INTERNATIONAL STANDARD

ISO 15998

First edition
2008-04-15

Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety

Engins de terrassement — Systèmes de contrôle-commande utilisant des composants électroniques — Critères et essais de performances de sécurité fonctionnelle

Reference number
ISO 15998:2008(E)

Contents

Page

Foreword

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

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

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

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

ISO 15998 was prepared by Technical Committee ISO/TC 127, *Earth-moving machinery*, Subcommittee SC 3, *Operation and maintenance*.

Introduction

Systems consisting of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems, generically referred to as programmable electronic systems (PES), are at present being used in all application sectors to perform non-safety-related and, increasingly, safety-related functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to base these decisions.

This International Standard addresses systems comprising electrical and/or electronic and/or programmable electronic components [electrical/electronic/programmable electronic systems (E/E/PES)] used for functional safety in earth-moving machinery.

In most situations, safety is achieved by a number of protective systems which rely on many technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system, such as sensors, controlling devices and actuators, but also all the safety-related systems. Therefore, while this International Standard is concerned with safety-related E/E/PES, it could also provide guidance for safety-related systems based on other technologies.

This International Standard

— has been conceived with a rapidly developing technology in mind, with a framework sufficiently robust and comprehensive to meet the demands of that technology,

— provides a method for the development of safety requirement specifications necessary to define the required functional safety for E/E/PES, and

— presents a methodology for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PES, using a risk-based approach.

Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety

1 Scope

This International Standard specifies performance criteria and tests for functional safety of safety-related machine-control systems (MCS) using electronic components in earth-moving machinery and its equipment, as defined in ISO 6165. The procedures of ECE R79, Annex 6, ISO 13849-1 or IEC 62061 can be used as an alternative, provided verification and testing is carried out by the manufacturer using Clause 7 of this International Standard.

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 6165:2006, *Earth-moving machinery — Basic types — Identification and terms and definitions*

ISO 13766, *Earth-moving machinery — Electromagnetic compatibility*

IEC 60529, *Degrees of protection provided by enclosures (IP Code)*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions and abbreviations given in IEC 61508-4 and the following apply.

3.1 Terms and definitions

3.1.1
earth-moving machinery
self-propelled or towed machine on wheels, crawlers or legs, having equipment or attachment (working tool), or both, primarily designed to perform excavation, loading, transportation, drilling, spreading, compacting or trenching of earth, rock and other materials

[ISO 6165:2006]

3.1.2
machine-control system
MCS
system consisting of the components needed to fulfil the function of the system, including sensors, signal processing unit, monitor, controls and actuators or several of these

NOTE The extent of the system is not limited to the electronic controls, but is defined by the machine-related function of the complete system. It therefore consists generally of electronic, non-electronic and connection devices. This can include mechanical, hydraulic, optical or pneumatic components/systems.

3.1.3
system unit
part of a machine-control system that contains any given number of components and/or parts integrated in one or more units

EXAMPLE Control unit of the power shift transmission.

NOTE Generally, components and/or parts are installed in a common enclosure, but the system unit can also be built as a mechanical composite with several functional elements.

3.1.4
connection devices
devices used for power supply and for the transmission of signals and data

3.1.5
basic function
⟨machine-control system⟩ controlling task

3.1.6
basic function
⟨system unit⟩ receiving of signals and data, processing and/or actuation

3.1.7
system function
any function that has to be processed by a machine-control system or system unit

NOTE In addition to the basic function, system functions include diagnostics, self-monitoring, signal processing and data transmission to other systems.

3.1.8
safety concept
concept contained in a description of the methods designed into the system to address system performance and safe operation in the event of a failure

3.1.9
safety-related machine-control systems
machine-control systems that control the safety-related functions of the machine

3.1.10
safe state
state automatically or manually applied after a malfunction of the machine-control system, where the controlled equipment, process or system is stopped or switched to a safe mode to prevent unexpected movements or the potentially hazardous build-up of stored energy (e.g. high-voltage electricity, hydraulic pressures or compressed springs)

3.1.11
well-tried component
component for a safety-related application which has been widely used in the past with successful results in similar applications, and which has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications

NOTE 1 In some well-tried components, certain faults can also be excluded because the fault rate is known to be very low.

NOTE 2 The decision to accept a particular component as well-tried depends on the application.

3.1.12
substitute function
function which allows a continuous process in the case of a malfunction or failure of the system

3.1.13
emergency motion function
function to be adopted in the case of a malfunction or failure of the system to allow the operator an emergency motion

EXAMPLE Moving a machine off a public road.

3.1.14
programmable electronic system
PES
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system, such as power supplies, sensors and other input devices, data busses and other communication paths, and actuators and other output devices

3.2 Abbreviated terms

PES programmable electronic system

MCS machine-control systems

FMEA failure modes and effects analysis

FTA fault tree analysis

ETA event tree analysis

SIL safety integrity level (see IEC 61508-4:1998, 3.5.6)

IP Code international protection code

EMC electromagnetic compatibility (see ISO 13766:2006, 3.1)

OSI open systems interconnection

ASIC application-specific integrated circuit

RF radio-frequency

4 General safety requirements

4.1 Application

The following performance criteria are valid for all safety-related machine-control systems using electronic components. These performance criteria are applicable to any type of MCS.

4.2 Description of machine-control system

The system description and overview shall contain

— a list of all system units used by the safety-related functions, and

— a schematic layout of the connection devices and system units, representing the safety-related functions of the machine-control system.

An example of the structure and content of the system description is given in Annex B.

The basic functions and their interfaces to other system units shall be specified for each system unit. This may be done in schematic form or through a block diagram.

The connection shall be illustrated in a suitable way; for the electrical system, a circuit diagram is suitable.

The illustration shall unambiguously classify each connection device (e.g. wires) in relation to the system units (e.g. by terminal identification).

The system units shall be marked by an identification code (e.g. numbers, symbols, characters), so that the correlation between the illustration of the system and the MCS installed in the machine can be verified.

By using the identification code, the manufacturer proves that the system units are in agreement with the documentation with regard to the basic function, safety concept and interfaces. The structure of the identification code (e.g. alphanumerical) may be specified by the manufacturer, but shall be unambiguous.

The system description shall also include requirements for the environmental conditions during the intended operation of the machine:

— climatic conditions (temperature, humidity);

— mechanical conditions (vibration, shock);

— corrosion conditions (salt spray, gas pollution);

— electrical conditions (over- and under-voltage);

— electromagnetic conditions;

— power-source-voltage fluctuation.

4.3 Description of basic function

The basic function of the machine-control system shall be specified in a short description, which may be supported by graphical tools, such as functional schematic or block diagrams. The description shall contain

— an enumeration of the input types and values of the MCS,

— an enumeration of the controlled output types and values of the MCS,

- the open-loop- and closed-loop-control objectives and data/sensors used, and
- the permissible operating and adjusting ranges.

4.4 Risk analysis and assessment

A risk analysis and assessment of the MCS shall be carried out using the systems description in accordance with 4.2 to evaluate the hazards. This may be made in accordance with risk assessment methodologies such as ISO 14121-1 or IEC 61508-5:1998, Annex D. An example is given in Annex A of this International Standard.

