INTERNATIONAL STANDARD

ISO 25119-4

First edition
2010-06-01

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 25119-4:2010(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 v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 2
5 Configuration management 3
5.1 Objectives 3
5.2 General 3
5.3 Prerequisites 3
5.4 Requirements 3
5.5 Work products 3
6 Verification and validation 3
6.1 Objectives 3
6.2 General 3
6.3 Prerequisites 3
6.4 Requirements 4
6.5 Work products 5
7 Product release 5
7.1 Objectives 5
7.2 General 5
7.3 Prerequisites 6
7.4 Requirements 6
7.5 Work products 7
8 Production, production testing 7
8.1 Objectives 7
8.2 General 7
8.3 Prerequisites 7
8.4 Requirements 8
8.5 Work products 8
9 Operation planning and maintenance (instructions for operating, servicing, repair, and decommissioning) 9
9.1 Objectives 9
9.2 General 9
9.3 Prerequisites 9
9.4 Requirements 9
9.5 Work products 10
10 Modifications (change management) 11
10.1 General 11
10.2 Objectives 11
10.3 General 11
10.4 Prerequisites 11
10.5 Requirements 11
10.6 Work products 14
11 Procedure for suppliers of SRS, subsystems and components 15
11.1 Objectives 15

11.2 General **15**
11.3 Prerequisites **15**
11.4 Requirements **15**
11.5 Work products **17**
12 Technical documentation **17**
12.1 Objectives **17**
12.2 Requirements **17**
Annex A (informative) **Technical documentation checklist** **19**
Bibliography **22**

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 25119-4 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 4: Production, operation, modification and supporting processes

1 Scope

This part of ISO 25119 provides general principles for the production, operation, modification and supporting processes 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 3600, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Operator's manuals — Content and presentation*

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 25119-3:2010, *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 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
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

5 Configuration management

5.1 Objectives

The first objective is to ensure that the SRP/CS and associated documents for a given function can be uniquely identified and reproduced at any time.

The second objective is to ensure that the relations and differences between earlier and current versions of the SRP/CS and associated documents can be traced.

5.2 General

All ISO 25119 work products shall be handled by a configuration management system.

5.3 Prerequisites

See the prerequisites for each phase of the safety life cycle.

5.4 Requirements

Software tools and software development environments shall be subject to configuration management.

Configuration management data shall be maintained in accordance with a company document retention policy.

5.5 Work products

The applicable work product is the listing of SRP/CS with reference to associated documents for a given configuration.

6 Verification and validation

6.1 Objectives

One objective is to provide proof that the safety-related requirements are appropriate for the E/E/PES system and have duly been met.

A further objective is to provide proof that the safety goals at the machine level are satisfied.

6.2 General

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

6.3 Prerequisites

The following are the prerequisites for this phase:

— project plan according to ISO 25119-1:2010, 5.4.7 — deadlines, resources, equipment, degree of maturity, etc.;

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

— risk analysis according to ISO 25119-2:2010, Clause 6 — identification of potential hazards;

— safety goals, as well as safe states;

— technical safety concept according to ISO 25119-3:2010, Clause 5 — technical safety requirements.

6.4 Requirements

6.4.1 SRP design validation/verification

The design of the SRP of the control system shall be validated/verified (see ISO 25119-1:2010, Figure 1).

The validation/verification shall demonstrate that each SRP meets

— all the requirements of the specified category (see ISO 25119-2:2010, Annex A), and

— the specified safety characteristics for that part as set out in the design requirements.

6.4.2 Scope of safety validation/verification

Within the safety life cycle, validation/verification of safety attributes 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/verification:

— validation/verification planning;

— validation/verification specification;

— validation/verification execution;

— report on validation/verification result.

All variants or versions of the E/E/PES system that were subject to the validation/verification activities shall be clearly labelled.

6.4.4 Validation/verification plan

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

— validation/verification and possible variants;

— degree of maturity of the system;

— validation/verification goals;

— validation/verification techniques;

— statement of independence between the person in charge of validation/verification and the developer;

— equipment and environmental conditions required, including calibration specifications for tools;

— specified reference to the overall project plan;

— pass/fail criteria for all tests.

6.4.5 Validation/verification, test specification of hardware and software

The item function shall be validated/verified at E/E/PES system level, considering fulfilment of the hardware/software safety requirements.

6.4.6 Validation/verification test specification of the complete system

The characteristics of the SRP/CS shall be validated/verified at machine level, considering fulfilment of the functional safety concept.

6.4.7 Validation/verification test specification

The following methods and measures shall be used and specified:

— tests (black-box, HIL, machine testing, field testing, etc.);

— analysis (e.g. simulation);

— reviews of relevant documents (input from hardware/software, e.g. FMEA, circuit diagram).

6.5 Work products

The following work products are applicable to this phase:

a) detailed validation/verification plan;

b) test specification;

c) validation/verification report that shall include proof that validation/verification goals have been met for

   1) the complete system at machine level,

   2) hardware, and

   3) software.

7 Product release

7.1 Objectives

The objective of this phase is to specify the conditions for product release as the completion of the E/E/PES systems development. Product release confirms that the requirements for functional safety in the machine have been met.

7.2 General

Figure 1 shows the approvals needed for an E/E/PES system development and the order of their completion that will satisfy the conditions for product release.

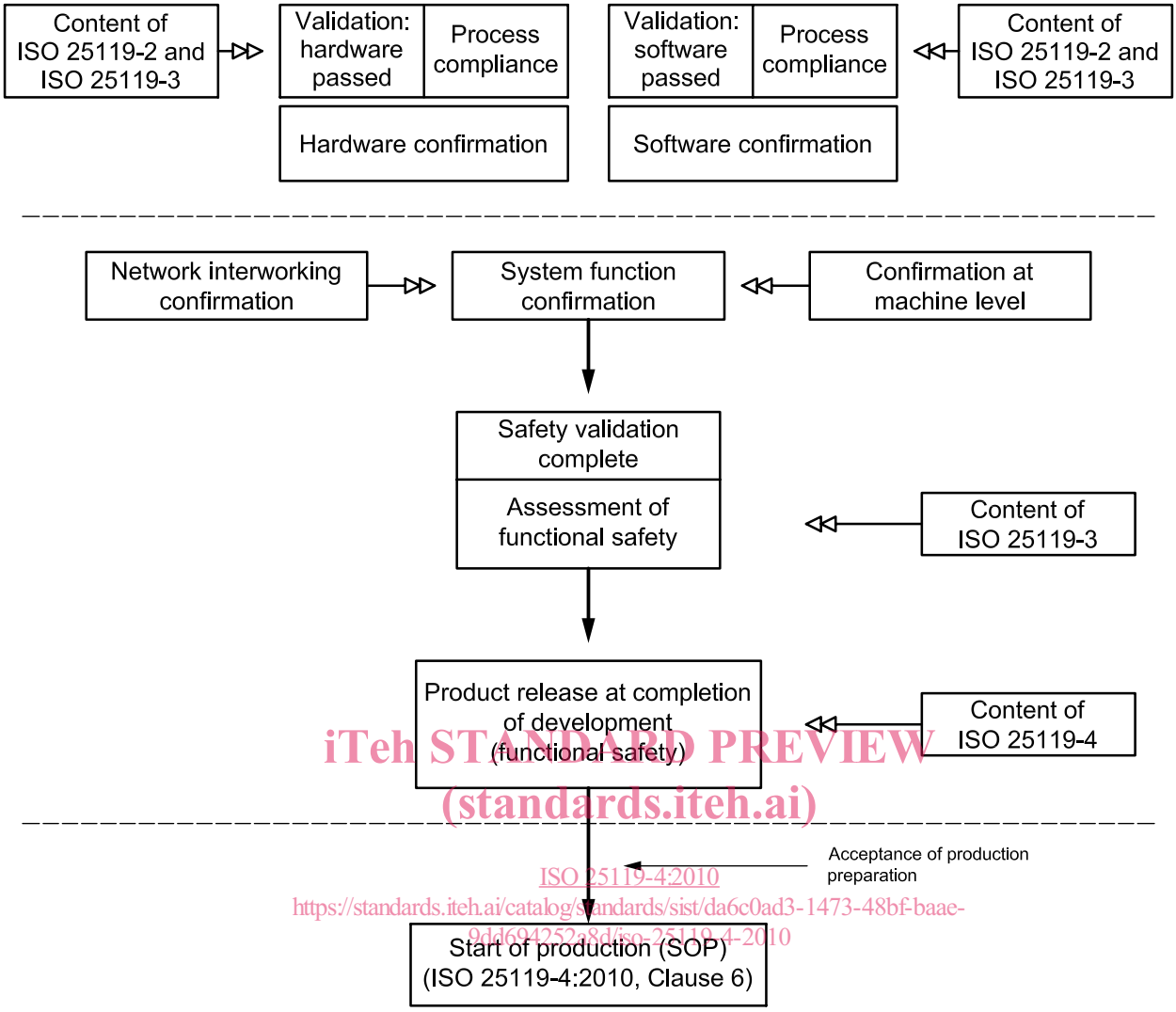

Figure 1 — Approval hierarchy

7.3 Prerequisites

The following are the prerequisites for this phase:

— confirmation report: hardware;

— confirmation report: software;

— confirmation report: machine level;

— assessment report on functional safety.

7.4 Requirements

7.4.1 Conditions for product release

Product release may only be approved if the following results are available from previous stages in the life cycle (see Annex A):

— an accepted assessment;

— hardware confirmation;