INTERNATIONAL STANDARD

ISO 25119-4

Second edition
2018-10

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 25119-4:2018(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 25119-4:2010), 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 scope has been slightly modified;

— and a new Clause 5 (quality management system) has been added;

— the former Clause 5 (configuration management) has been moved after Clause 6;

— Clause 6 has been revised;

— the example of technical documentation checklist 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, 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 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 4: Production, operation, modification and supporting processes

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 3600, *Tractors, machinery for agriculture and forestry, powered lawn and garden equipment — Operator's manuals — Content and format*

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 25119-2:2018, *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*

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
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 Quality management system

A quality management system is an important part of functional safety. Users of this document shall demonstrate conformance to Clauses 7, 8, 9 and 11 by

— applying quality management principles, for example, those found in ISO 9001, using Clauses 7, 8, 9, and 11 as guidance, or

— applying the requirements in Clauses 7, 8, 9, and 11 as they are written in this document.

6 Safety validation and verification

6.1 Objectives

One objective is to provide proof that each functional safety requirement has been duly met and is appropriate for the safety goals of the UoO.

A further objective is to provide proof that each safety goal has been realized as initially desired and specified and is appropriate for the functional safety of the UoO.

6.2 General

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

6.3 Prerequisites

The following are the prerequisites for this phase:

— safety plan according to ISO 25119-1:2018, 6.4.6.3 — deadlines, resources, equipment, degree of maturity, etc.;

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

— HARA according to ISO 25119-2:2018, Clause 6 — identification of potential hazards;

— functional safety concept according to ISO 25119-2:2018, Clause 7 — safety goals, as well as safe states, and functional safety requirements;

— technical safety concept according to ISO 25119-3:2018, Clause 5 — technical safety requirements.

6.4 Requirements

6.4.1 SRP/CS design validation and verification

The design of the SRP/CS shall be validated and verified (see ISO 25119-1:2018, Figure 1).

The validation and verification shall demonstrate that each SRP/CS meets:

— the requirements of the specified AgPL including as appropriate:

  a) hardware category, $MTTF_{DC}$, DC, CCF (see ISO 25119-2:2018, Annexes A, B, C, D);

  b) SRL (see ISO 25119-3:2018, Clause 7);

— the safety goals, safe states and remaining functional and technical safety requirements;

— the fulfilment of the assigned safety-related functions.

6.4.2 Scope of safety validation and verification

Within the safety life cycle, validation and verification of safety requirements 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 and verification:

— validation and verification planning;

— validation and verification specification;

— validation and verification execution;

— documentation of validation and verification result.

6.4.4 Validation and verification plan

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

— validation and verification and possible variants;

— degree of maturity of the system;

— validation and verification goals;

— validation and verification techniques;

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

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

— specified reference to the overall safety plan;

— pass/fail criteria for all tests.

6.4.5 Validation and verification test specification

The following methods and measures as appropriate shall be used and specified:

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

— 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 shall be provided for this phase:

a) detailed validation and verification plan;

b) test specification;

c) validation and verification documentation that shall include proof that validation and verification goals have been met for

   1) the complete system at system level or at the machine level as appropriate,

   2) hardware, and

   3) software.

7 Configuration management

7.1 Objectives

The first objective shall be to ensure that the SRP/CS and associated technical documentation for a given safety-related 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 technical documentation can be traced.

7.2 Prerequisites

See the work products for each phase of the safety life cycle.

7.3 Requirements

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

SRP/CS specifications and associated technical documentation shall be subject to configuration management.

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

All variants or versions of the E/E/PES system that contain a SRP/CS shall be clearly labelled. Labelling could be in the form of a serial number or date code.

7.4 Work products

The applicable work product shall be the listing of SRP/CS with reference to associated technical documentation for a given configuration.

8 Product release

8.1 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.

8.2 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.

