INTERNATIONAL STANDARD

ISO 19014-2

First edition
2022-06

Earth-moving machinery — Functional safety —

Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system

Engins de terrassement — Sécurité fonctionnelle —

Partie 2: Conception et évaluation des exigences de matériel et d'architecture pour les parties relatives à la sécurité du système de commande

Reference number
ISO 19014-2:2022(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

This document was prepared by Technical Committee ISO/TC 127, *Earth-moving machinery*, Subcommittee SC 2, *Safety, ergonomics and general requirements,* in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 151, *Construction equipment and building material machines - Safety*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition, together with ISO 19014-1, ISO 19014-3, ISO 19014-4 and ISO 19014-5 cancels and replaces the first editions (ISO 15998:2008 and ISO/TS 15998-2:2012), which have been technically revised.

The main changes are as follows:

- elimination of alternative procedures ECE R79, Annex 6, and IEC 62061;
- application of ISO 13849-1 to mobile Earth-moving machinery, including analysis of non-electronic control systems used in Earth-moving machine applications.

A list of all parts in the ISO 19014 series can be found on the ISO website.

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

Introduction

This document addresses systems comprising all technologies used for functional safety in earth-moving machinery.

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

- Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.
- Type-B standards (generic safety standards) deal with one or more safety aspects, or one or more types of safeguards that can be used across a wide range of machinery:
  - type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);
  - type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).
- Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

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

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

- machine manufacturers (small, medium and large enterprises);
- health and safety bodies (regulators, accident prevention organisations, market surveillance etc.)

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

- machine users/employers (small, medium and large enterprises);
- machine users/employees (e.g. trade unions, organizations for people with special needs);
- service providers, e. g. for maintenance (small, medium and large enterprises);
- consumers (in case of machinery intended for use by consumers).

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

The machinery concerned and the extent to which hazards, hazardous situations or hazardous events are covered are indicated in the Scope of this document.

When requirements of this type-C standard are different from those which are stated in type-A or type-B standards, the requirements of this type-C standard take precedence over the requirements of the other standards for machines that have been designed and built according to the requirements of this type-C standard.

This document is the adaptation of ISO 13849 to provide a type-C standard to address the specific application of functional safety to earth-moving machinery.

This document is to be used in conjunction with the ISO 13849 series when applied to earth-moving machinery (EMM) and supersedes ISO 15998.

This document complements the safety life cycle activities of safety control systems per ISO 13849-1:2015 and ISO 13849-2:2012 on earth-moving machinery as defined in ISO 6165.

Earth-moving machinery — Functional safety —

Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system

1 Scope

This document specifies general principles for the development and evaluation of the machine performance level achieved (MPL_a) of safety-control systems (SCS) using components powered by all energy sources (e.g. electronic, electrical, hydraulic, mechanical) used in earth-moving machinery and its equipment, as defined in ISO 6165.

The principles of this document apply to machine control systems (MCS) that control machine motion or mitigate a hazard; such systems are assessed for machine performance level required (MPL_r) per ISO 19014-1 or ISO/TS 19014-5.

Excluded from the scope of this document are the following systems:

- awareness systems that do not impact machine motion (e.g. cameras and radar detectors);
- fire suppression systems, unless the activation of the system interferes with, or activates, another SCS.

Other systems or components whereby the operator would be aware of failure (e.g. windscreen wipers, head lights, etc.), or are primarily used to protect property, are excluded from this document. Audible warnings are excluded from the requirements of diagnostic coverage.

In addition, this document addresses the significant hazards as defined in ISO 12100 mitigated by the hardware components within the SCS.

This document is not applicable to EMM manufactured before the date of its publication.

2 Normative references

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

ISO 12100, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2015, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

ISO 19014-1, *Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements*

ISO 19014-3, *Earth-moving machinery — Functional safety — Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system*

ISO 19014-4:2020, *Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system*

ISO/TS 19014-5, *Earth-moving machinery — Functional safety — Part 5: Table of Machine Performance Levels*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100, ISO 13849-1, ISO 19014-1 and the following apply.

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

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
ESCS
electronic safety control system
safety control system made of electronic components from input device to output device

3.2
function
defined behaviour of one or more MCS

Note 1 to entry: A control unit (e.g. electronic control unit) can execute more than one function. When multiple safety functions are contained in a control unit, each safety function and the associated circuit are analysed separately.

