INTERNATIONAL STANDARD

ISO 25119-4

Second edition
2018-10

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

Part 4: Production, operation, modification and supporting processes

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

Reference number
ISO 25119-4:2018(E)

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

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 25119-4:2010), 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 scope has been slightly modified;

— and a new Clause 5 (quality management system) has been added;

— the former Clause 5 (configuration management) has been moved after Clause 6;

— Clause 6 has been revised;

— the example of technical documentation checklist has been modified;

— 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.

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 to 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 4: Production, operation, modification and supporting processes

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 limiting current flow in electric hybrids to prevent insulation failure/shock hazards;

— electromagnetic interference with the SRP/CS;

— SRP/CS 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.

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

ISO 25119-1:2018, *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 25119-3:2018, *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 in ISO 25119-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

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
FMEA	failure mode and effects analysis

FSM	functional safety management
FTA	fault tree analysis
HARA	hazard analysis and risk assessment
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/CS	safety-related parts of control systems
UoO	unit of observation

5 Quality management system

A quality management system is an important part of functional safety. Users of this document shall demonstrate conformance to Clauses 7, 8, 9 and 11 by

— applying quality management principles, for example, those found in ISO 9001, using Clauses 7, 8, 9, and 11 as guidance, or

— applying the requirements in Clauses 7, 8, 9, and 11 as they are written in this document.

6 Safety validation and verification

6.1 Objectives

One objective is to provide proof that each functional safety requirement has been duly met and is appropriate for the safety goals of the UoO.

A further objective is to provide proof that each safety goal has been realized as initially desired and specified and is appropriate for the functional safety of the UoO.

6.2 General

The purpose of the preceding verification and validation stages (e.g. reviews, safety analyses, component integration tests) is to demonstrate that the results of each particular phase conforms with the relevant design and implementation safety requirements described in ISO 25119-3.

6.3 Prerequisites

The following are the prerequisites for this phase:

— safety plan according to ISO 25119-1:2018, 6.4.6.3 — deadlines, resources, equipment, degree of maturity, etc.;

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

— HARA according to ISO 25119-2:2018, Clause 6 — identification of potential hazards;

— functional safety concept according to ISO 25119-2:2018, Clause 7 — safety goals, as well as safe states, and functional safety requirements;

— technical safety concept according to ISO 25119-3:2018, Clause 5 — technical safety requirements.

6.4 Requirements

6.4.1 SRP/CS design validation and verification

The design of the SRP/CS shall be validated and verified (see ISO 25119-1:2018, Figure 1).

The validation and verification shall demonstrate that each SRP/CS meets:

— the requirements of the specified AgPL including as appropriate:

  a) hardware category, $MTTF_{DC}$, DC, CCF (see ISO 25119-2:2018, Annexes A, B, C, D);

  b) SRL (see ISO 25119-3:2018, Clause 7);

— the safety goals, safe states and remaining functional and technical safety requirements;

— the fulfilment of the assigned safety-related functions.

6.4.2 Scope of safety validation and verification

Within the safety life cycle, validation and verification of safety requirements 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 and verification:

— validation and verification planning;

— validation and verification specification;

— validation and verification execution;

— documentation of validation and verification result.

6.4.4 Validation and verification plan

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

— validation and verification and possible variants;

— degree of maturity of the system;

— validation and verification goals;

— validation and verification techniques;