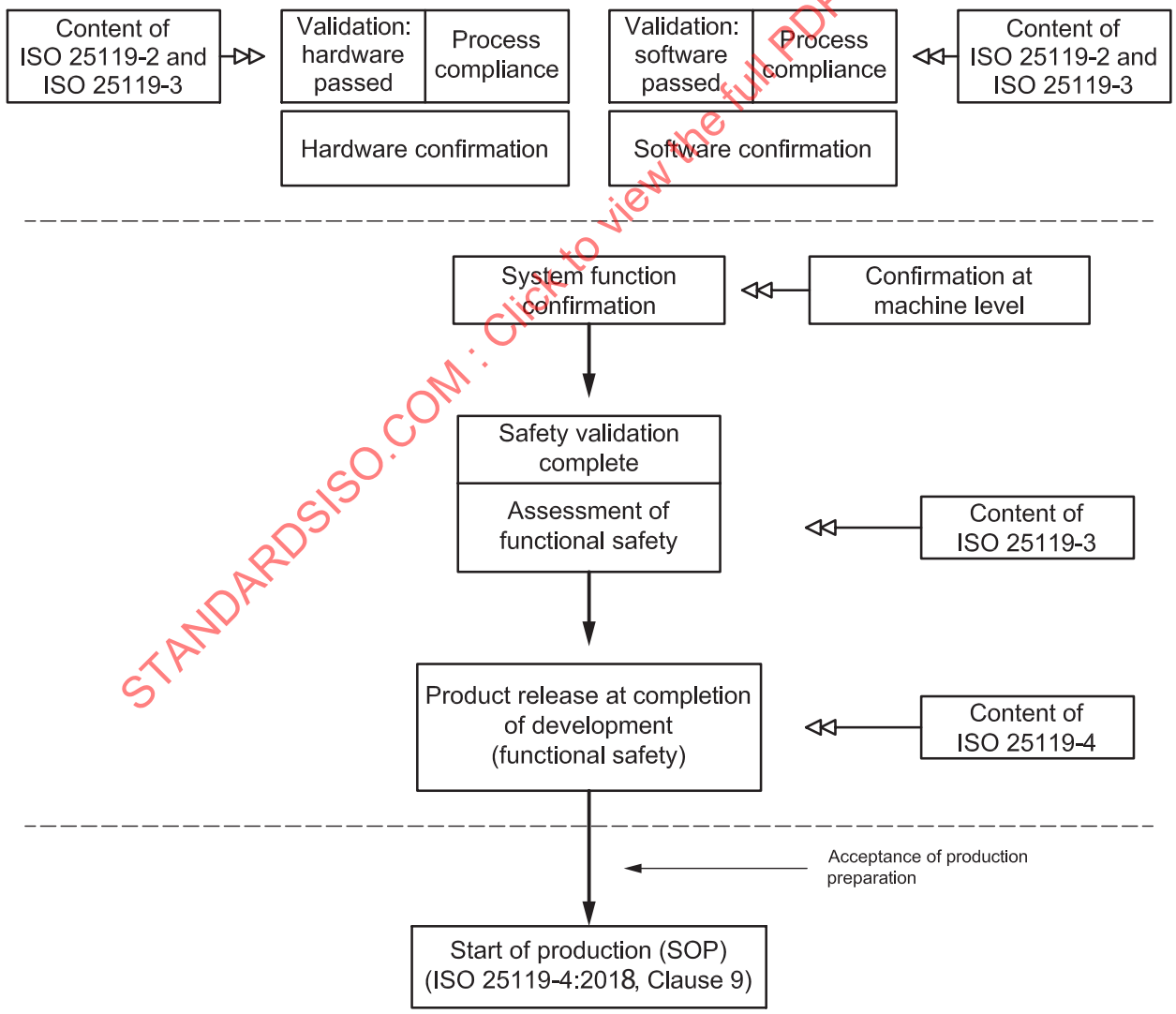

Figure 1 — Approval hierarchy

8.3 Prerequisites

The following are the prerequisites for this phase:

— confirmation documentation: hardware;

— confirmation documentation: software;

— confirmation documentation at the system level or machine level as appropriate;

— assessment documentation on functional safety.

8.4 Requirements

8.4.1 Conditions for product release

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

— an accepted assessment;

— hardware confirmation;

— software confirmation;

— system confirmation at the E/E/PES system level or machine level as appropriate (including data parameterisation).

8.4.2 Documentation of product release

Product release shall be documented and shall contain the following:

— version(s) of the released E/E/PES system;

— configuration of the released E/E/PES system;

— references to associated documents;

— release date.

NOTE The release document for functional safety can be part of the document for product release of the E/E/PES system or a separate document.

8.5 Work products

The applicable work product shall be the product release documentation.