3.3
N/ESCS
non-electronic safety control system
safety control system made of non-electronic components from input device to output device

3.4
safe state
condition in which, after a fault of the safety control system, the controlled equipment, process or system is automatically or manually stopped or switched into a mode that prevents unintended behaviour or the potentially hazardous release of stored energy

Note 1 to entry: A safe state can also include maintaining the *function* (3.2) of the safety control system (e.g. steering) in the presence of a single fault depending on the hazard being mitigated.

[SOURCE: ISO 3450:2011, 3.15, modified – "malfunction" has been replaced by "fault"; "performance" has been replaced by "behaviour"; Note 1 to entry has been added.]

3.5
well-tried component
component for a safety-related application that has been widely used in the past with successful results in the same or similar applications and which has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications

4 Symbols and abbreviated terms

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

a, b, c, d, e	graduation of machine performance levels
ASIC	application specific integrated circuit
B, 1, 2, 3, 4	denotation of categories

CCF	common cause failure
DC	diagnostic coverage
DC_{avg}	average diagnostic coverage
ECU	electronic control unit
EMM	earth-moving machinery
ESCS	electronic safety control system
FMEA	failure modes and effects analysis
FMEDA	failure modes, effects and diagnostics analysis
FPGA	field programmable gate array
HFT	hardware fault tolerance
HSR	hydraulic system robustness
MCS	machine control system
MPL	machine performance level
MPL_a	machine performance level achieved
MPL_r	machine performance level required
MTTF	mean time to failure
$MTTF_d$	mean time to dangerous failure
N/ESCS	non-electronic safety control system
OTE	output of test equipment
SCS	safety control system
SRP/CS	safety-related part of the control system
TE	test equipment

5 General requirements

5.1 Application

The ISO 19014 series shall be used in conjunction with the ISO 13849 series when applied to earth moving machinery (EMM) and supersedes ISO 15998. Where specific requirements are given in this document, they take precedence over the requirements in the ISO 13849 series; however, where no specific requirements are given in this document, the ISO 13849 series shall apply, using PL instead of MPL (e.g. MPL = b is analogous to PL = b). For a summary of applicable clauses in the ISO 13849 series or this document, see Tables E.1 and E.2 in Annex E.

The principles of this document shall be applied to MCS that are deemed SCS in ISO 19014-1 or ISO/TS 19014-5. Other machine control systems that interfere with or mute a safety function of the safety control system shall be assigned the same machine performance level as the system it is interfering with or muting.

Machinery shall comply with the safety requirements and/or protective/risk reduction measures of this clause. In addition, the machine shall be designed according to the principles of ISO 12100:2010 for relevant but not significant hazards which are not dealt with by this document. Safety related software within any components within the SCS shall meet the requirements of ISO 19014-4:2020.

5.2 Existing SCS

Where an existing SCS has been developed to a previous standard and demonstrated through application usage and validation to reduce the likelihood of a hazard to as low as reasonably practicable, there shall be no requirement to update the lifecycle documentation. When the previously utilized SCS is modified, an impact analysis (see ISO 19014-4:2020, 3.28) of the modifications shall be performed and an action plan developed and implemented to ensure that the safety requirements are met.

6 System design

6.1 Overview

Many safety functions on mobile machines do not have run/stop outputs like non-mobile machine safety functions normally do and are not always added to a machine purely to mitigate a hazard. For example, steering, service brakes, swing, and equipment controls can have modulated or variable outputs within a certain range. While these types of systems can fit into the ISO 13849 architectures, designers need to consider how the characteristics of the safety functions can differ on a mobile machine (e.g. does the system need closed loop control rather than open loop to address incorrect application rates, does the system need to address hazards associated with uncommanded activation as well as failure on demand etc.).

A safety function which relies on a control system to provide necessary hazard mitigation for the machine can be implemented by an SCS within the scope of this document. An SCS can contain one or more SRP/CS, and several SCS can share one or more SRP/CS (e.g. a logic unit, power control elements). It is also possible that one SRP/CS implements both safety and non-safety functions.

NOTE For immediate action warning indicators, refer to ISO 19014-1:2018, Annex B.

Some systems on mobile machines need to maintain an operable state during a failure. While ISO 13849-1:2015 allows for this, additional measures are necessary to ensure this happens safely and that parallel channels do not conflict with each other and that the systems function as the requirements for the claimed architecture specifies.

