INTERNATIONAL STANDARD

ISO 25119-2

First edition
2010-06-01

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

Part 2: **Concept phase**

Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité —

Partie 2: Phase de projet

Reference number
ISO 25119-2:2010(E)

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 1
5 Concept — Unit of observation 3
5.1 Objectives 3
5.2 Prerequisites 3
5.3 Requirements 3
5.4 Work products 4
6 Risk analysis and method description 4
6.1 Objectives 4
6.2 Prerequisites 4
6.3 Requirements 5
6.4 Work products 8
7 System design 8
7.1 Objectives 8
7.2 Prerequisites 8
7.3 Requirements 8
7.4 Work products 10
Annex A (normative) Designated architectures for SRP/CS 11
Annex B (informative) Simplified method to estimate channel $MTTF_{dC}$ 17
Annex C (informative) Determination of diagnostic coverage (DC) 20
Annex D (informative) Estimates for common-cause failure (CCF) 24
Annex E (informative) Systematic failure 26
Annex F (informative) Characteristics of safety functions 29
Annex G (informative) Example of a risk analysis 32
Bibliography 37

Foreword

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

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

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

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

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

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

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

— *Part 2: Concept phase*

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

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

Introduction

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

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

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

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

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

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

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

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

Part 2: Concept phase

1 Scope

This part of ISO 25119 specifies the concept phase of the development of safety-related parts of control systems (SRP/CS) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It can also be applied to municipal equipment (e.g. street-sweeping machines). It specifies the characteristics and categories required of SRP/CS for carrying out their safety functions.

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

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

2 Normative references

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

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

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

3 Terms and definitions

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

4 Abbreviated terms

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

ADC	analogue to digital converter
AgPL	agricultural performance level
AgPL_r	required agricultural performance level

CAD	computer-aided design
Cat	hardware category
CCF	common-cause failure
CRC	cyclic redundancy check
DC	diagnostic coverage
DC_{avg}	average diagnostic coverage
ECU	electronic control unit
ETA	event tree analysis
E/E/PES	electrical/electronic/programmable electronic systems
EMC	electromagnetic compatibility
EUC	equipment under control
FMEA	failure mode and effects analysis
FMECA	failure mode effects and criticality analysis
EPROM	erasable programmable read-only memory
FSM	functional safety management
FTA	fault tree analysis
HAZOP	hazard and operability study
HIL	hardware in the loop
MTTF	mean time to failure
$MTTF_d$	mean time to dangerous failure
$MTTF_{dC}$	mean time to dangerous failure for each channel
PES	programmable electronic system
QM	quality measures
RAM	random-access memory
SOP	start of production
SRL	software requirement level
SRP	safety-related parts
SRP/CS	safety-related parts of control systems
SRS	safety-related system

5 Concept — Unit of observation

5.1 Objectives

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

5.2 Prerequisites

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

5.3 Requirements

5.3.1 Unit of observation and ambient conditions

A safety-related concept shall include the following:

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

b) functional requirements for the unit of observation;

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

- technical or physical requirements, e.g. operating, environmental and surrounding conditions and constraints, and
- legal requirements, especially safety-related legislation, regulations and standards (national and international);

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

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

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

- the limits of the unit of observation;
- its interfaces and interactions with other units of observation and components;
- requirements regarding other units of observation;
- mapping and allocation of relevant functions to involved units of observation.

5.3.3 Sources of stress

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

- the interaction of different units of observation;
- hazards of a physical or chemical nature (energy content, toxicity, explosiveness, corrosiveness, reactivity, combustibility, etc.);

- other external events [temperature, shock, electromagnetic compatibility (EMC), etc.];
- reasonable foreseeable human operating errors;
- hazards originating from the unit of observation, and events triggering failure (e.g. during assembly or maintenance).

5.3.4 Additional determinations

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

- determination as to whether the unit of observation is a new development or a modification, adaptation or derivative of an existing unit of observation and, in the case of modification, the carrying out of an impact analysis to adjust the safety life cycle accordingly;
- preparing a plan and a specification to validate the requirements regarding the unit of observation defined in 5.3.1;
- definition of project management for the appropriate phases in the life cycle;
- adequate input data for the reliability assessment;
- adequate procedures and application of tools and technologies;
- utilization of qualified staff.