9 Production planning, production and production testing

9.1 Objectives

The objectives of this phase are to develop a production and installation plan for SRP/CS, and to ensure that the required functional safety is maintained during the production process by the relevant product manufacturer, or person or organization in charge of the process (machine manufacturer, supplier, sub-supplier, etc.).

9.2 General

By including safety-relevant characteristics in production planning and checking, this phase defines the steps required to ensure that functional safety is maintained during the production process as well.

9.3 Prerequisites

The following are the prerequisites for production and production testing:

— assembly notes (documentation of the parts or functions that can be affected by assembly);

— test notes;

— product release document;

— test criteria (safety-relevant characteristics to be tested);

— product monitoring — required for safety-relevant characteristics and ensuring that the safety-relevant characteristics of components are maintained in line with their specifications in the machine manufacturer's production process.

9.4 Requirements

9.4.1 Production plan

A production plan taking the assembly instructions into account shall include:

— identification of safety-related characteristics;

— sequence and methods of production steps;

— assembly equipment/tools.

9.4.2 Production test plan

The test plan shall include:

— identification of safety-related characteristics;

— sequence and methods of testing steps;

— test equipment/tools, test criteria;

— production test frequency.

9.4.3 Personnel

Production and testing shall be carried out by trained personnel, according to the production and test plans.

9.4.4 Process capability

Process capability shall be ensured by means of standard industry requirements.

9.4.5 Documentation

The implementation of testing according to the test plan shall be documented. As a minimum, test documentation shall include test date, tester, unique part identification and test results.

9.4.6 Non-compliance

A procedure for non-compliance with a test criterion of SRP/CS shall be established. Reworking is permissible only upon proof of appropriate process control.

9.4.7 Storage and transport conditions

Any special handling and packaging requirements of SRP/CS shall be followed when storing and transporting the product.

9.5 Work products

The following work products shall be provided for this phase:

a) documentation of tests performed according to the test plan;

b) non-compliance procedure;

c) storage and transport conditions.

10 Operation planning and maintenance (instructions for operating, servicing, repair and decommissioning)

10.1 Objectives

The objective of this phase is to define the scope of the servicing, customer information and repair instructions of SRP/CS, in order to maintain the required functional safety during operation, field observation, servicing, repair and decommissioning.

10.2 General

This clause presents the areas with safety-relevant characteristics relevant to the development of repair instructions and user information, and the planning, execution and monitoring of maintenance work.

10.3 Prerequisites

The following are the prerequisites for operation planning and maintenance:

— product release — release document regarding functional safety;

— quality management system (an implemented, routinely applied quality management system such as ISO 9001);

— maintenance notes — documentation of the safety-related areas that can be influenced through maintenance (maintenance tasks), and notes on experiences gathered through field analyses;

— configuration management plan — documented procedure for configuration management.

10.4 Requirements

10.4.1 General

The functional safety requirements during the maintenance and repair activities can be different from those required during operation and these shall be taken into account.

10.4.2 Servicing schedule

A servicing schedule shall be prepared in parallel with the system design and shall include

— identification of components of the SRP/CS that require scheduled service, taking the relevant released subsystem or system configuration into account, and

— sequence, methods (tools, if necessary) and definition of the time interval and scope of servicing for the operating time to be defined.

10.4.3 Repair instructions

Repair instructions shall include

— identification of repairable components of the SRP/CS,

— work steps and workflow, methods and tools (e.g. programming and diagnostic equipment, if applicable),

— the relevant released configuration of the system or subsystem,

— permissible deactivation of subsystems or systems and the additional adjustments required on the complete machine, and

— identification of manufacturers spare parts and when appropriate approved replacement parts.

10.4.4 Service technician instructions

Repair and servicing work should:

— be performed by appropriately authorized and trained personnel;

— be performed and documented according to the servicing schedule or repair instructions.

10.4.5 User information

User information (e.g. operating instructions) shall be prepared. Such operating instructions shall be included in the operator's manual in accordance with ISO 3600 and shall include

— warnings of potential hazards including those arising from the interaction with third-party products,

— description of subsystem or system and status information (display concept) and of the required customer reaction,

— description of the required components of servicing, and

— warnings against making modifications to the SRP/CS (applies to AgPL = a to AgPL = e).

10.4.6 Field observation

A process of field observation shall be established. Appropriate measures based on the results of the analyses shall be initiated.