Annex C sets the minimum requirements that shall be met for utilizing systems, sub-systems and SRP/CS developed and evaluated by methods other than the ISO 19014 series.

6.2 General requirements

After the safety functions of the SCS have been identified, the safety function requirements shall be documented. During the safety lifecycle, safety requirements are detailed and specified in greater detail at hierarchical levels. All safety requirements shall be described such that they are unambiguous, consistent with other requirements, and feasible to implement.

The following design considerations shall be taken into account:

- conflicting input or output signals;
- loss of signal and actuation energies to either system (e.g. separate oil supplies for each channel, redundant power supplies for ECUs);
- conflicting safe states required by multiple failure types that are being addressed by the system;
- systems that require fail-operational functionality;

— the assessment processes are independent from the design process;

— when SCS are designed to be used in a synchronized manner (e.g. task automation), the control system shall be designed to mitigate hazards due to lack of synchronization.

NOTE An EMM example of this synchronization is an excavator boom, arm, and bucket being controlled simultaneously by a grade control system.

6.3 Hardware design

The hardware structure of the SCS can provide measures (e.g. redundancy, diversity, and monitoring) for avoiding, detecting, or tolerating faults. Practical measures can include redundancy, diversity, and monitoring.

The hardware development process shall follow ISO 13849-1:2015 as outlined in Annex E. The designer should begin at the system level where safety functions and associated requirements are identified. The system may be decomposed into subsystems for easier development.

Where applicable, each phase of the development cycle shall be verified.

See Figure 1 for a depiction of the hardware development process in the form of a V-model. Any organized, proven design process which meets the requirements of ISO 19014 may be used to complete the design process.