4.5 Performance criteria for the safety concept

The basic concept and system functions specified by the manufacturer for the safety concept of the machine shall be taken into account during development and production of the machine-control system. The safety concept includes all measures which provide for safe operation beyond the standard operation (for guidance, see IEC 61508-2:2000, 7.2.3.1). These shall be listed in a generally understandable way, such as in the following examples:

- redundancy;
- fault-detection procedures;
- “safe state”, a safe state may initiate, for example, an emergency motion function (see 5.4).

A documented analysis shall be included, indicating the realization of the safety concept as described. This may be done by an analysis (e.g. FMEA, FTA, ETA) or using equivalent methods suitable for the safety concept of the MCS.

The manufacturer shall document the manner in which the validation of the systems logic has been made during the development stage.

The transition from standard operation mode to safe state shall take into account the stability of the machine and the minimization of the risk of injury to people.

The movement (active or passive) of the machine or its working equipment/attachment out of the hazardous area or position in the case of a malfunction of the MCS should be possible.

4.6 Physical environment and operating conditions

4.6.1 General

The environmental conditions in which the machines are used shall be the basis for the specification of the MCS.

4.6.2 Environment temperature and humidity

The machine-control system shall operate safely under the conditions described in 7.2.2.

Restrictions not having any influence on the safe functioning of the MCS are acceptable.

For special operating conditions of the machine and installation conditions of the electronic parts, other environmental conditions may be specified by the manufacturer.

4.6.3 Degree of protection (IP Code)

Based on the installation conditions, the parts of the MCS carrying out the functional safety shall meet at least the following degrees of protection, in accordance with IEC 60529:

— IP 66 [1)] for all electronic parts, which are fitted outside the machine or are exposed directly to environmental influences.

For special operating conditions of the machine and installation conditions of the electronic parts, other environmental conditions may be specified by the manufacturer.

4.6.4 Electromagnetic compatibility (EMC)

The machine-control system shall fulfil the requirements of ISO 13766.

4.6.5 Mechanical vibration and shock

The system units, components and parts of the MCS shall be designed and fitted so that their safe function is maintained for vibration and shock loads during the typical operation of the machine.

See 7.2.3 and 7.2.4 for test conditions.

For special operating conditions of the machine and installation conditions of the electronic parts, other environmental conditions may be specified by the manufacturer.

4.7 Emergency stop function

An emergency stop function shall be provided if the safety concept requires it. The emergency stop shall shift the MCS or the system unit or the machine into a defined safe state, in the case of failure that could lead to a hazardous motion or condition of the machine.

5 Additional requirements for safety-related machine-control systems

5.1 General

This clause applies to machine-control systems with safety-related functions that have a minimum SIL-Level 1 or equivalent (see A.3.2).

Machine-control systems with safety-related functions shall fulfil the following additional requirements in accordance with the risk assessment.

5.2 Fault avoidance and fault control

5.2.1 IEC 61508-2:2000, Annexes A and B, or other comparable methods, shall be used as a guide to measures and the techniques for the avoidance and control of faults.

5.2.2 Failures in a safety-related system vary essentially according to the time of their origin:

a) failures caused by faults originating before or during system installation, for example, software faults include specification and program faults, hardware faults include manufacturing faults and incorrect selection of components;

1) For special installation conditions, other degrees of protection may be selected, e.g. in the case of higher voltage, malfunction by moisture, dirt or foreign-conductor particles which could lead to an unacceptable situation (risk).

b) failures caused by faults or human errors originating during machine life/operation and, in general, after system installation (e.g. random hardware failures, failures caused by incorrect use).

Failures of the type mentioned in a) can be detected, corrected and avoided by measures made during the different phases of the life-cycle (see IEC 61508-2:2000, Annex B). The measures for failure avoidance are primarily design and analytical procedures.

Failures of the type mentioned in b) can only be controlled during normal operation (see IEC 61508-2:2000, Annex A). The measures for the control of those failures shall be integrated in the safety concept.

Some of the measures and techniques given in IEC 61508-2 are of basic importance (see Annexes A and B), thus they should be used independently from the safety integrity level. Others should also be used independently of this level. The effort required to realize these measures should be chosen such that the effectiveness demanded by IEC 61508-2:2000, Tables B.1 to B.5 (low/medium/high), is achieved. All other measures are replaceable in principle. They can be replaced individually or in connection with other measures.

5.3 Requirements for programmable electronic systems (PES)

The software shall be developed and validated according to appropriate measures (see, for example, IEC 61508-3:1998, Annex A or ISO 13849-1:2006).

The concepts and the development methods and tools for programmable electronic systems (PES) used in machine-control systems shall be documented.

5.4 Malfunction or failure of the electronic components used in machine-control systems

The entering of a safe state shall be achieved in the case of a malfunction or failure of the electronic components used on machine-control systems, in accordance with risk assessment. Reduced system performance or (a) substitute function(s) may be used to achieve a safe state as a part of the safety concept.

The safe state may be achieved by an automatic shift into a substituting function (see Figure 1). If this transition is automatically applied by the MCS, then there shall be some form of indication to the operator, such as alarms, indicators or derated performance (e.g. slow motion).

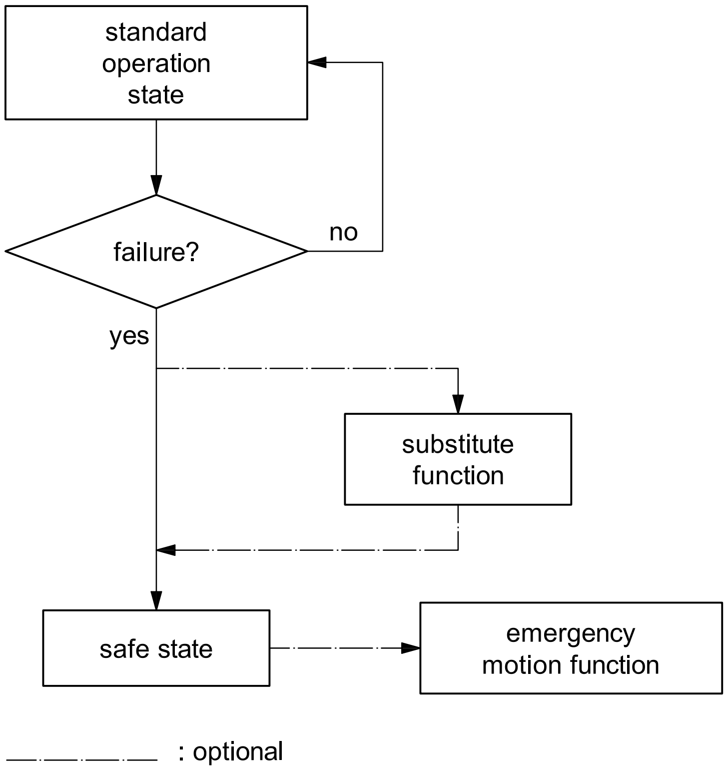


Figure 1 — Example for entering a safe state

5.5 Restart-up procedure

An automatic restart-up, in the case of a fault that disappears (de-validated by the MCS), shall not be allowed, unless the evaluation of the risk assessment demonstrates that the safe operation can be maintained.

6 Documentation

The manufacturer shall retain, according to the manufacturer's record retention policy, all relevant documents for the general safety requirements of the machine-control system in accordance with Clause 4. The documentation shall include at least the following:

— a description of the machine-control system in accordance with 4.2;

— a description of the basic function in accordance with 4.3;

— risk analysis and assessment in accordance with 4.4;

— requirements for the safety concept in accordance with 4.5 (including block diagram with functional description of each block, circuit diagram for external connection, description of external signals);

— the test case and test results, in order to prove the complete fault-coverage test.