10.4.7 Storage and transport information

For the definition of storage and transport conditions of the product, safety-related characteristics for operating modes deviating from normal operation shall be taken into account (e.g. being towed, reduced driving operation).

10.4.8 Decommissioning and disassembling

The requirements regarding the decommissioning and disassembling of the machine shall be provided by the manufacturer.

10.5 Work products

The following work products shall be provided for this phase:

a) repair instructions;

b) user instructions;

c) storage and transport instructions;

d) decommissioning and disassembly instructions.

11 Modifications (change management)

11.1 Objective

The objective is to ensure that the functional safety system is appropriate, both during and after the modification and retrofit phase has taken place.

11.2 General

In case of modifications to the product initiated by production, operation, field observation, servicing, repair or decommissioning of sub-functions, an impact analysis shall be used to decide which phases of the safety life cycle are to be repeated.

Change management helps to ensure systematic planning, controlling, monitoring, implementation and documentation of changes, while maintaining the consistency of all work products. Before changes are carried out, potential impacts on functional safety are assessed. For this purpose, decision-making processes for changes shall be introduced and established, with an assignment of responsibilities between the parties involved.

NOTE Here, "changes" are understood as modifications (corrections, removals, additions and enhancements, etc.).

11.3 Prerequisites

The following are the prerequisites for change management:

— safety plan;

— configuration management plan.

11.4 Requirements

11.4.1 Product modification and improvement procedures

Procedures for carrying out any product modification or product improvement activity shall be described (standard operating procedure). An example of a modification procedure model is shown in Figure 2 and an example of an operation and maintenance management model is shown in Figure 3.

Modifications made to SRP/CS with an AgPL equal to "a" or higher should only be performed by responsible persons or service providers authorized by the manufacturer of the system.

The product modification and product improvement phase shall be initiated only by the issue of an authorized request under the procedures for the management of functional safety (see ISO 25119-1:2018, Clause 6).

