SLOVENSKI STANDARD
SIST EN 16590-1:2014

01-julij-2014

Traktorji ter kmetijski in gozdarski stroji - Varnostni deli krmilnih sistemov - 1. del: Osnovna načela za načrtovanje in razvoj (ISO 25119-1:2010, spremenjen)

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)

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

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 modifiée)

Ta slovenski standard je istoveten z: **EN 16590-1:2014**

ICS:

35.240.99	Uporabniške rešitve IT na drugih področjih	IT applications in other fields
65.060.01	Kmetijski stroji in oprema na splošno	Agricultural machines and equipment in general

SIST EN 16590-1:2014 **en,fr,de**

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

Ref. No. EN 16590-1:2014 E

Contents

Page

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.

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 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.

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

3.3
category
classification of the safety-related parts of a control system with respect to its resistance to faults and its subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts and/or by their reliability

3.4
channel
series combination of input, logic, and output elements

3.5
common-cause failure
CCF
failures of different items, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: Common-cause failures ought not be confused with *common mode failures* (see EN ISO 12100).

3.6
controllability
involved individual's possibility of avoiding harm in the situation that is putting him/her at risk

3.7
dangerous detected failure rate
λ_{dd}
dangerous failure rate of those components where fault detection is realised

3.8
dangerous failure
failure in which an SRP/CS is no longer able to maintain the required performance level, even if the safety-related function is maintained by other (redundant) system components (due to reduction of the resulting performance level)

3.9
dangerous failure rate
λ_{d}
fraction of all components with dangerous failure per time unit

3.10
diagnostic coverage
DC
fraction of the probability of detected dangerous failures, λ_{dd}, and the probability of total dangerous failures, λ_{d}, expressed by:

$$DC = \sum \lambda_{dd} \Big/ \sum \lambda_{d}$$

Note 1 to entry: Diagnostic coverage can exist for the whole or parts of a high-risk functional system, e.g. for sensors and/or logic system and/or final elements.

Note 2 to entry: The value of DC is defined according to Table 1.

Note 3 to entry: For SRP/CS consisting of several parts, an average value, DC_{avg}, is used (see EN 16590-2:2014, Annex C).

Table 1 — Diagnostic coverage (DC)

Denotation	Range
Low	DC < 60 %
Medium	60 % ≤ DC < 90 %
High	90 % ≤ DC

3.11
diagnostic test interval
interval between online tests used to detect faults in a safety-related system that have a specified diagnostic coverage

3.12
E/E/PES-system architecture
allocation of critical functions to electronic control units (ECU) and classification into hardware and software, including communication

3.13
environmental condition
physical condition under which a system is used

3.14
exposure
duration of time and frequency in which an individual is in a situation in which the potential hazard exists

3.15
failure
termination of the ability of an item to perform a required function

Note 1 to entry: Failures which do not affect the availability of the process under control are outside the scope of EN 16590.

Note 2 to entry: After a failure, the item will have a fault.

Note 3 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

Note 4 to entry: The concept as defined does not apply to items consisting of software only.

3.16
fault
state of an item characterised by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

Note 1 to entry: A fault is often the result of a failure of the item itself, but may exist without prior failure.

Note 2 to entry For the purposes of EN 16590, a fault is a *random* fault.

3.17
function
defined behaviour of one or more electronic control units

3.18
functional concept
basic functions and interactions necessary to achieve a desired behaviour

Note 1 to entry: It is developed during the concept phase of the safety life cycle.

3.19
functional requirement
requirement for an intended function of the E/E/PES system

3.20
functional safety
system that performs in a way that does not present an unreasonable risk of injury to operators or bystanders

3.21
functional safety concept
entire collection of safety-related functions and interactions necessary to achieve a desired behaviour

Note 1 to entry: It is developed during the concept phase of the safety life cycle.

3.22
functional safety requirement
requirement for a safety-related function of the E/E/PES system

3.23
hardware safety requirement
requirement that applies to safety-related hardware and which is included as an element of a technical safety requirement

3.24
harm
physical injury

3.25
hazard
potential source of harm

3.26
hazardous situation
circumstance in which a person is exposed to a hazard or hazards, exposure to which can have immediate or long-term effects

3.27
intended use
⟨of a machine⟩ use in accordance with the information provided in the operator's manual

3.28
inspection
systematic, formal verification method used to review product quality

Note 1 to entry: During an inspection, the work product is checked by one or more assessors to see whether it complies with the requirements. The inspection is organised and moderated by an inspection leader. The author of the work product participates in the inspection but cannot lead the process.

3.29
life of the machine
life cycle
time between production and decommissioning

3.30
manual reset
function within the safety-related parts of the control system used to manually restore one or more safety-related functions before restarting the machine