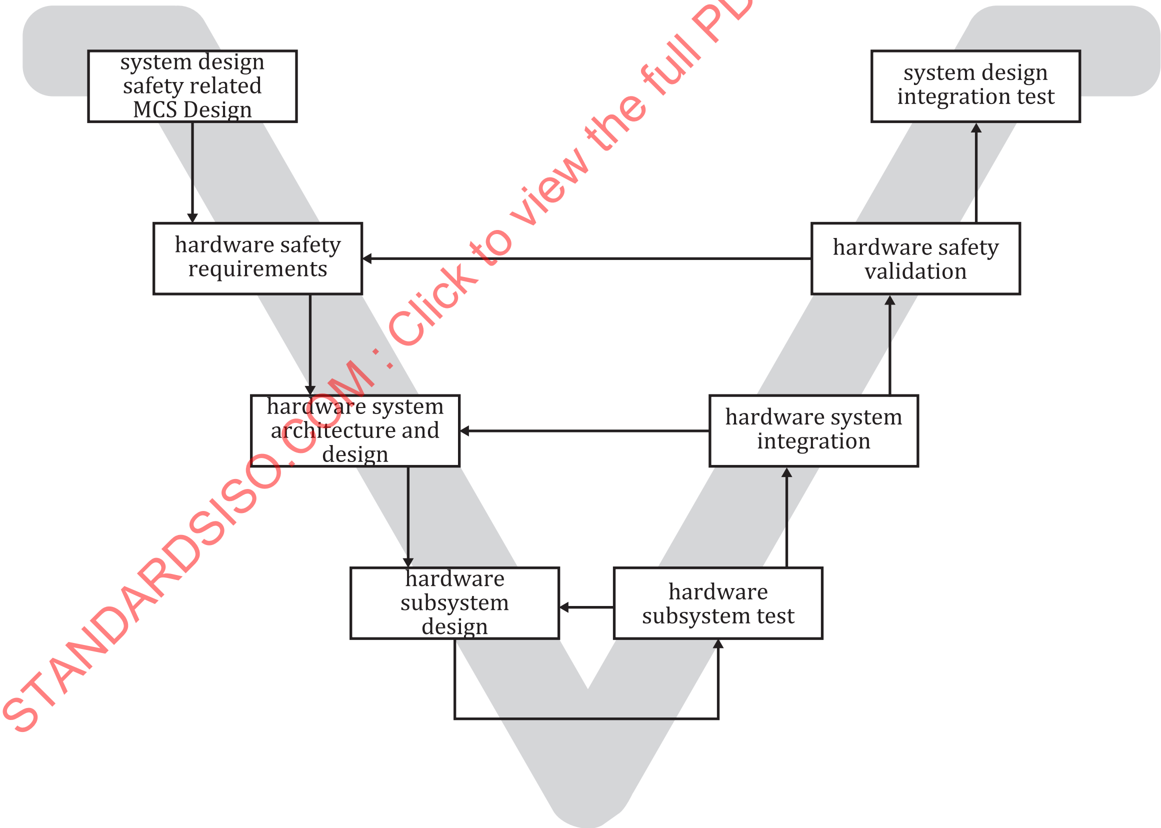

system design safety related MCS Design
system design integration test
hardware safety requirements
hardware safety validation
hardware system architecture and design
hardware system integration
hardware subsystem design
hardware subsystem test

Figure 1 — Hardware development V-model

7 System safety performance evaluation

7.1 Machine performance level achieved (MPL$_a$)

The achieved integrity of safety-related parts to perform a safety function is expressed through the determination of the MPL$_a$.

The ability to perform a safety function under expected environmental conditions as specified in ISO 19014-3 shall be demonstrated and documented.

The procedure for evaluating MPL$_a$ is as follows:

a) identify the component operating environment and stress level;

b) identify components;

c) identify and document fault exclusions (7.2), or by using the appropriate system analysis (e.g. FMEA, fault-tree analysis, etc.);

d) calculate the MTTF$_d$ (see ISO 13849-1:2015, Annex D,), and verify the MTTF$_d$ meets the required level (see ISO 13849-1:2015);

e) determine if the hardware can provide the required level of DC (ISO 13849-1:2015, Annex E). For systems relying on software interaction to determine diagnostic coverage, this analysis can only determine if the hardware is available to support DC, not verify that the DC requirement for the system has been met;

f) consider CCF (see ISO 13849-1:2015, Annex F) if required;

g) consider systematic failure (ISO 13849-1:2015, Annex G);

h) consider possible interaction from other safety functions;

i) for FPGA and ASIC design, see IEC 61508-2:2010, Annexes E or F.

See Annex D for supplementary information on safety function evaluation.

7.2 Hardware safety evaluation

7.2.1 General

ISO 13849-2:2012, Annexes A to D list the faults, fault exclusions and failures for various types of components; these lists are not exhaustive. If necessary, additional faults, fault exclusions, and failures shall be considered and listed; in such cases, the method of evaluation should also be clearly elaborated.

A failure mode and effects analysis (FMEA), fault-tree analysis, or equivalent system analysis shall be performed to establish the faults and fault exclusions.

7.2.2 Fault consideration

In general, the following fault criteria can be considered:

— if, because of a fault, further components fail, the first fault together with all following faults shall be considered as a single fault;

— two or more faults having a common cause shall be considered as a single fault (known as a CCF);

— the simultaneous occurrence of two or more faults having separate causes is considered highly unlikely and therefore need not be considered.

7.2.3 Fault exclusion

Fault exclusions are used in the development of hardware as a means of mitigating the failure mechanisms leading to known hazards in accordance with recognized industry best practices. Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault.

Fault exclusion can be based on the following criteria:

- the technical improbability of occurrence of some faults;
- generally accepted technical experience, independent of the considered application; and
- technical requirements related to the application and the specific hazard.

If faults are excluded, a detailed justification shall be given in the technical documentation.

Fault exclusions can be applied through the following hierarchy.

1. Fault by fault basis - after all faults are identified, some faults may be excluded based on the above criteria; those not fault excluded may be handled by diagnostic means within the control system.
2. Component level - if all known SCS faults can be fault-excluded at a component level, then the component can be fault-excluded entirely.
3. System level – if all faults in all components have been addressed by fault exclusion, analysis of hydraulic systems may be performed using the HSR process in 7.4. Purely mechanical systems can be fault excluded at the system level if components are designed to an appropriate safety factor and maintenance requirements to maintain the correct functionality of the system are included in the service literature per Clause 8.

7.2.4 Mean time to dangerous failure (MTTF$_d$)

The process for determining MTTF$_d$ is outlined in ISO 13849-1:2015, 4.5.2. While ISO 13849-1 recommends the principle assumption of 50 % for hazardous failure rate (e.g. $B_{10d} = 2 \times B_{10}$), lower failure rates may be used if supported by analysis (e.g. empirical data, FMEA).

7.3 Diagnostic coverage (DC)

7.3.1 DC of ESCS

Refer to ISO 13849-1:2015, 4.5.3.

