INTERNATIONAL STANDARD

ISO 25119-3

First edition
2010-06-01

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 25119-3:2010(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 25119-3 was prepared by Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 19, *Agricultural electronics*.

ISO 25119 consists of the following parts, under the general title *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems*:

— *Part 1: General principles for design and development*

— *Part 2: Concept phase*

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

— *Part 4: Production, operation, modification and supporting processes*

Introduction

ISO 25119 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising electrical and/or electronic and/or programmable electronic components (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 municipal equipment. It covers the possible hazards caused by the functional behaviour of E/E/PES safety-related systems, as distinct from hazards arising from the E/E/PES equipment itself (electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety, etc.).

The control system parts of the machines concerned are frequently assigned to provide the critical functions of the *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 critical 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 protective measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

ISO 25119 allocates the ability of safety-related parts to perform a critical 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 are considered: systematic, common-cause and random.

In order to guide the designer during design, and to facilitate the assessment of the achieved performance level, ISO 25119 defines an approach based on a classification of structures 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 adopts a customer risk-based approach for the determination of the risks, while providing a means of specifying the target 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.

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

Part 3: Series development, hardware and software

1 Scope

This part of ISO 25119 provides general principles for the series development, hardware and software 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 municipal equipment (e.g. street-sweeping machines). It specifies the characteristics and categories required of SRP/CS for carrying out their safety functions.

This part of ISO 25119 is applicable to the safety-related parts of electrical/electronic/programmable electronic systems (E/E/PES). As these relate to mechatronic systems, it does not specify which safety functions or categories are to be used in a particular case.

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

2 Normative references

The following referenced documents are indispensable for the application 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 25119-1:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

ISO 25119-2:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: concept phase*

ISO 25119-4:2010, *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 given in ISO 25119-1 apply.

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
EUC	equipment under control
FMEA	failure mode and effects analysis
FMECA	failure mode effects and criticality analysis
EPROM	erasable programmable read only memory
FSM	functional safety management
FTA	fault tree analysis
HAZOP	hazard and operability study
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
SRS	safety-related system
UML	unified modelling language.

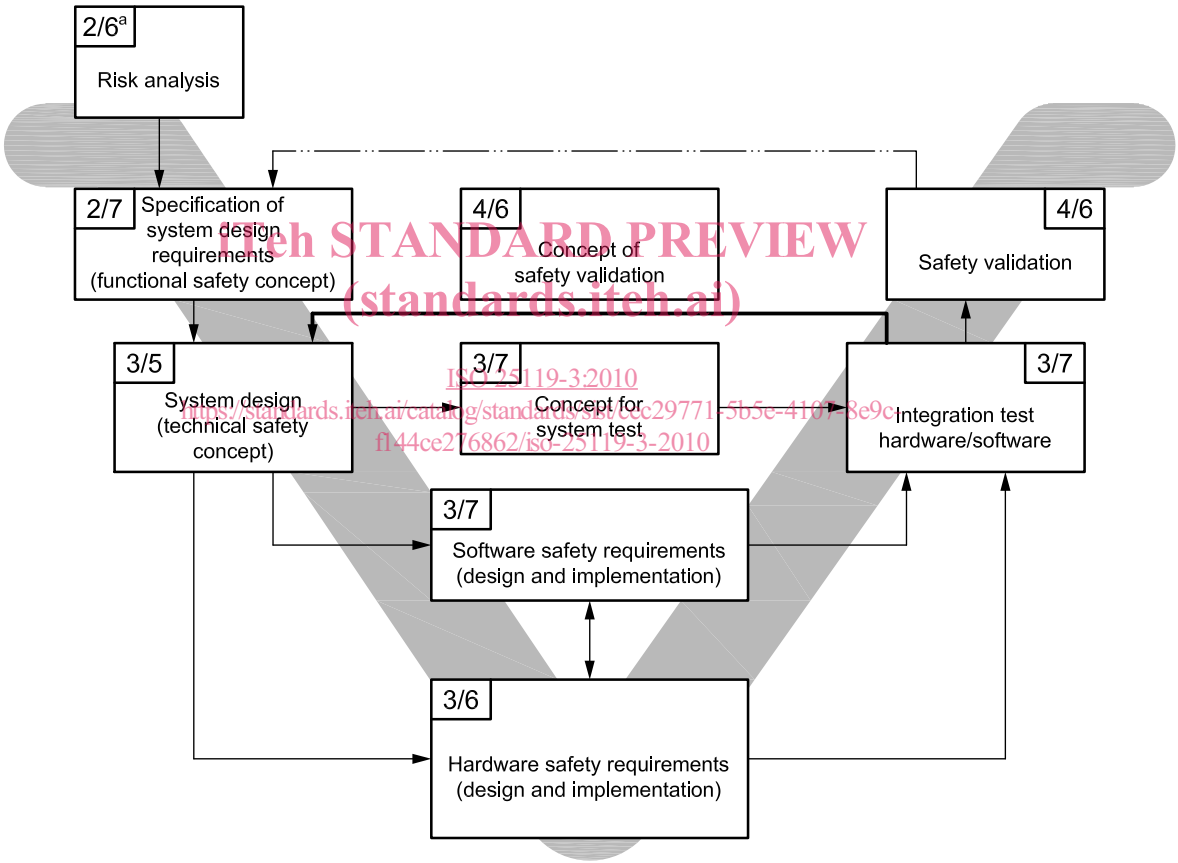
5 System design

5.1 Objectives

The objective is to define a development process for producing a 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.



