INTERNATIONAL STANDARD

ISO 25119-1

First edition
2010-06-01

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 25119-1:2010(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 25119-1 was prepared by Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 19, *Agricultural electronics*.

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

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

— *Part 2: Concept phase*

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

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

Introduction

ISO 25119 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising of electrical and/or electronic and/or programmable electronic components (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to municipal equipment. It covers the possible hazards caused by the functional behaviour of E/E/PES safety-related systems, as distinct from hazards arising from the E/E/PES equipment itself (e.g. electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety).

The control system parts of the machines concerned are frequently assigned to provide the critical functions of the *safety-related parts of control systems* (SRP/CS). These can consist of hardware or software, can be separate or integrated parts of a control system, and can either perform solely critical functions or form part of an operational function.

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

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

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

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

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

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

Part 1: General principles for design and development

1 Scope

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

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

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO 25119-3:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 3: Series development, hardware, software*

ISO 25119-4:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: production, operation, modification and supporting processes*

3 Terms and definitions

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

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

NOTE For the purposes of ISO 25119, the performance for each hazardous situation is divided into fives 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 (AgPL) needed to achieve the required functional safety for each safety-related function

3.3
category
classification of the safety-related parts of a control system with respect to its resistance to faults and its subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts and/or by their reliability

3.4
channel
series combination of input, logic, and output elements

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

NOTE Common-cause failures ought not be confused with *common mode failures* (see ISO 12100).

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}
dangerous failure rate of those components where fault detection is realized

3.8
dangerous failure
failure in which an SRP/CS is no longer able to maintain the required performance level, even if the safety-related function is maintained by other (redundant) system components (due to reduction of the resulting performance level)

3.9
dangerous failure rate
λ_d
fraction of all components with dangerous failure per time unit

3.10
diagnostic coverage
DC
fraction of the probability of detected dangerous failures, λ_{dd}, and the probability of total dangerous failures, λ_d, expressed by:

$$DC = \sum \lambda_{dd} / \sum \lambda_d$$

NOTE 1 Diagnostic coverage can exist for the whole or parts of a high-risk functional system, e.g. for sensors and/or logic system and/or final elements.

NOTE 2 The value of DC is defined according to Table 1.

NOTE 3 For SRP/CS consisting of several parts, an average value, DC_{avg}, is used (see ISO 25119-2:2010, Annex C).

Table 1 — Diagnostic coverage (DC)

Denotation	Range
Low	DC < 60 %
Medium	60 % ⩽ DC < 90 %
High	90 % ⩽ DC

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

3.12
E/E/PES-system architecture
allocation of critical 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 item to perform a required function

NOTE 1 Failures which do not affect the availability of the process under control are outside the scope of ISO 25119.

NOTE 2 After a failure, the item will have a fault.

NOTE 3 “Failure” is an event, as distinguished from “fault”, which is a state.

NOTE 4 The concept as defined does not apply to items consisting of software only.

3.16
fault
state of an item characterized 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 A fault is often the result of a failure of the item itself, but may exist without prior failure.

NOTE 2 For the purposes of ISO 25119, a fault is a *random* fault.

3.17
function
defined behaviour of one or more electronic control units

3.18
functional concept
basic functions and interactions necessary to achieve a desired behaviour

NOTE It is developed during the concept phase of the safety life cycle.

3.19
functional requirement
requirement for an intended function of the E/E/PES system

3.20
functional safety
system that performs in a way that does not present an unreasonable risk of injury to operators or bystanders

3.21
functional safety concept
entire collection of safety-related functions and interactions necessary to achieve a desired behaviour

NOTE It is developed during the concept phase of the safety life cycle.

3.22
functional safety requirement
requirement for a safety-related function of the E/E/PES system

3.23
hardware safety requirement
requirement that applies to safety-related hardware and which is included as an element of a technical safety requirement

3.24
harm
physical injury

3.25
hazard
potential source of harm

3.26
hazardous situation
circumstance in which a person is exposed to a hazard or hazards, exposure 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 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 safety-related parts of the control system used to manually restore one or more safety-related functions before restarting the machine

3.31
manufacturer
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 municipal equipment

cf. **supplier** (3.50)

3.32
mean time to dangerous failure
$MTTF_d$
average value of the expected time to a dangerous failure

NOTE 1 It is defined by the ranges low, medium and high. See Table 2.

NOTE 2 For the purposes of ISO 25119, it is important that $MTTF_d$ be taken into account for each channel of an SRP/CS individually ($MTTF_{dC}$).