7.3.2 DC of N/ESCS

The DC of non-electronic systems is determined by one or more of the following.

1.) Selecting the most applicable analogous type of diagnostic coverage score in ISO 13849-1:2015, Annex E. For example, a shuttle valve comparing oil pressures and performing an action based on those pressures is comparable to continuous monitoring; therefore, a score of 99 % may be given.

2.) Calculation of DC percentage through an FMEDA.

3.) Fault exclusion may be applicable for all or some failures. If this is done for some failures, but not all, then the appropriate DC would need to be calculated.

4.) Direct mechanical linkage of components can be considered 99 % DC.

7.4 System-level fault reduction measures of hydraulic systems based on hydraulic system robustness (HSR)

7.4.1 General

Evaluating the MPL$_a$ of hydraulic steering and braking systems requires assessment of faults within the components in the primary channel. Due to the characteristics of hydraulic components and their application to earth-moving machinery, these faults cannot be addressed through fault detection techniques used in electronic systems. The hydraulic system robustness (HSR) assessment score is determined using the criteria in Table 1. The basis of this assessment is the robustness of the hydraulic system design in safety applications on earth-moving machines. The criteria in Table 1 extend and build on basic safety principles, criteria for fault exclusions and well-tried safety principles (e.g. as found in ISO 13849-2:2012, as well as established best practices for the design, development and manufacturing of hydraulic SCS).

NOTE These criteria can also be applied to hydraulic systems not used in steering and braking applications but given that these systems are typically category 1, the use of Table 2 to calculate a DC value would not be necessary for the analysis of a category 1 system.

7.4.2 HSR score calculation

The HSR score is defined as a percentage using the formula below:

$$r = \frac{t}{100 - q} \times 100$$

where

r is the hydraulic system robustness (HSR);

q is the sum of the criteria that does not reduce the likelihood of the hazardous failure for the intended safety function that the safety function mitigates;

t is the sum of the remaining applicable criteria that are met by the system.

A criterion that the system does not meet shall not be included in q. (For example, a secondary energy source would not be an applicable criterion for a spring applied, hydraulically released system where the safe state of the system is in the engaged state.)

Each SRP/CS in the hydraulic system being evaluated shall meet the requirements for the given criteria to achieve a score. Partial scores are not allowed; (for example, if there are three spools and only two meet the requirements for a given criteria then the score for the criteria would be zero).

The hydraulic systems shall follow the requirements of ISO 13849-2:2012, C.1 and C.2. Fault exclusion may be applied at a component level if all applicable faults can be excluded per ISO 13849-2:2012, Annex C.

Table 1 — Hydraulic system robustness scoring criteria

Ref	Criteria	Score
A	Over-dimensioning (for example, enough spool clearance, straightness and cylindricity)	10
B	Countermeasures for spool adherence or spinning	10
C	Countermeasures for objectionable hydraulic input (for example, the instantaneous high pressure to both ports of a hydraulic motor)	10
D	Secondary energy source (for example, pilot accumulator) or failsafe design during loss of primary energy source	20

Table 1 *(continued)*

Ref	Criteria	Score
E	Slow or stepwise progressive fault (for example, decrease in steering assist force before significant fault)	10
F	Hose burst mitigation (for example, piercing debris/abrasion-avoidance routing)	10
G	System designed to maintain required hydraulic fluid cleanliness	10
H	Countermeasures for cavitation caused by aeration in or viscosity of hydraulic fluid	10
I	Countermeasures for pressure transfer problems caused by aeration in or viscosity of hydraulic fluid (for example, air vent circuit)	10
	Total score	

Table 2 defines the DC to which a given HSR score is correlated, and a MPL$_a$ can be determined using that DC value, system architecture category, MTTF$_d$ and CCF adapted from ISO 13849-1:2015 Table 6. See Table 3 for an explanation of Category 2M.

Table 2 — HSR to DC correlation to determine MPL$_a$

HSR score	DC equivalent	MPL			
		MTTF$_d$=Medium		MTTF$_d$=High	
		Category B	Category 2M	Category 1	Category 2M
50 % to ≤ 80 %	60 %	MPL$_a$ = b	MPL$_a$ = b	MPL$_a$ = c	MPL$_a$ = c
>80 %	90 %	MPL$_a$ = b	MPL$_a$ = c	MPL$_a$ = c	MPL$_a$ = d

See Annex B for examples of evaluations using HSR scoring.