5.4 Work products

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

a) the unit of observation and ambient conditions,

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

c) sources of stress, and

d) additional determinations.

6 Risk analysis and method description

6.1 Objectives

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

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

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

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

6.2 Prerequisites

There are no prerequisites for this phase.

6.3 Requirements

6.3.1 Procedures for preparing a risk analysis

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

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

6.3.2 Tasks in risk analysis

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

6.3.3 Participants in risk analysis

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

6.3.4 Assessment and classification of a potential harm

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

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

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

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

Table 1 — Examples of the descriptions of injuries

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

6.3.5 Assessment of exposure in the situation observed

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

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

Table 2 — Exposure to the hazardous event

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

t_{exp} exposure time

$t_{\text{av op}}$ average operating time

6.3.6 Assessment of a possible avoidance of harm

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

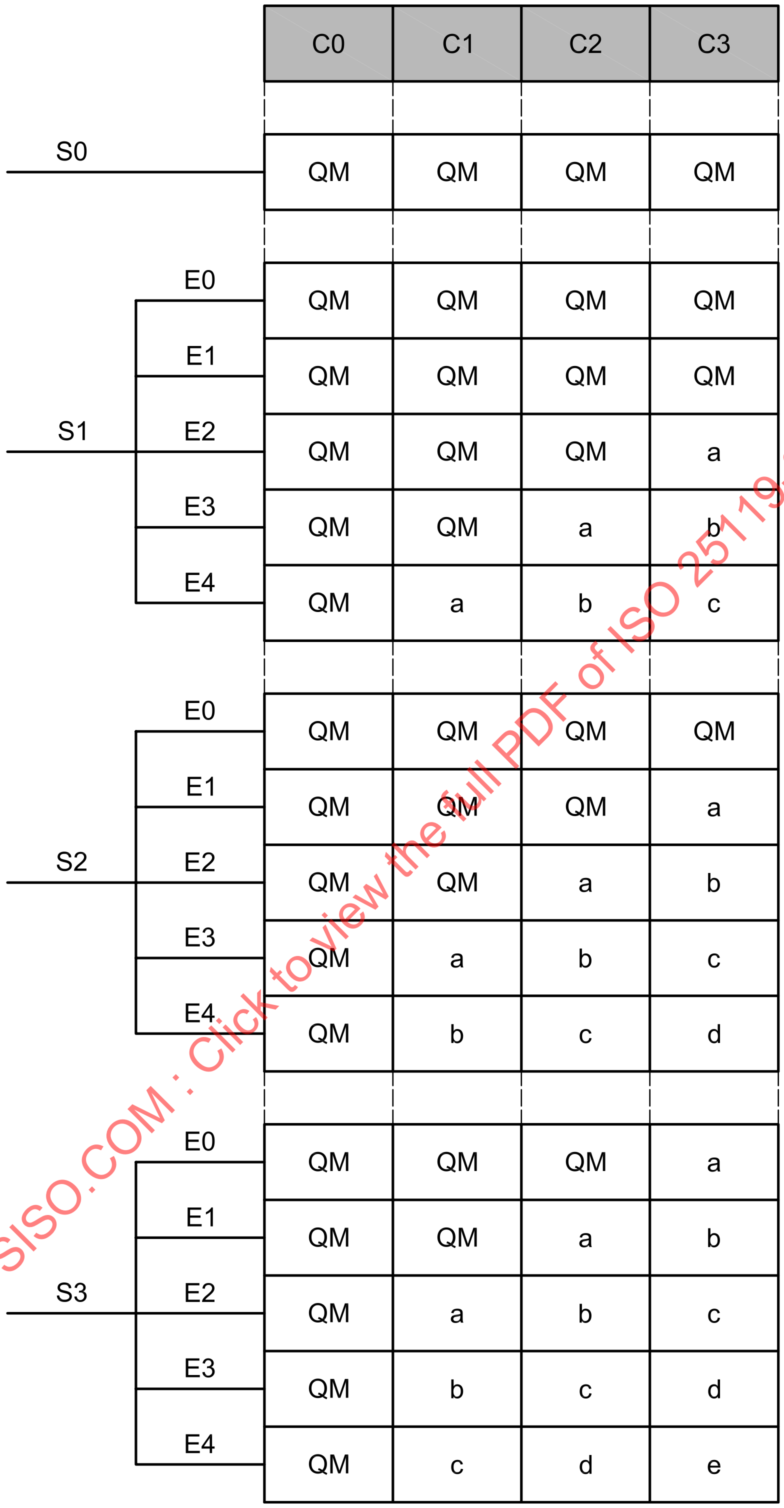
Table 3 — Possible avoidance of harm

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

6.3.7 Selecting the required AgPL$_r$

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

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



		C0	C1	C2	C3
S0		QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	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

6.4 Work products

There are no work products from this phase.