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 to the clause in that document: 2/6 is ISO 25119-2:2010/Clause 6, 3/5 is ISO 25119-3:2010/Clause 5, and so on.

Figure 1 — Structuring of safety requirements

5.3 Prerequisites

Before beginning system design, define the safety-related function requirements, application and operation environment.

5.4 Requirements

5.4.1 Structuring safety requirements

The functional safety concept specifies the basic functioning of the safety-related system with 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 in the form of technical safety requirements. This system architecture is comprised of both hardware and software.

The hardware safety requirements refine and solidify the requirements of the technical safety concept. 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 safety concept requirements during system design, thereby providing a basis for error-free system design.

5.4.2 Functional safety concept

5.4.2.1 General requirements of functional safety concept

Safety functions are normally identified during the system risk analysis, and the functional safety concept document includes the functional safety requirements for the system.

The implementation for each safety concept requirement shall consider the following.

— **Feasibility**

When listing functional safety requirements, attention shall be paid to the feasibility of the requirement, considering constraints, such as available technology, as well as financial and time resources. The persons in charge of implementation shall understand and accept the technical safety requirements.

— **Unambiguousness**

The functional safety requirements shall be formulated as precisely and unambiguously as possible.

NOTE A functional safety requirement is unambiguously formulated when it permits only one interpretation by the anticipated readers.

— **Consistency**

Functional safety requirements shall not be self-contradicting (internal consistency), nor shall they contradict other requirements (external consistency).

Analyses of the requirements and comparisons between different requirements are necessary to ensure external consistency. This is a requirement management task.

— **Completeness**

The functional safety concept shall take all relevant norms, standards and statutory regulations into account.

The functional safety concept shall take into account all relevant safety goals derived from the risk analysis according to ISO 25119-2.

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

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

2) the requirements from change management (see ISO 25119-4:2010, Clause 10) shall be met and, for this reason, the functional safety requirements shall be structured and formulated to provide support for a modification process;

3) the functional safety requirements shall be reviewed (see ISO 25119-4:2010, Clause 6).

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

5.4.2.2 Specification of the functional safety concept

This clause presents the information that is required to be specified in the functional safety concept. The functional safety concept may be derived from the machine failure scenarios evaluated during a risk analysis.

Each failure scenario description shall include the following:

— environmental conditions (moving on an ice covered road, up-hill, down-hill, weather, etc.);

— machine conditions (engine running, in-gear, standing still, etc.);

— resulting AgPL;

— safe state descriptions (engine stopped, valve off, transmission in park, continue function at reduced performance, etc.).

5.4.3 Technical safety concept

5.4.3.1 General requirements of technical safety concept

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

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

— other technical safety requirements,

— functional safety requirements, or

— safety goals and objectives.

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

Just as for the *functional* safety concept, the implementation of each technical safety concept requirement shall take account of feasibility, unambiguousness, consistency and completeness.

— **Feasibility**

When listing technical safety requirements, attention shall be paid to the feasibility of the requirement considering constraints, such as available technology, as well as financial and time resources. Those in charge of implementation shall understand and accept the technical safety requirements.

— **Unambiguousness**

The technical safety requirements shall be formulated as precisely and unambiguously as possible.

NOTE A technical safety requirement is unambiguously formulated when it permits only one interpretation by the anticipated readers.

— **Consistency**

Technical safety requirements shall not be self-contradicting (internal consistency), nor shall they contradict other requirements (external consistency).

Analyses of the requirements and comparisons between different requirements are necessary to ensure external consistency. This is a requirement management task.

— **Completeness**

The technical safety concept shall take the following into account:

1) all safety objectives and functional safety requirements;

2) all relevant norms, standards and statutory regulations;

3) 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:

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

5) the requirements from change management (see ISO 25119-4:2010, Clause 10) shall be met and, for this reason, the technical safety requirements shall be structured and formulated to provide support for a modification process;

6) the technical safety requirements shall be reviewed (see ISO 25119-4:2010, Clause 6).

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

5.4.3.2 Specification of the technical safety concept

5.4.3.2.1 General

The technical safety concept shall include hardware and software safety requirements sufficient for the design of the unit of observation, and shall be determined in accordance with 5.4.3.1.

5.4.3.2.2 States and times

The behaviour of the unit of observation, its modules 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 unit of observation 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.

5.4.3.2.3 Safety architecture, interfaces and marginal conditions

The safety architecture and its sub-modules shall be described. In particular, the technical measures shall be specified. The technical safety concept shall separately describe the following modules (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 modules;

— signal transmission from/to systems external to the unit of observation;

— power supply.

