SLOVENSKI STANDARD
SIST EN 16590-2:2014

01-julij-2014

Traktorji ter kmetijski in gozdarski stroji - Varnostni deli krmilnih sistemov - 2. del: Faza koncepta (ISO 25119-2:2010, spremenjen)

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 2: Concept phase (ISO 25119-2:2010 modified)

Sicherheit von Land- und Forstmaschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Konzeptphase (ISO 25119-2:2010 modifiziert)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 2: Phase de projet (ISO 25119-2 modifié)

Ta slovenski standard je istoveten z: EN 16590-2:2014

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 16590-2:2014 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16590-2

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 2: Concept phase (ISO 25119-2:2010 modified)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 2: Phase de projet (ISO 25119-2:2010 modifié)

Sicherheit von Land- und Forstmaschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Konzeptphase (ISO 25119-2:2010 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

Contents

Page

Foreword

This document (EN 16590-2:2014) 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 25119-2:2010 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 specifies the concept phase of the 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).

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

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.

ADC	analogue to digital converter
AgPL	agricultural performance level
$AgPL_r$	required agricultural performance level
CAD	computer-aided design
Cat	hardware category
CCF	common-cause failure
CRC	cyclic redundancy check
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
$MTTF_{dC}$	mean time to dangerous failure for each channel
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 Concept — Unit of observation

5.1 Objectives

The objective of this phase is to develop an adequate understanding of the unit of observation in order to satisfactorily complete all of the tasks defined in the safety life cycle (see EN 16590-1:2014, Figure 2). On the basis of the chosen safety concept, a suitable method shall be used to determine the required performance level. Suitable methods include risk analysis (described below), other standards, legal requirements and test body expertise or a combination of these.

5.2 Prerequisites

The necessary prerequisites are a description of the unit of observation, its interfaces, already-known safety and reliability requirements and the scope of application

5.3 Requirements

5.3.1 Unit of observation and ambient conditions

A safety-related concept shall include the following:

a) the scope, context and purpose of the unit of observation;

b) functional requirements for the unit of observation;

c) other requirements regarding the unit of observation and ambient conditions, including

— technical or physical requirements, e.g. operating, environmental and surrounding conditions and constraints, and

— legal requirements, especially safety-related legislation, regulations and standards (national and international);

d) historical safety and reliability requirements and the level of safety and reliability achieved for similar or related units of observation.

5.3.2 Limits of unit of observation and its interfaces with other units of observation

The following information shall be considered in order to gain an understanding of the operation of the unit of observation in its environment:

— the limits of the unit of observation;

— its interfaces and interactions with other units of observation and components;

— requirements regarding other units of observation;

— mapping and allocation of relevant functions to involved units of observation.

5.3.3 Sources of stress

The sources of stress which could affect the safety and reliability of the unit of observation shall be determined, including the following:

— the interaction of different units of observation;

— hazards of a physical or chemical nature (energy content, toxicity, explosiveness, corrosiveness, reactivity, combustibility, etc.);

— other external events [temperature, shock, electromagnetic compatibility (EMC), etc.];

— reasonable foreseeable human operating errors;

— hazards originating from the unit of observation, and events triggering failure (e.g. during assembly or maintenance).

5.3.4 Additional determinations

In addition to the activities described in 5.3.2, the following determinations or actions shall be implemented:

— determination as to whether the unit of observation is a new development or a modification, adaptation or derivative of an existing unit of observation and, in the case of modification, the carrying out of an impact analysis to adjust the safety life cycle accordingly;

— preparing a plan and a specification to validate the requirements regarding the unit of observation defined in 5.3.1;

— definition of project management for the appropriate phases in the life cycle;

— adequate input data for the reliability assessment;

— adequate procedures and application of tools and technologies;

— utilisation of qualified staff.

5.4 Work products

The work products of the concept/definition of the unit of observation are

a) the unit of observation and ambient conditions,

b) limits of the unit of observation and its interfaces with other units of observation,

c) sources of stress, and

d) additional determinations.

6 Risk analysis and method description

6.1 Objectives

Risk is defined (see EN 16590-1:2014, definition 3.39) as the combination of the probability of occurrence of harm and the severity of that harm.

When considering the frequency of the occurrence of harm, as a rule, the probability of being exposed to a hazardous situation is taken into account.

When considering systems, the possibility that the operator will react in many cases to avoid harm is generally to be taken into account.

The procedure described in 6.2 through 6.4 provides guidance for determining the AgPL.

6.2 Prerequisites

There are no prerequisites for this phase.

6.3 Requirements

6.3.1 Procedures for preparing a risk analysis

The risk analysis shall take into account the overall scope of the application. If decisions are made later in the safety life cycle changing the scope of application, a new risk analysis shall be carried out.

The architecture of the SRP/CS shall not be considered as part of the risk analysis.

6.3.2 Tasks in risk analysis

The operating conditions in which the unit of observation can initiate hazards when correctly used (including reasonable foreseeable human operating errors and part failures) shall be considered.

6.3.3 Participants in risk analysis

The risk analysis shall involve several individuals from different departments, e.g. electronic or electrical development, testing or validation, machine or hydraulics design, service, or external consultants (e.g. technical inspection authority).

6.3.4 Assessment and classification of a potential harm

Potentially harmful effects can be deduced by considering possible malfunctions and systematic failures in relevant operating conditions. The potential severity of harm shall be described as precisely as possible for each relevant scenario.