The documentation showing how the validation of the systems logic has been made during the development stage (see 4.5) shall include

— a block diagram with a functional description of each block, and

— a circuit diagram for external connection, and description of external signals.

A verification of the safety concept for safety-related machine-control systems in accordance with Clause 5 is based on a detailed documentation of the safety-related part of the system. This may be in the form of

— circuit diagrams for internal electronic circuits with a description of the individual blocks and components,

— a functional description of the circuit diagrams,

— parts lists, including parts identification and names of the individual positions, rating values and tolerances,

— a description of the relevant loads, type nomination and manufacturer of the components, data sheets for special and critical components, and

— a failure mode and effects analysis of the fault conditions.

7 Tests for safety-related MCS

7.1 General

The tests given in 7.2, which are intended to meet the general requirements in accordance with Clause 4, are recommended for MCS; however, alternative means for verification are also permitted. Tests may be performed at the system unit level (e.g. sub-assembly) of the MCS and sequentially. The verification shall demonstrate that the MCS operates as intended under the machine's specified operating conditions (design specifications).

7.2 Tests of machine-control systems

7.2.1 Test content

The tests are as follows:

a) test of basic functions (see function and system description in accordance with 4.2 and description of the basic function in accordance with 4.3);

b) entering of safe-state test (see 5.4);

c) functional test at operating temperature and humidity in accordance with 4.6.2 and 7.2.2;

d) EMC test in accordance with 4.6.4;

e) shock and vibration tests in accordance with 4.6.5, 7.2.3 and 7.2.4.

7.2.2 Test of the function at environmental temperature and humidity

The complete functionality of the components of the safety-related machine-control system shall be tested to meet the performance requirements of 4.6.2, in accordance with either the manufacturer's specifications or with guidance from IEC 60068-2-14, for the following environmental conditions:

— environmental temperature of – 25 °C;

— environmental temperature of + 70 °C;

— relative humidity of 30 %;

— relative humidity of 95 %.

The temperature change should be 1 °C per 3 min. Two temperature-test cycles are required.

The maximum nominal voltage should be chosen during the heat-up and at the maximum environmental temperature, and the minimum nominal voltage should be chosen at the lowest environmental temperature.

The test load at the maximum environmental temperature should be 3/4 and at the maximum value of the maximum operating load for each 1 h cycle. The function should also be checked during these tests.

7.2.3 Vibration test

7.2.3.1 The components of the MCS should be tested in the same position and with the same mountings as those fitted on the machine.

7.2.3.2 The tests should be performed in accordance with IEC 60068-2-6 at the following sine-shaped sweep or in accordance with the manufacturer's specifications, such that they meet the special conditions of 4.6.2, 4.6.3 and 4.6.5:

Frequency range (f): 5 Hz to 200 Hz

The relation between amplitude and acceleration is given in Table 1.

Table 1

Frequency	Engine compartment	All other locations
$f < f_T$	amplitude ± 21 mm	amplitude ± 15 mm
$f \geqslant f_T$	acceleration = 70 m/s^2 (7g)	acceleration = 50 m/s^2 (5g)
	amplitude < ± 21 mm	amplitude < ± 15 mm

Transition frequency (f_T): 8 Hz to 9 Hz

Number of frequency cycles: 20

Sweep rate: 1 octave/min

An interruption of the frequency cycles is allowed.

The test should be performed in axes perpendicular to each other, such that one of the axes is the same as the longitudinal axis of the machine.

7.2.3.3 The test specimen shall be supplied with the nominal voltage and a defined functional test shall be made during the test procedure. There shall be no loss of the safety function.

7.2.3.4 There shall be no cracks or deformations and the whole MCS shall be functional after the test.

7.2.4 Shock test

Shock testing should be performed either in accordance with the manufacturer's specifications or under the guidance of IEC 60068-2-27.

The test specimen should be fixed to the test equipment with the same mountings as fitted at the machine. It should be tightened as specified by the machine manufacturer. The minimum shock load shall be in accordance with the manufacturer's specifications (e.g. an acceleration of 150 m/s^2 (15 g) with an 11 ms pulse duration, or preferably 300 m/s^2 (30 g) with an 18 ms pulse duration).

7.2.5 Additional functional tests for safety-related machine-control systems

All safety-related machine-control systems shall be tested in accordance with Clause 5 with the following addition.

A simple functional test, e.g. in accordance with IEC 61508-7:2000, B.5.1 and an expanded functional test, e.g. in accordance with IEC 61508-7:2000, B.6.8, shall be made.

NOTE Alternative means for verification are also permitted besides those of the IEC 61508 standards cited in this International Standard.

Annex A
(informative)

Guidance for risk assessment

A.1 General

Risk assessment deals with each hazardous situation of the machine application. It is recommended that a small team of experts deal with all hazards from two points of view:

a) hazards to the machine operator;

b) hazards to people working in the environment of the machinery.

The method described in this annex supports the selection of safety integrity levels for the corresponding safety function (see the risk graphs shown in Figures A.1 and A.2). For detailed information on risk assessment, see ISO 14121-1, IEC 61508-5 or other equivalent risk assessment methodologies.

A.2 describes the risk graph method, a qualitative method that enables the safety integrity level of the MCS to be determined from knowledge of the risk factors. This qualitative approach uses a number of parameters which together describe the nature of the hazardous situation when the system fails or is not available. One parameter is chosen from each of four sets (see Table A.1) and the selected parameters are then combined to determine the safety integrity level allocated to the system.

A.2 Use of risk graphs

It is essential that the determination of the risk parameters be made without the consideration of any safety feature integrated in the MCS. An explanation of the risk graphs shown in Figures A.1 and A.2 follows.

— The use of risk parameters C, F and P as defined in Table A.1 leads to a number of outputs. Each of these outputs is mapped onto one of three scales (W_1, W_2 and W_3). Each point on these scales is an indication of the necessary safety integrity that has to be met by the MCS under consideration.

— The mapping onto W_1, W_2 or W_3, as defined in Table A.1, allows the contribution of other risk-reduction measures to be made. The offset feature of the scales for W_1, W_2 and W_3 is to allow for three different levels of risk reduction from other measures. That is, scale W_3 provides the minimum risk reduction contributed by other measures (i.e. the highest probability of the unwanted occurrence taking place), scale W_2 provides a medium contribution and scale W provides the maximum contribution. For a specific intermediate output of the risk graph (after the use of risk parameters C, F and P) and for a specific W scale (i.e. W_1, W_2 or W_3) the final output of the risk graph gives the safety integrity level of the MCS (i.e. 1, 2, 3 or 4) and is a measure of the required risk reduction for this system. This risk reduction, together with the risk reductions achieved by other measures (e.g. by other technology safety-related systems and external risk-reduction facilities) which are taken into account by the W scale mechanism, gives the necessary risk reduction for the specific situation.