7 System design

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

There are no prerequisites for this phase.

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 can 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).

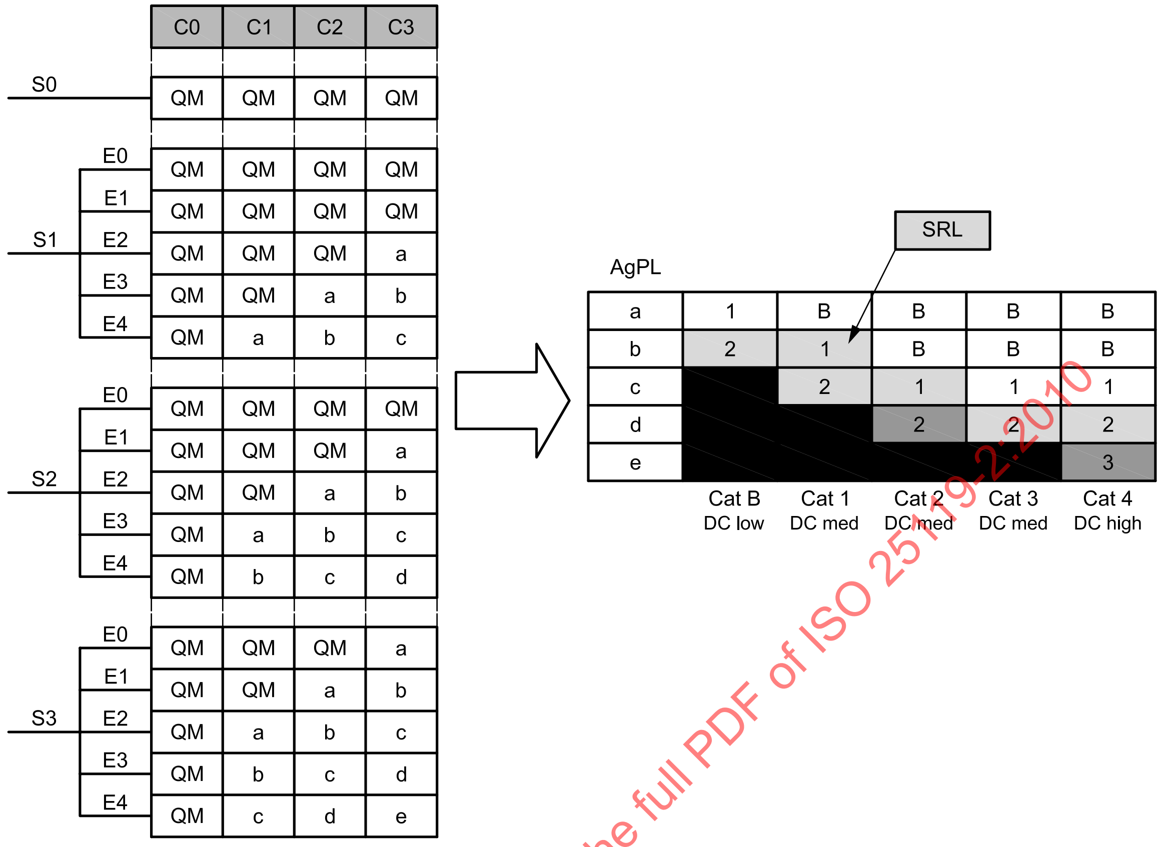
The agricultural performance level of a safety-related control system is a function of the following four aspects:

- category (see Annex A);
- MTTF (see Annex B);
- DC (see Annex C);
- SRL (see ISO 25119-3:2010, 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 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.



