INTERNATIONAL STANDARD

ISO 25119-1

Second edition
2018-10

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

Part 1: General principles for design and development

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

Partie 1: Principes généraux pour la conception et le développement

Reference number
ISO 25119-1:2018(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO 25119-1:2010), which has been technically revised. The main changes compared from the previous edition are as follows:

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

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

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

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

— Figure 2 has been modified;

— the document has been editorially revised.

A list of all parts in the ISO 25119 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

ISO 25119 (all parts) sets out an approach to the assessment, design and verification, for all safety life cycle activities, of safety-related parts comprising electrical and/or electronic and/or programmable electronic systems (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to mobile municipal equipment.

A prerequisite to the application of ISO 25119 (all parts) is the completion of a suitable hazard identification and risk analysis (e.g. ISO 12100) for the entire machine. As a result, an E/E/PES is frequently assigned to provide safety-related functions that create safety-related parts of control systems (SRP/CS). These can consist of hardware or software, can be separate or integrated parts of a control system, and can either perform solely safety-related functions or form part of an operational function.

In general, the designer (and to some extent, the user) will combine the design and validation of these SRP/CS as part of the risk assessment. The objective is to reduce the risk associated with a given hazard (or hazardous situation) under all conditions of use of the machine. This can be achieved by applying various measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

ISO 25119 (all parts) allocates the ability of safety-related parts to perform a safety-related function under foreseeable conditions into five performance levels. The performance level of a controlled channel depends on several factors, such as system structure (category), the extent of fault detection mechanisms (diagnostic coverage), the reliability of components (mean time to dangerous failure, common-cause failure), design processes, operating stress, environmental conditions and operation procedures. Three types of failures that can cause E/E/PES malfunctions leading to potential hazardous situations are considered: systematic, common-cause and random.

In order to guide the designer during design, verification, and to facilitate the assessment of the achieved performance level, ISO 25119 (all parts) defines an approach based on a classification of architecture with different design features and specific behaviour in case of a fault.

The performance levels and categories can be applied to the control systems of all kinds of mobile machines: from simple systems (e.g. auxiliary valves) to complex systems (e.g. steer by wire), as well as to the control systems of protective equipment (e.g. interlocking devices, pressure sensitive devices).

ISO 25119 (all parts) adopts a risk-based approach for the determination of the risks, while providing a means of specifying the required performance level for the safety-related functions to be implemented by E/E/PES safety-related channels. It gives requirements for the whole safety life cycle of E/E/PES (design, validation, production, operation, maintenance, decommissioning), necessary for achieving the required functional safety for E/E/PES that are linked to the performance levels.

The structure of safety standards in the field of machinery is as follows.

a) Type-A standards (basic safety standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:

   — type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

   — type-B2 standards on safeguards (e.g. two-hand controls, interlocking devices, pressure sensitive devices, guards).

c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This document is a type-B1 standard as stated in ISO 12100.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organizations, market surveillance, etc.).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions, organizations for people with special needs);

— service providers, e.g. for maintenance (small, medium and large enterprises);

— consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

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

Part 1: General principles for design and development

1 Scope

This document sets out general principles for the design and development of safety-related parts of control systems (SRP/CS) on tractors used in agriculture and forestry and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It can also be applied to mobile municipal equipment (e.g. street-sweeping machines).

This document is not applicable to:

— aircraft and air-cushion vehicles used in agriculture;

— lawn and garden equipment.

This document specifies the characteristics and categories required of SRP/CS for carrying out their safety-related functions. It does not identify performance levels for specific applications.

NOTE 1 Machine specific type-C standards can specify performance levels (AgPL) for safety-related functions in machines within their scope. Otherwise, the specification of AgPL is the responsibility of the manufacturer.

This document is applicable to the safety-related parts of electrical/electronic/programmable electronic systems (E/E/PES), as these relate to mechatronic systems. It covers the possible hazards caused by malfunctioning behaviour of E/E/PES safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards, unless directly caused by malfunctioning behaviour of E/E/PES safety-related systems. It also covers malfunctioning behaviour of E/E/PES safety-related systems involved in protective measures, safeguards, or safety-related functions in response to non-E/E/PES hazards.

Examples included within the scope of this document:

— SRP/CS limiting current flow in electric hybrids to prevent insulation failure/shock hazards;

— electromagnetic interference with the SRP/CS;

— SRP/CS designed to prevent fire.

Examples not included in the scope of this document:

— insulation failure due to friction that leads to electric shock hazards;

— nominal electromagnetic radiation impacting nearby machine control systems;

— corrosion causing electric cables to overheat.

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

NOTE 2 See also ISO 12100 for design principles related to the safety of machinery.

