This is a free page sample. Access the full version online.

NSAI Standards

Irish Standard
I.S. EN 16590-1:2014

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 1: General principles for design and development (ISO 25119-1:2010 modified)

© CEN 2014 No copying without NSAI permission except as permitted by copyright law.

This is a free page sample. Access the full version online.

I.S. EN 16590-1:2014

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:	*Published:*
EN 16590-1:2014	2014-04-23

This document was published under the authority of the NSAI and comes into effect on:	ICS number:
2014-05-03	35.240.99 65.060.01
	NOTE: If blank see CEN/CENELEC cover page

NSAI	T +353 1 807 3800	Sales:
1 Swift Square,	F +353 1 807 3838	T +353 1 857 6730
Northwood, Santry	E standards@nsai.ie	F +353 1 857 6729
Dublin 9	W NSAI.ie	W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

This is a free page sample. Access the full version online.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16590-1

April 2014

ICS 35.240.99; 65.060.01

English Version

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 1: General principles for design and development (ISO 25119-1:2010 modified)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux pour la conception et le développement (ISO 25119-1:2010 modifié)

Sicherheit von Land- und Forstmaschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungs- und Entwicklungsleitsätze (ISO 25119-1:2010 modifiziert)

This European Standard was approved by CEN on 23 February 2014.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 16590-1:2014 E

This is a free page sample. Access the full version online.

Contents

Page

Foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Abbreviated terms 14

5 Management during complete safety life cycle 15
5.1 Objectives 15
5.2 General 15
5.2.1 Introduction to the safety life cycle concept 15
5.2.2 External functional safety measures 15
5.3 Prerequisites 15
5.4 Requirements — Functional safety management activities across safety life cycle 17
5.4.1 Functional safety culture 17
5.4.2 Continuous improvement 17
5.4.3 Training and qualification 18
5.4.4 Safety management during development 18
5.4.5 Assignment of safety responsibilities 18
5.4.6 Assignment of tasks 18
5.4.7 Planning of all safety management activities during development 18
5.5 Work products 21

6 Assessment of functional safety 21
6.1 Objectives 21
6.2 General 21
6.3 Prerequisites 21
6.4 Requirements 21
6.4.1 Considerations for the assessment of the functional safety 21
6.4.2 Verification 22
6.5 Work products 23

7 Safety management activities after start of production (SOP) 24
7.1 Objectives 24
7.2 General 24
7.3 Prerequisites 24
7.4 Requirements 24
7.4.1 Management of production and modification procedures 24
7.4.2 Tasks for preparing and conducting production and end of line inspections 24
7.4.3 Tasks for safe machine operation and decommissioning 24
7.5 Work products 25

8 Production and installation of safety-related systems 25
8.1 Objectives 25
8.2 General 25
8.3 Prerequisites 25
8.4 Requirements 25
8.4.1 Production plan 25
8.4.2 Test plan 25
8.4.3 Production and testing 26
8.4.4 Process capability 26

This is a free page sample. Access the full version online.

8.4.5 Documentation 26
8.4.6 Non-compliance 26
8.4.7 Traceability 26
8.4.8 Storage and transport conditions 26
8.4.9 Modification 26
8.5 Work products 26

Annex A (informative) Example of the structure of a project-specific safety plan 27

A.1 General 27

A.2 Change log 27

A.3 Objective of overall project 27

A.4 Schedule 27

A.5 Project organisation 27

A.5.1 Project team organisation 27

A.5.2 Project team members 28

A.5.3 Safety management 28

Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Machinery Directive 2006/42/EC 30

Bibliography 31

This is a free page sample. Access the full version online.

Foreword

This document (EN 16590-1:2014) has been prepared by Technical Committee CEN/TC 144 “Tractors and machinery for agriculture and forestry”, the secretariat of which is held by AFNOR.

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 October 2014, and conflicting national standards shall be withdrawn at the latest by October 2014.

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 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).

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

EN 16590 *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems* consists of the following parts:

— *Part 1: General principles for design and development*

— *Part 2: Concept phase*

— *Part 3: Series development, hardware and software*

— *Part 4: Production, operation, modification and supporting processes*

The modifications to ISO 25119-1:2010 are indicated by a vertical line in the margin.

According to the CEN/CENELEC Internal Regulations, the national standards organizations 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.

This is a free page sample. Access the full version online.