Table A.1 — Example data relating to risk graph (see Figures A.1 and A.2)

Risk parameter		Classifications	Comments
Consequence (*C*)	C_1	Minor injury	For the interpretation of C_1, C_2, C_3 and C_4, the consequences of the accident and normal healing should be taken into account.
	C_2	Serious permanent injury to one or more persons; death of one person	
	C_3	Death of several people	
	C_4	A large number of people killed	
Frequency and exposure time in hazardous zone (*F*)	F_1	Rare-to-more-frequent exposure in the hazardous zone	
	F_2	Frequent-to-permanent exposure in the hazardous zone	
Possibility of avoiding hazardous event (*P*)	P_1	Possible under certain conditions	This parameter takes into account — operation of a process (supervised [i.e. operated by skilled or unskilled people] or unsupervised), — rate of development of the hazardous event (e.g. suddenly, quickly or slowly), — ease of recognition of danger (e.g. seen immediately, detected by technical measures or detected without technical measures), — avoidance of hazardous event (e.g. escape routes possible, not possible, or possible under certain conditions), and — actual safety experience (such experience may exist with an identical MCS or a similar MCS or may not exist).
	P_2	Almost impossible	
Probability of unwanted occurrence (*W*)	W_1	Very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely	The purpose of the *W* factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any MCS but including any external risk-reduction facilities. If little or no experience exists of the MCS, or of a similar MCS, the estimation of the *W* factor may be made by calculation. In such an event, a worst-case prediction should be made.
	W_2	Slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely	
	W_3	Relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely	

A.3 Example of risk analysis of electronic powershift control

A.3.1 Hazard identification and allocation of risk parameters

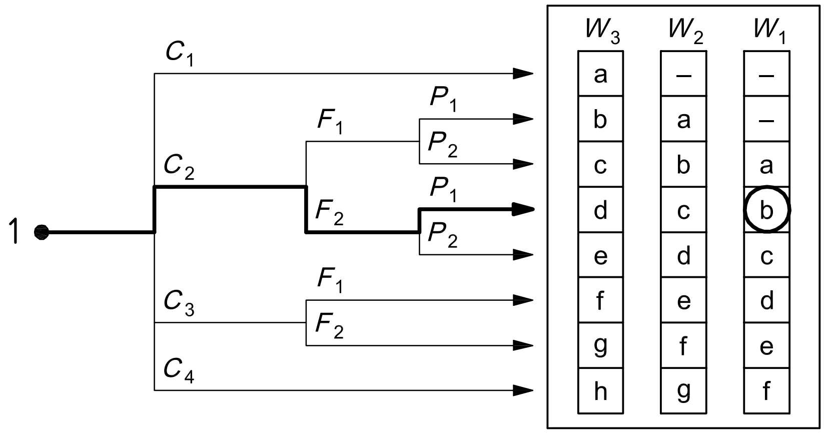
It could be appropriate to list all considered hazards in a small document. Table A.2 presents an example of hazard identification and allocation of risk parameters when an electronically controlled powershift transmission is used.

Table A.2 — Example of hazard identification and risk parameter allocation

Hazard to operator	**Risk parameter**			
	C	*F*	*P*	*W*
Unexpected gearing down in the case of a malfunction, e.g. from fourth to first gear	C_2 Operator could be seriously injured by sudden decrease in speed	F_2 Operator permanently exposed	P_1 Operator can use safety-belt	W_1 Experience shows that the probability of such incidents can be estimated as W_1
Unexpected start-up (from stationary) in the case of malfunction	C_2 In the worst case, machinery will move into dangerous area (collision or rollover)	F_2 Operator permanently exposed	P_1 Operator able to use brakes	W_1 Experience shows that the probability of such incidents can be estimated as W_1
Hazard to other people				
Unexpected gearing down in the case of a malfunction, e.g. from fourth to first gear, on a construction site	— No hazards expected while travelling	—	—	—
Unexpected gearing down in the case of a malfunction, e.g. from fourth to first gear, when travelling on public roads	C_2 Possibility of collision with sudden stopping of machine	F_1 Travelling on public roads is limited	P_1 Possible to use brakes, or other vehicles may be able to swerve	W_1 Experience shows that the probability of such incidents can be estimated as W_1
Unexpected start-up (from stationary) in the case of malfunction on a construction site	C_2 Possibility of serious injury to other people	F_1 In general, machinery is used for moving so that other people are not permanently within the operational area	P_1 People may be able to swerve (low speed)	W_1 Experience shows that the probability of such incidents can be estimated as W_1
Unexpected start-up (from stationary) in the case of malfunction when travelling on public roads	C_2 Possibility of serious injury to other people	F_1 Travelling on public roads is limited	P_1 People may be able to swerve (low speed)	W_1 Experience shows that the probability of such incidents can be estimated as W_1
NOTE This table represents an example only. The estimated risk parameters should be adapted to each individual MCS. The hazards are not complete and it might be necessary to consider additional hazards and situations.				

A.3.2 Risk analysis

The use of the estimated risk parameters as input data for the risk graphs shown in Figures A.1 and A.2 gives a safety integrity level (SIL) of 1 in the example shown in Figure A.1, where the risk to the operator is analysed, and no SIL in the example shown in Figure A.2, where the risk to other people is analysed.



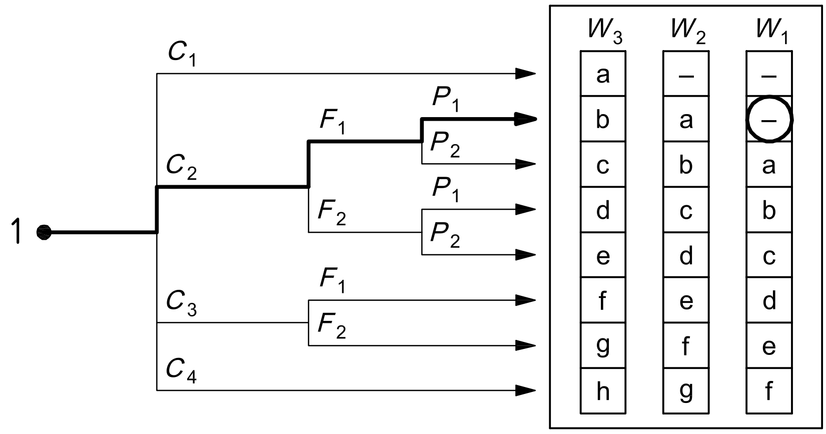
Necessary minimum risk reduction	Performance Level (PL) in accordance with ISO 13849-1	SIL
—	—	No safety requirements
a	a	No special safety requirements
b, c	b, c	1
d	d	2
e, f	e	3
g		4
h		An MCS is not sufficient

Key

1 starting point for risk estimation
C consequence risk parameter
F frequency and exposure risk time parameter
P possibility-of-failing-to-avoid-risk parameter
W probability of the unwanted occurrence
a to h estimates of required risk reduction for MCS

Consequence	C_2	(serious permanent injury to one or more persons; death of a person)
Frequency and exposure time	F_2	(frequent-to-permanent exposure in hazardous zone)
Possibility of avoiding the hazardous event	P_1	(possible under certain conditions)
Probability of the unwanted occurrence	W_1	(very slight probability of unwanted occurrence and few unwanted occurrences likely)

Figure A.1 — Risk graph — Risk to operator



Necessary minimum risk reduction	SIL
—	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An MCS is not sufficient

Key

1 starting point for risk estimation

C consequence risk parameter

F frequency and exposure risk time parameter

P possibility-of-failing-to-avoid-risk parameter

W probability of the unwanted occurrence

a to h estimates of required risk reduction for MCS

Consequence	C_2	(serious permanent injury to one or more persons; death of a person)
Frequency and exposure time	F_1	(rare-to-more-frequent exposure in hazardous zone)
Possibility of avoiding the hazardous event	P_1	(possible under certain conditions)
Probability of the unwanted occurrence	W_1	(very slight probability of unwanted occurrence and few unwanted occurrences likely)

Figure A.2 — Risk graph — Risk to other people

A.3.3 Conclusion

Both risk analyses lead to the conclusion that the powershift transmission should be developed according to safety integrity level 1.