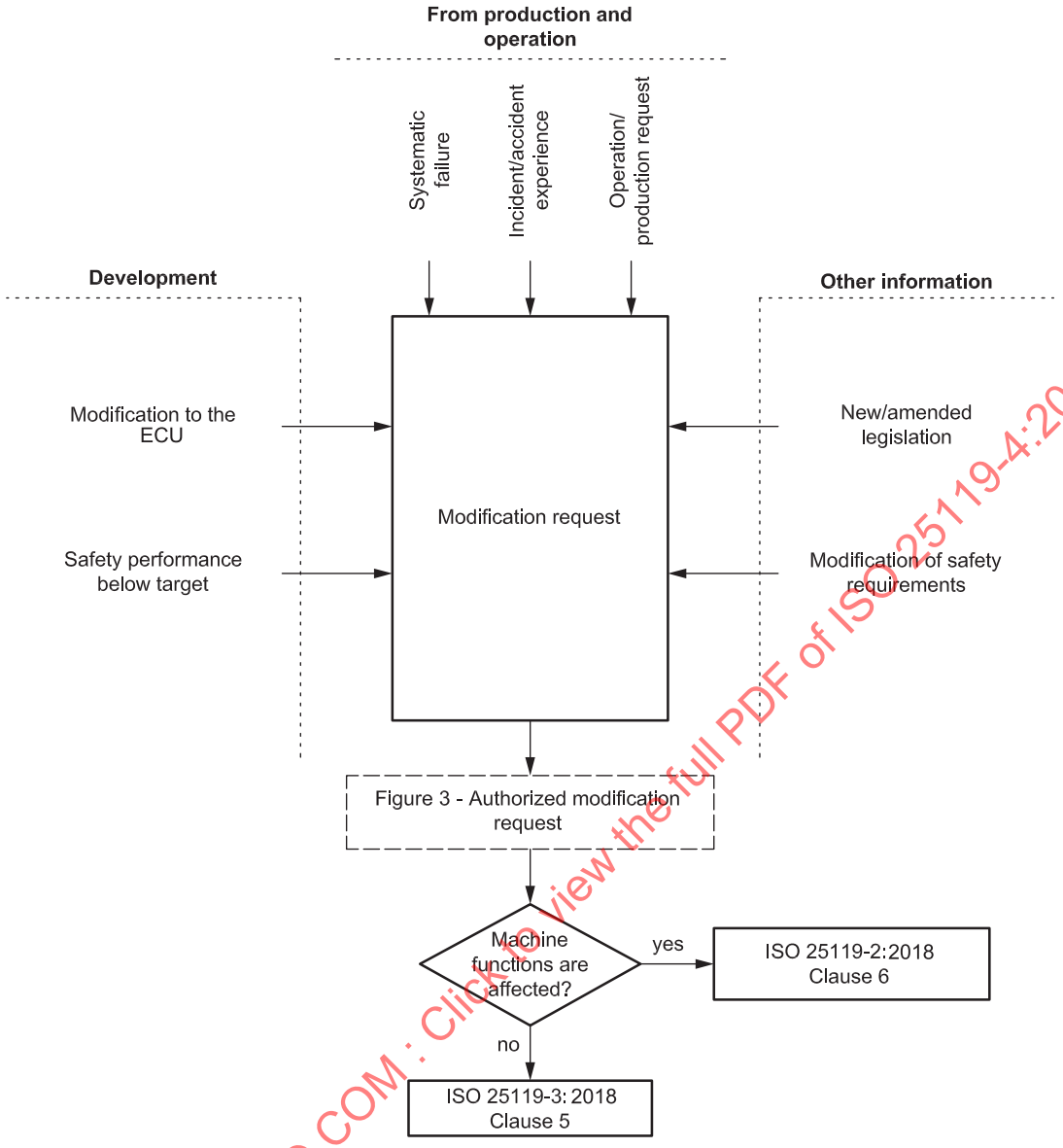

Figure 2 — Example modification procedure model

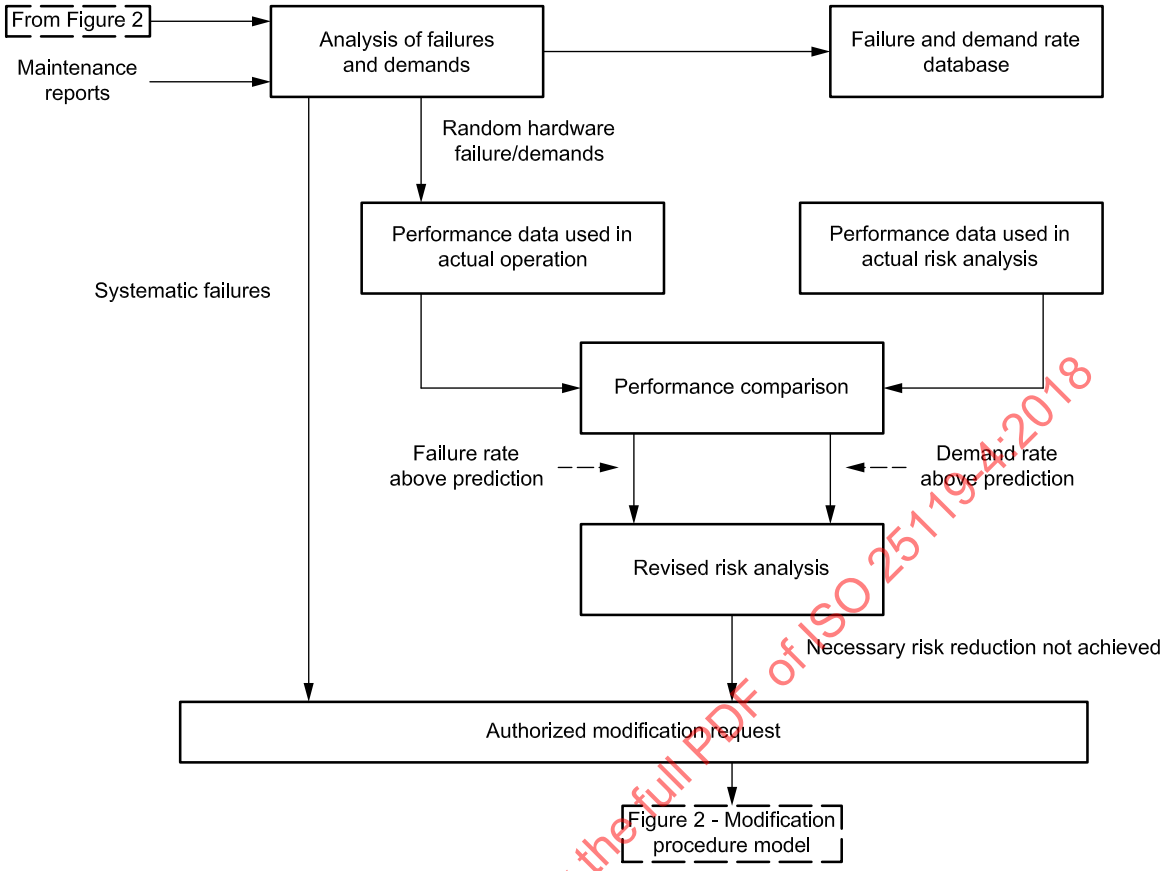

Figure 3 — Example operation and maintenance management model

11.4.2 Modification request

The request shall detail the following:

a) the reasons for the modification;

b) the proposed modification (both hardware and software);

c) the determined hazards which could be affected (impact analysis);

d) compatibility across machines.

NOTE The reason for the request for the modification could arise from:

— functional safety below that specified;

— systematic fault experience;

— new or amended safety legislation;

— modifications to the equipment under control or its use;

— modification to the overall safety requirements;

— analysis of operations and maintenance performance, indicating that the performance is below target;

— customer operation requests.

11.4.3 Assessing impact of modification

11.4.3.1 General

The responsible person shall decide whether the UoO has been modified to the extent of requiring a risk analysis (see ISO 25119-2:2018, Clause 6), or whether the UoO has not been modified (see ISO 25119-3:2018, Clause 5). This shall be determined after the impact analysis (see also Figure 2).

If the DC or $MTTF_{DC}$ for a channel is modified, then evaluation according to ISO 25119-2:2018, Clause 6, is required. If there is no modification of DC or $MTTF_{DC}$, but the micro-controller is changed (e.g. upgrading a micro-controller from 16 bit to 32 bit), then evaluation according to ISO 25119-3:2018, Clause 6, is required.

The assessment shall also consider the impact of other concurrent product modification or product improvement activities.

11.4.3.2 Modification examples

Three modification examples follow, giving the required response in each case.

a) Change of a brake sensing function.

   If the brake sensing function is changed from dual- to single-channel, the classification of the category shall be reviewed. The development workflow shall then be continued from ISO 25119-2:2018, Clause 7.

b) Change speed limit from 40 km/h to 50 km/h.

   The speed of a machine is increased from 40 km/h to 50 km/h, and different functions in the machine could be affected. This involves a complete re-assessment with respect to the risk analysis. The review shall then be started again in accordance with ISO 25119-2:2018, Clause 6.

