

STN	Poľnohospodárske a lesnícke stroje a traktory Bezpečnostné časti riadiacich systémov Časť 3: Sériový vývoj, hardvér a softvér (ISO 25119-3: 2018)	STN EN ISO 25119-3 47 0014
------------	--	--

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 3: Series development, hardware and software (ISO 25119-3:2018)

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

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 05/19

Obsahuje: EN ISO 25119-3:2018, ISO 25119-3:2018

Oznámením tejto normy sa ruší
STN EN 16590-3 (47 0014) z augusta 2014

128770

EUROPEAN STANDARD

EN ISO 25119-3

NORME EUROPÉENNE

EUROPÄISCHE NORM

December 2018

ICS 35.240.99; 65.060.01

Supersedes EN 16590-3:2014

English Version

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 3: Series development, hardware and software (ISO 25119-3:2018)

Tracteurs et matériels agricoles et forestiers - Parties
des systèmes de commande relatives à la sécurité -
Partie 3: Développement en série, matériels et logiciels
(ISO 25119-3:2018)

Traktoren und Maschinen für die Land- und
Forstwirtschaft - Sicherheitsbezogene Teile von
Steuerungen - Teil 3: Serienentwicklung, Hardware
und Software (ISO 25119-3:2018)

This European Standard was approved by CEN on 15 October 2018.

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, Serbia, 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: Rue de la Science 23, B-1040 Brussels

EN ISO 25119-3:2018 (E)

Contents	Page
European foreword.....	3
Annex ZA (informative) Relationship between this European Standard and the essential requirements of EU Machinery Directive 2006/42/EC aimed to be covered.....	4

European foreword

This document (EN ISO 25119-3:2018) has been prepared by Technical Committee ISO/TC 23 "Tractors and machinery for agriculture and forestry" in collaboration with 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 June 2019, and conflicting national standards shall be withdrawn at the latest by June 2019.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 16590-3:2014.

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 the relationship with EU Directive(s) see informative Annex ZA, which is an integral part of this document.

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, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 25119-3:2018 has been approved by CEN as EN ISO 25119-3:2018 without any modification.

Annex ZA (informative)

Relationship between this European Standard and the essential requirements of EU Machinery Directive 2006/42/EC aimed to be covered

This European Standard has been prepared under a Commission's standardization request M/396 to provide one voluntary means of conforming to essential requirements of the Directive 2006/42/EC on Machinery.

Once this standard is cited in the Official Journal of the European Union under that Directive, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirement of that Directive, and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Annex I of Directive 2006/42/EC

Essential requirements of EU Machinery Directive 2006/42/EC	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
Annex I, 1.2.1	All normative clauses and sub-clauses	Compliance with the requirements of EN ISO 25119-1:2018, EN ISO 25119-2:2018, EN ISO 2519-3:2018 and EN ISO 25119-4:2018 is required to achieve conformity with essential requirement 1.2.1, paragraph 1, of Directive 2006/42/EC within the limits of the scope of these standards.

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

**INTERNATIONAL
STANDARD**

**ISO
25119-3**

Second edition
2018-10

**Tractors and machinery for
agriculture and forestry — Safety-
related parts of control systems —**

**Part 3:
Series development, hardware and
software**

*Tracteurs et matériels agricoles et forestiers — Parties des systèmes
de commande relatives à la sécurité —*

Partie 3: Développement en série, matériels et logiciels



Reference number
ISO 25119-3:2018(E)

© ISO 2018

ISO 25119-3:2018(E)**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Abbreviated terms	2
5 System design	3
5.1 Objectives.....	3
5.2 General.....	3
5.3 Prerequisites.....	4
5.4 Requirements.....	4
5.4.1 Structuring safety requirements.....	4
5.4.2 Technical safety concept.....	5
5.5 Work products.....	7
6 Hardware	7
6.1 Objectives.....	7
6.2 General.....	7
6.3 Prerequisites.....	7
6.4 Requirements.....	7
6.5 Hardware categories.....	9
6.6 Work products.....	9
7 Software	10
7.1 Software development planning.....	10
7.1.1 Objectives.....	10
7.1.2 General.....	10
7.1.3 Prerequisites.....	10
7.1.4 Requirements.....	10
7.1.5 Work products.....	13
7.2 Software safety requirements specification.....	13
7.2.1 Objectives.....	13
7.2.2 General.....	13
7.2.3 Prerequisites.....	13
7.2.4 Requirements.....	13
7.2.5 Work products.....	17
7.3 Software architecture design.....	17
7.3.1 Objectives.....	17
7.3.2 General.....	17
7.3.3 Prerequisites.....	17
7.3.4 Requirements.....	17
7.3.5 Work products.....	19
7.4 Software component design and implementation.....	19
7.4.1 Objectives.....	19
7.4.2 General.....	19
7.4.3 Prerequisites.....	19
7.4.4 Requirements.....	19
7.4.5 Work products.....	29
7.5 Software component testing.....	29
7.5.1 Objectives.....	29
7.5.2 General.....	29
7.5.3 Prerequisites.....	29
7.5.4 Requirements.....	29
7.5.5 Work products.....	37