Annex B
(informative)

Example of schematic breakdown of systems specification

No.	Item
1	**Functional specification**
1.1	External interfaces
1.2	Man/machine interfaces
1.3	Operating mode
1.4	System functions
2	**Requirements for safety technology**
2.1	Safety guidelines and rules for the safety record
2.2	Faults and failures to be taken into consideration
2.3	Response to faults and failures (including time-related behaviour)
2.4	Re-start-up procedures
2.5	Limit values for safety and dependability
2.6	Special measures for assuring the required fault tolerance
2.7	Organizational measures for protection against external influences
3	**Environmental conditions to be taken into consideration**
3.1	Type of environmental conditions
3.2	Admissible limit values
3.3	Response of the system to certain environmental conditions
4	**Design requirements**
4.1	Special specifications for designing and implementation
4.2	Available components
4.3	Responsible personnel
4.4	Available means of operation, supplies
4.5	Available means of communication
5	**Outlined conditions of operation and maintenance**
5.1	Necessary devices and interfaces for testing and maintenance
5.2	General technical conditions for installation
5.3	General organizational conditions for operation and maintenance
5.4	Final test requirements and serial production control

Annex C
(informative)

List of well-tried components

C.1 General

Well-tried safety principles are, for example,

- avoidance of certain faults, such as avoidance of short circuit by separation,
- reducing the probability of faults, e.g. by over-dimensioning or underrating of components,
- orientating the mode of fault, e.g. by ensuring an open circuit when it is vital to remove power in the event of a fault,
- early detection of faults, and
- restricting the consequences of a fault, e.g. by grounding of equipment.

Newly developed components and safety principles may be considered as equivalent to “well-tried components” if they fulfil the above-mentioned conditions.

A well-tried component for some applications can be inappropriate for other applications.

Tables C.1 and C.2 are examples and need to be checked by the designer for applicability.

C.2 Mechanical parts/components

Table C.1

Well-tried component	Condition for “well-tried” status	Standard or specification
Screw	All factors influencing the screw connection and the application are to be considered.	Mechanical jointing elements, such as screws, nuts, washers, rivets, pins, bolts, etc. are standardized.
Spring	See “use of a well-tried spring” descriptions in ISO 13849-2:2003, Table A.2.	Technical specifications for spring steels and other special applications are given in ISO 4960.
Cam	All factors influencing the cam arrangement (e.g. part of an interlocking device) are to be considered.	See ISO 14119 (interlocking devices).
Break-pin	All factors influencing the application are to be considered.	—
Steering-rod	All factors influencing the application are to be considered.	—
Boom, lift arm	All factors influencing the application are to be considered.	—

C.3 Hydraulic parts/components

- Hydraulic cylinders
- Pipes, hoses
- Main control valves

C.4 Electrical components

Table C.2

Well-tried component	Condition for "well-tried" status	Standard or specification
Switch with positive mode actuation (direct opening action), for example: — push-button; — position switch; — cam-operated selector switch, e.g. for mode operation.	—	IEC 60947-5-1:2003, Annex K
Emergency stop device	—	ISO 13850
Fuse	—	IEC 60269-1
Circuit breaker	—	IEC 60947-2
Differential circuit breaker/ RCD (residual current detection)	—	IEC 60947-2:2006, Annex B
Main contactor	Only well-tried if a) other influences, such as vibration, are taken into account, and b) failure is avoided by appropriate methods, e.g. over-dimensioning (see ISO 13849-2:2003, Table D.2), and c) current to load is limited by a thermal protection device, and d) circuits are protected by a protection device against overloads.	ISO 13849-2
Control and protective switching device (or equipment) (CPS)	—	IEC 60947-6-2

Table C.2 (*continued*)

Well-tried component	Condition for "well-tried" status	Standard or specification
Auxiliary contactor (e.g. contactor relay)	Only well-tried if a) other influences, such as vibration, are taken into account, b) positively energized action, c) failure avoided by appropriate methods, e.g. over-dimensioning (see ISO 13849-2:2003, Table D.2), d) the current in contacts is limited by a fuse or circuit-breaker to avoid welding of contacts, and e) contacts are positively mechanically guided when used for monitoring.	EN 50205 IEC 60204-1:1997, 5.3.2 and 9.3.3 IEC 60947-5-1
Transformer	—	IEC 61558-1
Cable	Cabling external to enclosure should be protected against mechanical damage (including, for example, vibration or bending).	IEC 60204-1:1997, Clause 13
Plug and socket	—	In accordance with electrical standard relevant for the intended application. For interlocking, see also ISO 14119
Temperature switch	—	For electrical side, see IEC 60947-5-1:2003, Annex K
Pressure switch	—	For electrical side, see IEC 60947-5-1:2003, Annex K For pressure side, see ISO 13849-2:2003, Annexes B and C
Solenoid valve	—	No European or International Standards exist

Annex D
(informative)

Recommendations for bus-systems for transmission of safety-related messages

D.1 Scope

This annex gives recommendations for the transmission of safety-related messages used in MCS. The communication can take place between various system units of a MCS and/or between intelligent sensors/actors and system units of a MCS.

NOTE 1 At this point in time, only those encapsulated bus-systems in which the manufacturer has defined the number and type of bus participants (i.e. units connected to the bus) are considered. An extension of this system to long-distance data transmission is not considered here. Internal-data- and address-busses are excluded from the scope.

NOTE 2 The bus system used can be a system with SAE J 1939 protocol and standard components for the transmission (see the models in D.3).

D.2 Terms and definitions

For the purposes of this annex, the following terms and definitions apply.

D.2.1
bus system
system for the transmission of safety-related messages, consisting of, in addition to the system units (sources and sinks of information), a transmission path/transmission medium (e.g. electrical lines, fibre-optical lines, RF transmission) and the interface between message source/sink and bus electronics (protocol ASICs, transceivers, etc.)

See Figure D.1.

NOTE For remote control, see ISO 15817.

D.2.2
encapsulated bus system
encapsulated system comprising a fixed number or a predetermined maximum number of bus participants connected to each other through a transmission medium with well-defined and fixed performance/characteristics

D.2.3
message source
message sender
sender of a safety-related message

D.2.4
message sink
message receiver
receiver of a safety-related message

D.2.5
message
message consisting of user data, address and data to ensure transmission integrity, etc.

D.2.6
maximum extension size
maximum permissible number of senders and receivers that are engaged in the message exchange as defined for the system

D.2.7
process safety time
period of time between a failure occurring in the MCS and the occurrence of the hazardous event if the safety function is not performed

D.2.8
electrical reaction time
time from the “electrical” detection of a safety-related event until the “electrical” initiation of a safety reaction

NOTE The electrical reaction time consists of several individual times, e.g. bus transmission times.

D.2.9 Transmission errors

D.2.9.1
repetition
error due to a fault of a bus participant, whereby old, non-up-to-date messages are repeated at an incorrect point in time, causing a hazardous disturbance of the receiver (e.g. signalling “access door closed” when it is already open)

D.2.9.2
loss
unintended deletion (e.g. request for safe stop) of a message due to a fault of a bus participant

D.2.9.3
insertion
unintended insertion (e.g. cancellation of a safe stop) due to a fault of a bus participant

D.2.9.4
incorrect sequence
unintended modification of the sequence of messages due to a fault of a bus participant

EXAMPLES Correct sequence: before going to a safe stop, the reduced speed is selected.