7.5 Category classifications

7.5.1 General

The appropriate architecture shall be selected to meet the requirements of the system. Although the variety of possible structures is high, the basic concepts are often similar. Thus, most structures which are present can be mapped into one of the categories described in ISO 13849-1:2015, 6.2; however, for some structures used in steering and braking systems, adaptation is required due to hydraulic system characteristics specific to the earth-moving machine application. For each category, a typical representation as a safety-related block diagram is given. These typical realizations are called designated architectures and are listed in the context of each of the following categories.

Some SCS are highly complex and do not necessarily match one of the designated architectures exactly. Designs fulfilling the properties of the respective category in general are equivalent to the respective designated architecture of the category. Figures 2 and 3 show general architectures not specific examples. A deviation from these architectures is always possible, but any deviation shall be justified by means of appropriate analytical tools, demonstrating the system meets the required performance level. For alternate architectures, the hardware fault tolerance (HFT), and any other requirement, shall remain equivalent to the relevant category. The designated architectures shall be considered as logical diagrams, not simply circuit diagrams. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a fault cannot lead to the loss of a safety function (e.g. an ECU with parallel processing, cross monitoring and external watch dogs is considered category 3 or 4).

Table 3 gives an overview of the categories for SCS, the requirements and the system behaviour in case of faults. 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 and technologies which demonstrate suitability and reliability for safety-related applications. Design and verification activities used should include (where applicable):

- fitting the definition of a well-tried component in this document;
- bench testing of load ability and functionality;
- proof testing to loads to a suitable safety factor;
- accelerated durability testing;
- computer-aided analysis and physical correlation studies;
- environmental testing per ISO 19014-3;
- supporting the required MTTF_d.

MCS that interfere with, or mute, a safety function of the SCS shall be assigned the same machine performance level as the SCS, unless it can be shown to require a different MPL_r per ISO 19014-1 or ISO/TS 19014-5.

Table 3 — Summary of requirements for categories

Category	Summary of requirements	System behaviour	MTTF_d	DC	CCF evaluation	HFT
B	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled, and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of a safety function.	low to medium	none	NA	0
1	Requirements of category B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of a safety function. The safe performance of the machine is greater than what is required for a category B system.	high	none	NA	0
2	Requirements of category B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.	The occurrence of a fault can lead to the loss of a safety function, but an action to reduce the risk associated to the fault is taken. Faults in the input and output devices are detected as appropriate and reasonably practicable at or before the next demand upon the safety function.	low	low to medium	required[a]	0

[a] A category 2 architecture could be sensitive to a CCF.

Table 3 *(continued)*

Category	Summary of requirements	System behaviour	MTTF$_d$	DC	CCF evaluation	HFT
2M	Requirements for category 1 shall apply for hydraulic SRP/CS. Requirements for category 2 shall apply for other technologies.	The occurrence of a fault can lead to the loss of a safety function. The system's ability to perform the function is monitored or applicable faults are fault excluded. The system will respond in the presence of a non-fault excluded fault.	high for hydraulic SRP/CS, low for other technologies	low to medium (see Table 2 for hydraulic components)	required[a]	0
3	Requirements of category B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that "a single fault in any of these parts does not lead to the loss of the safety function, and" whenever reasonably practicable, the single fault is detected.	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. Some faults in the input, logic and output devices are detected at or before the next demand upon the safety function.	low to high	low to medium	required	1
4	Requirements of category B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that "a single fault in any of these parts does not lead to a loss of the safety function, and" the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	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. The safe performance of the machine is greater than what is required for a category 3 system. All faults in the input, logic and output devices are detected at or before the next demand upon the safety function or the accumulation of faults cannot lead to the loss of the safety function.	high	high	required	1

[a] A category 2 architecture could be sensitive to a CCF.

For the designated architectures described in Table 4 below the following typical assumptions are made:

- mission time, 20 years;
- constant failure rates within the mission time;

- for category 2, demand rate ≤ 1/100 test rate (see also NOTE in ISO 13849-1:2015, Annex K); or testing occurs immediately upon demand of the safety function and the overall time to detect the fault and to bring the machine to a safe state (usually to stop the machine) is shorter than the time to reach the hazard;
- for category 2, $\text{MTTF}_{\text{d,}}$ of the test channel is greater than half the $\text{MTTF}_{\text{d,}}$ base or function channel.