This document is not applicable to safety related parts of control systems manufactured before the date of its publication.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 25119-2:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 2: Concept phase*

ISO 25119-3:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware and software*

ISO 25119-4:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: production, operation, modification and supporting processes*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.13
environmental condition
physical condition under which a system is used

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

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

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

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

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

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

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

Note 2 to entry: For the purposes of ISO 25119 (all parts), a fault is a *random* fault.

3.17
function
defined behaviour of one or more electronic control units

3.18
functional requirement
requirement for an intended function of the E/E/PES system

3.19
functional safety
system that performs in a way that does not present an unreasonable risk of injury to operators or bystanders

3.20
functional safety concept
entire collection of *functional safety requirements* (3.21) including their interactions to achieve functional safety

Note 1 to entry: It is developed during the concept phase of the safety life cycle.

3.21
functional safety requirement
requirement for a safety-related function of the E/E/PES system

3.22
hardware safety requirement
requirement that applies to safety-related hardware and which is included as an element of a technical safety requirement

3.23
harm
physical injury or damage to health of persons

3.24
hazard
potential source of *harm* (3.23)

3.25
hazard analysis and risk assessment
HARA
method to identify and categorize hazardous situations of the UoO and to specify safety goals, $AgPL_r$, related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk

3.26
hazardous situation
circumstance in which a person is exposed to a *hazard* (3.24) or hazards, *exposure* (3.14) to which can have immediate or long-term effects

3.27
intended use
<of a machine> use in accordance with the information provided in the operator's manual

3.28
inspection
systematic formal verification method used to review product quality

Note 1 to entry: During an inspection, the work product is checked by one or more assessors to see whether it complies with the requirements. The inspection is organized and moderated by an inspection leader. The author of the work product participates in the inspection but cannot lead the process.

3.29
life of the machine
life cycle
time between production and decommissioning

3.30
manual reset
function within the SRP/CS used to manually restore one or more safety-related functions before restarting the machine

3.31
machine manufacturer
manufacturer of tractors for agriculture and forestry, self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture, and of mobile municipal equipment

Note 1 to entry: See also *supplier* (3.50).

3.32
mean time to dangerous failure
$MTTF_D$
average value of the expected time to a *dangerous failure* (3.8)

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

3.33
monitoring
automatic monitoring
automatic function which ensures that a *protective measure* (3.36) is initiated if the ability of the SRP/CS to perform a function is diminished, or if the process conditions are changed such that hazards are generated

3.34
muting
temporary automatic suspension of a safety-related function by safety-related parts of the control system

3.35
programmable electronic system
PES
system for control, protection or monitoring which uses one or more programmable electronic devices

Note 1 to entry: It comprises all elements of the system, including power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices.

3.36
protective measure
measure intended to achieve functional safety, as implemented by the designer (intrinsic design, safeguarding and complementary measures, information for use), and the user (organization, safe working procedures, supervision, permit to work, systems, additional safeguards, personal protective equipment, training)

3.37
reasonably foreseeable misuse
use of a machine in a way not intended by the designer, but which can result from readily predictable human behaviour

3.38
response time
maximum time that can elapse between the occurrence of an error and the attainment of a *safe state* (3.43)

3.39
risk
combination of the probability of occurrence of *harm* (3.23) and the *severity* (3.47) of that harm

3.40
risk analysis
combination of the specification of the limits of the machine, hazard identification and risk estimation

3.41
risk assessment
overall process comprising *risk analysis* (3.40) and *risk evaluation* (3.42)

3.42
risk evaluation
judgment on the basis of risk analysis as to whether a given risk is acceptable

3.43
safe state
operating mode of a system with an acceptable level of risk

EXAMPLE Intended operating mode, back-up operating mode, or switched-off modes.

3.44
safety goal
description of how a given hazard is to be avoided

EXAMPLE Avoid propel when neutral is commanded.

Note 1 to entry: It is the top level objective as a result of the hazard analysis and risk assessment and where safety-related functions are derived.

Note 2 to entry: One safety goal can be related to several hazards and several safety goals can be related to a single hazard.

3.45
safety-related function
function of the machine whose failure can result in an immediate increase of risk

3.46
safety-related part of a control system
SRP/CS
part or subpart of a control system that responds to input signals and generates safety-related output signals

Note 1 to entry: The combined safety-related parts of a control system start at the point where the safety-related signals are initiated (e.g. the actuating cam and the roller of the position switch) and end at the output of the power control elements (e.g. the main contacts of the contactor), and include monitoring systems.

3.47
severity
degree of the most probable harm to an endangered individual, assuming harm has occurred

3.48
software requirement level
SRL
ability of safety-related parts to perform a software *safety-related function* (3.45) under foreseeable conditions

Note 1 to entry: The SRL is categorized into four groups: SRL = B, 1, 2 and 3.

