MASINATE OHUTUS. JUHTIMISSÜSTEEMIDE OHUTUSEGA SEOTUD OSAD. OSA 2: VALIDEERIMINE

Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2012)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO 13849-2:2012 sisaldab Euroopa standardi EN ISO 13849-2:2012 ingliskeelset teksti.	This Estonian standard EVS-EN ISO 13849-2:2012 consists of the English text of the European standard EN ISO 13849-2:2012.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 15.10.2012.	Date of Availability of the European standard is 15.10.2012.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 13.110

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 13849-2

October 2012

ICS 13.110

Supersedes EN ISO 13849-2:2008

English Version

Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2012)

Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 2: Validation (ISO 13849-2:2012)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung (ISO 13849-2:2012)

This European Standard was approved by CEN on 14 October 2012.

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. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists 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-CENELEC 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO 13849-2:2012: E

Foreword

This document (EN ISO 13849-2:2012) 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 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 April 2013, and conflicting national standards shall be withdrawn at the latest by April 2013.

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

This document supersedes 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.

For relationship with EU Directive, see informative Annex ZA, which is an integral part of this document.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 13849-2:2012 has been approved by CEN as a EN ISO 13849-2:2012 without any modification.

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**

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),