Table 4 — Categories for different technologies

Category	Mechanical	Pneumatic	Hydraulic	Electronic	Electrical
1	✓	✓	✓	N/A	✓
2	N/A	✓	✓	✓	N/A
3	P/A	P/A	P/A	✓	P/A
4	P/A	P/A	P/A	✓	P/A

Key

N/A: Not applicable

P/A: Parallel add

✓: Applicable

NOTE 1 For more information on P/A, see 7.6 and the examples in Annex A.

NOTE 2 Complex electronic components (e.g. PLC, microprocessor, application-specific integrated circuit) cannot be used in a category 1 architecture.

7.5.2 Category B/Category 1

7.5.2.1 Explanation for application of category B/category 1 for N/ESCS

Most hydraulic and pneumatic valves and mechanical linkages have category B/category 1 architectures. In the case of a hydraulic valve, the function of input, logic and output are done intrinsically in the spring and spool design within the valve. They can be considered as input, logic, and output components all in one. These systems are analogous to their electrical counterparts in that they can perform the same function using a different technology to carry the signal. Figure 2 shows an example of a steering system implemented using two different technologies.

NOTE One way to consider the boundary of the input, logic and output within a system is by considering where the energy in the signal process changes type.

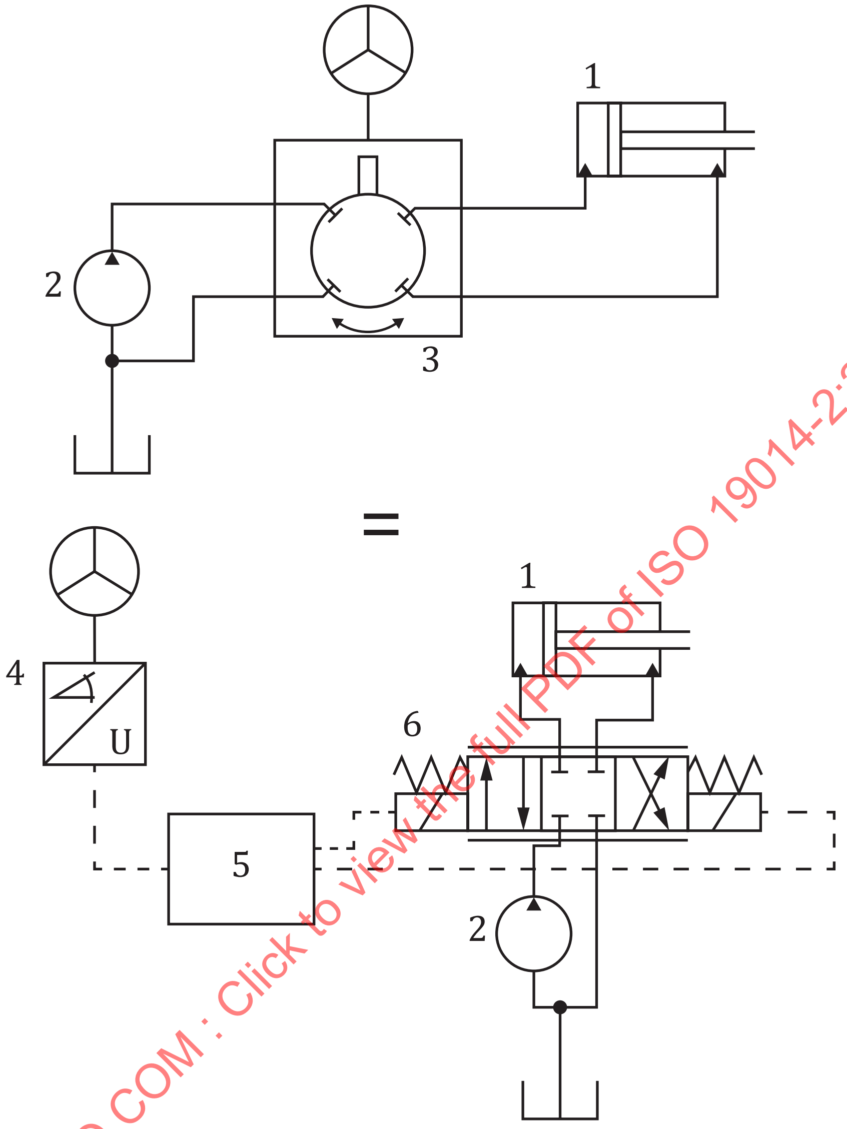
The following is a non-exhaustive list of generic examples:

a) An operator depresses a pedal – the energy changes from kinetic to hydraulic.

b) An operator depresses a pedal – the kinetic energy changes to electrical energy. The signal remains electrical through the I – L components and is then converted to hydraulic pressure.

c) A pilot hydraulic system is very similar to b). The pilot signal is low hydraulic pressure instead of electrical. The output is high pressure hydraulic energy.

