INTERNATIONAL STANDARD

ISO 25119-2

First edition
2010-06-01

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

Part 2: Concept phase

Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité —
Partie 2: Phase de projet

Reference number
ISO 25119-2:2010(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 25119-2 was prepared by Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 19, *Agricultural electronics*.

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

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

— *Part 2: Concept phase*

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

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

Introduction

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

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

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

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

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

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

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

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

Part 2: Concept phase

1 Scope

This part of ISO 25119 specifies the concept phase of the 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).

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 25119-1:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 25119-1 apply.

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

ADC analogue to digital converter

AgPL agricultural performance level

$AgPL_r$ required agricultural performance level

CAD	computer-aided design
Cat	hardware category
CCF	common-cause failure
CRC	cyclic redundancy check
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 Concept — Unit of observation

5.1 Objectives

The objective of this phase is to develop an adequate understanding of the unit of observation in order to satisfactorily complete all of the tasks defined in the safety life cycle. On the basis of the chosen safety concept, a suitable method should be used to determine the required performance level. Suitable methods include risk analysis (described below), other standards, legal requirements and test body expertise.

5.2 Prerequisites

The necessary prerequisites are a description of the unit of observation, its interfaces, already-known safety and reliability requirements and the scope of application

5.3 Requirements

5.3.1 Unit of observation and ambient conditions

A safety-related concept shall include the following:

a) the scope, context and purpose of the unit of observation;

b) functional requirements for the unit of observation;

c) other requirements regarding the unit of observation and ambient conditions, including

— technical or physical requirements, e.g. operating, environmental and surrounding conditions and constraints, and

— legal requirements, especially safety-related legislation, regulations and standards (national and international);

d) historical safety and reliability requirements and the level of safety and reliability achieved for similar or related units of observation.

5.3.2 Limits of unit of observation and its interfaces with other units of observation

The following information shall be considered in order to gain an understanding of the operation of the unit of observation in its environment:

— the limits of the unit of observation;

— its interfaces and interactions with other units of observation and components;

— requirements regarding other units of observation;

— mapping and allocation of relevant functions to involved units of observation.

5.3.3 Sources of stress

The sources of stress which could affect the safety and reliability of the unit of observation shall be determined, including the following:

— the interaction of different units of observation;

— hazards of a physical or chemical nature (energy content, toxicity, explosiveness, corrosiveness, reactivity, combustibility, etc.);

— other external events [temperature, shock, electromagnetic compatibility (EMC), etc.];

— reasonable foreseeable human operating errors;

— hazards originating from the unit of observation, and events triggering failure (e.g. during assembly or maintenance).

5.3.4 Additional determinations

In addition to the activities described in 5.3.2, the following determinations or actions shall be implemented:

— determination as to whether the unit of observation is a new development or a modification, adaptation or derivative of an existing unit of observation and, in the case of modification, the carrying out of an impact analysis to adjust the safety life cycle accordingly;

— preparing a plan and a specification to validate the requirements regarding the unit of observation defined in 5.3.1;

— definition of project management for the appropriate phases in the life cycle;

— adequate input data for the reliability assessment;

— adequate procedures and application of tools and technologies;

— utilization of qualified staff.

5.4 Work products

The work products of the concept/definition of the unit of observation are

a) the unit of observation and ambient conditions,

b) limits of the unit of observation and its interfaces with other units of observation,

c) sources of stress, and

d) additional determinations.

6 Risk analysis and method description

6.1 Objectives

Risk is defined (see ISO 25119-1:2010, definition 3.39) as the combination of the probability of occurrence of harm and the severity of that harm.

When considering the frequency of the occurrence of harm, as a rule, the probability of being exposed to a hazardous situation is taken into account.

When considering systems, the possibility that the operator will react in many cases to avoid harm is generally to be taken into account.

The procedure described below provides one appropriate methodology for determining the $AgPL_r$.

6.2 Prerequisites

There are no prerequisites for this phase.

6.3 Requirements

6.3.1 Procedures for preparing a risk analysis

If a risk analysis method is performed, it shall take account of information defining the overall scope of the application. If decisions are made later in the safety life cycle that change the basis on which earlier decisions were made, a new risk analysis shall be carried out.

The architecture of the SRP/CS shall not be considered as part of the risk analysis.

6.3.2 Tasks in risk analysis

The operating conditions in which the unit of observation can initiate hazards when correctly used (including reasonable foreseeable human operating errors and part failures) shall be considered.

6.3.3 Participants in risk analysis

The risk analysis shall involve several individuals from different departments, e.g. electronic or electrical development, testing or validation, machine or hydraulics design, service, or external consultants (e.g. technical inspection authority).

6.3.4 Assessment and classification of a potential harm

Potentially harmful effects can be deduced by considering possible malfunctions and systematic failures in relevant operating conditions. The potential severity of harm is described as precisely as possible for each relevant scenario.

A certain categorization shall be used in the description of the harms. For this reason, a classification of the severity of harm is presented in four categories: S0, S1, S2 and S3 (see Table 1).

The operator of the involved machine and other parties (e.g. people lending assistance, other operators of machinery, bystander, etc.) shall be used in a detailed description of the harm.

An examination of risk for safety functions is focused on the origin of injuries to people. If in the analysis of potential harm it can be established that damage is clearly limited to property and does not involve injury to people, this would not be cause for classification as a safety-related function. The introduction of an S0 harm classification allows for this fact. No advanced risk assessment need be carried out for functions assigned to harm class S0.

Table 1 — Examples of the descriptions of injuries

S0	S1	S2	S3
No significant injuries, requires only first aid	Light and moderate injuries, requires medical attention, total recovery	Severe and life-threatening injuries (survival probable), permanent partial loss in work capacity	Life-threatening injuries (survival uncertain), severe disability

6.3.5 Assessment of exposure in the situation observed

A risk analysis reflects the effects of possible failures in specific regional working and operating conditions. These situations range from daily routine activities to extreme, rare situations. The variable “E” shall be used to categorize the different frequencies or duration of exposure. Five categories, designated E0, E1, E2, E3 and E4, are used (see Table 2), where “E” serves as an estimation of how often and how long an operator or bystander is exposed to a hazard where a failure could result in an injury to the operator or bystander. The exposure for a given situation is determined by frequency and duration, and the highest of these evaluations shall be used in the determination of $AgPL_r$.

NOTE A hazard can be a combination of conditions (e.g. environmental and/or operational) of the machine.

Table 2 — Exposure to the hazardous event

Description	E0	E1	E2	E3	E4
Definition of frequency	Improbable (theoretically possible; once during lifetime)	Rare events (less than once per year)	Sometimes (more than once per year)	Often (more than once per month)	Frequently (almost every operation)
Definition of duration $\frac{t_{exp}}{t_{av\,op}}$	< 0,01 %	0,01 % to 0,1 %	0,1 % to 1 %	1 % to 10 %	> 10 %
t_{exp} exposure time $t_{av\,op}$ average operating time					

6.3.6 Assessment of a possible avoidance of harm

Assessing possible avoidance of harm involves appraising whether or not the properly trained operator of the machine has control over the dangerous situation that could arise and can avoid it, or if the situation is completely uncontrollable. Even the bystander can himself avoid a harmful situation. In turn, four classifications have been set up by which the avoidance of harm can be rated. The rating for a possible avoidance of harm assumes only the function *without* additional safety precautions (avoidance of harm beyond the technical system). The classifications C0, C1, C2 and C3 represent "easily controllable", "simply controllable", "mostly controllable" and "none" (see Table 3).

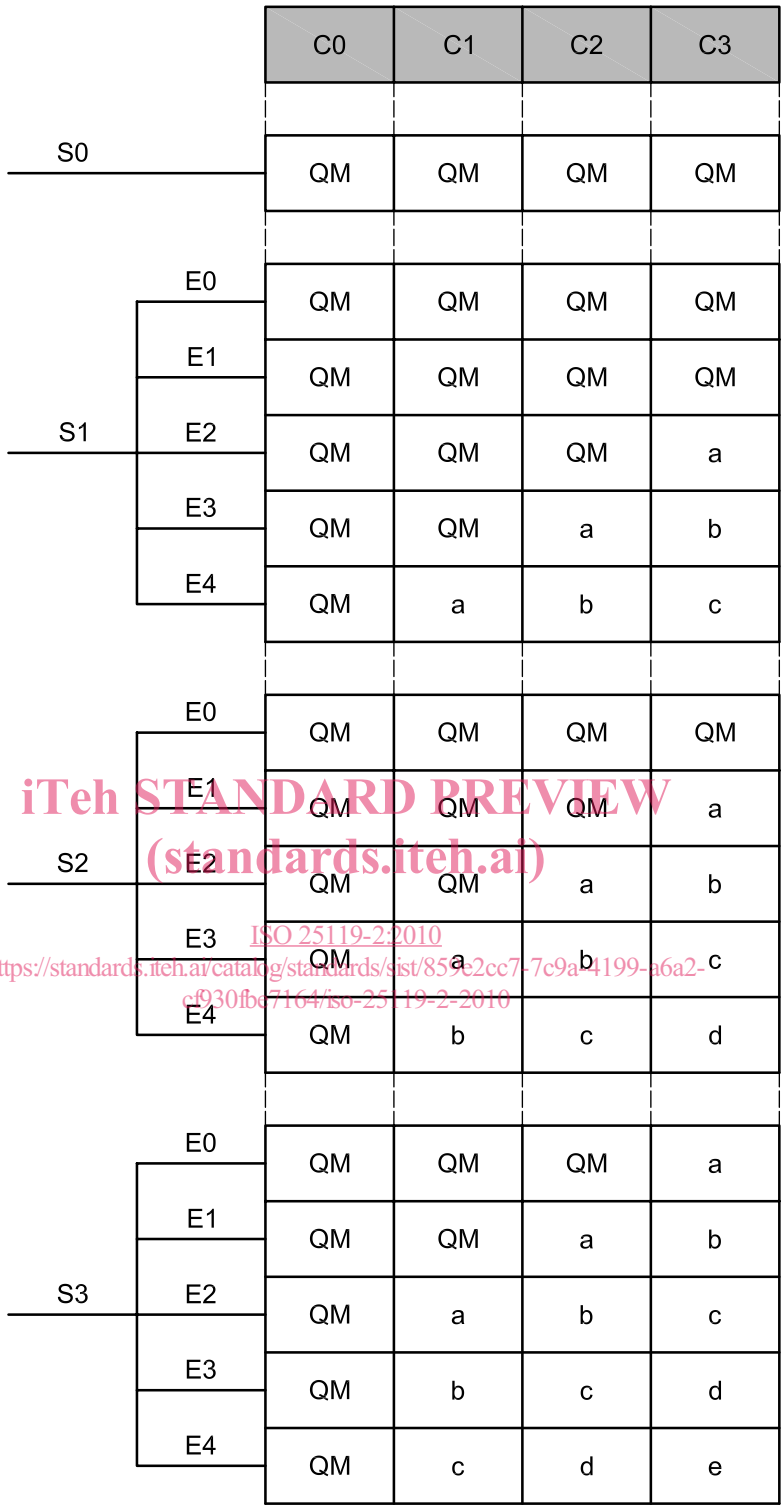
Table 3 — Possible avoidance of harm

C0	C1	C2	C3
Easily controllable The operator or bystander controls the situation, and harm is avoided.	Simply controllable More than 99% of people control the situation. In more than 99% of the occurrences, the situation does not result in harm.	Mostly controllable More than 90% of people control the situation. In more than 90% of the occurrences, the situation does not result in harm.	None The average operator or bystander cannot generally avoid the harm.

6.3.7 Selecting the required $AgPL_r$

The required $AgPL_r$ is illustrated in Figure 1 by combining the severity, exposure, and controllability values for each identified hazard.

The required $AgPL_r$ are designated from AgPL = a to AgPL = e. AgPL = a has the lowest system requirements and AgPL = e has the highest system requirements. In addition to these levels, there is a quality measure designation, QM, whose implicit requirement is to carry out system development in accordance with standards like ISO 9001. A function classified as QM shall not be considered as a safety-related function.



Key

S	severity
E	exposure to hazardous event
C	controllability
QM	quality measures
a, b, c, d, e	required agricultural performance level ($AgPL_r$)

Figure 1 — Determination of AgPLr