Introduction

EN 16590 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising of electrical and/or electronic and/or programmable electronic systems (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to municipal equipment. It covers the possible hazards caused by the functional behaviour of E/E/PES safety-related systems, as distinct from hazards arising from the E/E/PES equipment itself (e.g. electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety).

The control system parts of the machines concerned are frequently assigned to provide the critical functions of the *safety-related parts of control systems* (SRP/CS). These can consist of hardware or software, can be separate or integrated parts of a control system, and can either perform solely critical functions or form part of an operational function.

In general, the designer (and to some extent, the user) will combine the design and validation of these SRP/CS as part of the risk assessment. The objective is to reduce the risk associated with a given hazard (or hazardous situation) under all conditions of use of the machine. This can be achieved by applying various protective measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

EN 16590 allocates the ability of safety-related parts to perform a critical function under foreseeable conditions into five performance levels. The performance level of a controlled channel depends on several factors, including system structure (category), the extent of fault detection mechanisms (diagnostic coverage), the reliability of components (mean time to dangerous failure, common-cause failure), design processes, operating stress, environmental conditions and operation procedures. Three types of failures are considered: systematic, common-cause and random.

In order to guide the designer during design, and to facilitate the assessment of the achieved performance level, EN 16590 defines an approach based on a classification of structures with different design features and specific behaviour in case of a fault.

The performance levels and categories can be applied to the control systems of all kinds of mobile machines: from simple systems (e.g. auxiliary valves) to complex systems (e.g. steer by wire), as well as to the control systems of protective equipment (e.g. interlocking devices, pressure sensitive devices).

EN 16590 adopts a risk-based approach for the determination of the risks, while providing a means of specifying the required performance level for the safety-related functions to be implemented by E/E/PES safety-related channels. It gives requirements for the whole safety life cycle of E/E/PES (design, validation, production, operation, maintenance, decommissioning), necessary for achieving the required functional safety for E/E/PES that are linked to the performance levels.

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

a) Type-A standards (basic safety standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:

— type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

— type-B2 standards on safeguards (e.g. two-hand controls, interlocking devices, pressure sensitive devices, guards).

c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This is a free page sample. Access the full version online.

This part of EN 16590 is a type-B1 standard as stated in EN ISO 12100.

For machines which are covered by the scope of a machine specific type-C standard and which have been designed and built according to the provisions of that standard, the provisions of that type-C standard take precedence over the provisions of this type-B standard.

This is a free page sample. Access the full version online.

1 Scope

This part of EN 16590 sets out general principles for the design and development of safety-related parts of control systems (SRP/CS) on tractors used in agriculture and forestry and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It can also be applied to municipal equipment (e.g. street-sweeping machines). It specifies the characteristics and categories required of SRP/CS for carrying out their safety functions.

This part of EN 16590 is applicable to the safety-related parts of electrical/electronic/programmable electronic systems (E/E/PES), as these relate to mechatronic systems. It does not specify which safety functions, categories or performance levels are to be used for particular machines.

Machine specific standards (type-C standards) can identify performance levels and/or categories or they should be determined by the manufacturer of the machine based on risk assessment.

It is not applicable to non-E/E/PES systems (e.g. hydraulic, mechanic or pneumatic).

NOTE See also EN ISO 12100 for design principles related to the safety of machinery.

2 Normative references

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

EN 16590-2:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase*

EN 16590-3:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software*

EN 16590-4:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: production, operation, modification and supporting processes*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
agricultural performance level
AgPL
level which specifies the ability of safety-related parts to perform a safety-related function under foreseeable conditions

Note 1 to entry: For the purposes of EN 16590, the performance for each hazardous situation is divided into five levels, a, b, c, d and e, where the functional safety contributed by the SRP/CS in “a” is low and in “e” is high.

3.2
required agricultural performance level
$AgPL_r$
performance level (AgPL) needed to achieve the required functional safety for each safety-related function

This is a free page sample. Access the full version online.
I.S. EN 16590-1:2014

INTERNATIONAL STANDARD

ISO 25119-1

First edition
2010-06-01

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems —

Part 1: General principles for design and development

Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité —

Partie 1: Principes généraux pour la conception et le développement

Reference number
ISO 25119-1:2010(E)

© ISO 2010

This is a free page sample. Access the full version online.

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.

COPYRIGHT PROTECTED DOCUMENT

© ISO 2010

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

This is a free page sample. Access the full version online.