		C0	C1	C2	C3
S0		QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	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

AgPL	Cat B DC low	Cat 1 DC med	Cat 2 DC med	Cat 3 DC med	Cat 4 DC high
a	1	B	B	B	B
b	2	1	B	B	B
c	■	2	1	1	1
d	■	■	2	2	2
e	■	■	■	■	3

Key

□ low MTTF$_{dc}$

▒ medium MTTF$_{dc}$

▓ high MTTF$_{dc}$

Figure 2 — Relationship between agricultural performance level, categories, DC, MTTF$_{dC}$ and SRL

The AgPL$_r$ is shown on the vertical axis of Figure 2. The hardware categories are listed on the horizontal axis. Each category has an associated diagnostic coverage (DC), mean time to dangerous failure (MTTF$_{dC}$) and software requirement level (SRL) for a given performance level.

For the required AgPL$_r$ the designer shall select one hardware category.

NOTE Choosing a higher category for a given AgPL could allow lower MTTF$_d$ and/or SRL.

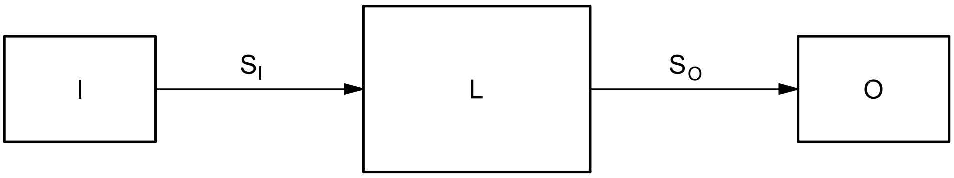
7.3.2 Achieving the required AgPL$_r$

The system design requirements shall be derived from the safety goals and, if necessary, from information about the safe state defined in the risk analysis (e.g. switching off or maintain function). The selected design shall be verified in an appropriate manner for effectiveness.

NOTE The effectiveness can be verified, for example, in clinics, studies, by test subjects, or by simulation. The measures can also be defined in standards.

A safety function may be implemented by one or more safety-related parts of the control system. The designer may use any of the technologies available singularly, or in combination. A safety E/E/PES can be combined with a mechanical function (e.g. mechanically linked contacts).

A typical safety-function control channel with associated safety-related parts is shown in Figure 3, with input (I), E/E/PES (L), output/power control elements (O) and interconnecting means (e.g. electrical, optical).



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

All interconnecting means are included in the safety-related parts. Each safety-related part of a safety-function control channel can consist of a different technology or technologies. Different technologies can be used for implementing within each safety-related part.

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

7.3.3 Validation of the performance level

The selection of SRP/CS shall be made to achieve the required performance level characteristics.

7.4 Work products

The work product of system design is the assignment of AgPL for the covered safety function, comprising the

- selected category (see Annex A),
- resulting MTTF (see Annex B),
- resulting DC (see Annex C),
- resulting SRL,
- resulting CCF for categories 3 and 4 architectures (see Annex D),
- consideration of systematic failure (see Annex E), and
- consideration of other typical functions (see Annex F).

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 apply well-tried safety principles, including

- avoidance of certain faults, e.g. avoidance of short circuit by separation,
- reducing the probability of faults, e.g. over-dimensioning or underrating 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), and
- detecting faults very early.

The use of well-tried components is recommended. 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.

NOTE 1 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 2 Redundancy, e.g. redundant sensors, can be used to improve diagnostic coverage.

A.2 Category B (basic)

See Figure 3 for the designated architecture.

Properties

- DC = low.
- $\mathrm{MTTF}_{\mathrm{dC}}$ for channel = low to medium, the use of well-tried components is recommended.
- The consideration of common-cause failure is not relevant.
- The occurrence of a single fault can lead to the loss of the safety function.
- Not suitable for a single-point fail operational system.

A.3 Category 1

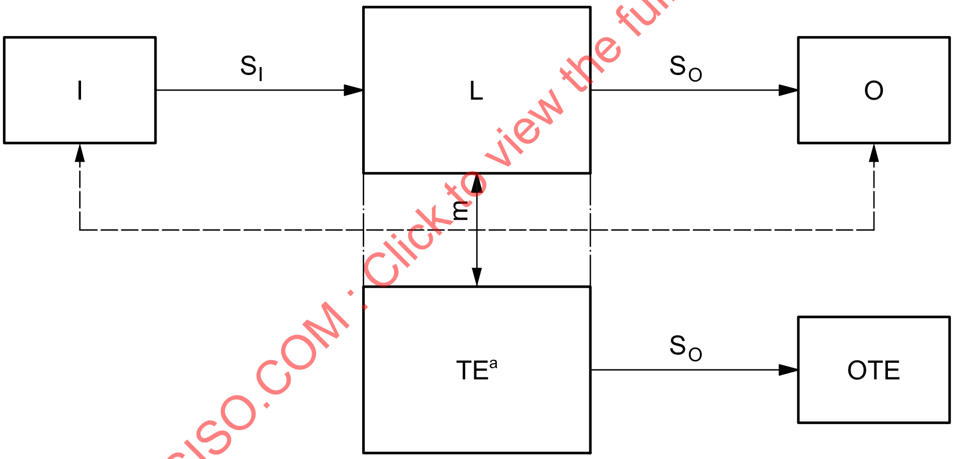
See Figure 3 for the designated architecture.

Properties

- DC = medium.
- $\mathrm{MTTF}_{\mathrm{dC}}$ 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.
- The occurrence of a single fault can lead to the loss of the safety function, but the probability of occurrence is lower than for category B.

A.4 Category 2

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

Properties

- Input sensor 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 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.
- The occurrence of a single fault can lead to the loss of the safety function, but a safe state is achieved.

  The single fault is detected at or before the next demand upon the safety functions by testing at switch-on of the safety 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. The checking equipment may be integral with, or separate from, the safety-related part(s) providing the safety function. Any check of the safety function(s) shall either

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

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

     Whenever possible 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, a 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 function cannot be applied to all components, e.g. pressure switch or temperature sensor.

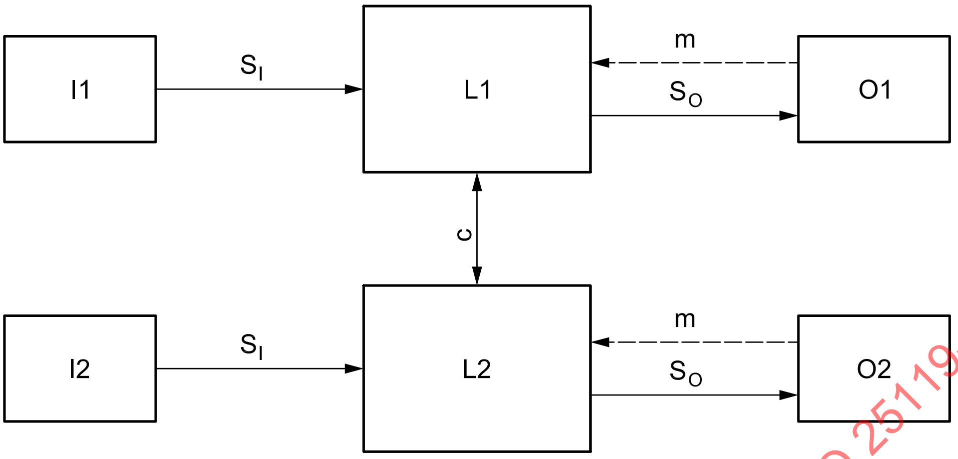
NOTE 2 In general, category 2 can be realized with electric techniques (e.g. in protective equipment and in particular control systems).

NOTE 3 Some components are of high reliability and 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 4 In some cases, the operator has to make a periodical manual test to check safety-related parts, e.g. seat switches.

A.5 Category 3

See Figure A.2 for the designated architecture.



Key

I1, I2	input device (e.g. sensor)
L1, L2	logic
O1, O2	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

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.
- When a single fault occurs, the safety function is always performed, but an accumulation of undetected faults can lead to the loss of the safety function.

  Whenever reasonably practicable, the single fault is detected at or before the next demand upon the safety functions by testing at switch-on of the safety 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. The checking equipment may be integral with, or separate from, the safety-related part(s) providing the safety function. Any check of the safety function(s) shall either

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

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

   Whenever possible, 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, a 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.