NOTE 3 $MTTF_d$ is the reciprocal value of λ_d.

Table 2 — Mean time to dangerous failure

Denotation	Range
Low	3 years < $MTTF_d$ < 10 years
Medium	10 years < $MTTF_d$ < 30 years
High	$MTTF_d$ > 30 years

3.33
monitoring
automatic monitoring
automatic function which ensures that a protective measure is initiated if the ability of a component or an element to perform its 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 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

3.39
risk
combination of the probability of occurrence of harm and the severity 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 and risk evaluation

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

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

NOTE 1 It is the top level safety requirement, derived from the hazard analysis and risk assessment.

NOTE 2 The existence of several safety goals for one item is possible.

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 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
measure of the most likely degree of harm to an endangered individual

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

NOTE 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

3.50
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

cf. **manufacturer** (3.31)

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

NOTE 1 Corrective maintenance without modification will usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

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

3.53
technical safety concept
entire collection of technical safety requirements necessary to implement the functional safety concept and to partition it on the system architecture

NOTE 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

3.55
unit of observation
electrical, electronic, electrically-programmable system or function

NOTE The unit of observation can encompass safety-related function(s) that may be distributed across multiple systems.

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

NOTE 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
EUC	equipment under control
FMEA	failure mode and effects analysis
FMECA	failure mode effects and criticality analysis
EPROM	erasable programmable read-only memory
FSM	functional safety management
FTA	fault tree analysis
HAZOP	hazard and operability study
HIL	hardware in the loop
MTTF	mean time to failure
$MTTF_d$	mean time to dangerous failure
$MTTF_{dC}$	mean time to dangerous failure for each channel
PES	programmable electronic system
QM	quality measures
RAM	random-access memory
SOP	start of production
SRL	software requirement level
SRP	safety-related parts

SRP/CS safety-related parts of control systems

SRS safety-related system

5 Management during complete safety life cycle

5.1 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 item, 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 should 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 addresses only the evaluation of the safety aspects of the E/E/PES.

5.2 General

5.2.1 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.

5.2.2 External functional safety measures

These measures cannot be influenced by the unit of observation described in the system definition. External functional safety includes the characteristics of involved persons (physical, language, etc.) or of the environment. It is described in the system definition. In risk analysis, consideration can be given to external functional safety.

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

NOTE 2 Other technologies such as mechanics and hydraulics are not taken into consideration by ISO 25119. These are included in the assessment of functional safety. Verification of the functional safety of these technologies is not within the scope of ISO 25119.

5.3 Prerequisites

The necessary prerequisites are a proven quality assurance plan (e.g. ISO/TS 16949 or equivalent) and an overall project plan.

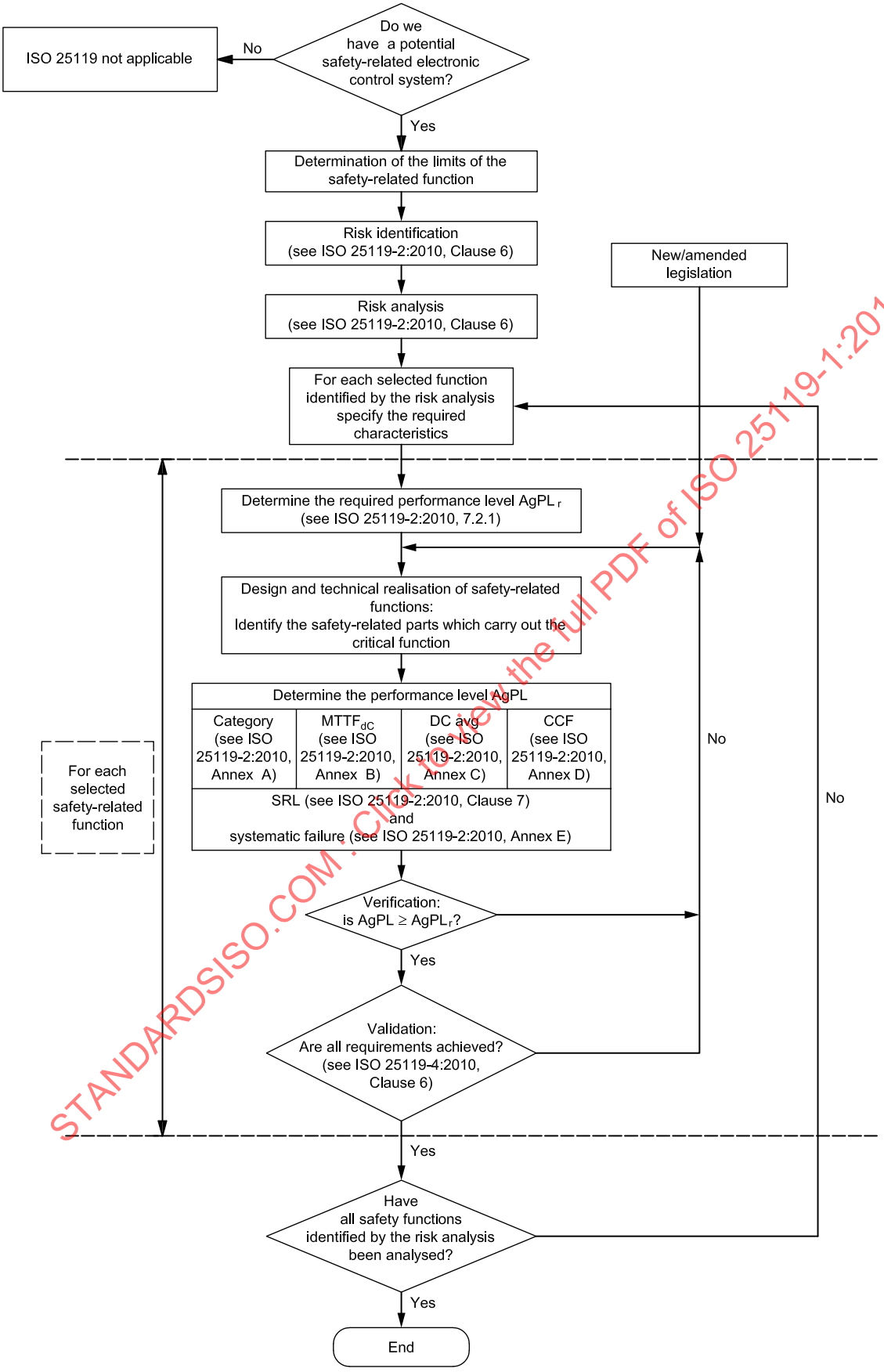
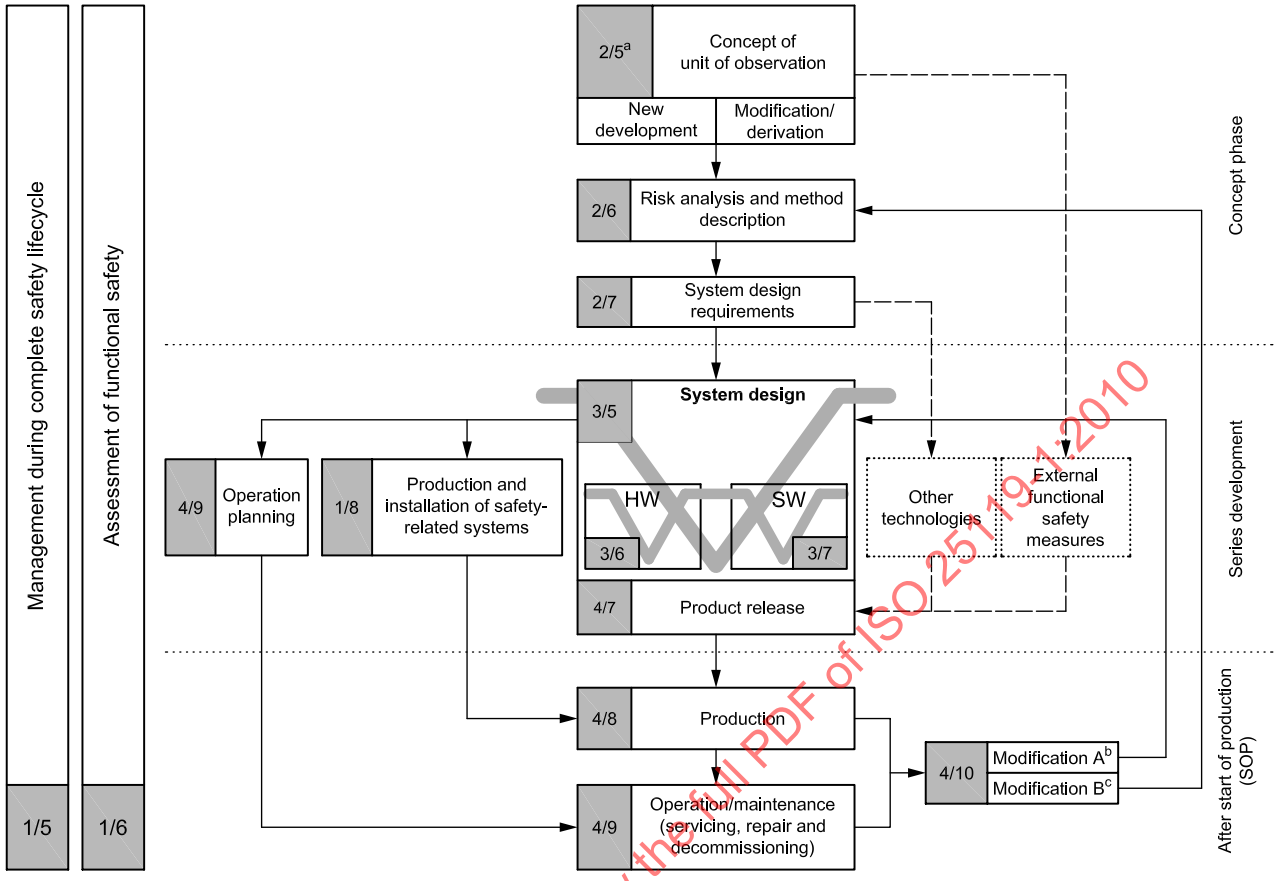


Figure 1 — Iterative process for design of safety-related parts of control systems



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 25119-2:2010, Clause 5.

b If machine functions are *not* affected, then go to ISO 25119-3:2010, Clause 5.

c If machine functions *are* affected, then carry out hazard and risk analysis according to ISO 25119-2:2010, Clause 6.

Figure 2 — Safety life cycle

5.4 Requirements — Functional safety management activities across safety life cycle

5.4.1 Functional safety culture

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

5.4.2 Continuous improvement

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

— the creation of company-specific procedures to fulfil the requirements of ISO 25119,

— 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.

5.4.3 Training and qualification

Performing the tasks in the safety life cycle requires appropriately qualified staff. The aim should 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.

5.4.4 Safety management during development

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

5.4.5 Assignment of safety responsibilities

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

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 unit of observation. Appropriately qualified individuals can also carry out multiple tasks. In particular, it is possible that tasks will be performed by appropriately qualified developers.

5.4.6 Assignment of tasks

The following is an outline of functional safety essential tasks.

Functional safety management tasks are 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.

5.4.7 Planning of all safety management activities during development

5.4.7.1 General

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;

— ensuring sufficient qualification of persons and organizational entities when assigning and delegating safety activities;

— specification of safety responsibilities between development partners;

— provision for establishment of supporting processes within the project;

— conducting risk analysis according to ISO 25119-2:2010, Clause 6;

— implementation of safety requirements in the context of development activities according to ISO 25119-2:2010, Clause 7, and ISO 25119-3:2010, Clauses 6 and 7;

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

— planning of the verification and validation of safety requirements according to ISO 25119-4:2010, Clause 6;

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

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

5.4.7.2 Writing safety documentation

Safety documentation shall be written in such a way that others can understand the process that was followed. The documentation shall be retained in accordance with company document retention policy.

5.4.7.3 Safety plan

5.4.7.3.1 Objectives

The safety plan is used for the systematic planning and allocation of resources required for safety-related activities. The scope of consideration is described in the system definition, taking the entire life cycle into consideration.

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.

The safety plan is written by the product safety manager, and put into effect by the project manager.

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

5.4.7.3.2 Contents of the safety plan

The safety plan should include all activities that are specified in the life cycle, supporting activities, assessment, and management activities. A more detailed subdivision can be made if required.

Safety-related activities are described in the safety plan. In doing so, it is worthwhile to describe the following characteristics of an activity:

— objective(s);

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

— person in charge;

— necessary resources;

— duration, deadline;

— documentation of results.

5.4.7.3.3 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 shall be subject to version and change management.

5.4.7.4 Tailoring activities within processes (to AgPL)

The characteristic of all activities is always dependent on the AgPL and functional 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.

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

5.4.7.5 Verification of functional safety

Activities for ensuring functional safety shall include the safety audit, safety review and safety assessment as set out in Table 3.

