

STN	Poľnohospodárske a lesnícke stroje a traktory. Bezpečnostné časti riadiacich systémov. Časť 2: Etapa konceptu (ISO 25119-2: 2010 mod.).	STN EN 16590-2 47 0014
------------	--	--

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Obsahuje: EN 16590-2:2014

119244

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, odbor SÚTN, 2014
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

EUROPEAN STANDARD

EN 16590-2

NORME EUROPÉENNE

EUROPÄISCHE NORM

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.....	5
Introduction	6
1 Scope	8
2 Normative references	8
3 Terms and definitions	8
4 Abbreviated terms	8
5 Concept — Unit of observation	9
5.1 Objectives	9
5.2 Prerequisites	9
5.3 Requirements	9
5.3.1 Unit of observation and ambient conditions	9
5.3.2 Limits of unit of observation and its interfaces with other units of observation.....	10
5.3.3 Sources of stress.....	10
5.3.4 Additional determinations	10
5.4 Work products.....	11
6 Risk analysis and method description	11
6.1 Objectives	11
6.2 Prerequisites	11
6.3 Requirements	11
6.3.1 Procedures for preparing a risk analysis	11
6.3.2 Tasks in risk analysis.....	11
6.3.3 Participants in risk analysis	11
6.3.4 Assessment and classification of a potential harm	11
6.3.5 Assessment of exposure in the situation observed	12
6.3.6 Assessment of a possible avoidance of harm.....	12
6.3.7 Selecting the required $AgPL_r$	13
6.4 Work products.....	15
7 System design.....	15
7.1 Objectives	15
7.2 Prerequisites	15
7.3 Requirements	15
7.3.1 Assignment of $AgPL$	15
7.3.2 Achieving the required $AgPL_r$	16
7.3.3 Achievement of the performance level.....	17
7.4 Work products.....	17
Annex A (normative) Designated architectures for SRP/CS	18
A.1 General.....	18
A.2 Category B (basic)	18
A.3 Category 1	19
A.4 Category 2	19
A.5 Category 3	20
A.6 Category 4	22
Annex B (informative) Simplified method to estimate channel $MTTF_{dC}$	24

B.1	General	24
B.2	Component $MTTF_d$ values.....	24
B.2.1	Determination of component $MTTF_d$ values	24
B.2.2	$MTTF_d$ for components from B_{10}.....	25
B.3	Parts count method.....	25
B.4	Calculation of symmetric $MTTF_{dC}$ for two-channel architectures.....	26
Annex C (informative) Determination of diagnostic coverage (DC).....		27
C.1	General	27
C.2	Estimation of the required DC.....	27
C.3	Estimation of channel DC	29
C.4	Calculation of channel DC	30
C.5	Calculation of DC.....	30
Annex D (informative) Estimates for common-cause failure (CCF).....		31
Annex E (informative) Systematic failure		33
E.1	General	33
E.2	Procedure for the control of systematic failures	33
E.3	Procedure for the avoidance of systematic failures	33
Annex F (informative) Characteristics of safety functions		36
F.1	General	36
F.2	Start interlock	36
F.3	Stop function	36
F.4	Manual reset.....	36
F.5	Start and restart.....	37
F.6	Response time	37
F.7	Safety-related parameters	37
F.8	External control function.....	37
F.9	Muting (manual suspension of safety functions)	37
F.10	Operator warning.....	37
Annex G (informative) Example of a risk analysis.....		38
G.1	Workflow.....	38
G.2	Example risk analysis of an electro-hydraulic transmission for a self-propelled working machine (forage harvester) — Extract from a complete risk analysis.....	38
G.2.1	System description	38
G.2.2	Surrounding conditions.....	39
G.2.3	System states and transitions	39
G.2.4	System failures	40
G.3	Assessment	41
G.3.1	System failure — Stops unintentionally.....	41

G.3.2	System failure — Does not move when commanded	42
G.4	Results	42
Annex ZA (informative)	Relationship between this European Standard and the Essential Requirements of EU Machinery Directive 2006/42/EC	43
Bibliography		44

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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN