INTERNATIONAL STANDARD

ISO 25119-2

Third edition
2019-08

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

Part 2: Concept phase

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

Partie 2: Phase de projet

Reference number
ISO 25119-2:2019(E)

COPYRIGHT PROTECTED DOCUMENT

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 third edition cancels and replaces the second edition (ISO 25119-2:2018), of which it constitutes a minor revision. The changes compared to the previous edition are as follows.

— A minor revision was made to Annex H to improve the clarity and understanding of the requirements to be followed by the end user about subsystems, elements, or components designed according to ISO 26262.

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 (such as 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 (such as auxiliary valves) to complex systems (such as steer by wire), as well as to the control systems of protective equipment (such as 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 2: Concept phase

1 Scope

This document 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 mobile municipal equipment (such as 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 protection 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 within 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 (such as 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 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 25119-3:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software*

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*

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.

ADC	analogue to digital converter
AgPL	agricultural performance level
$AgPL_r$	required agricultural performance level
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
FMEA	failure mode and effects analysis
EPROM	erasable programmable read-only memory
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
$MTTF_{DC}$	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/CS	safety-related parts of control systems
UoO	unit of observation

5 Concept — UoO

5.1 Objectives

The objective of this phase is to develop an adequate understanding of the UoO in order to satisfactorily complete all of the tasks defined in the safety life cycle (see ISO 25119-1:2018, Figure 2). For each UoO, 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 safety-related function to be provided by the UoO, its interfaces, already-known safety and reliability requirements and the scope of application.

5.3 Requirements

5.3.1 Basic requirements and ambient conditions

The following information shall be available for the safety-related function of the UoO:

a) the scope, context, purpose and known elements;

b) functional requirements;

c) other requirements and ambient conditions that should be taken into account include:

   — technical or physical requirements, such as operating, environmental and surrounding conditions and constraints;

   — 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 UoO.

5.3.2 Limits of UoO and its interfaces with other UoO

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

— the limits of the UoO;

— its interfaces and interactions with other UoO and components;

— requirements for the safety-related functions related to other UoO.

5.3.3 Mapping and allocation of relevant functions to involved UoO, sources of stress

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

— the interaction of different UoO;

— stresses 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;

— stresses originating from the UoO, 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 UoO is a new development or a modification, adaptation or derivative of an existing UoO 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 verify and validate the requirements regarding the UoO 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;

— utilization of suitably qualified staff.

5.4 Work products

The work products if applicable of the UoO shall be:

a) elements included within the UoO;

b) specification of the basic requirements and ambient conditions;

c) limits of the UoO and its interfaces with other UoO;

d) sources of stress;

e) additional determinations.

6 HARA — Determination of the $AgPL_r$

6.1 Objectives

The main objectives are to analyse risks associated with a faulted UoO (one not performing safety-related functions as intended, such as not stopping properly, propelling while in neutral, steering in the wrong direction) and then, assign an appropriate $AgPL_r$. Risk is defined as the combination of the probability of occurrence of harm and the severity of that harm (see ISO 25119-1:2018, 3.39). When considering the probability of the occurrence of harm, when appropriate, the probability of being exposed to a hazardous situation with a faulted UoO can be taken into account.

The procedure described in 6.2 to 6.4 provides guidance for determining the $AgPL_r$ based on the HARA.

6.2 Prerequisites

The UoO definition associated with each safety-related function.

6.3 Requirements

6.3.1 Procedures for preparing a HARA

The HARA shall take into account the entire safety-related function so that an appropriate specification for the SRP/CS can be provided. If decisions are made later in the safety life cycle changing the scope of application, the HARA shall be reworked accordingly. To identify the changes and their impacts on the work products, an impact analysis shall be carried out in accordance with ISO 25119-4.

6.3.2 Tasks in the HARA

The operating conditions, in which the malfunctioning behaviour of the UoO will result in hazardous situations, when correctly used and when incorrectly used in a reasonably foreseeable way, shall be taken into account.

6.3.3 Participants in HARA

The HARA shall involve sufficient people to ensure that all relevant expertise is available.

NOTE Involving individuals from different disciplines often provides valuable input to the HARA.

6.3.4 Classification of a potential harm

The potential severity of harm shall be determined and documented.

Potentially harmful effects shall be deduced by considering all hazardous situations resulting from malfunctions of the safety-related function in relevant operating conditions, modes and situations.

A categorization shall be used in the description of the harm. For this reason, a classification of the severity of harm is presented in four categories: S0, S1, S2 and S3 (see Table 1).

The actions of the operator of the involved machine and bystanders (e.g. people lending assistance, other operators of machinery, other traffic participants, etc.) shall be taken into account and their exposure to harm documented.

The objective of the assessment and classification of a potential harm shall be focused on and limited to harm to people. If the analysis of the malfunction of the safety-related function is clearly limited to property and does not involve harm to people, then these malfunctions need not be classified as safety-related.

No advanced risk assessment need to be carried out for functions assigned to harm class S0.

Table 1 — Classification of injuries

S0	S1	S2	S3
No injuries, damage limited to property	Light and moderate injuries, requires medical attention, total recovery	Severe and life-threatening injuries (survival probable), permanent partial loss in work capacity	Life-threatening injuries (survival uncertain), severe disability

6.3.5 Classification of exposure in the situation observed

A HARA shall take into account the exposure effects of possible malfunctions of the safety-related function in all specific relevant regional working and operating conditions. These situations range from daily routine activities to extreme, rare situations. The variable "E" shall be used to categorize the different frequencies or duration of exposure. Five categories, designated E0, E1, E2, E3 and E4, are used (see Table 2), where "E" serves as an estimation of how often and how long an operator or bystander is exposed to a hazard where a failure could result in harm to the operator or bystander. The most appropriate method for each hazardous situation, frequency or duration, shall be used for the determination of $AgPL_r$. When more than one category is determined to be appropriate for a particular hazardous situation, the method returning the highest category shall be used.

NOTE A hazard capable of producing harm can result from a combination of machine conditions (such as environmental and/or operational).

Table 2 — Classification of exposure to the hazardous situation

Description	E0	E1	E2	E3	E4
Definition of frequency	Improbable (theoretically possible; once during lifetime)	Rare events (less than once per year)	Sometimes (more than once per year)	Often (more than once per month)	Frequently (almost every operation)
Definition of duration $\frac{t_{exp}}{t_{av\,op}}$	Less than 0,01 %	0,01 % to less than 0,1 %	0,1 % to less than 1 %	1 % to less than 10 %	Greater than or equal to 10 %
t_{exp} exposure time. $t_{av\,op}$ average operating time.					

6.3.6 Classification of a possible avoidance of harm

Assessing possible avoidance of harm involves appraising whether a typical trained machine operator has a level of control over the harm that could arise and can avoid it or, the situation is completely uncontrollable. Similarly, an untrained bystander may have a level of control to avoid a harmful situation. The variable C shall be used to classify the ability to avoid harm. The value of C for a possible avoidance of harm shall consider only the ability of persons to avoid the harm following the malfunction of the safety-related function and shall not take into account the reliability or any measures provided in the SRP/CS which mitigate risk in the event of a malfunction. The classifications C0, C1, C2 and C3 represent "easily controllable", "simply controllable", "mostly controllable" and "none" (see Table 3).