ISO 25119-3:2018(E)

7.6	Software integration and testing.....	37
	7.6.1 Objectives.....	37
	7.6.2 General.....	38
	7.6.3 Prerequisites.....	38
	7.6.4 Requirements.....	38
	7.6.5 Work products.....	39
7.7	Software safety testing.....	40
	7.7.1 Objectives.....	40
	7.7.2 General.....	40
	7.7.3 Prerequisites.....	40
	7.7.4 Requirements.....	40
	7.7.5 Work products.....	44
7.8	Software-based parameterisation.....	44
	7.8.1 Objective.....	44
	7.8.2 General.....	44
	7.8.3 Prerequisites.....	45
	7.8.4 Requirements.....	45
	7.8.5 Work products.....	46
Annex A (informative) Example of agenda for assessment of functional safety at AgPL = e.....		47
Annex B (normative) Independence by software partitioning.....		49
Bibliography.....		59

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 19, *Agricultural electronics*.

This second edition cancels and replaces the first edition (ISO 25119-3:2010), which has been technically revised. The main changes compared to the previous edition are as follows:

- the introduction has been modified to add specific information on safety standards;
- the prerequisites of functional safety have been specified;
- Clause 5 has been revised to:
 - specify the prerequisites of functional safety, and
 - simplify the general requirements of technical safety concepts;
- additional instructions have been added throughout the document to verify consistency of test specifications and reports;
- Annex B has been changed to a normative annex;
- the document has been editorially revised.

A list of all parts in the ISO 25119 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

ISO 25119-3:2018(E)

Introduction

ISO 25119 (all parts) sets out an approach to the assessment, design and verification, for all safety life cycle activities, of safety-related parts 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 mobile municipal equipment.

A prerequisite to the application of ISO 25119 (all parts) is the completion of a suitable hazard identification and risk analysis (e.g. ISO 12100) for the entire machine. As a result, an E/E/PES is frequently assigned to provide safety-related functions that create 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 safety-related 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 measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

ISO 25119 (all parts) allocates the ability of safety-related parts to perform a safety-related 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 that can cause E/E/PES malfunctions leading to potential hazardous situations are considered: systematic, common-cause and random.

In order to guide the designer during design, verification, and to facilitate the assessment of the achieved performance level, ISO 25119 (all parts) defines an approach based on a classification of architecture 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 the control systems of protective equipment (e.g. interlocking devices, pressure sensitive devices).

ISO 25119 (all parts) 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 document is a type-B1 standard as stated in ISO 12100.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

- machine manufacturers (small, medium and large enterprises);
- health and safety bodies (regulators, accident prevention organizations, market surveillance, etc.).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

- machine users/employers (small, medium and large enterprises);
- machine users/employees (e.g. trade unions, organizations for people with special needs);
- service providers, e.g. for maintenance (small, medium and large enterprises);
- consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems —

Part 3: Series development, hardware and software

1 Scope

This document 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 mobile municipal equipment (e.g. street-sweeping machines).

This document is not applicable to:

- aircraft and air-cushion vehicles used in agriculture;
- lawn and garden equipment.

This document specifies the characteristics and categories required of SRP/CS for carrying out their safety-related functions. It does not identify performance levels for specific applications.

NOTE 1 Machine specific type-C standards can specify performance levels (AgPL) for safety-related functions in machines within their scope. Otherwise, the specification of AgPL is the responsibility of the manufacturer.

This document is applicable to the safety-related parts of electrical/electronic/programmable electronic systems (E/E/PES), as these relate to mechatronic systems. It covers the possible hazards caused by malfunctioning behaviour of E/E/PES safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards, unless directly caused by malfunctioning behaviour of E/E/PES safety-related systems. It also covers malfunctioning behaviour of E/E/PES safety-related systems involved in protective measures, safeguards, or safety-related functions in response to non-E/E/PES hazards.

Examples included within the scope of this document:

- SRP/CS's limiting current flow in electric hybrids to prevent insulation failure/shock hazards;
- electromagnetic interference with the SRP/CS;
- SRP/CS's designed to prevent fire.

Examples not included in the scope of this document:

- insulation failure due to friction that leads to electric shock hazards;
- nominal electromagnetic radiation impacting nearby machine control systems;
- corrosion causing electric cables to overheat.

This document is not applicable to non-E/E/PES systems (e.g. hydraulic, mechanic or pneumatic).

NOTE 2 See also ISO 12100 for design principles related to the safety of machinery.

This document is not applicable to safety related parts of control systems manufactured before the date of its publication.

ISO 25119-3:2018(E)**2 Normative references**

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 25119-1, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

ISO 25119-2:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: concept phase*

ISO 25119-4:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production, operation, modification and supporting processes*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN