INTERNATIONAL STANDARD

ISO 25119-2

Second edition
2018-10

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 25119-2:2018(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

This second edition cancels and replaces the first edition (ISO 25119-2:2010), which has been technically revised. The main changes compared to the previous edition are as follows:

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

— Table 2 has been modified to specify exact values;

— Clauses 6 and 7 have been revised;

— new tables (Tables 4 and 5) have been added to indicate values of DC and $MTTF_D$;

— Figure 2 has been replaced;

— normative Annexes H and J have been added;

— informative Annex I has been added;

— the document has been editorially revised.

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

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

Introduction

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

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

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

ISO 25119 (all parts) allocates the ability of safety-related parts to perform a safety-related function under foreseeable conditions into five performance levels. The performance level of a controlled channel depends on several factors, 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 that can cause E/E/PES malfunctions leading to potential hazardous situations are considered: systematic, common-cause and random.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Part 2: Concept phase

1 Scope

This document 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 mobile municipal equipment (e.g. street-sweeping machines).

This document is not applicable to:

— aircraft and air-cushion vehicles used in agriculture;

— lawn and garden equipment.

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

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

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

Examples included within the scope of this document:

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

— electromagnetic interference with the SRP/CS;

— SRP/CS's designed to prevent fire.

Examples not included within the scope of this document:

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

— nominal electromagnetic radiation impacting nearby machine control systems;

— corrosion causing electric cables to overheat.

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

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

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

2 Normative references

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

ISO 25119-1:2018, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 1: General principles for design and development*

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

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

3 Terms and definitions

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

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

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

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

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
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
FMEA	failure mode and effects analysis
EPROM	erasable programmable read-only memory
FTA	fault tree analysis
HARA	hazard analysis and risk assessment

HIL	hardware in the loop
MTTF	mean time to failure
$MTTF_D$	mean time to dangerous failure
$MTTF_{DC}$	mean time to dangerous failure for each channel
PES	programmable electronic system
QM	quality measures
RAM	random-access memory
SOP	start of production
SRL	software requirement level
SRP/CS	safety-related parts of control systems
UoO	unit of observation

5 Concept — UoO

5.1 Objectives

The objective of this phase is to develop an adequate understanding of the UoO in order to satisfactorily complete all of the tasks defined in the safety life cycle (see ISO 25119-1:2018, Figure 2). For each UoO, 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 safety-related function to be provided by the UoO, its interfaces, already-known safety and reliability requirements and the scope of application.

5.3 Requirements

5.3.1 Basic requirements and ambient conditions

The following information shall be available for the safety-related function of the UoO:

a) the scope, context, purpose and known elements;

b) functional requirements;

c) other requirements and ambient conditions that should be taken into account include:

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

   — 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 UoO.

5.3.2 Limits of UoO and its interfaces with other UoO

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

— the limits of the UoO;

— its interfaces and interactions with other UoO and components;

— requirements for the safety-related functions related to other UoO.

5.3.3 Mapping and allocation of relevant functions to involved UoO, sources of stress

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

— the interaction of different UoO;

— stresses 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;

— stresses originating from the UoO, 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 UoO is a new development or a modification, adaptation or derivative of an existing UoO 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 verify and validate the requirements regarding the UoO 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 suitably qualified staff.

5.4 Work products

The work products if applicable of the UoO shall be:

a) elements included within the UoO;

b) specification of the basic requirements and ambient conditions;

c) limits of the UoO and its interfaces with other UoO;

d) sources of stress;

e) additional determinations.

6 HARA — Determination of the $AgPL_r$

6.1 Objectives

The main objectives are to analyse risks associated with a faulted UoO (one not performing safety-related functions as intended, such as not stopping properly, propelling while in neutral, steering in the wrong direction) and then, assign an appropriate $AgPL_r$. Risk is defined as the combination of the probability of occurrence of harm and the severity of that harm (ISO 25119-1:2018, 3.39). When considering the probability of the occurrence of harm, when appropriate, the probability of being exposed to a hazardous situation with a faulted UoO can be taken into account.

The procedure described in 6.2 to 6.4 provides guidance for determining the $AgPL_r$ based on the HARA.

6.2 Prerequisites

The UoO definition associated with each safety-related function.

6.3 Requirements

6.3.1 Procedures for preparing a HARA

The HARA shall take into account the entire safety-related function so that an appropriate specification for the SRP/CS can be provided. If decisions are made later in the safety life cycle changing the scope of application, the HARA shall be reworked accordingly. To identify the changes and their impacts on the work products, an impact analysis shall be carried out in accordance with ISO 25119-4

6.3.2 Tasks in the HARA

The operating conditions, in which the malfunctioning behaviour of the UoO will result in hazardous situations, when correctly used and when incorrectly used in a reasonably foreseeable way, shall be taken into account.

6.3.3 Participants in HARA

The HARA shall involve sufficient people to ensure that all relevant expertise is available.

NOTE Involving individuals from different disciplines often provides valuable input to the HARA.

6.3.4 Classification of a potential harm

The potential severity of harm shall be determined and documented.

Potentially harmful effects shall be deduced by considering all hazardous situations resulting from malfunctions of the safety-related function in relevant operating conditions, modes and situations.

A categorization 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 actions of the operator of the involved machine and bystanders (e.g. people lending assistance, other operators of machinery, other traffic participants, etc.) shall be taken into account and their exposure to harm documented.

The objective of the assessment and classification of a potential harm shall be focused on and limited to harm to people. If the analysis of the malfunction of the safety-related function is clearly limited to property and does not involve harm to people, then these malfunctions need not be classified as safety-related.

No advanced risk assessment need be carried out for functions assigned to harm class S0.

Table 1 — Classification of injuries

S0	S1	S2	S3
No injuries, damage limited to property	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 Classification of exposure in the situation observed

A HARA shall take into account the exposure effects of possible malfunctions of the safety-related function in all specific relevant 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 harm to the operator or bystander. The most appropriate method for each hazardous situation, frequency or duration, shall be used for the determination of $AgPL_r$. When more than one category is determined to be appropriate for a particular hazardous situation, the method returning the highest category shall be used.

NOTE A hazard capable of producing harm can result from a combination of machine conditions (e.g. environmental and/or operational).

Table 2 — Classification of Exposure to the hazardous situation

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 $\frac{t_{exp}}{t_{av\,op}}$	Less than 0,01 %	0,01 % to less than 0,1 %	0,1 % to less than 1 %	1 % to less than 10 %	greater than or equal to 10 %

t_{exp} exposure time.

$t_{av\,op}$ average operating time.

6.3.6 Classification of a possible avoidance of harm

Assessing possible avoidance of harm involves appraising whether a typical trained machine operator has a level of control over the harm that could arise and can avoid it or, the situation is completely uncontrollable. Similarly, an untrained bystander may have a level of control to avoid a harmful situation. The variable C shall be used to classify the ability to avoid harm. The value of C for a possible avoidance of harm shall consider only the ability of persons to avoid the harm following the malfunction of the safety-related function and shall not take into account the reliability or any measures provided in the SRP/CS which mitigate risk in the event of a malfunction. The classifications C0, C1, C2 and C3 represent "easily controllable", "simply controllable", "mostly controllable" and "none" (see Table 3).

Table 3 — Classification of 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 trained operator or bystander cannot generally avoid the harm.

6.3.7 Selecting the $AgPL_r$

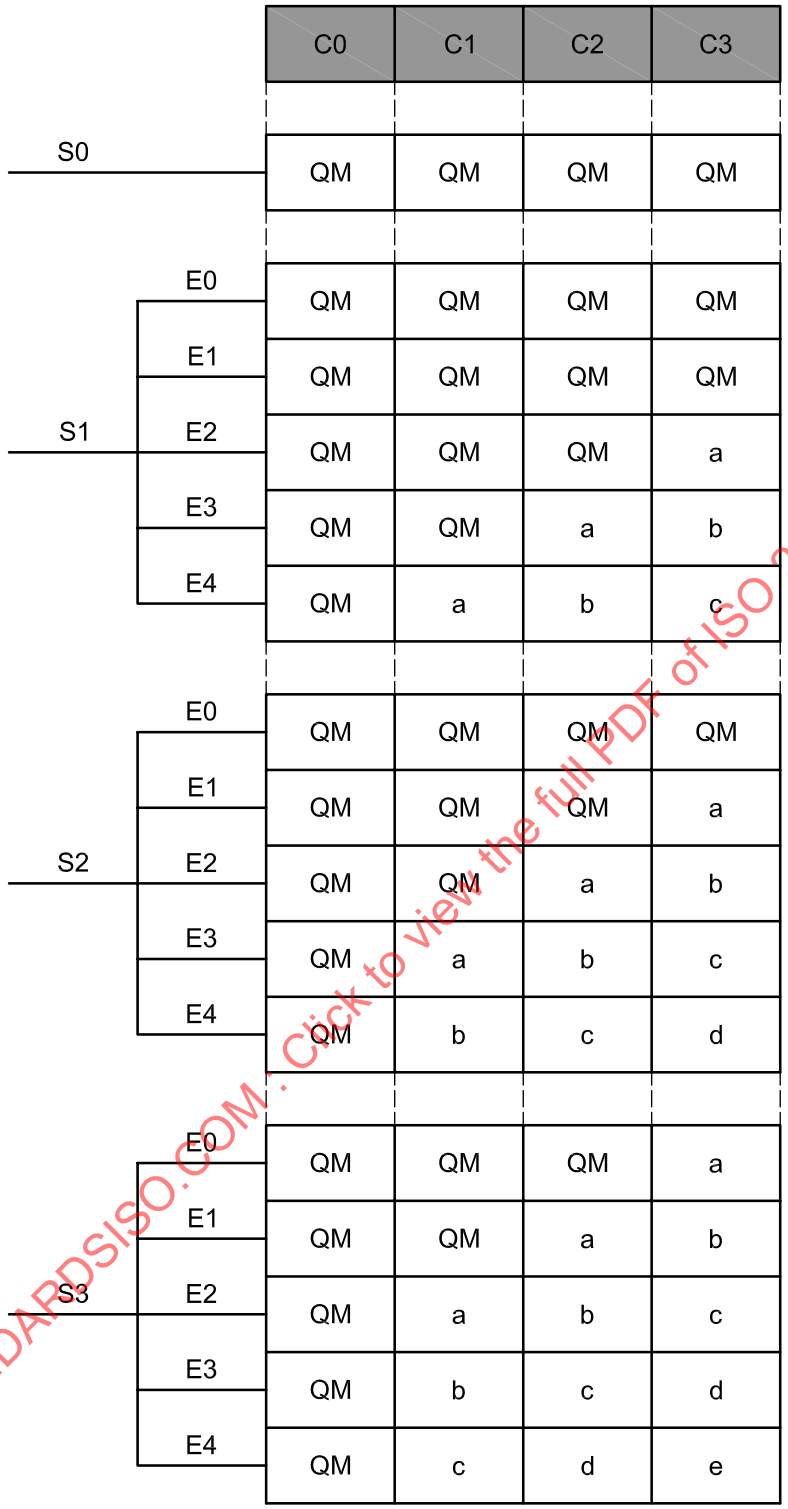
Figure 1 gives guidance for the determination of $AgPL_r$ by combining the severity (S), exposure (E), and controllability (C) values for each identified hazardous situation.

NOTE Experience of the safe use of the same or similar machinery and general competence in the safeguarding of machinery is required to establish the $AgPL_r$ when applying Figure 1.

$AgPL_r$ are designated from $AgPL_r$ = a to $AgPL_r$ = e. $AgPL_r$ = a has the least stringent system requirements and $AgPL_r$ = e has the most stringent system requirements. In addition to these levels, there is a quality measure designation, QM, which implicitly requires system development in accordance with a recognized quality management standard (e.g. ISO 9001). QM applies only to functions where the risk is sufficiently low to allow the function to be classified as non-safety related for the purposes of ISO 25119 (all parts).

The identified hazards that define the $AgPL_r$ related to the safety-related function of the UoO (see 7.3.2) and their associated $AgPL_r$ shall be described and documented in a HARA report.

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



Key

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

NOTE See 6.3.7 for description of QM.

Figure 1 — Determination of $AgPL_r$

6.4 Work products

The following shall be determined and documented:

a) HARA report.

NOTE Document retention per ISO 25119-4.

7 Functional safety concept

7.1 Objectives

Derived from the results of the previous phases, the objectives of the requirements of this phase are to define high level design concepts and requirements at the system level.

7.2 Prerequisites

— Results of HARA;

— $AgPL_r$ for the safety-related functions.

7.3 Requirements

7.3.1 Safety goals

Each hazardous situation with an $AgPL_r$ greater than QM shall be associated with a safety goal. A safety goal may address multiple hazardous situations. If similar safety goals are determined, these may be combined into one safety goal.

NOTE Safety goals are top-level safety objectives for the UoO. They lead to the functional safety requirements needed to avoid an unreasonable risk for each hazardous situation.

7.3.2 Functional safety requirements

Functional safety requirements realize the safety goals in a more specific way ensuring the functional safety of the respective UoO. Adequate functional safety requirements shall be derived from the safety goals. The functional safety requirements inherit the $AgPL_r$ of the hazardous situations and related safety goals.

If functional safety requirements address similar hazardous situations with different $AgPL_r$'s, the functional safety requirements shall implement the highest $AgPL_r$.

Safe states, if applicable, shall be evaluated for each functional safety requirement that is derived from the relevant safety goal. The transition to and the maintenance of safe states shall be defined in the technical safety requirements.

When defining functional safety requirements, the following shall be considered:

— 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).

7.3.3 Value of $MTTF_D$

For the purposes of ISO 25119 (all parts), $MTTF_D$ shall be:

— classified as low, medium or high;

— taken into account for each safety-related channel of an SRP/CS individually ($MTTF_{DC}$).

It may be calculated directly per Table 4 or determined by methods found in Annex B.

NOTE $MTTF_D$ is the reciprocal value of λ_D.

Table 4 — Mean time to dangerous failure

Denotation	$MTTF_D$ Requirement
Low	from 3 years to less than 10 years
Medium	from 10 years to less than 30 years
High	30 years and greater

7.3.4 Value of DC

The value of DC shall be classified as low, medium or high for the purposes of ISO 25119 (all parts). It may be calculated directly per Table 5 or determined by methods found in Annex C.

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 For SRP/CS consisting of several parts, an average value, DC_{avg}, is used (see Annex C).

Table 5 — Diagnostic coverage (DC)

DC	$\sum\lambda_{DD}/\sum\lambda_D \times 100\ \%$
Low	from 0 % to less than 60 %
Medium	from 60 % to less than 90 %
High	90 % and greater

7.3.5 Selection of categories, $MTTF_{DC}$, DC and SRL

The AgPL is a function of the following four aspects:

— category (see Annex A);

— $MTTF_{DC}$ (see Annex B);

— DC (see Annex C);

— SRL specified in ISO 25119-3:2018, Clause 7.

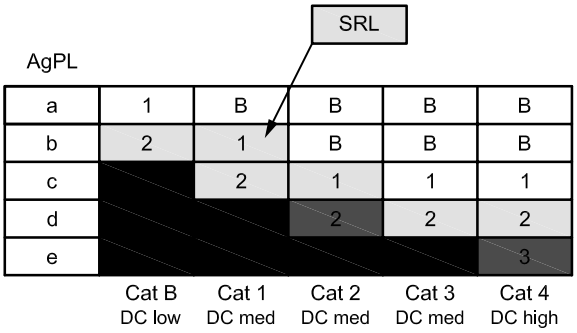
Additionally, the following items shall be considered during system design:

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

— modifications made to SRP/CS with an AgPL equal to “a” or higher should only be performed by responsible persons (or service providers) authorized by the manufacturer of the system. Practicable protection against unauthorized modification according to ISO 25119-4:2018, Clause 11 shall be considered.

As indicated at Figure 2, it may be possible to use more than one combination of reliability (DC, SRL) and architecture (Cat) to achieve the $AgPL_r$. For example, it is possible for single-channel architecture

of high reliability to achieve the same AgPL as that provided by dual-channel architecture of lower reliability (see Figure 2).



Key

low $MTTF_{DC}$

medium $MTTF_{DC}$

high $MTTF_{DC}$

Figure 2 — Relationship between AgPL, categories, $MTTF_{DC}$, DC and SRL

The AgPL is shown on the vertical axis of Figure 2. The hardware categories are listed on the horizontal axis with each category having an associated diagnostic coverage (DC), mean time to dangerous failure ($MTTF_{DC}$) and software requirement level (SRL) for a given AgPL.

For the AgPL, the designer shall select one hardware category.

NOTE Choosing a higher category for a given AgPL could allow lower $MTTF_{DC}$ and/or SRL.

7.3.6 Achieving the $AgPL_r$

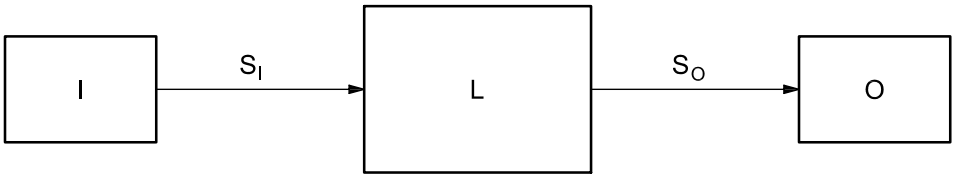
A safety-related function may be implemented by one or more SRP/CS. The designer may use any of the technologies available singularly, or in combination. Each element may consist of a different technology or technologies that are based on E/E/PES. SRP/CS may be combined with safety measures from other technologies such as mechanical safety functions (e.g. mechanically linked contacts).

NOTE Failures of non E/E/PES are not within the scope of this document.

The functional safety concept shall be developed by specifying the characteristics of individual SRP/CS or combinations of SRP/CS that meet the functional safety requirements. Selection of hardware categories, $MTTF_{DC}$, DC and SRL shall be made such that the resultant AgPL of the individual or combination SRP/CS meets or exceeds all $AgPL_r$'s of the assigned functional safety requirements.

A typical control channel with its associated elements being tasked to perform a safety-related function is shown in Figure 3, with input (I), E/E/PES (L), output/power control element (O) and interconnecting means (e.g. electrical, optical). All interconnecting means are included in the SRP/CS.

EXAMPLE Input comprising a speed sensor linked to a light-activated signal converter.



Key

I input device (e.g. sensor)
L logic
O output device (e.g. actuator)
S_I interconnecting signal input
S_O interconnecting signal output

Figure 3 — Diagram of combination of safety-related parts

7.3.7 Compatibility with other functional safety standards

The use of SRP/CS derived from the application of other functional safety standards is allowed only per Annex H.

7.3.8 Joining E/E/PES

Guidance regarding the combination of E/E/PES (e.g. tractor and implement) is found in Annex I.

7.3.9 Alternate combinations of SRP/CS to achieve overall AgPL

The alternate methods found in Annex J shall be used for the determination of the overall AgPL when it is practical to join multiple SRP/CS with existing separate AgPLs.

7.4 Work products

The work products of functional safety concept shall be:

a) safety goals;

b) functional safety requirements and associated $AgPL_r$;

c) selected categories, $MTTF_{DC}$, DC and SRL;

d) CCF if applicable.

Annex A
(normative)

Designated architectures for SRP/CS

A.1 General

Figure 3 and Figures A.1 to A.3 define the architecture required for each respective hardware category.

All architectures shall apply well-tried safety principles, such as:

— avoidance of certain faults, e.g. avoidance of short circuit by separation;

— reducing the probability of faults, e.g. over-dimensioning or derating of components;

— controlling the fault mode, e.g. by ensuring an open circuit when it is vital to remove power in the event of fault (normally open contact);

— detecting faults prior to exposure to the hazard when practicable.

The use of well-tried components is recommended for Category B and shall be provided for Categories 1 to 4. A well-tried component for a safety-related application shall be a component which has been

a) widely used in the past with successful results in similar applications, or

b) made and verified using principles which demonstrate suitability and reliability for safety-related applications.

Newly developed components may be considered as being equivalent to well-tried components if they correspond to b), above.

The figures do not show examples but general architectures. A deviation from these architectures is always possible. Nevertheless, any deviation from these categories will require justification, by means of appropriate analytical tools, that the architecture meets the required category.

NOTE 1 Redundancy, such as redundant sensors, can be used to improve diagnostic coverage.

NOTE 2 Other hardware architectures can be found, for example, in IEC 61508-6:2010, Annex B.

A.2 Category B (basic)

A.2.1 General

See Figure 3 for the designated architecture.

A.2.2 Properties

— DC = low.

— $MTTF_{DC}$ for channel = low to medium.

— The consideration of common-cause failure is not relevant.

— The occurrence of a single fault can lead to the loss of the safety-related function.

— Not suitable for a single-point fail operational system.

A.3 Category 1

A.3.1 General

See Figure 3 for the designated architecture.

A.3.2 Properties

— DC = medium.

— $MTTF_{DC}$ for channel = low to medium.

— The consideration of common-cause failure is not relevant.

— Redundant inputs can be required for diagnostic coverage.

— Not suitable for a single-point fail operational system.

— Use of well-tried components.

The occurrence of a single fault can lead to the loss of the safety-related function, but in some cases a safe state is achievable (for example, detected fault on the inputs).

The single fault is detected at, or before, the next demand upon the safety-related functions by testing at switch-on of the safety-related function and/or periodic testing, if necessary.

The initiation of this check may be automatic or manual. The check itself shall not lead to a hazardous situation. Any check of the safety-related function(s) shall either

a) allow operation if no faults have been detected, or

b) generate an output which initiates appropriate control action, if a fault is detected.

Appropriate control actions can include but are not limited to:

— safe state;

— operator warning;

— disabling the function on startup.

After the detection of a fault, if a safe state is initiated by the SRP/CS, the safe state shall be maintained until the fault is cleared.

NOTE 1 No SRL, $MTTF_D$, DC is allocated on the component(s) which provide control actions after fault is detected.

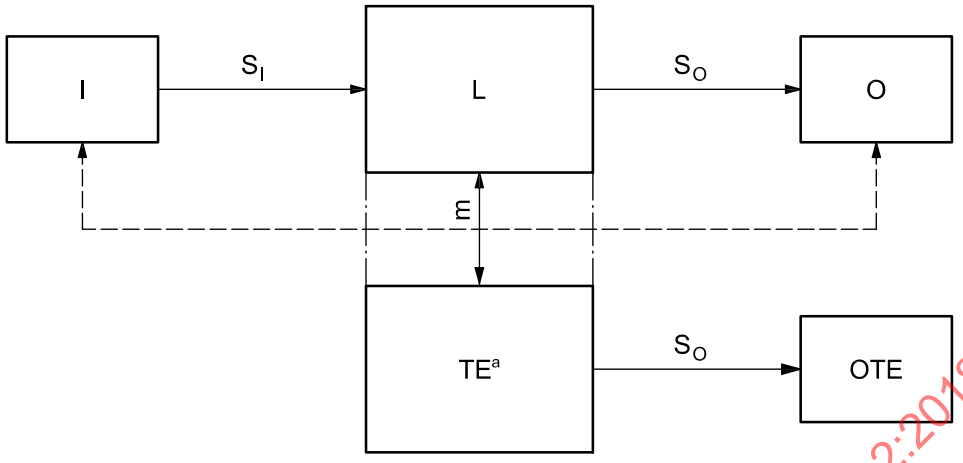
NOTE 2 No SRL, $MTTF_D$, DC is allocated on the component(s) which provide(s) the operator warning.

The occurrence of a single fault can lead to the loss of the safety-related function, but the probability of occurrence is lower than for category B.

A.4 Category 2

A.4.1 General

See Figure A.1 for the designated architecture.



Key

I	input device (e.g. sensor)
L	logic
O	output device (e.g. actuator)
TE	test equipment (additional to logic)
OTE	output of test equipment
S_I	interconnecting signal input
S_O	interconnecting signal output
m	monitoring
a	Required to provide diagnostic coverage on logic, but not necessarily a separate channel.

Figure A.1 — Designated architecture for category 2

A.4.2 Properties

— Input sensor and output actuator faults are detected by the test equipment.

— DC = medium.

— $MTTF_{DC}$ for channel = low, medium, high.

— The consideration of common-cause failure is not relevant.

— Redundant inputs can be required for diagnostic coverage.

— Output and output of test equipment may be arranged in series or parallel depending on the safe state.

— Not suitable for single-point fail operational system.

— Operator warning is required.

— Use of well-tried components.

— The MTTF of the OTE is considered.

— The occurrence of a single fault can lead to the loss of the safety-related function, but if the fault is detected a safe state is achieved if practicable.

The single fault is detected at or before the next demand upon the safety-related functions by testing at switch-on of the safety-related function and/or periodic testing, if necessary.

The initiation of this check shall be automatic so far as practicable or manual if not. The check itself shall not lead to a hazardous situation. The checking equipment may be integral with, or separate from, the

safety-related part(s) providing the safety-related function. Any check of the safety-related function(s) shall either

a) allow operation if no faults have been detected, or

b) generate an output which initiates appropriate control action, if a fault is detected.

Whenever possible, and with consideration of $MTTF_D$ and DC, this output shall initiate a safe state. When it is not possible to initiate a safe state (e.g. welding of the contact in the final switching device), the output shall provide an operator warning of the hazard. After the detection of a fault, if a safe state is initiated by the SRP/CS, the safe state shall be maintained until the fault is cleared.

NOTE 1 In some cases, category 2 is not applicable because the checking of the safety-related function cannot be applied to all components and then DC is not achievable, for example, pressure switch or temperature sensor.

NOTE 2 In general, category 2 can be realized with electric techniques (e.g. in protective equipment and in particular control systems).

NOTE 3 Some components are of high reliability and only need to be checked periodically. Speed sensors can be checked only during operation (sensor is counting), but the functionality and line breakdown can be checked during the start routine. Machines are normally started several times a day, allowing multiple checks per day.

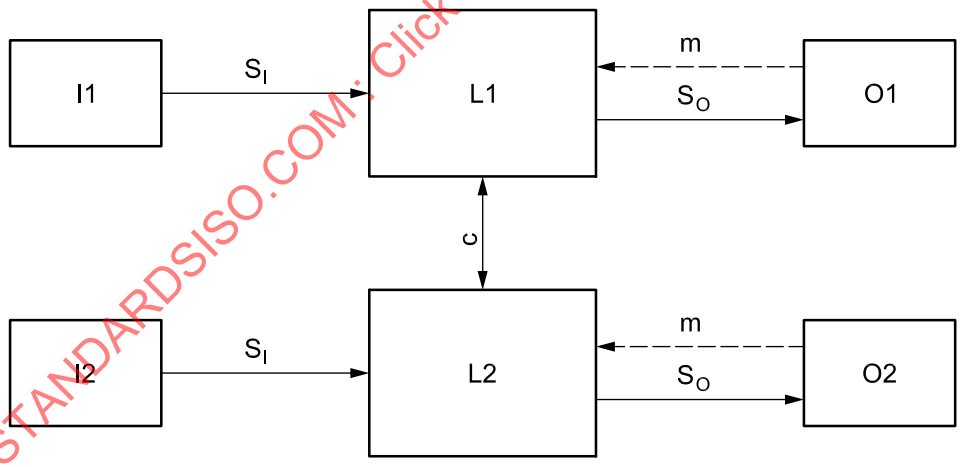
NOTE 4 In some cases, the operator makes a periodical manual test to check safety-related parts, for example, seat switches.

NOTE 5 No SRL, $MTTF_D$, DC is allocated on the component(s) which provide(s) the operator warning.

A.5 Category 3

A.5.1 General

See Figure A.2 for the designated architecture.



Key

I1, I2	input device (e.g. sensor)
L1, L2	logic
O1, O_2	output device, e.g. actuator
S_I	interconnecting signal input
S_O	interconnecting signal output
m	monitoring
c	cross-monitoring

Figure A.2 — Designated architecture for category 3

A.5.2 Properties

— Input sensor, logic and output actuator faults are detected in the control logic.

— DC = medium.

— $MTTF_{DC}$ for channel = low, medium.

— The consideration of common-cause failure is required (see Annex D).

— Redundant inputs can be required for diagnostic coverage.

— Additional redundant outputs can be required for safe state.

— Outputs 1 and 2 may be arranged in series or parallel depending on the safe state.

— Suitable for a single point fail operational system with a redundant power supply.

— Operator warning is required.

— Use of well-tried components.

— When a detected single fault occurs, the safety-related function is always performed or the system fails to a safe state. An accumulation of undetected faults can lead to the loss of the safety-related function.

Whenever reasonably practicable, the single fault is detected at or before the next demand upon the safety-related functions by testing at switch-on of the safety-related function and/or periodic testing, if necessary.

The initiation of this check shall be automatic so far as practicable or manual if not. The check itself shall not lead to a hazardous situation. The checking equipment may be integral with, or separate from, the safety-related part(s) providing the safety-related function. Any check of the safety-related function(s) shall either

a) allow operation if no faults have been detected, or

b) generate an output which initiates appropriate control action, if a fault is detected.

Whenever possible, and with consideration of $MTTF_D$, DC and CCF, this output shall initiate a safe state. The system shall provide a warning to the operator when a failure condition is detected. After the detection of a fault, if a safe state is initiated by the SRP/CS, the safe state shall be maintained until the fault is cleared.

NOTE 1 Some components are of high reliability and only need to be checked periodically. Speed sensors can be checked only during operation (sensor is counting), but the functionality and line breakdown can be checked during the start routine. Machines are normally started several times a day, allowing multiple checks per day.

NOTE 2 In some cases, the operator makes a periodical manual test to check safety-related parts, e.g. seat switches.

NOTE 3 The requirement of single-fault detection does not mean that all faults will be detected. Consequently, the accumulation of undetected faults can lead to an unintended output and a hazardous situation at the machine. Typical examples of practicable measures for fault detection are the movement of relay contacts and the monitoring of redundant electrical outputs.

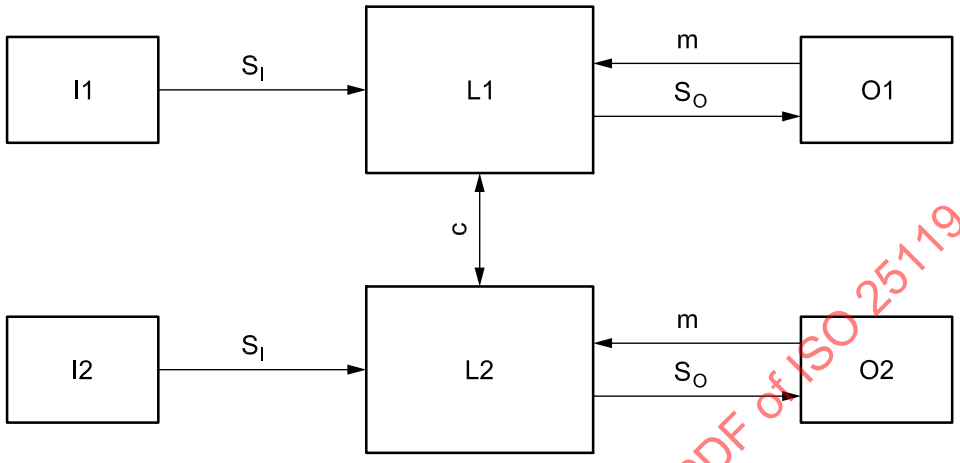
NOTE 4 It is preferable that the error condition(s) be stored for later appraisals.

NOTE 5 No SRL, $MTTF_D$, DC is allocated on the component(s) which provide(s) the operator warning.

A.6 Category 4

A.6.1 General

See Figure A.3 for the designated architecture.



Key

I1, I2	input device (e.g. sensor)
L1, L2	logic
O1, O_2	output device, e.g. actuator
S_I	interconnecting signal input
S_O	interconnecting signal output
m	monitoring
c	cross-monitoring

NOTE Solid lines for monitoring represent diagnostic coverage that is higher than in the designated architecture for category 3.

Figure A.3 — Designated architecture for category 4

A.6.2 Properties

— Input sensor, logic and output actuator faults are detected in the control logic.

— DC = high.

— $MTTF_{DC}$ for channel = low, medium, high.

— The consideration of common-cause failure is required (see Annex D).

— Redundant inputs can be required for diagnostic coverage.

— Additional redundant outputs can be required for safe state.

— Outputs 1 and 2 may be arranged in series or parallel, depending on the safe state.

— Suitable for a single point fail operational system with a redundant power supply.

— Operator warning is required.

— Use of well-tried components.

— When a single detected fault occurs, the safety-related function is always performed or the system fails to a safe state. An accumulation of undetected faults can lead to the loss of the safety-related function; however, the probability of occurrence is lower than for category 3.

The single fault is detected at or before the next demand upon the safety-related functions by testing at the switching on of the safety-related function and/or by periodic testing, if necessary.

The initiation of this check shall be automatic so far as practicable or manual if not. The check itself shall not lead to a hazardous situation. The checking equipment may be integral with, or separate from, the safety-related part(s) providing the safety-related function. Any check of the safety-related function(s) shall either

a) allow operation if no faults have been detected, or

b) generate an output which initiates appropriate control action, if a fault is detected.

Whenever possible, and with consideration of $MTTF_D$, DC, and CCF, this output shall initiate a safe state. The system shall provide a warning to the operator when a dangerous failure condition is detected. After the detection of a fault, if a safe state is initiated by the SRP/CS, the safe state shall be maintained until the fault is cleared.

NOTE 1 Some components are of high reliability and need be checked only periodically. Speed sensors can be checked only during operation (sensor is counting), but the functionality and line breakdown can be checked during the start routine. Machines are normally started several times a day, allowing multiple checks per day.

NOTE 2 In some cases, the operator makes a periodical manual test to check safety-related parts, e.g. seat switches.

NOTE 3 The requirement of single-fault detection does not mean that all faults will be detected. Consequently, the accumulation of undetected faults can lead to an unintended output and a hazardous situation at the machine. Typical examples of practicable measures for fault detection are the movement of relay contacts and the monitoring of redundant electrical outputs.

NOTE 4 It is preferable that the error condition(s) be stored for later appraisals.

NOTE 5 No SRL, $MTTF_D$, DC is allocated on the component(s) which provide(s) the operator warning.

Annex B
(informative)

Simplified method to estimate channel $MTTF_{DC}$

B.1 General

This annex illustrates the methods used to calculate the channel $MTTF_{DC}$.

For dual channel architectures (categories 3 and 4), a symmetric channel $MTTF_{DC}$ calculation formula is provided.

For these calculations, a ground mobile model is used when accessing component failure rate databases. Design, software and manufacturing problems are not considered.

When considering the causes of failures in some components, it may be possible to exclude certain faults. In this case, supporting analysis or data should be provided (e.g. over-dimensioned conductor).

NOTE 1 See also ISO 13849-1:2015, Clause 7 and ISO 13849-2:2012, Annex D for useful information on fault analysis and fault exclusions.

B.2 Component $MTTF_D$ values

B.2.1 Determination of component $MTTF_D$ values from standards/databases

The following standards/databases, among others, provide values of MTTF for single components:

— MIL-HDBK-217F[9];

— SN 29500[10];

— RDF 2000[11];

— IEC/TR 62380[12];

— FIDES Guide 2004[13].

Software tools are available for accessing these databases. When retrieving data from them, the designer should specify duty cycle and component stress level (thermal, power, etc.). For connectors, contactors, fuses, etc., special care should be taken when specifying duty cycle, as these components are often rated in number of cycles (B_{10D}). Conductors are not included.

However, if the designer of the E/E/PES has reliable specific data on the components used, it is highly recommended that this specific data be used instead of the above-listed references.

When converting MTTF to $MTTF_D$, it is recommended to either

— evaluate the failure mode of each component using a hazard analysis in conjunction with a fault tree analysis or equivalent to determine the actual percentage of dangerous failures, or

— use a conservative assumption that 50 % of all failures are dangerous.

A failure that is corrected before it generates any hazardous situation in an E/E/PES system can be neglected. In controller memory, error correction code (ECC) is an example of a mechanism which corrects an error before it can cause any harm. Monitoring of ECC during operation and testing of the correction mechanism during the boot phase of the controller memory is highly recommended.

$MTTF_D$ = MTTF/percentage of dangerous failures (see Table B.1).

The components should not be utilized in systems that operate beyond the limits specified by the component manufacturer.

Alternatively, determination of the MTTF may be carried out using one or a combination of the following methods:

c) proven in use under given environmental and operating requirements;

d) testing;

e) analyses.

When testing, the electronic component is exposed to the environmental and operational conditions for which it is designed, and fulfilment of its requirements is verified.

B.2.2 Determination of component $MTTF_D$ values from proven in use components

Existing hardware can use proven in use data in the following method to determine $MTTF_D$ for the channel or system.

Use data (e.g. incident reporting and analysis) from a controlled process to calculate historically achieved $MTTF_D$ by:

a) Determine statistical significant sample of the population:

   1) Determine total time in use of the sample of the population (T);

   2) Determine total number of dangerous failures of the sample of the population (r);

b) The formula for confidence around $MTTF_D$ is as follows:

   1) $MTTF_D = \frac{2T}{X^2(\alpha, 2r+2)}$;

   2) $X^2_{(\alpha,\ 2r+2)}$ = Chi Squared Distribution:

      i) X^2 is the symbol for Chi Squared Distribution;

      ii) $(\alpha, 2r + 2)$ define the parameters for calculating chi squared;

      iii) $\alpha = 1 -$ Confidence Level;

   3) Confidence Level shall be 70 % or greater;

c) Impact analysis should be used to adjust historical data when the expected use environment is more or less stressful.

   1) This can be done with an Acceleration Model such as Arrhenius or Inverse Power Law.

B.2.3 $MTTF_D$ for components from B_{10}

For electromechanical components (e.g. relays, contactors, switches, etc.), it can be difficult to calculate the mean time to dangerous failure ($MTTF_D$). Often, the manufacturers of these kinds of components give only the mean number of cycles until 10 % of the components fail (B_{10}) or fail dangerously (B_{10D}). The following describes a method for calculating an $MTTF_D$ for components using B_{10} given by the component manufacturer.

If the component manufacturer does not provide B_{10D}, it is common to convert B_{10} to B_{10D} by assuming that 50 % of failures are dangerous:

$$B_{10D} = 2\ B_{10}$$

$MTTF_D$ can be approximated by using Formula (B.1):

$$MTTF_D = \frac{B_{10D}}{0{,}1 \times n_{op}} \tag{B.1}$$

To calculate the number of operations, n_{op}, some assumptions on the application of the component need to be made. See Formula (B.2):

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600}{t_{cycle}} \tag{B.2}$$

where

h_{op} is the mean operation, in hours per day;

d_{op} is the mean operation, in days per year;

t_{cycle} is the mean time between the beginning of two successive cycles of the component (e.g. switching of a valve), in seconds.

B.3 Parts count method

The general formula for N components is shown in Formula (B.3):

$$\frac{1}{MTTF_{DC}} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}} \tag{B.3}$$

where

$MTTF_{DC}$ is for the complete channel;

$MTTF_{Di}$ is the $MTTF_D$ of each component of the channel.

Care should be taken to include only those components required for the safety-related function.

Formula (B.3) is not suitable for complex electronic components or components in parallel channels.

NOTE Complex electronic components include but are not limited to PLC, microprocessors and application-specific integrated circuits.

For further guidance in evaluating $MTTF_D$, see IEC 61508-6:2010 Annex B, IEC 62061 or use automated computational tools.

An example calculation of the $MTTF_{DC}$ is given in Table B.1.

Table B.1 — Example $MTTF_{DC}$ calculation of circuit board

Part number	Part description	$MTTF_i$ (from database) years	Dangerous failures %	$MTTF_{Di}$ years	$1/MTTF_{Di}$ 1/years	Number of parts	Total
1	Transistor, bipolar, low power	1 142	50	2 284	0,000 438	2	0,000 876
2	Resistor, carbon film	11 416	50	22 832	0,000 043 8	5	0,000 219
3	Capacitor, standard, no power	5 708	50	11 416	0,000 087 6	4	0,000 350
4	Relay (data coming from component manufacturer)	1 256	30	4 187	0,000 239	4	0,000 956
5	Contactor	32	20	160	0,006 25	1	0,006 25
$\sum(1/MTTF_{Di})$							0,008 65
$MTTF_{DC} = 1/\sum(1/MTTF_{Di})$ in years							115,6

This example gives an $MTTF_{DC}$ of 115,6 years.

B.4 Calculation of symmetric $MTTF_{DC}$ for two-channel architectures

Formula (B.4) is used to calculate a symmetric $MTTF_{DC}$ for a two-channel system (categories 3 and 4).

$$MTTF_{DC} = MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}} \quad \text{(B.4)}$$

where $MTTF_{DC1}$ and $MTTF_{DC2}$ are the values for two different redundant channels.

Formula (B.4) is not suitable for systems that are more complex. For further guidance in evaluating $MTTF_D$, see IEC 61508-6:2010, Annex B, IEC 62061 or use automated computational tools.

Annex C
(informative)

Determination of diagnostic coverage (DC)

C.1 General

The required DC can either be estimated by the use of the following tables or calculated using the formula given in Table 5.

For redundant architectures, each channel should satisfy the required DC for $AgPL_r$.

It is very important to consider each component of the focused safety-related function.

C.2 Estimation of the required DC

The listings in Tables C.1 to C.7 illustrate how to achieve the required DC. For channels without micro-controllers, use Table C.1. For channels with micro-controllers, use Table C.2. In either case, the effectiveness of the fault detection mechanism should be checked. The use of other methods (e.g. other standards) is also allowed, but should be documented in detail.

Only one method is required for each SRP/CS, and the estimated channel DC is limited by the lowest DC level selected in Tables C.1 to C.7 (see the example in C.3).

Table C.1 — Electrical subsystems (without micro-controllers)

Technique/measure	Recommended maximum diagnostic coverage	Example
Failure detection by online monitoring	Medium	Indication lamp for turn-signal
Monitoring of relay contacts	Medium	Indication lamp for mechanical front wheel drive (MFWD)
Comparator	Medium	Indication lamp for charging system
Positive-activated switch	High	Switch with mechanical interlock

Table C.2 — Electronic subsystems (with micro-controllers)

Technique/measure	Recommended maximum diagnostic coverage	Example
Failure detection by online monitoring (analogue or digital signal)	Medium	Monitoring feedback signal (within range)
Majority voter	High	Compare redundant signals
Tests by redundant hardware	Medium (for periodic tests) High (for continuous tests)	Test at start-up (medium) Watchdog (high)
Dynamic principles	Medium	Test stimulus (see category 2)
Monitored redundancy	High	Redundant micro controllers

Table C.3 — Processing units

Technique/measure	Recommended maximum diagnostic coverage	Example
Comparator	High	Compare output and/or synchronised deterministic intermediate data of redundant processors (see categories 2, 3 and 4)
Self-test by software: limited number of patterns (one channel)	High	Walking bit
Self-test by software (one channel)	Low	Internal watchdog
Self-test supported by hardware (one channel)	Medium	External watchdog

Table C.4 — Invariable memory ranges

Technique/measure	Recommended maximum diagnostic coverage	Example
Word saving multi-bit redundancy	Medium	Partial byte redundancy
Modified checksum	Low	Memory block checksum
Signature of one word (8 bit)	Medium	Memory block CRC (8 bit)
Signature of a double word (16 bit)	High	Memory block CRC (16 bit)
Block replication	High	Dual memory (mirror)
RAM supervision with a Hamming—Code with additional parity (SECDED)	High	ECC included in a FLASH controller. Refer to the safety manual of the controller. Depending on the Hamming Distance, the DC can be higher—monitoring of errors corrected by this mechanism is highly recommended.