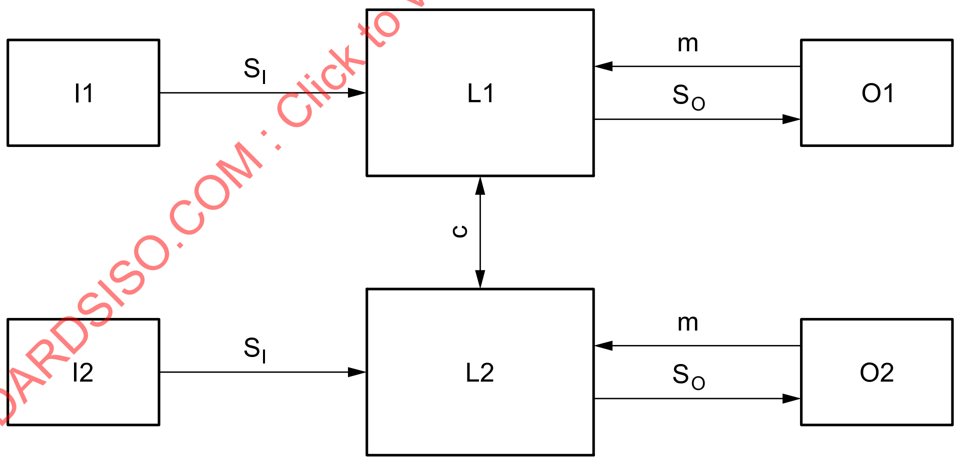
NOTE 2 In some cases, the operator has to make a periodical manual test to check safety-related parts, e.g. seat switches.

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.

A.6 Category 4

See Figure A.3 for the designated architecture.



Key

I1, I2	input device (e.g. sensor)
L1, L2	logic
O1, O2	output device, e.g. actuator
S_I	interconnecting signal input
S_O	interconnecting signal output
m	monitoring
c	cross-monitoring

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

Properties

- Input sensor, logic and output actuator faults are detected in the control logic.
- DC = high.
- $\mathrm{MTTF}_{\mathrm{dC}}$ 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.
- When a single fault occurs, the safety function is always performed, but an accumulation of undetected faults can lead to the loss of the safety 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 functions by testing at the switching on of the safety function and/or by periodic testing, if necessary.

  The initiation of this check may be automatic or manual. 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 function. Any check of the safety function(s) shall either

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

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

     Whenever possible, 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, a 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 has to make 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.

Annex B
(informative)

Simplified method to estimate channel $\mathrm{MTTF}_{\mathrm{dC}}$

B.1 General

This annex illustrates the methods used to calculate the channel $\mathrm{MTTF}_{\mathrm{dC}}$.

For dual channel architectures (categories 3 and 4) a symmetric channel $\mathrm{MTTF}_{\mathrm{dC}}$ 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).

B.2 Component $\mathrm{MTTF}_{\mathrm{d}}$ values

B.2.1 Determination of component $\mathrm{MTTF}_{\mathrm{d}}$ values

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

- MIL-HDBK-217F,
- SN 29500,
- RDF 2000,
- IEC/TR 62380,
- FIDES Guide 2004.

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 ($B_{10\mathrm{d}}$). 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 $\mathrm{MTTF}_{\mathrm{d}}$, it is common to assume that 50 % of all failures are dangerous. It is also possible to evaluate the failure mode of each component to determine the actual percentage of dangerous failures.

$\mathrm{MTTF}_{\mathrm{d}}$ = MTTF/percentage of dangerous failures (see Table B.1).

The components should not be operated beyond the limits specified by the manufacturer.

When MTTF data is not available for a selected component, determination of the MTTF should be carried out using one or a combination of the following methods:

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

b) testing;

c) 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 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 manufacturer.

If the 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:

$$\text{MTTF}_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

To calculate the number of operations, n_{op}, some assumptions on the application of the component need to be made:

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3\,600}{t_{cycle}}$$

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:

$$\frac{1}{\text{MTTF}_{\text{dC}}} = \sum_{i=1}^{N} \frac{1}{\text{MTTF}_{\text{d}i}}$$

where

MTTF_{dC} is for the complete channel;

$\text{MTTF}_{\text{d}i}$ is the MTTF_{d} of each component of the channel.

