სსტ ენ 16590-3:2014/2014

საქართველოს სტანდარტი

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.

ტრაქტორები და მანქანები სოფლის და სატყეო მეურნეობაში - კონტროლის სისტემების უსაფრთხოების ნაწილები - ნაწილი 3: სერიული წარმოება, ტექნიკა და პროგრამული უზრუნველყოფა (ISO 25119-3:2010 მოდიფიცირებული)

საქართველოს სტანდარტების და მეტროლოგიის
ეროვნული სააგენტო
თბილისი

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.

სსტ ენ 16590-3:2014/2014

საინფორმაციო მონაცემები

1 დამტკიცებულია და შემოღებულია სამოქმედოდ საქართველოს სტანდარტების და მეტროლოგიის ეროვნული სააგენტოს 2014 წლის 19 სექტემბრის № 78 და 2014 წლის 1 ივლისის № 55 განკარგულებებით

2 მიღებულია გარეკანის თარგმნის მეთოდით სტანდარტიზაციის ევროპული კომიტეტის სტანდარტი ენ 16590-3:2014 „ ტრაქტორები და მანქანები სოფლის და სატყეო მეურნეობაში - კონტროლის სისტემების უსაფრთხოების ნაწილები - ნაწილი 3: სერიული წარმოება, ტექნიკა და პროგრამული უზრუნველყოფა (ISO 25119-3:2010 მოდიფიცირებული)”

3 პირველად

4 რეგისტრირებულია საქართველოს სტანდარტების და მეტროლოგიის ეროვნული სააგენტოს რეესტრში: 2014 წლის 19 სექტემბერი №268-1.3-6205

წინამდებარე სტანდარტის სრული ან ნაწილობრივი აღწარმოება, ტირაჟირება და გავრცელება საქართველოს სტანდარტების და მეტროლოგიის ეროვნული სააგენტოს ნებართვის გარეშე არ დაიშვება

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16590-3

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 3: Series development, hardware and software (ISO 25119-3:2010 modified)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 3: Développement en série, matériels et logiciels (ISO 25119-3:2010 modifié)

Sicherheit von Land- und Forstmaschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 3: Serienentwicklung, Hardware, Software (ISO 25119-3:2010 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 16590-3:2014 E

Contents

Page

Foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Abbreviated terms 7

5 System design 8
5.1 Objectives 8
5.2 General 8
5.3 Prerequisites 9
5.4 Requirements 9
5.4.1 Structuring safety requirements 9
5.4.2 Functional safety concept 10
5.4.3 Technical safety concept 11

6 Hardware 13
6.1 Objectives 13
6.2 General 13
6.3 Prerequisites 14
6.4 Requirements 14
6.5 Hardware categories 15
6.6 Work products 16

7 Software 16
7.1 Software development planning 16
7.1.1 Objectives 16
7.1.2 General 17
7.1.3 Prerequisites 17
7.1.4 Requirements 17
7.1.5 Work products 20
7.2 Software safety requirements specification 20
7.2.1 Objectives 20
7.2.2 General 20
7.2.3 Prerequisites 20
7.2.4 Requirements 21
7.2.5 Work products 24
7.3 Software architecture and design 24
7.3.1 Objectives 24
7.3.2 General 24
7.3.3 Prerequisites 24
7.3.4 Requirements 24
7.3.5 Work products 27
7.4 Software module design and implementation 27
7.4.1 Objectives 27
7.4.2 General 27
7.4.3 Prerequisites 27
7.4.4 Requirements 27
7.4.5 Work products 36
7.5 Software module testing 36

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.

7.5.1 Objectives 36
7.5.2 General 36
7.5.3 Prerequisites 36
7.5.4 Requirements 36
7.5.5 Work products 44
7.6 Software integration and testing 44
7.6.1 Objectives 44
7.6.2 General 44
7.6.3 Prerequisites 45
7.6.4 Requirements 45
7.6.5 Work products 46
7.7 Software safety validation 47
7.7.1 Objectives 47
7.7.2 General 47
7.7.3 Prerequisites 47
7.7.4 Requirements 47
7.7.5 Work products 49
7.8 Software-based parameterisation 49
7.8.1 Objective 49
7.8.2 General 49
7.8.3 Prerequisites 49
7.8.4 Requirements 50
7.8.5 Work products 50
Annex A (informative) Example of agenda for assessment of functional safety at AgPL = e 52
A.1 Functions of system 52
A.2 Hardware 52
A.3 Safety concept 52
A.4 Safety analysis and safety data 52
A.5 Safety design process for phases of life cycle 52
A.6 Software development 53
A.7 Verification and testing 53
A.8 Documentation and safety documentation 53
A.9 Summary and assessment 53
Annex B (informative) Independence by software partitioning 54
B.1 General 54
B.2 Terms, definitions and abbreviated terms 54
B.3 Objectives 56
B.4 General 57
B.5 Requirements 57
B.5.1 General requirements 57
B.5.2 Several partitions within a single microcontroller 57
B.5.3 Several partitions within the scope of a micro-controller network 60
Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Machinery Directive 2006/42/EC 63
Bibliography 64

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.

Foreword

This document (EN 16590-3:2014) 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 25119-3:2010 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.

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.

Introduction

EN 16590 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising 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 (electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety, etc.).

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-hands 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.

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.

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.

საინფორმაციო ნაწილი. სრული ტექსტის სანახავად შეიძინეთ სტანდარტი.