3.49
software safety requirement
requirement that applies to safety-related software and that is included as an element of a *technical safety requirement* (3.54)

3.50
supplier
manufacturer and distributor of new and spare parts for tractors for agriculture and forestry, self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture, and municipal equipment

3.51
symmetric channel
numerical combination of single-channel $MTTF_{DC}$ for a dual- or redundant-channel system

3.52
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

EXAMPLE Human error in the safety requirements specification, the design, manufacture, installation, operation of the hardware, or the design and implementation of the software.

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

3.53
technical safety concept
entire collection of *technical safety requirements* (3.54) necessary to implement the *functional safety concept* (3.20)and to partition it on the system architecture

Note 1 to entry: It is part of the system specification, specified during system design.

3.54
technical safety requirement
requirement that applies to the SRP/CS as applied to a given *technical safety concept* (3.53)

3.55
unit of observation
units of observation
UoO
electrical, electronic, electrically-programmable system or function and its scope, context and purpose

Note 1 to entry: The UoO can encompass safety-related function(s) that may be distributed across multiple systems and their safety-related interactions.

3.56
walk-through
systematic, informal verification method used to review product quality

Note 1 to entry: During a walk-through, the author of a work product provides a step-by-step report to one or more assessors. The objective is to create a common understanding of the work product, and to identify any errors, defects, discrepancies or problems in the work product. A walk-through is less stringent than an inspection.

3.57
work product
output of a design or development activity

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/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 6 to 9 by

— applying the quality management principles, such as those found in ISO 9001 using Clauses 6 to 9 as guidance, or

— applying the specific clauses in Clauses 6 to 9 as they are written in this document.

NOTE These options relate only to this document.

6 Management during complete safety lifecycle

6.1 Objectives

The main objective, set out in this clause, is to define the responsibilities of the persons, departments and organizations responsible for each phase during the overall safety life cycle or for activities within the various phases. This relates to both the activities necessary to ensure the required level of functional safety for the UoO, and to the confirmation measures endorsing that level of functional safety. Another objective is to define management activities during the complete safety life cycle.

The E/E/PES shall be designed and constructed so that the principles of risk analysis, risk assessment and an iterative process for the design of safety-related parts of control systems are fully taken into account (see Figure 1).

NOTE ISO 25119 (all parts) address only the evaluation of the safety aspects of the E/E/PES.

6.2 General

6.2.1 Introduction to the safety life cycle concept

The safety life cycle (see Figure 2) combines the most important safety-related activities in the concept phase, during series development, and at the start of production (SOP). These activities are described in detail in ISO 25119-2 and ISO 25119-3. Planning, coordination and verification of these activities across all phases of the life cycle are a central management task.

NOTE The activities during the concept phase and series development and after SOP are described in detail in ISO 25119-2, ISO 25119-3 and ISO 25119-4.

6.2.2 External functional safety measures

These are measures that cannot be influenced by the UoO but shall be taken into account by the construction of the UoO. External functional safety includes the characteristics of involved persons (e.g. physical, language) or properties of the environment (e.g. EMC, temperature, moisture, and other properties). The risk analysis can give consideration to external functional safety.

NOTE 1 Proof of the effectiveness of external functional safety is not within the scope of ISO 25119 (all parts).

NOTE 2 Failures of other technologies such as mechanics and hydraulics are not taken into consideration by ISO 25119 (all parts). Verification of the functional safety of these technologies is not within the scope of ISO 25119 (all parts).

6.3 Prerequisites

A prerequisite to the application of ISO 25119 (all parts) is the completion of a suitable risk assessment and risk reduction (e.g. ISO 12100) for the entire machine.

The necessary prerequisites to the design, manufacturing, service and decommissioning process are a proven quality assurance plan (e.g. IATF 16949 or equivalent) and an overall project plan.