Table C.5 — Variable memory ranges

Technique/measure	Recommended maximum diagnostic coverage	Example
Self-test by software (one channel)	Medium	Internal watchdog
RAM test (at start-up or periodic)	Medium	"Checkerboard" or "march" "Walk-path" Parity bit
RAM supervision with a Hamming—Code with additional parity (SECDED)	High	ECC included in a RAM controller. Refer to the "Safety Manual" of the controller. Depending on the Hamming Distance, the DC can be higher—monitoring of errors corrected by this mechanism is highly recommended
Double RAM	High	Hardware or software comparison and read/write test
Redundant channel	High	See categories 2, 3 and 4

Table C.6 — I/O units and interface (external communication)

Technique/measure	Recommended maximum diagnostic coverage	Example
Failure detection by online monitoring (analogue or digital input; analogue or digital output)	Medium	Monitoring feedback signal (within range)
Comparator	High	Compare output and/or synchronised deterministic intermediate data of redundant processors (see categories 2, 3 and 4)
Message protection	Medium	1) Checksum on selected message data bytes
	Medium	2) Message enumeration (incrementing counter)
	Low	3) Send frequency verification
	High	1 to 3, combined
Reference sensor	High	Measure a specified signal to check the ADC and/or ECU
Majority voter	High	Compare redundant signals
Separation of electrical energy lines from information lines	High	
Spatial separation of multiple data lines	High	
Increase of interference immunity	High	Shielding and/or twisted pair

Table C.7 — Power supply (applies to system with and without micro-controllers)

Technique/measure	Recommended maximum diagnostic coverage	Example
Overvoltage protection	Low	Load dump protection on alternator
Voltage source control	High	Monitoring voltage and switching to alternative power supply, if required (operating limit is reached)
Power-down control	Medium	Monitoring key-switch (ignition-switch) voltage and initiating ECU shut-down, saving data to memory
		Shut system down when battery voltages drops down

Table C.8 — Program sequence monitoring

Program sequence technique/measure	Recommended maximum diagnostic coverage	Description
Watch-dog with separate time base without time-window	Low	External timing elements with a separate time base (for example watch-dog timers) are periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence. It is important that the triggering points are correctly placed in the program. The watch-dog is not triggered at a fixed period, but a maximum interval is specified.
Watch-dog with separate time base and time-window	Medium	External timing elements with a separate time base (for example watch-dog timers) are periodically triggered to monitor the computer's behaviour and the plausibility of the program sequence. It is important that the triggering points are correctly placed in the program. A lower and upper limit is given for the watch-dog timer. If the program sequence takes a longer or shorter time than expected, remedial action is taken.
Logical monitoring of program sequence	Medium	The correct sequence of the individual program sections is monitored using software (counting procedure, key procedure) or using external monitoring facilities. It is important that the checking points are placed in the program correctly.
Temporal monitoring with online check	Medium	The temporal monitoring is checked at start-up, and a start is only possible if the temporal monitoring operates correctly. For example, a heat sensor could be checked by a heated resistor at start-up.
Combination of temporal and logical monitoring of programme sequences	High	A temporal facility (for example a watch-dog timer) monitoring the program sequence is re-triggered only if the sequence of the program sections is also executed correctly.

C.3 Estimation of channel DC

Table C.9 gives an example for the estimation for channel DC. In this example, the resulting DC for the channel is low.

Table C.9 — Estimated DC

Description	DC	Method	Table reference
Input/output (all)	High	Monitored redundancy	Table C.2
Processor	Low	Internal watchdog	Table C.3
Invariable memory	Medium	Word saving	Table C.4
Variable memory	High	Double RAM	Table C.5
Communication	Medium	Checksum	Table C.6
Power supply	Medium	Power down control	Table C.7

C.4 Calculation of channel DC

In many systems, several measures for fault detection could be used. However, a single DC is calculated for a given channel. According to Table 5, an average DC is calculated by Formula (C.1):

$$DC_{avg} = \frac{\sum \lambda_{DD}}{\sum \lambda_{D}} \times 100\% \quad \text{(C.1)}$$

where

λ_{DD} is the probability of detected dangerous failures;

λ_{D} is the probability of total dangerous failures.

Here, all parts of the channel used in the $MTTF_{DC}$ calculation have to be considered and summed up. Only parts with failure detection contribute to the numerator (λ_{DD}) of Formula (C.1).

C.5 Example calculation of channel DC

Table C.9 gives an example for the calculation of channel DC. In this example, a DC_{avg} of 86 % is realized for the channel, which corresponds to a DC of medium.

Table C.10 — Calculated DC

No.	Component	$MTTF_D$ year	λ_D $1/MTTF_D$ 1/year	Detected Y/N	How detection is realized	λ_{DD} 1/year	DC_{avg}
1	Resistor 1	11 416	0,000 09	Y	Redundant hardware	8,759 64 E-05	
2	Resistor 2	11 416	0,000 09	N		0	
3	Transistor 1	1 142	0,000 88	Y	Monitor feedback	8,756 57 E-4	
4	Microprocessor 1	900	0,001 11	Y	External watchdog	1,111 111 E-3	
5	Capacitor 1	5 708	0,000 18	Y	Redundant hardware	1,751 93 E-4	
6	Capacitor 2	5 708	0,000 18	N		0	
7	Capacitor 1	200	0,005 00	N		0	
8	Contactor 2	32	0,031 25	Y	Monitor feedback	3,125 E-2	
Σ			0,038 76			0,033 5	86 %

Annex D
(informative)

Estimates for common-cause failure (CCF)

This quantitative process should be applied to every part of the control system.

Table D.1 lists common design measures with associated values. Based on engineering judgment, these values represent the contribution each measure makes in the reduction of common-cause failures. Quantifying of CCF is shown in Table D.2.

Table D.1 — Scoring process for measures against CCF

No.	Measure against CCF	Score %
1	**Separation/segregation**	
	Physical separation between signal and power paths? E.g. separation in wiring Sufficient clearances on printed-circuit boards	YES = 15 NO = 0
2	**Diversity**	
	Different technologies/design or physical principles applied? E.g. first channel programmable electronic and second channel hardwired E.g. measuring load by pressure x cylinder area and by strain gauge E.g. digital and analogue E.g. components of different manufacturers	YES = 20 NO = 0
3	**Design/application/experience**	
3.1	Protection against overvoltage, non-electrical over-actuation, overcurrent?	YES = 15 NO = 0
3.2	Selected components are successfully proven for several years under consideration of environmental conditions?	YES = 5 NO = 0
4	**Assessment/analysis**	
	Are the results of a failure mode and effect analysis (FMEA) taken into account to avoid common-cause failures in design?	YES = 5 NO = 0
5	**Competence/training**	
	Are designers/technicians trained to understand the causes and consequences of common-cause failures?	YES = 5 NO = 0
6	**Environmental**	
6.1	EMC Has the system been checked for EMC-aspects (e.g. as specified in relevant product standards)?	YES = 25 NO = 0
6.2	Other influences Are the requirements for immunity to all relevant environmental influences, such as temperature, shock, vibration, humidity (e.g. as specified in relevant standards e.g. ISO 15003) considered?	YES = 10 NO = 0
	Total, S	(max. achievable 100 %)

Table D.2 — Quantifying common-cause failure

Total score *S*	Measures to avoid CCF
65 % or better	Meets the requirements
Less than 65 %	Process failed → apply additional measures

Annex E
(informative)

Systematic failure

E.1 General

A systematic failure (see ISO 25119-1:2018, 3.52) is 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.

E.2 Procedure for the control of systematic failures

The following measures should be applied.

a) Power loss

The safety-related function should be designed so that, with loss of its electrical supply, a safe state of the machine can be achieved or maintained.

Safety-related function behaviour in response to voltage loss, overvoltage and undervoltage conditions should be predetermined so that the safety-related function can achieve or maintain a safe state of the machine.

