SLOVENSKI STANDARD
SIST EN 16590-4:2014

01-julij-2014

Traktorji ter kmetijski in gozdarski stroji - Varnostni deli krmilnih sistemov - 4. del: Proizvodni, obratovalni, spreminjevalni in podporni procesi (ISO 25119-4:2010, spremenjen)

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 4: Production, operation, modification and supporting processes (ISO 25119-4:2010 modified)

Sicherheit von Land- und Forstmaschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 4: Fertigung, Betrieb, Modifikation und unterstützende Prozesse (ISO 25119-4:2010 modifiziert)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 4: Procédés de production, de fonctionnement, de modification et d'entretien (ISO 25119-4:2010 modifié)

Ta slovenski standard je istoveten z: EN 16590-4:2014

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 16590-4:2014 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16590-4

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 4: Production, operation, modification and supporting processes (ISO 25119-4:2010 modified)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 4: Procédés de production, de fonctionnement, de modification et d'entretien (ISO 25119-4:2010 modifié)

Sicherheit von Land- und Forstmaschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 4: Fertigung, Betrieb, Modifikation und unterstützende Prozesse (ISO 25119-4:2010 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 16590-4:2014 E

Contents

Page

Foreword

This document (EN 16590-4:2014) 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 25119-4:2010 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 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-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 provides general principles for the production, operation, modification and supporting processes 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).

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 16590-1:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

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*

ISO 3600, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Operator's manuals — Content and format*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 16590-1:2014 apply.

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

AGPL	agricultural performance level
$AGPL_r$	required agricultural performance level
CAD	computer-aided design
Cat	hardware category
CCF	common-cause failure
DC	diagnostic coverage
DC_{avg}	average diagnostic coverage
ECU	electronic control unit

ETA	event tree analysis
E/E/PES	electrical/electronic/programmable electronic systems
EMC	electromagnetic compatibility
EUC	equipment under control
FMEA	failure mode and effects analysis
FMECA	failure mode effects and criticality analysis
EPROM	erasable programmable read-only memory
FSM	functional safety management
FTA	fault tree analysis
HAZOP	hazard and operability study
HIL	hardware in the loop
MTTF	mean time to failure
$MTTF_d$	mean time to dangerous failure
PES	programmable electronic system
QM	quality measures
RAM	random-access memory
SOP	start of production
SRL	software requirement level
SRP	safety-related parts
SRP/CS	safety-related parts of control systems
SRS	safety-related system

5 Configuration management

5.1 Objectives

The first objective is to ensure that the SRP/CS and associated documents for a given function can be uniquely identified and reproduced at any time.

The second objective is to ensure that the relations and differences between earlier and current versions of the SRP/CS and associated documents can be traced.

5.2 General

All EN 16590 work products shall be handled by a configuration management system.

5.3 Prerequisites

See the prerequisites for each phase of the safety life cycle.

5.4 Requirements

Software tools and software development environments shall be subject to configuration management.

Configuration management data shall be maintained in accordance with a company document retention policy.

5.5 Work products

The applicable work product is the listing of SRP/CS with reference to associated documents for a given configuration.

6 Verification and validation

6.1 Objectives

One objective is to provide proof that the safety-related requirements are appropriate for the E/E/PES system and have duly been met.

A further objective is to provide proof that the safety goals at the machine level are satisfied.

6.2 General

The purpose of the preceding verification stages (e.g. reviews, safety analyses, component integration tests) was to demonstrate that the results of each particular phase complied with the relevant design and specification requirements described in EN 16590-3.

6.3 Prerequisites

The following are the prerequisites for this phase:

— project plan according to EN 16590-1:2014, 5.4.7 — deadlines, resources, equipment, degree of maturity, etc.;

— machine test plan — part of the existing quality assurance process;

— risk analysis according to EN 16590-2:2014, Clause 6 — identification of potential hazards;

— safety goals, as well as safe states;

— technical safety concept according to EN 16590-3:2014, Clause 5 — technical safety requirements.

6.4 Requirements

6.4.1 SRP design validation/verification

The design of the SRP of the control system shall be validated/verified (see EN 16590-1:2014, Figure 1).

The validation/verification shall demonstrate that each SRP meets

— all the requirements of the specified category (see EN 16590-2:2014, Annex A), and

— the specified safety characteristics for that part as set out in the design requirements.

6.4.2 Scope of safety validation/verification

Within the safety life cycle, validation/verification of safety attributes shall be carried out for the following:

— complete system at machine level (e.g. bench testing, hardware in the loop testing, test machine);

— hardware;

— software.

6.4.3 Activities

The following sequence shall be followed for a structured safety validation/verification:

— validation/verification planning;

— validation/verification specification;

— validation/verification execution;

— report on validation/verification result.

All variants or versions of the E/E/PES system that were subject to the validation/verification activities shall be clearly labelled.

6.4.4 Validation/verification plan

A validation/verification plan shall be developed for the safety goals and technical safety requirements, and shall include the following items:

— validation/verification and possible variants;

— degree of maturity of the system;

— validation/verification goals;

— validation/verification techniques;

— statement of independence between the person in charge of validation/verification and the developer;

— equipment and environmental conditions required, including calibration specifications for tools;

— specified reference to the overall project plan;

— pass/fail criteria for all tests.

6.4.5 Validation/verification, test specification of hardware and software

The item function shall be validated/verified at E/E/PES system level, considering fulfilment of the hardware/software safety requirements.

6.4.6 Validation/verification test specification of the complete system

The characteristics of the SRP/CS shall be validated/verified at machine level, considering fulfilment of the functional safety concept.

6.4.7 Validation/verification test specification

The following methods and measures shall be used and specified:

— tests (black-box, HIL, machine testing, field testing, etc.);

— analysis (e.g. simulation);

— reviews of relevant documents (input from hardware/software, e.g. FMEA, circuit diagram).