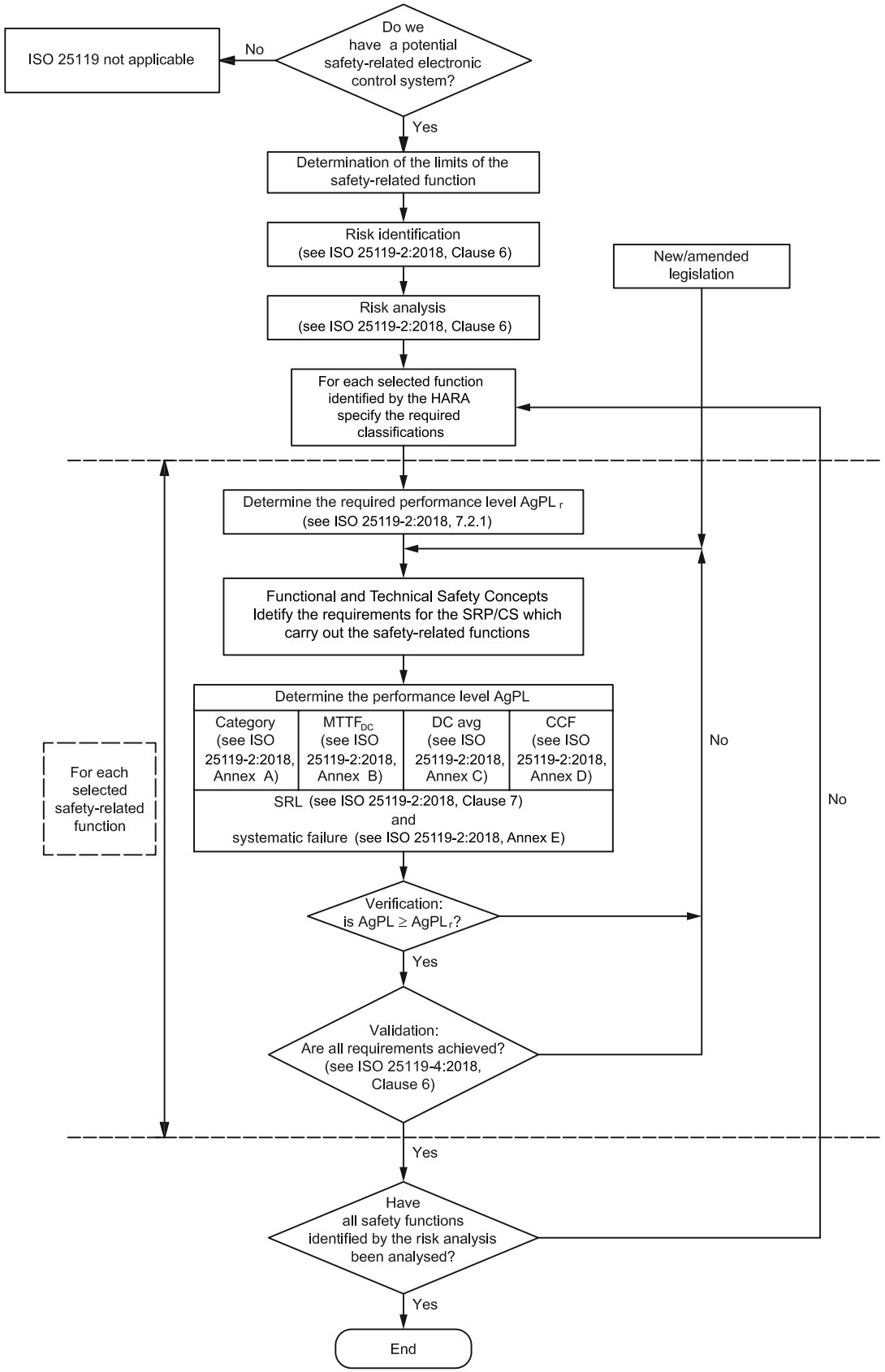
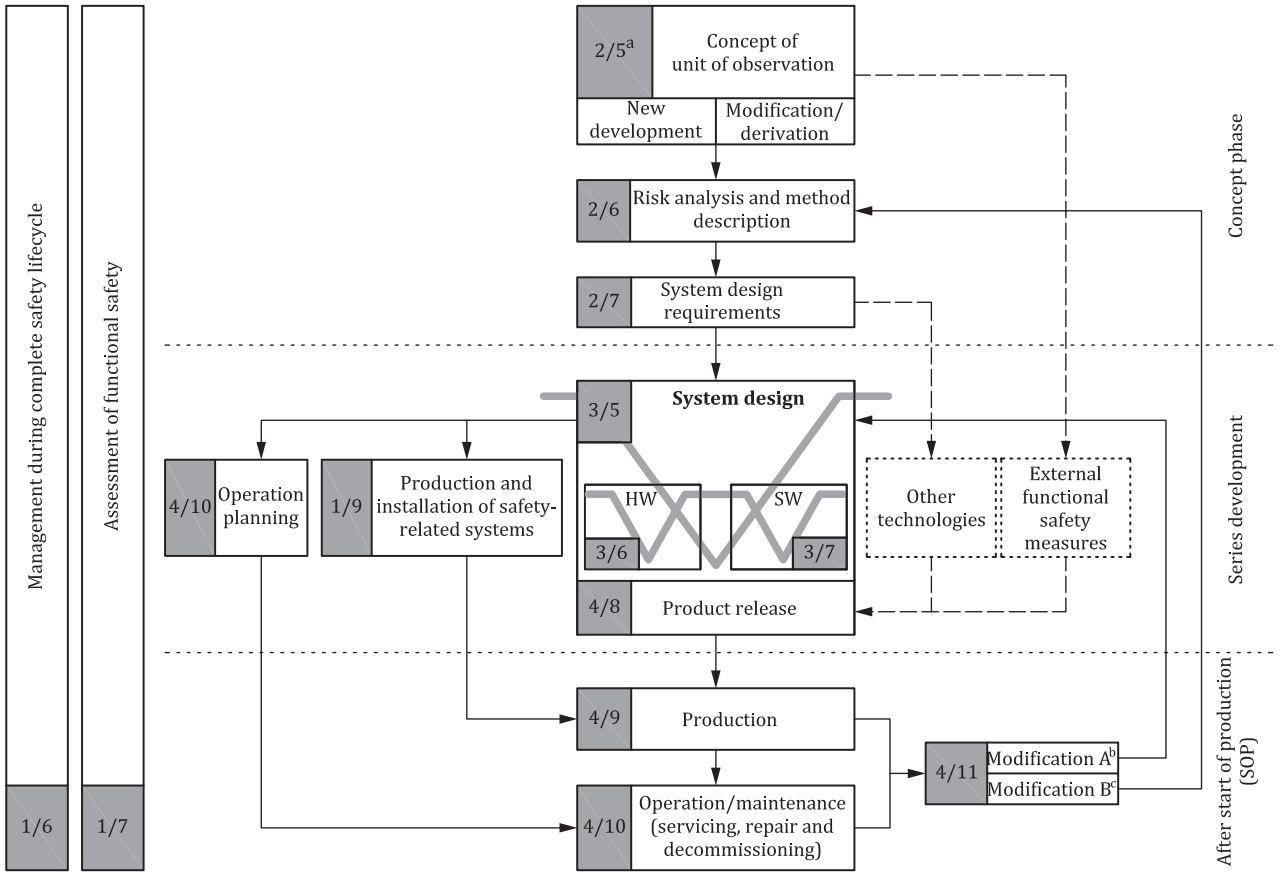


