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 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 25119-3:2010), 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.

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.

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*

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
$MTTF_{DC}$	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	safety-related parts
SRP/CS	safety-related parts of control systems
UML	unified modelling language

5 System design

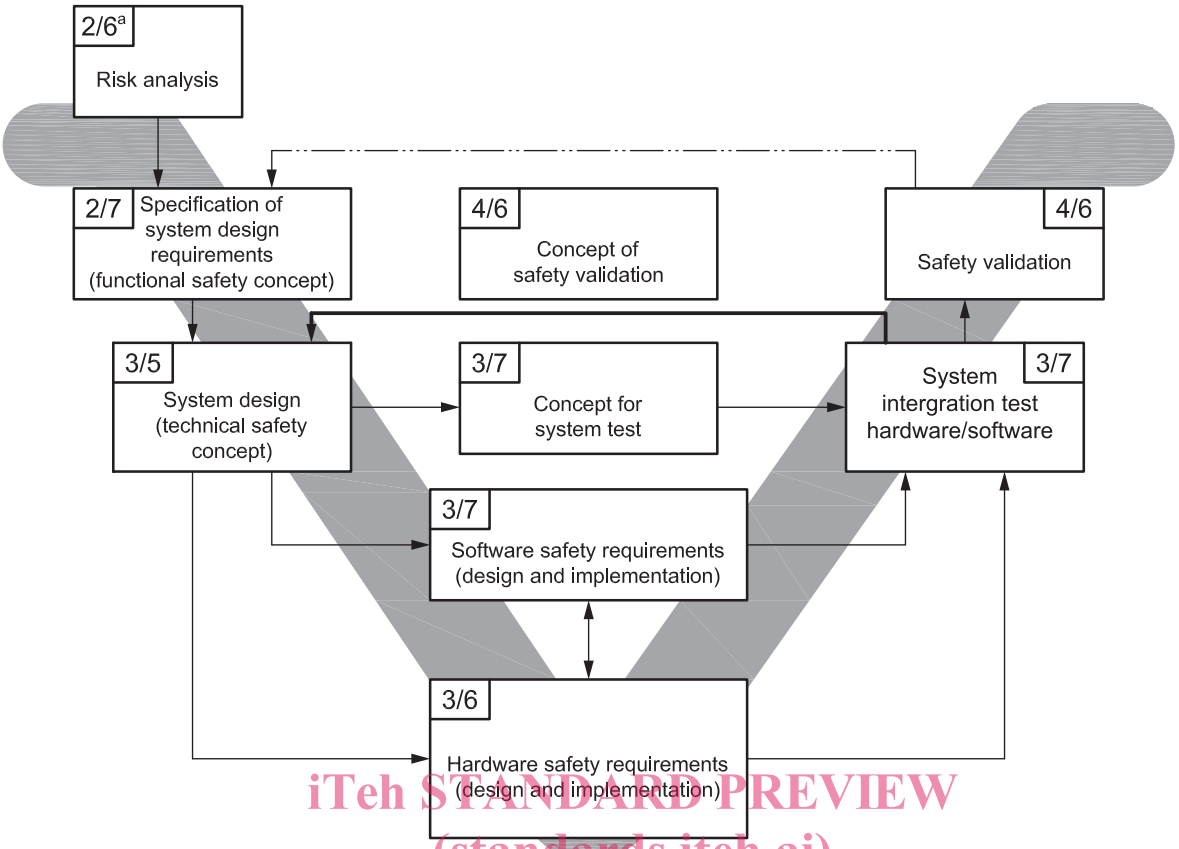
5.1 Objectives

The objective is to define a system design for producing a detail design that fulfils the safety requirements for the entire safety-related system.

5.2 General

Safety requirements constitute all requirements aimed at achieving and ensuring functional safety. During the safety life cycle, safety requirements are detailed and specified in ever greater detail at hierarchical levels. The different levels for safety requirements are illustrated in Figure 1. For the overall representation of the procedure for developing safety requirements, see also 5.4. In order to support management of safety requirements, the use of suitable tools for requirements management is recommended.

Annex A provides guidance for an example agenda of the assessment of functional safety associated with an AgPL = e.



Key

result
verification
validation

a The first of two numbers separated by a slash refers to the respective part of ISO 25119, and the second refers to the clause in that document: i.e. 2/6 is ISO 25119-2:2018/Clause 6, 3/5 is ISO 25119-3:2018/Clause 5, and so on.

Figure 1 — Structuring of safety requirements

5.3 Prerequisites

The functional safety concept (ISO 25119-2:2018, Clause 7) is the prerequisite.

5.4 Requirements

5.4.1 Structuring safety requirements

During the functional safety concept phase, functional safety requirements are created to describe the basic functioning of the safety-related system through which the safety goals are to be fulfilled. The basic allocation of functional safety requirements to the system architecture is specified by the technical safety concept specification in the form of technical safety requirements. This system architecture comprises both hardware and software.

The hardware safety requirements refine and solidify the technical safety requirements. Clause 6 describes how to specify the hardware requirements in detail.

The software safety requirements are derived from the requirements of the technical safety concept and the underlying hardware. The requirements for the software defined in Clause 7 shall be taken into account.

