process

4.1 Validation principles

The purpose of the validation process is to confirm the specification and the conformity of the design of the SRP/CS within the overall safety requirements specification of the machinery.

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

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

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

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

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

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

— the ability to perform a safety function under expected environmental conditions.

NOTE Validation of the design of SRP/CS includes review activities. Validation and review should be made by person(s) other than designer(s) of the relevant item. Review should be based on the safety requirements specification and design documentation.

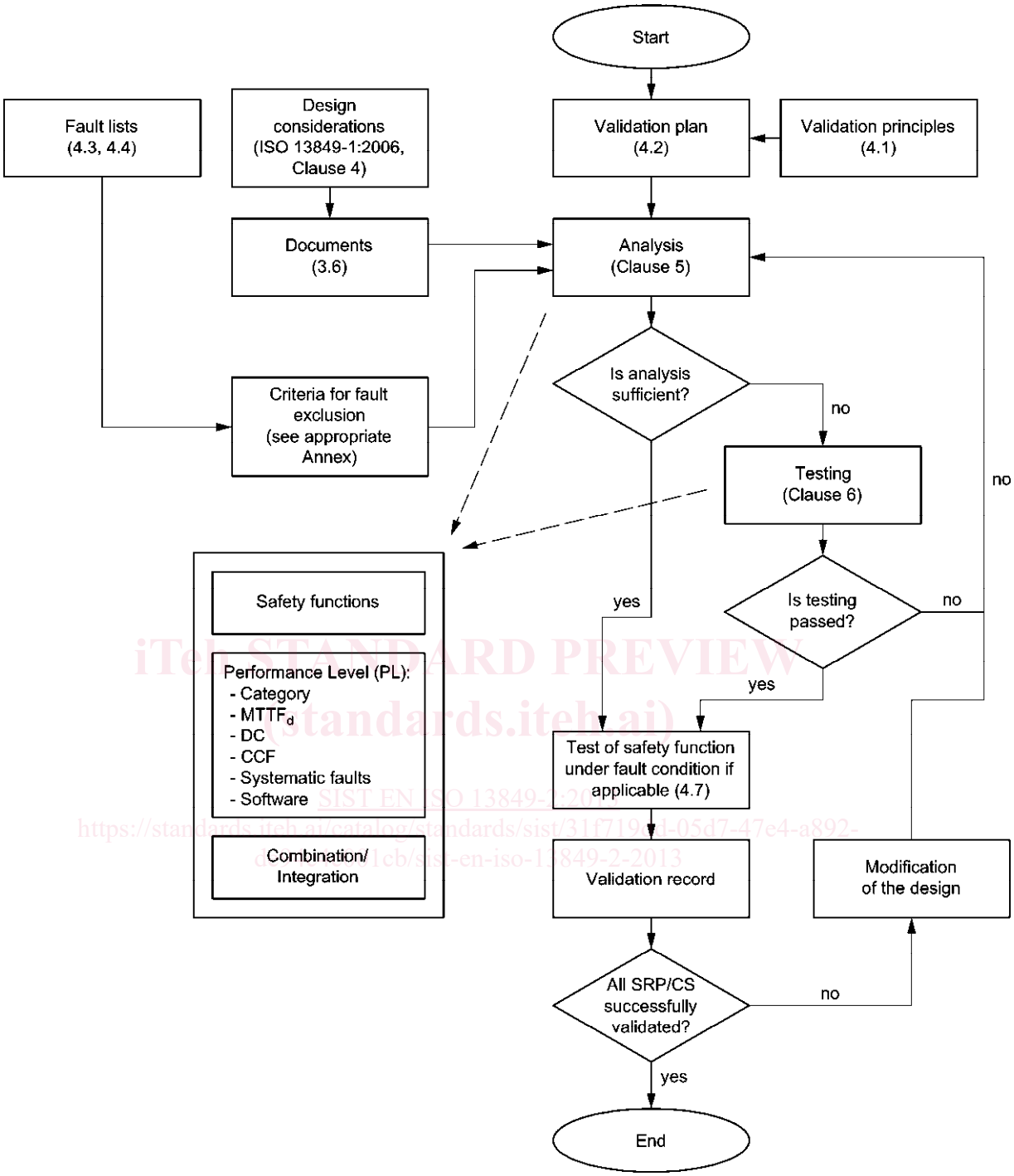
Validation consists of applying analysis and executing functional tests under normal conditions in accordance with the validation plan. Figure 1 gives an overview of the validation process. The balance between the analysis and testing depends on the technology and performance level. Where necessary for Category 2, 3 and 4 the safety function shall be validated by testing also under fault conditions.

The analysis should be started as early as possible and in parallel with the design process, so that problems can be corrected early whilst they are still relatively easy to correct, i. e. during steps “design and technical realisation of the safety function” and “evaluate the performance level PL” [box 4 and 5 of Figure 3 in ISO 13849-1:2006]. It can be necessary for some parts of the analysis to be delayed until the design is well developed.

For large systems, due to the size, complexity or integrated form (with the machinery) of the control system, special arrangements may be made for:

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

— 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.



NOTE The block "modification of the design" refers to the design process. If the validation cannot be successfully completed, changes in the design are necessary. Afterwards the validation concerning the changed parts should be repeated. This process should be iterated until all parts are successfully validated.

Figure 1 — Overview of the validation process

4.2 Validation plan

The validation plan shall identify and describe the requirements for carrying out the validation process of 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: