SLOVENSKI STANDARD
oSIST prEN ISO 25119-2:2017

01-marec-2017

Traktorji ter kmetijski in gozdarski stroji - Varnostni deli krmilnih sistemov - 2. del: Faza koncepta (ISO/DIS 25119-2:2017)

Tractors and machinery for agriculture and forestry - Safety-related parts of control systems - Part 2:Concept phase (ISO/DIS 25119-2:2017)

Tracteurs et matériels agricoles et forestiers - Parties des systèmes de commande relatives à la sécurité - Partie 2: Phase de projet (ISO/DIS 25119-2:2017)

Ta slovenski standard je istoveten z: prEN ISO 25119-2

ICS:

35.240.68	Uporabniške rešitve IT v kmetijstvu	IT applications in agriculture
65.060.01	Kmetijski stroji in oprema na splošno	Agricultural machines and equipment in general

oSIST prEN ISO 25119-2:2017 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 25119-2

ISO/TC **23**/SC **19** Secretariat: **DIN**

Voting begins on: **2017-01-04**

Voting terminates on: **2017-03-28**

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

ICS: 35.240.99; 65.060.01

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 25119-2:2017(E)

COPYRIGHT PROTECTED DOCUMENT

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

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 *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems* consists of the following parts:

— *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 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 municipal equipment.

A prerequisite to the application of ISO 25119 is the completion of a suitable hazard identification and risk analysis (e.g. ISO 12100) for the entire machine. As a result, 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 may 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 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 part of ISO 25119 is a type-B1 standard as stated in EN ISO 12100.

For machines which are covered by the scope of a machine specific type-C standard and which have been designed and built according to the provisions of that standard, the provisions of that type-C standard take precedence over the provisions of this type-B standard.

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 may also be applied to municipal equipment (e.g. street-sweeping machines).

This part of ISO 25119 is not applicable to:

— aircraft and air-cushion vehicles used in agriculture,

— lawn and garden equipment.

This part of ISO 25119 specifies the characteristics and categories required of SRP/CS for carrying out their safety-related 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-related functions or performance levels are to be used for particular machines. 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 protection measures, safeguards, or safety-related functions in response to non-E/E/PES hazards.

Examples included in scope:

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

— electromagnetic interference with the SRP/CS, and

— SRP/CS's designed to prevent fire.

Examples not included in scope:

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

— nominal electromagnetic radiation impacting nearby machine control systems, and

— corrosion causing electric cables to overheat.

Machine specific standards (type-C standards) can identify performance levels and/or categories or they should be determined by the manufacturer of the machine based on risk assessment.

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

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

2 Normative references

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

ISO 25119-1:2014, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

ISO 25119-3:2014, *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 25119-1:2014 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 (see ISO 25119-1:2014, Figure 2). On the basis of the chosen safety concept, a suitable method shall be used to determine the required performance level. Suitable methods include risk analysis (described below), other standards, legal requirements and test body expertise or a combination of these.

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;

— utilisation 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 Hazard and risk analysis method description

6.1 Objectives

Risk analysis provides information required for the risk evaluation, which in turn allows judgments to be made about whether or not risk reduction is required. Risk is defined (see ISO 25119-1:2014, 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 in 6.2 through 6.4 provides guidance for determining the $AgPL_r$.

6.2 Prerequisites

Definition of the unit of observation

6.3 Requirements

6.3.1 Procedures for preparing a risk analysis

The risk analysis shall take into account the overall scope of the application. If decisions are made later in the safety life cycle changing the scope of application, 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 shall be described as precisely as possible for each relevant scenario.

A certain categorisation shall be used in the description of the harm. 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-related 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 categorise 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 most appropriate should be used for 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 a typical machine operator, trained if practicable, has control over the dangerous situation that could arise and can avoid it, or if the situation is completely uncontrollable. Even a bystander can 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 typical 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 EN ISO 9001. A function classified as QM shall not be considered as a safety-related function because the risk analysis has defined the risk as sufficiently low.

		C0	C1	C2	C3
S0	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
S1	E2	QM	QM	QM	a
	E3	QM	QM	a	b
	E4	QM	a	b	c
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	a
	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	QM	b	c	d
S3	E0	QM	QM	QM	a
	E1	QM	QM	a	b
	E2	QM	a	b	c
	E3	QM	b	c	d
	E4	QM	c	d	e

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

NOTE See 6.3.7 for description of QM

6.4 Work products

The work product of hazard and risk analysis is the AgPLr for the safety functions".

7 Specification of system design requirements

7.1 Objectives

Derived from the results of the previous phases, the objectives of the requirements of this phase are to define design requirements.

7.2 Prerequisites

Results of hazard and risk analysis.

7.3 Requirements

7.3.1 Assignment of AgPL

An AgPL shall be assigned to each identified hazard within the safety-related function analysed. The AgPL with the highest rating shall define the $AgPL_r$ of the safety-related function.

Various combinations of reliability and architecture may be used to achieve the required $AgPL_r$. For example, it is possible (within certain limits) for a single-channel architecture of high reliability to provide the same or higher performance level as a dual-channel architecture of lower reliability (see Figure 2).

The agricultural performance level of a safety-related control system is a function of the following four aspects:

— category (see Annex A);

— $MTTF_{dC}$ (see Annex B);

— DC (see Annex C);

— SRL (see ISO 25119-3:201x, Clause 7).

Additionally, the following items shall be considered during system design:

— CCF for categories 3 and 4 architectures (see Annex D);

— systematic failure (see Annex E);

— the ability to perform a safety-related function under expected environmental conditions (such as those set out in ISO 15003);

— other typical functions (see Annex F).

An example risk assessment and resulting $AgPL_r$ is given in Annex G.