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 8

5 Management during complete safety life cycle 9
5.1 Objectives 9
5.2 General 9
5.3 Prerequisites 9
5.4 Requirements — Functional safety management activities across safety life cycle 11
5.5 Work products 15

6 Assessment of functional safety 15
6.1 Objectives 15
6.2 General 15
6.3 Prerequisites 15
6.4 Requirements 15
6.5 Work products 17

7 Safety management activities after start of production (SOP) 18
7.1 Objectives 18
7.2 General 18
7.3 Prerequisites 18
7.4 Requirements 18
7.5 Work products 18

8 Production and installation of safety-related systems 19
8.1 Objectives 19
8.2 General 19
8.3 Prerequisites 19
8.4 Requirements 19
8.5 Work products 20

Annex A (informative) **Example of the structure of a project-specific safety plan** 21

Bibliography 24

© ISO 2010 – All rights reserved

This is a free page sample. Access the full version online.

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 25119-1 was prepared by Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 19, *Agricultural electronics*.

ISO 25119 consists of the following parts, under the general title *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems*:

— *Part 1: General principles for design and development*

— *Part 2: Concept phase*

— *Part 3: Series development, hardware and software*

— *Part 4: Production, operation, modification and supporting processes*

© ISO 2010 – All rights reserved

This is a free page sample. Access the full version online.

Introduction

ISO 25119 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising of electrical and/or electronic and/or programmable electronic components (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to municipal equipment. It covers the possible hazards caused by the functional behaviour of E/E/PES safety-related systems, as distinct from hazards arising from the E/E/PES equipment itself (e.g. electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety).

The control system parts of the machines concerned are frequently assigned to provide the critical functions of the *safety-related parts of control systems* (SRP/CS). These can consist of hardware or software, can be separate or integrated parts of a control system, and can either perform solely critical functions or form part of an operational function.

In general, the designer (and to some extent, the user) will combine the design and validation of these SRP/CS as part of the risk assessment. The objective is to reduce the risk associated with a given hazard (or hazardous situation) under all conditions of use of the machine. This can be achieved by applying various protective measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

ISO 25119 allocates the ability of safety-related parts to perform a critical function under foreseeable conditions into five performance levels. The performance level of a controlled channel depends on several factors, including system structure (category), the extent of fault detection mechanisms (diagnostic coverage), the reliability of components (mean time to dangerous failure, common-cause failure), design processes, operating stress, environmental conditions and operation procedures. Three types of failures are considered: systematic, common-cause and random.

In order to guide the designer during design, and to facilitate the assessment of the achieved performance level, ISO 25119 defines an approach based on a classification of structures with different design features and specific behaviour in case of a fault.

The performance levels and categories can be applied to the control systems of all kinds of mobile machines: from simple systems (e.g. auxiliary valves) to complex systems (e.g. steer by wire), as well as to the control systems of protective equipment (e.g. interlocking devices, pressure sensitive devices).

ISO 25119 adopts a customer risk-based approach for the determination of the risks, while providing a means of specifying the target performance level for the safety-related functions to be implemented by E/E/PES safety-related channels. It gives requirements for the whole safety life cycle of E/E/PES (design, validation, production, operation, maintenance, decommissioning), necessary for achieving the required functional safety for E/E/PES that are linked to the performance levels.

© ISO 2010 – All rights reserved

This is a free page sample. Access the full version online.

This is a free page sample. Access the full version online.

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems —

Part 1: General principles for design and development

1 Scope

This part of ISO 25119 sets out general principles for the design and development of safety-related parts of control systems (SRP/CS) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It can also be applied to municipal equipment (e.g. street-sweeping machines). It specifies the characteristics and categories required of SRP/CS for carrying out their safety functions.

This part of ISO 25119 is applicable to the safety-related parts of electrical/electronic/programmable electronic systems (E/E/PES). As these relate to mechatronic systems, it does not specify which safety functions or categories are to be used in a particular case.

It is not applicable to non-E/E/PES systems (e.g. hydraulic, mechanic or pneumatic).

NOTE See also ISO 12100 for design principles related to the safety of machinery.

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 25119-2:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase*

ISO 25119-3:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware, software*

ISO 25119-4:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: production, operation, modification and supporting processes*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
agricultural performance level
AgPL
level which specifies the ability of safety-related parts to perform a safety-related function under foreseeable conditions

NOTE For the purposes of ISO 25119, the performance for each hazardous situation is divided into fives levels, a, b, c, d and e, where the functional safety contributed by the SRP/CS in “a” is low and in “e” is high.

© ISO 2010 – All rights reserved

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation