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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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:

$$\mathrm{DC} = \sum \lambda_{\mathrm{dd}} \Big/ \sum \lambda_{\mathrm{d}}$$

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$_{\mathrm{avg}}$, 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 ($\mathrm{MTTF}_\mathrm{dC}$).

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.