INTERNATIONAL STANDARD

ISO 25119-1

Second edition
2018-10

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

Part 1: General principles for design and development

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

Partie 1: Principes généraux pour la conception et le développement

Reference number
ISO 25119-1:2018(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 25119-1:2010), which has been technically revised. The main changes compared from the previous edition are as follows:

— the introduction has been modified to add specific information on safety standards;

— Tables 1 to 3 have been deleted and the succeeding tables have been renumbered;

— Clause 5 (management system) has been inserted and the succeeding clauses have been renumbered;

— in 8.5, work products from the safety management activities after SOP have been specified;

— Figure 2 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, such as 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 1: General principles for design and development

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 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*

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 following terms and definitions 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/

3.1
agricultural performance level
AgPL
level which specifies the ability of safety-related parts of control systems to perform a safety-related function under foreseeable conditions

Note 1 to entry: For the purposes of ISO 25119 (all parts), the performance for each function is divided into five levels (a, b, c, d and e) where the functional safety contributed by the SRP/CS in “a” is low and in “e” is high.

3.2
required agricultural performance level
$AgPL_r$
performance level(s) (AgPL) required to be achieved for each safety-related function

Note 1 to entry: Depending on the potential behaviours of a faulted UoO, a safety-related function may have more than one $AgPL_r$. For example, a partial loss of a function, the sudden complete loss of a function, and the inability to enable a function, may have three different $AgPL_r$’s.

3.3
category
classification of the safety-related parts of a control system with respect to its resistance to dangerous failures taking into account the subsequent behaviour in the fault condition, which is achieved by the structural arrangement (architecture) of the parts

3.4
channel
combination of input, logic and output elements necessary to perform a function(s)

3.5
common-cause failure
CCF
multiple failures within a UoO, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: Common-cause failures should not be confused with common-mode failures, as common-mode failures can result from different causes.

3.6
controllability
involved individual's possibility of avoiding harm in the situation that is putting him/her at risk

3.7
dangerous detected failure rate
λ_{DD}
detected failure rate within the UoO which result in no or minimal increase in risk, but if undetected, would result in an immediate increase in risk

3.8
dangerous failure
failure (and multiple failures due to common cause) in which an SRP/CS is no longer able to maintain the intended function and the resultant machine behaviour could result in a hazardous situation

3.9
dangerous failure rate
λ_D
fraction of all components with *dangerous failure* (3.8) per time unit

Note 1 to entry: λ_D is the reciprocal value of $MTTF_D$.

3.10
diagnostic coverage
DC
fraction of the probability of detected dangerous failures, λ_{DD}, and the probability of total *dangerous failures*, λ_D (3.9)

3.11
diagnostic test interval
interval between online tests used to detect faults in a safety-related system that have a specified *diagnostic coverage* (3.10)

3.12
E/E/PES architecture
allocation of safety-related functions to electronic control units (ECU) and classification into hardware and software, including communication

3.13
environmental condition
physical condition under which a system is used

3.14
exposure
duration of time and frequency in which an individual is in a situation in which the potential hazard exists

3.15
failure
termination of the ability of an element within a UoO to perform as intended

Note 1 to entry: After a failure, the UoO will have a fault.

Note 2 to entry: "Failure" is an event, as distinguished from *fault* (3.16), which is a state.

Note 3 to entry: The concept as defined does not apply to a UoO consisting of software only.

3.16
fault
state of a UoO characterised by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

Note 1 to entry: A fault is often the result of a *failure* (3.15), but can exist without prior failure.