Incorrect sequence: immediate safe stop and afterwards the reduced speed is selected.

Consequence: the machine is running instead of remaining in a safe stop.

NOTE Bus systems may contain elements with stored telegrams (FIFOs, etc.) that can modify the correct sequence.

D.2.9.5
message falsification
unintended falsification of messages due to an error of a bus participant or due to errors on the transmission medium

D.2.9.6
retardation
unintended delay or prevention of the safety function, due either to an overload of the transmission path by normal data exchange or to the fact that a bus participant causes overload by sending incorrect messages

D.2.9.7
coupling of safety-related and non-safety-related messages
unintended recognition of a non-safety-related message as a plausible safety-related message

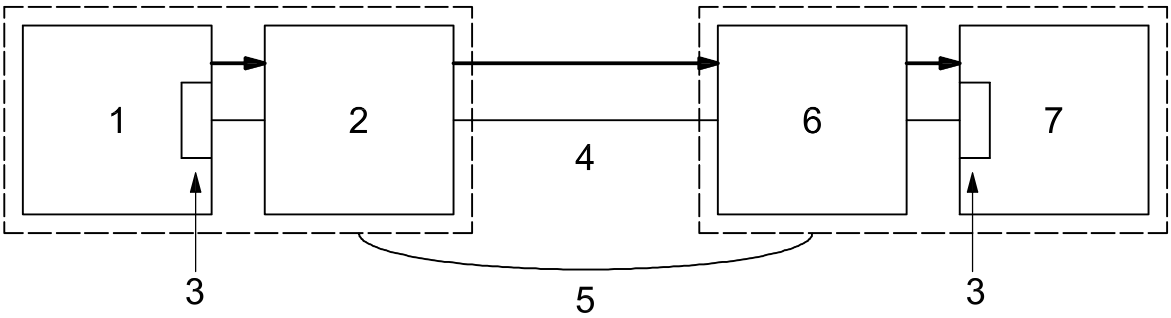
D.3 Models and descriptions

D.3.1 General

For the purposes of this annex, the following models describe certain bus system functions or bus system architectures.

D.3.2 Model for bus system

Figure D.1 shows a model for the bus system.



Key

1 message source

2 bus sender

3 bus interference

4 transmission medium

5 bus

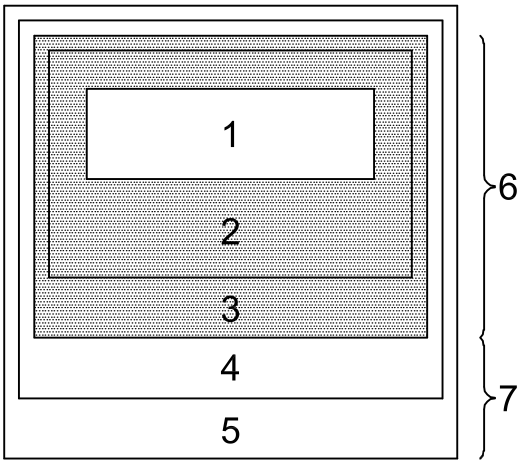
6 bus receiver

7 message sink

Figure D.1 — Simple model of bus system

D.3.3 Model for transmission of safety-related messages (according to OSI)

Figure D.2 shows a model for the transmission of safety-related messages.



Key

1 application data of safety circuits
2 safety procedures, e.g. for authentication
3 integrity coding, e.g. CRC
4 transmission protocol
5 transmission code (telegram)
6 safety layers
7 transmission layers

Figure D.2 — OSI model for transmission of safety-related messages

The safety layers contain the safety procedures and the integrity encoding. The transmission layers contain the transmission protocol and the transmission code.

In the safety layers, the safety-related user data are to be supplemented by safety procedures with integrity encoding (e.g. CRC) and to be transmitted by the transmission layers.

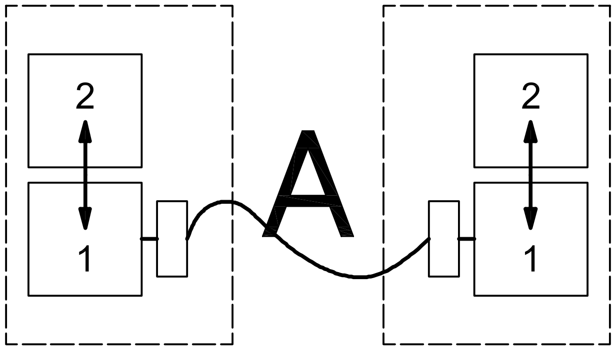
D.3.4 Bus architectures

D.3.4.1 General

Various architectures of bus systems are possible. The following models, A to D, describe typical bus architectures. They partly differ concerning their fault tolerance. The essential advantages and disadvantages are described.

D.3.4.2 Model A: single-channel system

The system shown in Figure D.3 serves as a reference model for the other models. The connection to the bus has only one channel (channel 1). The messages from channel 2, which is not connected to the bus, are saved and then forwarded to channel 1, which is connected to the bus.



Key

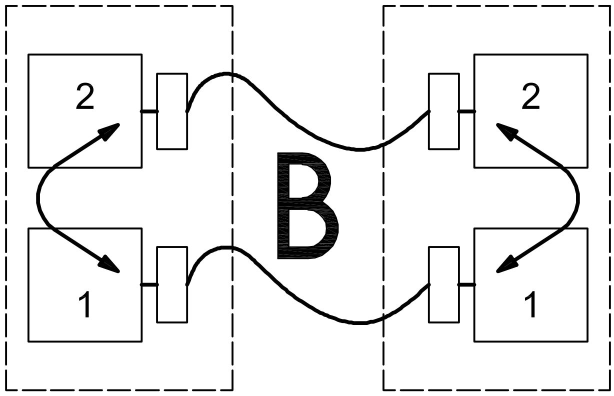
1 channel 1

2 channel 2

Figure D.3 — Architectural model A

D.3.4.3 Model B

Figure D.4 shows a redundant system. In this case, all safety layers and transmission layers are double.



Key

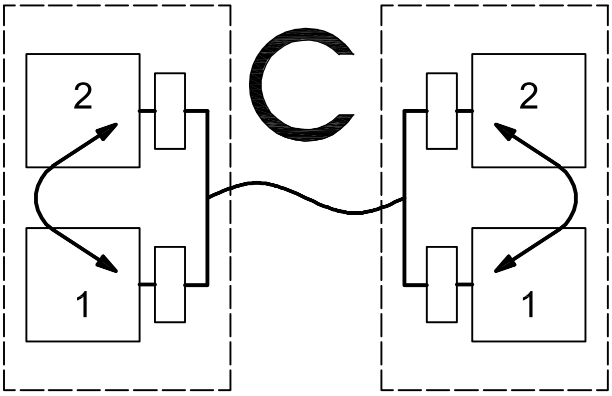
1 channel 1

2 channel 2

Figure D.4 — Architectural model B

D.3.4.4 Model C

Figure D.5 shows a model comparable to model B, but the transmission media is of only one channel.



Key

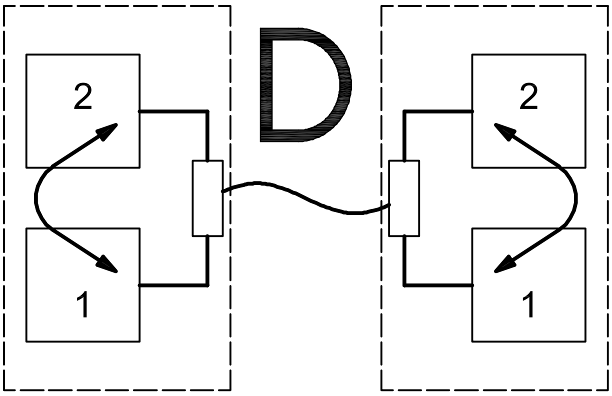
1 channel 1

2 channel 2

Figure D.5 — Architectural model C

D.3.4.5 Model D

Figure D.6 shows a system with two channels for the safety layers, while the transmission layer is of one channel. Both safety layers have independent access to the transmission layer. The user data may be transmitted in one or two telegrams.



Key

1 channel 1

2 channel 2

Figure D.6 — Architectural model D

D.4 Description of measures for control of transmission errors

D.4.1 General

This clause lists measures to control transmission errors.

D.4.2 Running number

A running number is added to each message exchanged between the sender and receiver. This running number may be defined as an additional data field containing a number that changes in a predetermined way from one message to the next.

D.4.3 Time stamp

The content of a message is usually valid at a given time. The time stamp is, for example, a date and time added to a message transmitted by the sender. The time stamp is distinguished by a relative time stamp, an absolute time stamp and a dual time stamp.

D.4.4 Time expiration (time-out)

During the transmission of a message, the receiver checks whether the delay between two messages exceeds a predetermined value. In this case, an error is considered.

D.4.5 Reception acknowledgement/echo

The message sink sends a message of the content of the original message received (echo) back to the source. For example, a reception acknowledgement could repeat the data received in order to allow the sender to check the correct reception.

NOTE Some bus systems use terms like “reception acknowledgement”, “echo” and “receipt” as synonyms.

D.4.6 Identification of message sender and receiver

Messages may contain a uniform sender and/or receiver identification that defines the logical address of the safety-related participant.

D.4.7 Redundancy with cross-monitoring

The sender and receiver have a complete two-channel structure, see models B and C. The messages are independently transmitted twice. In addition to this, the transmitted messages are cross-monitored over the bus or over a separate connection within the dual channel sender/receiver unit for valid action.

Where it differs, an error during the transmission, in the processing unit of the sender or in the processing unit of the receiver, should be considered. If a redundant media is used, a common cause failure should be considered (e.g. failure to detect a common-cause failure can be realized by using diversity in the redundant structure).

D.4.8 Different data-integrity-assurance safety-related (SR) and non-safety-related (NSR) data

If safety-related (SR) and non-safety-related (NSR) data are transmitted via the same bus, different data integrity assurance or encoding principles can be used (different CRC algorithms, different generator polynomials) in order to ensure that NSR messages cannot influence any safety function in an SR receiver.

NOTE Different data integrity assurance also means that NSR messages do not have a data integrity assurance.

D.5 Recommendations

D.5.1 Possible measures for controlling transmission errors

D.5.1.1 To be safely transmitted, messages should be generated in a safe manner (see 4.5). The transmission medium (e.g. bus line including interface ASICs) itself, is not regarded as sufficiently safe. The data assurance mechanism is solely under the responsibility of the processing units of the message source and the message sink (see example Figure D.7).

D.5.1.2 A time-expiration mechanism should principally be used.

D.5.1.3 A mechanism for detecting transmission errors and for reacting in case of failure should be built into the receiver and have the responsibility of starting the safety-related reaction within the process safety time.

D.5.1.4 In the case of the transmission errors defined in D.2.9, a defined error reaction should be initiated (e.g. stop request).

D.5.1.5 The process safety time per safety circuit as specified by the manufacturer and the time required to start a safety-related reaction should not be exceeded, even in the case of a fault.

NOTE In some bus systems, the transmission rate and the process safety time are related to the number of participants. Attention: the safety-related transmission rate and process safety time can restrict the number of participants.

D.5.1.6 For the transmission of safety-related messages by the bus system, at least one measure against each transmission error should be chosen (see Table D.1). The reaction should be based on the risk assessment.

D.5.1.7 The influence of non-safety-related bus participants (any electronic device connected to the bus) on safety-related bus participants should be considered (e.g. by sending multiple safety-related messages).

D.5.2 Data integrity assurance

D.5.2.1 General

The data integrity assurance is an essential component for reaching the required SIL.

All measures for the assurance of data integrity should be performed by the supervising parts of the MCS designed to fulfil the requirements of 4.4. The residual error rate, Λ, should be calculated from the residual error probability, $R(p)$, of the supervising safety-related data integrity assurance mechanism and the transmission rate of safety-related messages.

Use the following formula to calculate the residual error rate from the residual error probability:

$$\Lambda = 3\,600 \times R(p) \cdot \nu \cdot m \times 100 \text{ [transmission errors/h]}$$

where

3 600 is the factor used to calculate the transmissions per hour;

ν is the required rate (1/s) of safety-related messages to reach the required reaction time;

$R(p)$ is the residual error probability;

m is the number of messages required to realize the safety function.

The factor 100 ensures that the transmissions contribute only 1 % (safety margin) of the recommended safety integrity. This leads to the conclusion that the transmission is sufficiently safe. Depending on the risk assessment, the manufacturer can deviate from the safety margin.

For the estimation of $R(p)$, based on the manufacturer's information, the bit error probability should be assumed as $p = 0{,}01$, as long as no other proof is given.

For SIL 3, $\Lambda < 10^{-7}$ should be met.

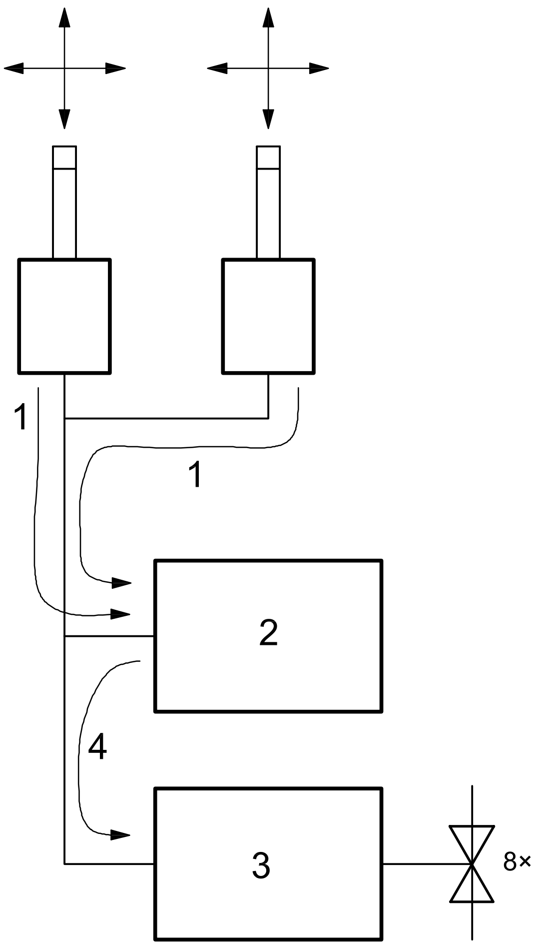
For SIL 2, $\Lambda < 10^{-6}$ should be met.