Figure 1 — Iterative process for design of SRP/CS



a The first number in this and the other toned boxes signifies the part of ISO 25119, while the second number, separated from the first by a slash, signifies the clause number of that part, e.g. "2/5" signifies ISO 25119-2:2018, Clause 5.

b If machine functions are *not* affected, then go to ISO 25119-3:2018, Clause 5.

c If machine functions *are* affected, then carry out hazard and risk analysis according to ISO 25119-2:2018, Clause 6.

Figure 2 — Safety life cycle

6.4 Requirements — Functional safety management activities across safety life cycle

6.4.1 Functional safety culture

One task of management and all members of staff shall be to create a culture in which functional safety is given appropriate attention. This can be achieved, for example:

— by formulating the goals of functional safety and communicating them within the organization, and

— reviewing the status of processes for achieving functional safety.

6.4.2 Continuous improvement

Management shall facilitate processes for continuous improvement. Examples for doing this include

— the creation of company-specific procedures to fulfil the requirements of ISO 25119 (all parts),

— the provision of tools, templates, databases and other resources that will assist in performing safety-related activities, and

— obtaining feedback from safety-related parts findings from projects and transferring these findings to the members of new project teams.

6.4.3 Training and qualification

Performing the tasks in the safety life cycle requires appropriately qualified staff. The aim shall be to maintain a balanced degree of proficiency in

— technical safety concepts,

— methodology, and

— knowledge of the functional safety process and information related to requirements.

6.4.4 Assignment of safety responsibilities

The planning and execution of activities that incorporate functional safety into projects falling within the scope of ISO 25119 (all parts) represent a central management task for the individual or organization responsible for the UoO.

Initially, responsibility for incorporation of functional safety lies with the project manager. The tasks resulting from this may be delegated. The lines of communication and decision-making with respect to the safety plan and the remedying of safety-related deficits shall be clearly defined.

In doing so, it shall be ensured that individuals have sufficient, documented qualifications and competency for their assigned tasks. The required training and experience can depend on the AgPL and the complexity of the UoO. Appropriately qualified individuals can also carry out multiple tasks.

6.4.5 Assignment of tasks

Functional safety management tasks shall be the responsibility of a product safety manager or the manager of a safety team appointed by the project manager.

A quality management system is essential for carrying out the safety management activities. Functional safety management tasks include the prompt and proper delivery of the results of safety-related activities in all phases of the development process. The implementation of individual tasks may be delegated.

6.4.6 Planning of all safety management activities during development

6.4.6.1 General

The objective shall be to coordinate all safety related aspects during development between all involved persons, departments and/or suppliers.

All safety activities during the development phases of safety life cycle shall be planned, including at least the following:

— procedures and strategy for achieving functional safety;

— specification of safety responsibilities between development partners;

— provision for establishment of supporting processes within the project;

— conducting risk analysis according to ISO 25119-2:2018, Clause 6;

— implementation of safety requirements in the context of development activities according to ISO 25119-2:2018, Clause 7, and ISO 25119-3:2018, Clauses 6 and 7;

— confirmation by development partners that they have fulfilled the safety requirements by means of assessments, reviews and audits;

— verification and validation of safety requirements according to ISO 25119-4:2018, Clause 6;

— specification of activities for confirmation of functional safety (audit, review, assessment);

— inclusion of overall project safety activities into project-specific safety management.

6.4.6.2 Technical documentation

Refer to ISO 25119-4:2018, Clause 13 for documentation requirements.

6.4.6.3 Safety plan

6.4.6.3.1 Objectives

The safety plan shall be used for the systematic planning for safety-related activities.

The safety plan shall be adapted to the project. Some activities could be unnecessary for a specific project or additional activities might have to be included.

Safety-related activities should be incorporated into overall project planning and allocated the required resources.

6.4.6.3.2 Contents of the safety plan

Safety-related activities shall be described in the safety plan. The following characteristics of an activity shall be specified as appropriate:

— objective(s);

— prerequisites (results needed from other activities, input documents);

— person in charge;

— necessary resources;

— duration, deadline;

— documentation of results.

6.4.6.3.3 Format of safety plan

The safety plan may be a stand-alone document or integrated into a general project plan. In the latter case, safety-related activities shall be labelled as such.

The safety plan may include references to other plans. In general, it is preferable to have references rather than parallel descriptions of activities in multiple documents.

The safety plan format shall be subject to version and change management.

NOTE An example of a structure of a project-specific safety plan is given in Annex A.

6.4.6.4 Tailoring activities within processes (to AgPL)

The characteristic of all activities shall always be related to the AgPL and safety plan for each project.

In addition, activities and entire phases of the life cycle that do not apply to specific projects may be omitted, with corresponding justification.

When compiling the safety plan, attention shall be paid to adapting the specific characteristic of all activities to the AgPL and the circumstances in the project.

In the quality management system, consider attaching milestones to the V model (see ISO 25119-3:2018, Figure 1).

Consider refining the existing V model over the course of the project.

A clear justification shall be specified if individual activities are omitted or performed in a scaled-down form.

6.5 Work products

The work products from management during the complete safety cycle shall be the following:

— safety plan.

7 Assessment of functional safety

7.1 Objectives

The objective of this phase is to examine and assess the functional safety attained by the UoO and the function implemented in it.

7.2 General

The organizational unit responsible for functional safety (e.g. machine manufacturer or supplier) carries out an assessment of functional safety. The implementation of this assessment may also be delegated to one person in charge of the assessment. The assessment shall cover all phases of the machine safety life cycle (e.g. system and safety concept, design, implementation, test for all integration levels, system release, production, operation) for each of the organizational units involved in the development of the UoO. The involved organizational units shall disclose all relevant assessment documents to the machine manufacturer/supplier or to the person in charge.

7.3 Prerequisites

a) Safety plan.

b) As a minimum, representatives from the following areas in the organizational unit in charge of development shall take part in the safety assessment:

   — the person responsible for the system;

   — the system developer;

   — the expert(s) on functional safety.

7.4 Requirements

7.4.1 Considerations for the assessment of the functional safety

These shall consist of the following requirements.

a) Management requirements for verification measures shall be in accordance with 7.4.2.

b) The organizational unit in charge of development shall provide an appropriate level of support for the safety assessment (sufficient preparation and availability of sufficient human resources).

c) The person performing the safety assessment shall have access to all individuals performing activities in the entire hardware and software life cycle and to all relevant information and tools.

d) The safety assessment shall include all phases of the machine safety life cycle (system and safety concept, design, implementation, test for all integration levels, system release, production, operation) for each of the departments involved in the development of the UoO.

e) If tools are used for development, implementation or testing, their application shall be assessed or verified.

f) The safety assessment may be performed in parallel with development or in a block.

g) The safety assessment shall take the following aspects into account:

   1) the work performed since the previous assessment;

   2) the planning/strategy for performing further assessments;

   3) recommendations for acceptance, conditional acceptance, or rejection, which shall be given at the conclusion of the safety assessment.

7.4.2 Verification

The following requirements apply to verification.

Verification measures shall be included in the safety plan. The UoO as well as the form of the result shall be defined. The independence of those performing verification shall be documented. The degree of independent verification depends on the AgPL level (see Table 1).

Planning for verification shall be done by those who perform the verification and accepted by those who are responsible for the scope to be verified.

The results of verification shall be documented. In particular, a statement shall be made about acceptance, conditional acceptance or rejection. Open items shall be documented, responsible individuals shall be appointed, and resolution shall be confirmed.

If the UoO is altered after the conclusion of reviews and assessments, the review or assessment shall be repeated or amended.

Audits, walk-throughs, inspections and assessments shall be carried out with reference to the AgPL. The following activities shall be reviewed regardless of the level of independence.

a) For QM and AgPL = a: hazard and risk analysis.

b) Additionally, for AgPL = b:

   — safety requirements (functional, technical, hardware, and software) and the adequacy of the level of detail for safety-related functions;

   — safety analyses, e.g. system FMEA, component FMEA.

c) Additionally, for AgPL = c:

   — safety plan;

   — quantitative safety analyses;

   — safety tests and testing scope (validation and verification plan).

d) Additionally, for AgPL = d:

   — safety analyses, e.g. FTA, FMEA;

   — safety tests and testing scope;

   — reference test cases to SRP/CS (safety audit).

e) Additionally, for AgPL = e:

— safety analyses, using analytic techniques such as FMEA and FTA, taking the CCF mechanisms into account;

— safety tests and testing scope (test case review to determine if all cases are included).

Table 1 — Degree of verification independence

Degree of verification independence	QM	AgPL = a	AgPL = b	AgPL = c	AgPL = d	AgPL = e
Review of hazard and risk analysis	U1	U2[a]	U2	U2	U3	U3
Review of safety plan independent of plan author	—	—	—	U1	U2	U3
Review of safety requirements (functional, technical, hardware, and software) independent of author and implementer of safety requirements	—	—	U1	U1	U1	U1
Review of V and V (verification and validation) plan independent of plan author	—	—	—	U1	U2	U2
Review of the safety analysis (e.g. FMEA, FTA) independent of author of analysis independent of developer of UoO	—	—	U1	U1	U1 U2	U1 U3
Review of safety tests and testing scope independent of planning and conducting of the tests	—	—	—	U1	U1	U1
Safety audit independent of those who work in association with the processes required for functional safety	—	—	—	—	U2	U3

— No requirement for verification. The verification measures that will have to be carried out are governed in 7.4.2.

U1 Another person

U2 Another team (not the same direct supervisor)

U3 Another department or third party (independent of the developing department, e.g. independent management, independent resources, independent from release responsibilities, independent organization)

[a] Independent review is required, especially in situations assessed as C0 or S0. See ISO 25119-2.

7.5 Work products

The work products from the assessment of functional safety are the results of the documented verification measures (see ISO 25119-4:2018, Clause 13):

— acceptance;

— conditional acceptance;

— rejection;

— open items;

— responsible persons.

8 Functional safety management activities after start of production (SOP)

8.1 Objectives

The objective of this phase is to define the responsibilities of the persons, departments and organizations responsible for functional safety after SOP. This relates to general activities necessary to ensure the

required level of functional safety for the UoO and to the confirmation measures endorsing that level of functional safety.

8.2 General

See Clause 5.

8.3 Prerequisites

The machine manufacturer shall implement a quality management system.

8.4 Requirements

8.4.1 Management of production and modification procedures

In the life cycle phases following SOP, organizational measures shall be taken in order to achieve the functional safety of all produced units and to maintain it for the life of the machine. The technical requirements for achieving and maintaining functional safety in all produced units for the life of the machine are generally specified during the development of the UoO, and may be modified in accordance with a modification process.

8.4.2 Tasks for preparing and conducting production and end of line inspections

The implementation of requirements for production/installation/adjustment and training of factory staff shall be listed and monitored. In addition, series conformity with respect to safety requirements and documentation shall be checked.

8.4.3 Tasks for safe machine operation, maintenance, repair and decommissioning

The following tasks shall be carried out.

— Draw up and include special content and warnings in the operating instructions.

— List the requirements for maintenance and qualifications for maintenance staff. Monitor the machine manufacturer-executed maintenance.

— List the requirements for repair and qualifications for repair staff. Draw up and include special content in the repair instructions.

— Provide feedback on faults observed.

— List the safety requirements for decommissioning (see ISO 25119-4:2018, Clause 10).

8.5 Work products

The work products from the safety management activities after SOP shall be as follows:

— safety-related content and warnings for operating instructions;

— safety-related content for repair, maintenance, and decommissioning instructions;

— qualification of staff, where required;

— safety-related content of the information made available to the user;

— instructions regarding field observations.

9 Plan for production and installation of safety-related systems

9.1 Objectives

The objectives in this phase are to develop a production and an installation plan for SRS. Another objective is to ensure that the required functional safety is maintained during the production process by the relevant manufacturer or the person/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 information shall be available:

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

— test notes and criteria (documents related to testing procedures and the criteria to be tested for the safety-related functions);

— product release (the release documents for production, testing and installation);

— product monitoring (required for safety-related characteristics and ensuring that the safety-related 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 be drawn up and include the following:

— identification of safety-related components and characteristics;

— sequence and methods of production steps;

— equipment/tools.

9.4.2 Test plan

A test plan taking instructions for testing into account shall be written and shall include the following:

— identification of safety-related components and characteristics;

— sequence and methods of testing steps;

— testing of equipment/tools, test criteria.

9.4.3 Production and testing

Production and testing shall be carried out by suitably qualified staff according to the production and testing plans.