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

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 %	$\text{MTTF}_{\text{d}i}$ years	$1/\text{MTTF}_{\text{d}i}$ 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 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
$\Sigma(1/\text{MTTF}_{\text{d}i})$							0,008 65
$\text{MTTF}_{\text{dC}} = 1/\Sigma(1/\text{MTTF}_{\text{d}i})$ 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

The following equation is used to calculate a symmetric MTTF_{dC} for a two-channel system (categories 3 and 4).

$$\text{MTTF}_{\text{dC}} = \frac{2}{3}\left(\text{MTTF}_{\text{dC1}} + \text{MTTF}_{\text{dC2}} - \frac{1}{\dfrac{1}{\text{MTTF}_{\text{dC1}}} + \dfrac{1}{\text{MTTF}_{\text{dC2}}}}\right)$$

where MTTF_{dC1} and MTTF_{dC2} are the values for two different redundant channels.

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 ISO 25119-1:2010, 3.10.

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 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, 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 on-line 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 on-line 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 synchronized 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)

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
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 on-line monitoring (analogue or digital input; analogue or digital output)	Medium	Monitoring feedback signal (within range)
Comparator	High	Compare output and/or synchronized deterministic intermediate data of redundant processors (see categories 2, 3 and 4)
Message protection	Medium Medium Low High	1. Checksum on selected message data bytes 2. Message enumeration (incrementing counter) 3. Send frequency verification 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

C.3 Estimation of channel DC

Table C.8 gives an example for the estimation for channel DC. In this example, the resulting DC for the channel is *low*.

Table C.8 — Estimated DC

Description	DC	Method	Table reference
Input/output (all)	Medium	Monitor feedback	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 the definition of DC (see ISO 25119-1:2010, definition 3.10), an average DC is calculated by:

$$\mathrm{DC}_{\mathrm{avg}} = \frac{\sum \lambda_{\mathrm{dd}}}{\sum \lambda_{\mathrm{d}}}$$

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 $\mathrm{MTTF}_{\mathrm{dC}}$ calculation have to be considered and summed up. Only parts with failure detection contribute to the numerator (λ_{dd}) of this equation.

C.5 Calculation of DC

Table C.9 gives an example for the estimation for channel DC. In this example, a DC of 86 % is realized for the channel.

Table C.9 — Calculated DC

No.	Component	$\mathrm{MTTF}_{\mathrm{d}}$	λ_{d}	Detected	How detection is realized	λ_{dd}	DC
			$1/\mathrm{MTTF}_{\mathrm{d}}$				$\Sigma\lambda_{\mathrm{dd}}/\Sigma\lambda_{\mathrm{d}}$
		year	1/year	Y/N		1/year	./.
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	0,86

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?	YES = 15
	E.g. separation in wiring	NO = 0
	Sufficient clearances on printed-circuit boards	
2	**Diversity**	
	Different technologies/design or physical principles applied?	YES = 20
	E.g. first channel programmable electronic and second channel hardwired	NO = 0
	E.g. measuring load by pressure x cylinder area and by strain gauge	
	E.g. digital and analogue	
	E.g. components of different manufacturers	
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 25119-1:2010, definition 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.

- Power loss

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

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

  For a single-point fail operational system (e.g. categories 3 and 4), a redundant power supply is required.

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

  SRS behaviour in response to the effects of the physical environment should be predetermined so that the SRS can achieve or maintain a safe state of the machine.

- Program sequence monitoring

  This should be used with SRS 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.

- Measures to control the effects of errors and other effects arising from any data communication process

E.3 Procedure for the avoidance of systematic failures

The following measures should be applied.

- 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.

- Correct dimensioning and shaping

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

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

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

- Compatibility

  Use components with compatible operating characteristics.

- Withstanding specified environmental conditions

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

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

- 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.

- 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 (see ISO 25119-3:2010, Clauses 6 and 7).

- Separation of SRS and non-SRS

  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 part of ISO 25119 and reduce the overall complexity.

- Limitation on the number of system states

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

- 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.

- 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 SRS 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 SRS design in terms of both the functional performance and the correct specification of components.

Annex F
(informative)

Characteristics of safety functions

F.1 General

This annex provides typical safety functions which should be considered in the design of a safety-related control system.

The designer should include the necessary safety functions to achieve the measures of safety required of the control system for the specific application.

F.2 Start interlock

Prevents safety 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 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 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 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.