This clause specifies the approach to be used in the specification of the technical safety concept requirements during system design, thereby providing a basis for error-free system design.

5.4.2 Technical safety concept

5.4.2.1 General requirements of technical safety concept

The technical safety concept document includes the technical safety requirements for the system.

Each technical safety requirement shall be associated (e.g. by cross-reference) with higher-level safety requirements, which may be:

— other technical safety requirements;

— functional safety requirements.

NOTE Traceability can be greatly facilitated by the use of suitable requirement management tools.

The implementation of each technical safety concept requirement shall take account of feasibility, unambiguousness, consistency and completeness.

The technical safety concept shall take the following into account:

a) all safety goals and functional safety requirements;

b) all relevant norms, standards and statutory regulations;

c) the relevant results from safety analysis tools (FMEA, FTA, etc.); the safety analysis provides iterative support for the technical safety concept during system development.

The completeness of the technical safety concept increases iteratively during system design. To ensure completeness:

1) the version of the technical safety concept and the version of the relevant underlying sources shall be specified;

2) the requirements from change management (see ISO 25119-4:2018, Clause 11) shall be met and, for this reason, the technical safety requirements shall be structured and formulated to provide support for a modification process;

3) the technical safety requirements shall be reviewed (see ISO 25119-4:2018, Clause 6).

The technical safety concept shall consider all phases of the life cycle (including production, customer operation, servicing and decommissioning).

5.4.2.2 Specification of the technical safety concept

5.4.2.2.1 General

The technical safety concept shall include hardware and software safety requirements sufficient for the design of the SRP/CS, and shall be determined in accordance with 5.4.2.1.

5.4.2.2.2 States and times

The behaviour of the SRP/CS, its components and their interfaces shall be specified for all relevant operating states, including

— start-up,

— normal operation,

— shut-down,

— restart after reset, and

— reasonably foreseeable unusual operating states (e.g. degraded operating states).

In particular, failure behaviour and the required reaction shall be described exactly. Additional emergency operation functions may be included.

The technical safety concept shall specify a safe state for each functional safety requirement, the transition to the safe state, and the maintenance of the safe state. In particular, it shall be specified whether shutting off the SRP/CS immediately represents a safe state, or if a safe state can only be attained by a controlled shut down.

The technical safety concept shall specify for each functional safety requirement the maximum time that may elapse between the occurrence of an error and the attainment of a safe state (response time). All response times for subsystems and sub-functions shall be specified in the technical safety concept.

If no safe state can be achieved by a direct shut down, a time shall be defined during which a special emergency operation function has to be sustained for all subsystems and sub-functions. This emergency operation function shall be documented in the technical safety concept.

5.4.2.2.3 Safety architecture, interfaces and marginal conditions

The safety architecture and its sub-components shall be described. In particular, the technical measures shall be specified. The technical safety concept shall separately describe the following components (as applicable):

— sensor system, separate for each physical parameter recorded;

— miscellaneous digital and analogue input and output units;

— processing, separate for each arithmetic unit/discrete logical unit;

— actuator system, separate for each actuator;

— displays, separate for each indicator unit;

— miscellaneous electromechanical components;

— signal transmission between components;

— signal transmission from/to systems external to the SRP/CS;

— power supply.

The interfaces between the components of the SRP/CS, interfaces to other systems and functions in the machine, as well as user interfaces, shall be specified.

Limitations and marginal conditions of the SRP/CS shall be specified. This applies in particular to extreme values for all ambient conditions in all phases of the life cycle.

5.5 Work products

The following work product shall be applicable to system design:

a) technical safety concept specification.

6 Hardware

6.1 Objectives

The objective is to define acceptable hardware architectures for SRP/CS.

6.2 General

Improving the hardware structure of the SRP/CS can provide measures for avoiding, detecting or tolerating faults. Practical measures can include redundancy, diversity and monitoring.

In general, the following fault criteria shall be taken into account.

— If, as a consequence of a fault, further components fail, the first fault and all following faults are considered to be a single fault.

— Two or more separate faults having a common cause are regarded as a single fault (known as common cause failure).

— The simultaneous occurrence of two independent faults is highly unlikely and therefore does not need to be considered.

Iterations between the hardware and software development may be required in order to complete the necessary hardware testing.

6.3 Prerequisites

The prerequisite is the parts of the functional safety concept to be realized by the hardware (ISO 25119-2:2018, Clause 7).

The prerequisite for the “hardware system integration” and the “hardware safety validation” shown in Figure 2 for hardware that is controlled by software is the operating software itself.

6.4 Requirements

The hardware development process shall begin at the system level where safety-related functions and associated requirements are identified (see Figure 2).

The functional safety concept shall be used to identify the performance level (AgPL) for each system safety-related function (ISO 25119-2).

Selection of hardware categories, $MTTF_{DC}$, DC and SRL shall be made such that the resultant AgPL of the individual or combination SRP/CS meets or exceeds all $AgPL_r$’s of the assigned functional safety requirements.

The system may be broken down into subsystems for easier development.

Each phase of the development cycle shall be verified.

The system integration hardware/software test shown in Figure 1 shall be performed using previously tested hardware and software components.