9.4.4 Process capability

Process capability shall be ensured by means of standard industry requirements. Process capability of equipment/tools and testing equipment is also to be ensured by customary industry practices. Testing equipment shall undergo a process of test equipment inspection.

9.4.5 Documentation

The implementation of testing according to the test plan shall be documented. As a minimum, test documentation shall include the following information:

— date of testing;

— tester;

— unique part identification;

— test results, including any deviations of observed from expected behaviour.

9.4.6 Non-compliance

A procedure for non-compliance with a test criterion shall be available. Reworking is permissible only upon proof of process control.

9.4.7 Traceability

Traceability of a given configuration of safety-related parts in a product shall be maintained throughout production.

9.4.8 Storage and transport conditions

Safety-related criteria shall be taken into account when defining the conditions for storing and preparation for transporting the product (see ISO 25119-4:2018, 10.4.7).

9.4.9 Modification

For modifications to the products initiated by production, an impact analysis shall be used to determine the life cycle step to which to return and the steps that are to be repeated (ISO 25119-4:2018, Clause 11).

NOTE For modifications to the process — without modifications to the product — see ISO 25119-4:2018, Clause 9.

9.5 Work products

The work products, if applicable from the production and installation of safety-related systems, shall be:

— documentation of safety-related production plan;

— documentation of safety-related test plan;

— documentation of non-compliance procedure;

— traceability of products for safety-related criteria;

— storing and transport criteria (safety-related).

Annex A
(informative)

Example of the structure of a project-specific safety plan

A.1 General

Title: Project/safety plan ("Project identification").

The author and editor (project manager, project safety manager) for the project plan are appointed by the management at the beginning of the system concept phase.

A.2 Change log

The stipulations in the safety plan are binding on all departments and people involved with implementing the project. This document is not retracted when changed.

Table A.1 presents an example of a change record.

Table A.1 — Change log

No.	Version	Change	Name	Department	Date
1.					
2.					
3.					
…					

A.3 Objective of overall project

A short description of functions with a detailed project objective specification is available.

For cooperation with component suppliers, general conditions are defined and accepted.

A.4 Schedule

Schedules are possible as a link to other schedules or documents.

A.5 Project organization

A.5.1 Project team organization

A link to a project team list is possible.

The project team list presents all involved persons (including customer and subcontractor) with their functions and relationships to one another. Alternatively, the list is included directly in the safety plan (see 6.4.6).

A graphical visualization of the relationship between customer and sub-suppliers is possible.

A.5.2 Project team members

The persons involved in the project and their tasks are named, as shown in Tables A.2 and A.3.

Table A.2 — Project team members

Name	Task	Department	Location	Telephone
	Project manager for the overall project			
	System definition/system specification			
	Person in charge of system analysis			
	Person in charge of hardware development			
	Person in charge of hardware development of sensor system			
	Person in charge of software development			
	Field trials			

Table A.3 — Tasks

Name	Task of person in charge of safety	Qualification	Location	Telephone
	Support the project safety manager	E.g. Experience in project management; refer to team member CV.		
	Project safety manager (like overall project manager) Maintain the safety plan			
	Safety manager on supplier side			
	Contact person at supplier for topic of functional safety			
	Contact person at subcontractor for topic of (functional safety) risk reduction			

A.5.3 Safety management

A.5.3.1 General

The requirements for safety management are included under A.5.3.2 or described in the “Management Guide”, if present, and are applied in a binding manner to this project.

A.5.3.2 Functional safety management activities above the project level

The following activities are assigned to the person in charge of functional safety management:

— ensure the availability of applicable standards;

— audit processes and standard operating procedures;

— monitor and analyse error messages (from the field);

— make comparisons between the calculated failure rate and experience in the field;

— modify and improve processes;

— training schedule;

— train staff for quality management or FSM system;

— initiate safety-related changes.

A.5.3.3 Functional safety management activities related to the project level

The following activities are assigned to the project manager in charge of functional safety management:

— assist in defining the project team;

— define the areas of responsibilities for team members;

— update project templates;

— use project templates;

— assess fault-prevention measures;

— assess fault-detection measures (in FMEA);

— observe test coverage (hardware and software) for module, integration and system tests;

— track the requirements;

— check completed reviews;

— check and fulfil the requirements of this document.

Bibliography

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

[2] ISO 9001, *Quality management systems — Requirements*

[3] ISO 12100, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

[4] IATF 16949, *Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations*

[5] IEC 61000-4-1, *Electromagnetic compatibility (EMC) — Part 4-1: Testing and measurement techniques — Overview of IEC 61000-4 series*

[6] IEC 61496-1, *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests*

[7] *HSE Guidelines on Programmable Electronic Systems in Safety-related Applications,* Part 1 (ISBN 0 11 883906 6) and Part 2 (ISBN 0 11 883906 3)

ICS 65.060.01; 35.240.99

Price based on 23 pages