For SIL 1, $\Lambda < 10^{-5}$ should be met.

NOTE These possible residual error rates are derived from the target failure measures of IEC 61508 (probabilities of dangerous failures per hour) and need to be seen as examples.

D.5.2.2 Example for calculation of residual error rate of the transmission of safety-related messages for a bus system (see Figure D.7)

The movement of earth-moving machinery is controlled by two joysticks. SIL 2 is required for the safety-function "safe movements" of the machine. Information, in respect of the positions of the joysticks, is transmitted by a bus system to a master control (master-link-control) which evaluates the messages and transmits the concerned control commands to eight hydraulic actuators.



Key

1 two messages

2 master control

3 hydraulic control

4 eight messages

Figure D.7 — Example of a safety-related bus system

For calculation of the residual error rate, the following assumptions are made.

a) Each message to be transmitted consists of one simple bus telegram.

b) Each joystick transmits one message for the joystick movement in the x-axis and in the y-axis.

c) The master control receives the messages and evaluates the output information and transmits eight messages to the hydraulic actuators for movement of the earth-moving machinery.

d) In order to comply with the required electrical reaction time, an actualization of the output information for the hydraulic actuators takes place every 100 ms. This means that the rate, v, of the transmission of safety-related messages must be 10/s.

e) The design for transforming the safety-related messages within the control system is not part of this consideration. It is assumed that the design meets the relevant safety-related recommendations.

f) For transmission, a standard bus system is used where the worst-case residual error probability is $R(p) = 7 \times 10^{-9}$. It is assumed that a failure of the standardized integrity encoding measures implemented in the protocol chips is also recognized by the other listening bus participants, and indicated by sending error frames.

For the residual error rate, the following estimation is made:

$$\Lambda = 3\,600 \times R(p) \cdot v \cdot m \times 100 \text{ [transmission errors/h]}$$

$$\Lambda = 3\,600 \times 7 \times 10^{-9} \times 10\ (8 + 2 + 2) \cdot 100 \text{ [transmission errors/h]}$$

$$\Lambda = 0{,}3 \text{ [transmission errors/h]}$$

$\Lambda > \Lambda_{\text{required}}$, and therefore this bus system is not in conformance with the recommendations.

For the improvement of the residual error rate, the following measures are taken.

— Each safety-related message to be transmitted consists of two bus telegrams.

— Each pair of bus telegrams is checked for consistency by the receiving bus participants. If an inconsistency is recognized, an error reaction will take place.

This means that a failure of the transmission is only possible by identical transmission errors in both messages. The probability of the falsification of one message is determined by the worst-case residual error probability of the standard bus system.

In the case of two telegrams, the resulting error probability $R(p)_{\text{total}}$ is determined by the square of the single worst-case residual error probability $R(p)_{\text{total}} = R(p)^2$.

These assumptions lead to the following:

$$\Lambda = 3\,600 \times R(p)_{\text{total}} \cdot v \cdot m \times 100 \text{ [transmission errors/h]}$$

$$\Lambda = 3\,600\ (7 \times 10^{-9})^2 \times 10 \times 12 \times 100 \text{ [transmission errors/h]}$$

$$\Lambda = 2{,}1 \times 10^{-9} \text{ [transmission errors/h]}$$

$\Lambda = \Lambda_{\text{required}} \times 10^{-6}$, and therefore this bus system is in conformance with the recommendations.

Table D.1 — Efficiency of various measures in case of possible transmission errors

Transmission error	Measures per message							
	Running number, see D.4.2	Time stamp, see D.4.3	Time expiration, see D.4.4	Reception acknowledgement, see D.4.5	Identification for sender and receiver, see D.4.6	Data integrity assurance, see D.4.8	Redundancy with cross-check, see D.4.7	Different data integrity assurance systems of SR and non-SR messages, see D.4.8
Repetition, see D.2.9.1	X	X					X	
Loss, see D.2.9.2	X			X			X	
Insertion, see D.2.9.3	X			X [a]	X [b]		X	
Incorrect sequence, see D.2.9.4	X	X					X	
Message falsification, D.2.9.5				X		X	Only for serial bus [d]	
Retardation, D.2.9.6		X	X [c]					
Coupling of SR and non-SR information D.2.9.7				X [a]	X			X

[a] Depends on application.

[b] Only for sender identification. Detects only insertion of an invalid source.

[c] Required in all cases.

[d] This measure is only comparable with a high-quality data assurance mechanism if, by calculation, it can be proved that the residual error rate Λ reaches the values in accordance with D.5.2 if two messages are sent through independent transceivers.

Bibliography

[1] ISO 4960:2007, *Cold-reduced carbon steel strip with a mass fraction of carbon over 0,25 %*

[2] ISO 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

[3] ISO 13849-2:2003, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

[4] ISO 13850, *Safety of machinery — Emergency stop — Principles for design*

[5] ISO 14119, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

[6] ISO 14121-1:2007, *Safety of machinery — Risk assessment — Part 1: Principles*

[7] ISO 15817:2005, *Earth-moving machinery — Safety requirements for remote operator control*

[8] IEC 60068-2-6, *Environmental testing — Part 2: Tests — Test Fc: Vibration (sinusoidal)*

[9] IEC 60068-2-14, *Environmental testing — Part 2: Tests — Test N: Change of temperature*

[10] IEC 60068-2-27, *Environmental testing — Part 2: Tests — Test Ea and guidance: Shock*

[11] IEC 60204-1:1997, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[12] IEC 60269-1:2006, *Low-voltage fuses — Part 1: General requirements*

[13] IEC 60947-2:2006, *Low-voltage switchgear and controlgear — Part 2: Circuit-breakers*

[14] IEC 60947-5-1:2003, *Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices*

[15] IEC 60947-6-2:2007, *Low-voltage switchgear and controlgear — Part 6-2: Multiple function equipment — Control and protective switching devices (or equipment) (CPS)*

[16] IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements*

[17] IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

[18] IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

[19] IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety related systems — Part 5: Examples of methods for the determination of safety integrity levels*

[20] IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines of the application of IEC 61508-2 and IEC 61508-3*

[21] IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

[22] IEC 61558-1, *Safety of power transformers, power supplies, reactors and similar products — Part 1: General requirements and tests*

[23] IEC 62061:2005, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

[24] EN 50205, *Relas with forcibly guided (linked) contacts*

[25] ECE R79, *Uniform provisions concerning the approval of vehicles with regard to steering equipment*, *Annex 6, Special requirements to be applied to the safety aspects of complex electronic vehicle control systems*

[26] SAE J 1939, *Recommended Practice for a Serial Control and Communications Vehicle Network*

[27] REINERT, D., SCHAEFER, M., *Sichere Bussysteme für die Automation,* Hüthig, Heidelberg, 2001. ISBN: 3-7785-2797-5 (language: D)

[28] REINERT, D., SCHAEFER, M., *Progress in the validation of safety-related distributed systems,* 2nd. International Conference Safety of Industrial Automated Systems, 13-15.11.2001, Bonn — Oral presentation. Proceedings pp. 243-251, Editor.: Hauptverband der gewerblichen Berufsgenossenschaften - HVBG, Sankt Augustin. ISBN: 3-88383-604-4 (in English)

ICS 53.100

Price based on 33 pages