The interfaces between the modules of the unit of observation, interfaces to other systems and functions in the machine, as well as user interfaces, shall be specified.

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

6 Hardware

6.1 Objectives

The objective is to define acceptable hardware architectures for safety-related control systems.

6.2 General

Improving the hardware structure of the safety-related parts of a control system can provide measures for avoiding, detecting or tolerating faults. Practical measures can include redundancy, diversity and monitoring.

In general, the following fault criteria should 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 considered highly unlikely.

6.3 Prerequisites

The prerequisite is $AgPL_r$, determined for each safety function to be realized by the hardware.

6.4 Requirements

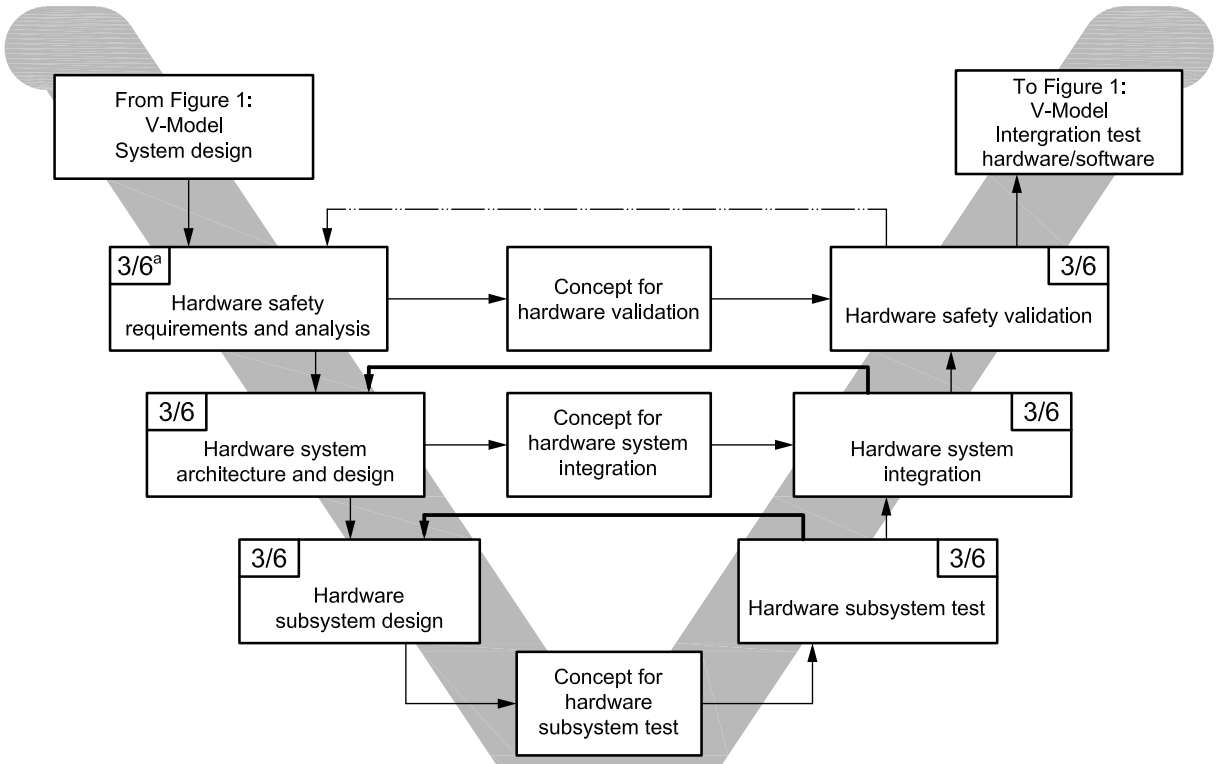
The hardware development process shall begin at the system level where safety functions and associated requirements are identified (see Figure 2).

The hardware safety analysis shall be used to identify the performance level ($AgPL_r$) for each system safety function (see ISO 25119-2).

The designer shall group functions into appropriate architectures (hardware category) with associated $MTTF_{dC}$, DC and CCF.

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

Each phase of the development cycle shall be verified.



Key

result

verification

validation

[a] The first of two numbers separated by a slash refers to this part of ISO 25119 and the second to Clause 6.

Figure 2 — Hardware development V-model

The design procedure for the hardware system architecture is as follows.

a) Select a hardware category (see ISO 25119-2:2010, Annex A).

b) Identify the component operating environment and stress level.

c) Select components.

d) Calculate and verify that the $MTTF_{dC}$ meets the required level (see ISO 25119-2:2010, Annex B).

e) Determine and verify that the DC meets the required level (see ISO 25119-2:2010, Annex C).

f) Consider CCF (see ISO 25119-2:2010, Annex D).

g) Consider systematic failures (see ISO 25119-2:2010, Annex E).

h) Consider other safety functions (see ISO 25119-2:2010, Annex F).

NOTE Iteration could be required for the above steps.