For single-point fail operational systems (e.g. categories 3 and 4), a redundant power supply is required (as per A.5 and A.6).

b) Measures to control or avoid the effects of the physical environment (e.g. temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference).

Safety-related function behaviour in response to the effects of the physical environment should be predetermined so that the safety-related function can achieve or maintain a safe state of the machine.

c) Measures to control the effects of errors and other effects arising from any data communication process (ISO25119-3:2018, Annex B).

d) Program sequence monitoring

This should be used with safety-related functions that contain software. A defective program sequence exists if the individual elements of a program (e.g. software modules, sub-programs or commands) are processed in the wrong sequence or period of time, or if the clock of the processor is faulty.

Table C.8 provides a list of techniques applicable for program sequence monitoring with, the achievable diagnostic coverage.

E.3 Procedure for the avoidance of systematic failures

The following measures should be applied.

a) Use of suitable materials and adequate manufacturing

Select material, manufacturing methods and treatment in relation to, for example, stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity.

b) Correct dimensioning and shaping

Consider, for example, stress, strain, fatigue, temperature, surface roughness, tolerances, manufacturing.

c) Proper selection, combination, arrangement, assembly and installation of components, including cabling, wiring and interconnections

Apply appropriate standards and manufacturer's application notes, such as catalogue sheets, installation instructions, specifications, and use of good engineering practice.

d) Compatibility

Use components with compatible operating characteristics.

e) Withstanding specified environmental conditions

Design each safety-related function so that it is capable of working in specified environmental conditions, e.g. temperature, humidity, vibration and electromagnetic compatibility (EMC).

Use components that are designed to an appropriate standard and have their failure modes well defined.

f) Design modularization

Use a hierarchical modularization of the system in smaller, clearly defined subunits to such an extent that

1) the functional and physical interfaces of each module are kept as simple as possible, i.e. the number of parameters exchanged with other modules should be manageable and testable, and

2) the number of safety-related states (e.g. start-up, operating, fault, etc.) for each module are manageable and testable.

g) Restrictive use of common resources

The use of common resources, such as memory (RAM, EPROM) or memory partitions, of an A/D converter by two and more modules, should either

1) be avoided, or

2) be done via standardized or defined interfaces with appropriate control measures (ISO 25119-3:2018, Clauses 6 and 7).

h) Separation of safety-related function and non-safety-related function

In system design, a decision should be made whether a separation into safety-related and non-safety-related modules is possible. The interfaces between the two should be clearly specified. A separation can greatly reduce the time and effort for a development complying with this document and reduce the overall complexity.

i) Limitation on the number of system states

The number of safety-related states that the UoO can have should be manageable and testable. This can be achieved, for example, through a hierarchical summary of module states.

j) Use of proven design principles

To reduce the risk of unknown and first-time errors, proven design principles should be used in the preparation of the technical safety concept. Examples of proven design principles are

1) proven safety architectures, and

2) proven measures for fault detection and fault control.

k) Use of standardized interfaces

To reduce the risk of unknown and first-time errors, wherever possible, the interfaces used should be defined in standards and should have been tried and tested in many applications.

In addition, one or more of the following measures should be applied, taking into account the complexity of the safety-related function and its performance level.

1) Design review

Carry out a design review to reveal discrepancies between the specification and implementation.

2) Computer-aided design tools capable of simulation or analysis

Perform the design procedure systematically and include appropriate automatic construction elements that are already available and tested.

3) Simulation

Perform a systematic and complete inspection of the safety-related function design in terms of both the functional performance and the correct specification of components.

Annex F
(informative)

Characteristics of safety-related functions that are often fundamental to risk reduction

F.1 General

This annex provides typical safety-related functions to reduce risk, which should be considered in the design of a safety-related control system. These are in contrast to those safety-related functions that mainly serve the basic functions of the machine to perform tasks such as braking, steering, propel, attachment movement and implement functions.

The designer should include the necessary safety-related functions below to achieve the measures of safety required of the control system for the specific application. The presence of these functions can reduce risks evaluated at the machine level, such as ISO 12100 when annualizing operator errors for example. But can also reduce the risk after a failure has occurred for example by improving the controllability or by reducing severity of the injury.

F.2 Start interlock

Prevents safety-related functions from starting up unintentionally.

F.3 Stop function

A stop function initiated by a protective device should, as soon as necessary after actuation, put the machine in a safe state. Such a stop should have priority over a stop for operational reasons.

When a group of machines is working together in a coordinated manner, provision should be made to signal to the supervisory control and/or the other machines that such a stop condition exists.

NOTE Such a stop can cause operational problems and a difficult restart. In some applications, this function can be combined with a stop for operational reasons to reduce the temptation to defeat the safety-related function.

F.4 Manual reset

After a stop command has been initiated by a protective device, the stop condition should be maintained until the manual reset function is actuated and safe conditions for restarting exist.

The re-establishment of the safety-related function by resetting the protective device cancels the stop command. If indicated by the risk assessment, this cancellation of the stop command should be confirmed by a manual, separate and deliberate action (manual reset).

The manual reset function should

a) be provided through a separate and manually operated function, different from start and restart, within the safety-related parts of the control system,

b) only be achieved if all safety-related functions and protective devices are operative and, if this is not possible, the reset should not be achieved,

c) not initiate motion or a hazardous situation by itself,

d) be activated only by deliberate action,

e) prepare the control system for accepting a separate start command, and

f) only be accepted by actuation of the actuator from its released (off) position.

The category of safety-related parts providing the manual reset should be selected so that the inclusion of the manual reset does not diminish the performance level of the relevant safety-related function.

The reset actuator should be situated outside the danger zone and in a safe position from which there is a good visibility for checking that no person is within the danger zone.

F.5 Start and restart

A restart should take place automatically only if a hazardous situation cannot exist. These requirements for start and restart should also apply to machines which can be controlled remotely.

F.6 Response time

The designer or supplier should declare the response time when the risk assessment of the safety-related parts of the control system indicates that this is necessary.

NOTE The response time of the control system is divided into three parts: failure recognition, initiate measures and reach safe state.

The required overall response time of the machine can influence the design of the safety-related part.

F.7 Safety-related parameters

When safety-related parameters (e.g. position, speed, temperature, pressure) deviate from pre-set limits, the control system should initiate appropriate measures (e.g. actuation of stopping, warning signal, alarm). If errors in manual inputting of safety-related data in programmable electronic systems can lead to a hazardous situation, then a data-checking system within the safety-related control system should be provided (e.g. check of limits, format and/or logic input values).

F.8 External control function

When a machine is controlled externally, for example, by a portable control device or master-slave system, the following should also apply:

a) the means for selecting external control are defined;

b) switching to an external control device does not create a hazardous situation;

c) in case of loss of control of an external control device, the system goes to a defined state;

d) when a machine is remote-controlled as one of several devices located on the machine, switching between other control devices and remote control device does not create a hazardous situation.

F.9 Muting (manual suspension of safety-related functions)

Muting may be required for diagnostics or repair. During muting, safe conditions should be provided by other means.

Other means may consist of:

a) instructions;

b) disabling of all other control or operating modes;

c) permit operation of hazardous functions only by control devices requiring sustained action;

d) permit the operation of hazardous functions only in reduced risk conditions while preventing hazards from linked sequences;

e) prevent any operation of hazardous functions by voluntary or involuntary action on the machine's sensors.

At the end of muting, all safety-related functions should be reinstated.

F.10 Operator warning

A suitable operator warning system should be considered as part of the safety-related function. Optical and/or audio methods may be used.