Table 3 — Verification measures — Safety audit, safety review and safety assessment

Verification measure	Audit	Review	Assessment
Subject	Implementation of the processes required for functional safety	Result of a specific safety-related activity (see review points in Table 4)	Entire unit of observation, described in the “system definition” phase
Scope and depth	Set by the auditor	Planned before performing review	Scope is complete verification of all processes and technical measures required for functional safety Depth is determined by the assessor
To be performed in life cycle	During the implementation of the required processes and before the completion of each activity	After completion of each safety-related activity	In parallel with development, or in a block Completion prior to series release
Responsibility	For verifying the processes sufficiently	For proper implementation of review	Takes joint responsibility for functional safety
Result	Audit report (can be part of an assessment)	Review protocol (can be part of an assessment)	Statement on the functional safety of the unit of observation

5.5 Work products

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

— verification measures — process instruction for auditing the processes during series development;

— safety plan.

6 Assessment of functional safety

6.1 Objectives

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

6.2 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. The assessment should cover 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 organizational units involved in the development of the unit of observation. The involved organizational units should disclose all relevant assessment documents to the machine manufacturer/supplier or to the person in charge.

6.3 Prerequisites

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

— the person responsible for the system;

— the system developer;

— the expert(s) on functional safety.

The result of the safety assessment should be documented. Documentation should be retained in accordance with the manufacturer document retention policy and any relevant legal requirements.

6.4 Requirements

6.4.1 Considerations for the assessment of the functional safety

These consist of the following requirements.

a) The management requirements for verification measures listed in 6.4.2 shall be observed.

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 unit of observation.

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.

6.4.2 Verification

The following requirements apply to verification.

Verification measures shall be included in the safety plan. The unit of observation as well as the form of the result shall be defined. The independence of those performing verification shall be documented.

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

Reviews, audits and assessments shall be carried out with reference to the AgPL. The following activities shall be reviewed.

a) Starting with AgPL = a: hazard and risk analysis.

b) Additionally, with AgPL = b:

— safety requirements, level of detail for safety-related functions;

— safety analyses — system FMEA, component FMEA.

c) Additionally, with AgPL = c:

— safety plan;

— quantitative safety analyses;

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

d) Additionally with AgPL = d:

— safety requirements — SRS;

— safety analyses, e.g. FTA, FMEA;

— safety tests and testing scope — reference test cases to safety-related system (SRS);

— safety audit;

— assessment of functional safety.

e) Additionally with 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).

The degree of verification depends on the AgPL level (see Table 4).

Table 4 — Degree of verification

Degree of verification	AgPL = a	AgPL = b	AgPL = c	AgPL = d	AgPL = e
Review of hazard analysis and risk assessment	U2[a]	U2	U2	U3	U3
Review of safety plan independent of plan author	—	—	U1	U2	U3
Review of safety requirements independent of author and implementer of safety requirements	—	U1	U1	U1	U1
Review of V & V (verification and validation) plan independent of plan author	—	—	U1	U2	U2
Review of the safety analysis (FMEA, FTA) independent of author of analysis independent of developer of unit of observation	—	U1	U1	U1 U2	U1 U3
Review of safety tests and trials independent of planning and conducting of the tests	—	—	U1	U1	U1
Review of safety documentation independent of plan author	—	—	U1	U2	U3
Safety audit independent of those who work in association with the processes required for functional safety	—	—	—	U2	U3
Assessment of safety plan	—	—	—	U2	U3

— No requirement for verification. The verification measures that will have to be carried out are governed in 6.4.2.

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.

6.5 Work products

The work products from the assessment of functional safety comprise the document verification measures:

— acceptance;

— conditional acceptance;

— rejection;

— open items;

— responsible persons.

7 Safety management activities after start of production (SOP)

7.1 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 item and to the confirmation measures endorsing that level of functional safety.

7.2 General

See Clause 5.

7.3 Prerequisites

The manufacturer should implement a quality management system.

7.4 Requirements

7.4.1 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 unit of observation, and may be modified in accordance with a modification process.

7.4.2 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.

7.4.3 Tasks for safe machine operation and decommissioning

The following tasks shall be carried out.

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

— List requirements for maintenance and manufacturer maintenance staff, and monitor their implementation.

— Provide feedback on faults observed.

— List safety requirements for decommissioning (see ISO 25119-4:2010, Clause 9).

— In the quality management system, consider attaching milestones to the V model (see ISO 25119-3:2010, Figure 1).

— A verification measure shall exist for every phase of the V model.

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

7.5 Work products

The work products from the safety management activities after SOP are special content and warnings for operating instructions.

8 Production and installation of safety-related systems

8.1 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 product manufacturer or the person/organization in charge of the process (machine manufacturer, supplier, sub-supplier, etc.).

8.2 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.

8.3 Prerequisites

The following information should 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.

8.4 Requirements

8.4.1 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.

8.4.2 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.

8.4.3 Production and testing

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