c) Controller upgrade.

   For the upgrade of a micro-controller from 16 bit to 32 bit without a change of the category, DC and MTTF for each channel, the point of continuation shall be ISO 25119-3:2018, Clause 5.

NOTE 1 It can be necessary to implement a full hazard and risk analysis which could generate a need for performance levels that are different to those currently specified for the equipment under control.

NOTE 2 It cannot be assumed that the test procedures originally developed for final inspection can be reused without checking their validity.

11.4.4 Modification authorization

Authorization to carry out the required modification or retrofit activity shall be dependent on the results of the impact analysis.

11.5 Work products

The work product applicable to this phase is chronological documentation, which shall be established and maintained so that it gives details of all modifications and retrofits, including

— the modification or retrofit request,

— the impact analysis,

— revalidation and reverification of data and results, and

— all documents affected by the modification and retrofit activity.

12 Procedure for suppliers of SRP/CS, subsystems and components

12.1 Objectives

The objective of this process is to describe the procedures and responsibilities within the relationship between machine manufacturers, suppliers and sub-suppliers of SRP/CS for distributed developments.

12.2 General

The machine manufacturer and the suppliers for SRP/CS shall jointly use the procedures of ISO 25119 (all parts). Responsibilities shall be clearly established between the machine manufacturer and the suppliers. Subcontractor relationships are permitted. Just as with the machine manufacturer, safety-related specifications concerning planning, execution and documentation for development, projects shall be established by all suppliers on distributed development projects, or development projects when the responsibility for safety is borne entirely by the supplier.

This does not apply for procurement of standard components, or development of supplied components that are not safety-related.

12.3 Prerequisites

The prerequisites for this phase are the following.

— Draft version of machine manufacturer/supplier development agreement: this agreement between the machine manufacturer and the supplier lays down the responsibilities for activities and work products.

— Supplier's quotation: these documents are of a general nature and therefore contain no prerequisite based on ISO 25119 (all parts).

12.4 Requirements

12.4.1 General

The activities relating the relationship between the machine manufacturer and supplier for distributed development shall encompass the following points; any necessary deviations shall be agreed upon:

— project initiation;

— project planning;

— project execution;

— assessment of functional safety;

— safety validation;

— documentation;

— confirmation measures;

— activities after SOP.

12.4.2 Scope of requirements

Machine manufacturer and supplier-related requirements apply to all SRP/CS of a system being developed under ISO 25119 (all parts), except to primary components in the case where

a) there are no specific system safety-related requirements allocated to these primary components, or

b) technical and quality specifications of these primary components comply with the allocated system safety-related requirements.

12.4.3 Supplier selection

When selecting a supplier, the following shall be taken into account:

— assessment and documentation of whether the supplier has a quality management system in place;

— the supplier's experience and capability in developing SRP/CS, subsystems, or systems — a documented process for functional safety management shall be checked, or this process can be jointly agreed between the machine manufacturer and the supplier.

When selecting a supplier, recommendations from all relevant departments (e.g. development, quality, logistics) shall be considered.

12.4.4 Project initiation

When a project is initiated, persons in charge of functional safety for the project and sub-project shall be appointed for both the machine manufacturer and the supplier.

The machine manufacturer's project leader shall present the relevant parts of the machine manufacturer's product development process and functional safety process to the supplier.

It shall be decided in cooperation with the supplier which processes of ISO 25119 (all parts) are to be carried out. Work product responsibilities shall be clearly established.

The agreement between machine manufacturer and supplier shall also account for subcontractor relationships.

12.4.5 Project planning

The machine manufacturer and the supplier shall agree on a project plan, including milestones and key dates.

The machine manufacturer and the supplier shall both coordinate their quality assurance activities.

If the supplier places orders with subcontractors, the supplier shall manage these subcontractors in accordance with ISO 25119 (all parts) or a comparable standard.

The supplier shall develop a safety plan.

The machine manufacturer shall inform the supplier of all changes affecting functional and technical safety requirements. Such changes shall be subject to change management.

12.4.6 Project execution

Over the entire project term, the machine manufacturer and the supplier shall monitor and control product quality.

The supplier shall report all safety-related events, incidents and project-threatening risks that occur during project activities in its area of responsibility or in that of its subcontractors to the machine manufacturer.

The supplier shall identify any function safety requirements that cannot be met. In this case, the functional safety concept shall be modified.

Any change introduced by the machine manufacturer or supplier that could affect the safety of the purchased system or planned measures to demonstrate conformance with ISO 25119 (all parts) shall be communicated to the other party for impact analysis.

12.4.7 Confirmation measures for the development partners' functional safety

The machine manufacturer and the supplier shall carry out an assessment of functional safety in all phases of the safety life cycle for which they are responsible.

The supplier shall report the results of the functional safety assessment to the machine manufacturer.

12.4.8 System validation

System validation shall be performed considering the integration requirements for the entire machine. The integration effort provided by the machine manufacturer shall be agreed upon.

Validation shall be performed and documented by the person in charge in accordance with project validation planning.

12.5 Work products

Documentation shall be compiled in accordance with ISO 25119 (all parts).

The supplier shall document the safety-related information obtained during planning, execution and completion of the project, to confirm that the product fulfils the safety requirements specified. The supplier shall provide the machine manufacturer with adequate documentation to complete his own documentation confirming that the product fulfils the safety requirements specified.

13 Technical documentation

13.1 Objectives

The objective is to provide required information (see Table A.1) in the form of documentation, so that every phase of the entire safety life cycle can be worked through effectively and can be reproduced.

13.2 Requirements

13.2.1 Document retention

The documentation shall be retained in accordance with company document retention policy on each phase of the entire safety life cycle.

NOTE 1 Only the information necessary for undertaking a particular activity, as required by ISO 25119 (all parts), need be held by each relevant party.

NOTE 2 This requirement assumes that company information retention policy is consistent with national legislation.

13.2.2 Document structure

The documentation needed for the effective completion of

— management of functional safety, and

— the carrying out of the assessment of functional safety,

shall:

— be accurate and concise,

— be easy to understand by those persons having to make use of it,

— be written such that others can understand the process that was followed,