7.5.2.2 Examples for application of category B/category 1



Key

1	steering cylinder
2	pump
3	orbital valve
4	steering sensor
5	ECU
6	steering valve

NOTE 1 Electronic systems normally decide how the input power is channelled and controls the output energy based on this. An N/ESCS has the output power channelled through the primary channel and either sends the energy back to tank or uses it to control the machine.

NOTE 2 An electronic system can be category-2 if the ECM has input/output diagnostics and output to mitigate hazard.

Figure 2 — Example of two analogous category B/category 1 steering systems of different technologies: hydraulic steering system(top) and analogous electronic steering system (bottom)

7.5.3 Category 2

7.5.3.1 General

The guidance in ISO 13849-1:2015, 6.2.5 applies with the exceptions and clarifications outlined in this clause.

- When a risk assessment has determined there is sufficient time for the operator to react, an immediate action warning indicator may be used as the OTE in an MPL_r = d SCS.

  NOTE Often, the operator is better suited than the SCS to determine the appropriate response to mitigate the hazard.

- OTE shall be able to put the machine in a safe state within an acceptable time. The safe state shall mitigate the hazard that the safety function is addressing.
- When there are two or more components in parallel within a function block (ILO), and the failure of more than one component is required to cause a loss of the safety function, that block can be considered a category 3 function (see 7.6 for parallel add).

7.5.3.2 Modification of category 2 to hydraulic systems (category 2M)

The application of a category 2M architecture follows the principles and requirements of the category 2 architecture, however, it looks slightly different due to the characteristics of hydraulic components and their application to earth-moving machinery, e.g. steering and braking systems. The term category 2M is used to denote the different approach taken for stationary machines in ISO 13849.

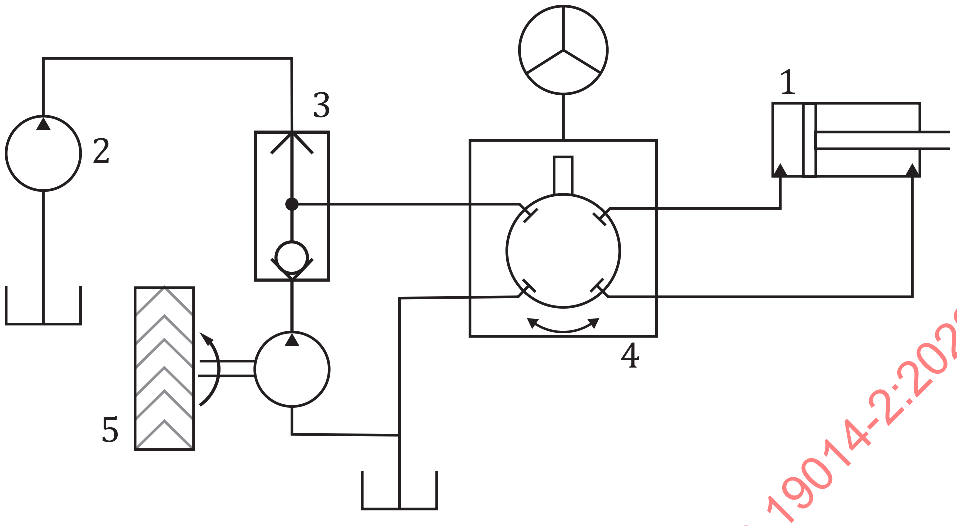
The test channels of category 2M systems do not monitor the primary channel for faults directly; instead, they monitor and maintain the ability of the system to perform its function (e.g. when oil supply is insufficient and switches to a secondary supply). Because their failure modes are well understood and their reliability proven, faults in the primary channel are addressed using the HSR assessment in 7.4; this assessment is used to determine the DC of the system.

NOTE 1 The oil supply is usually monitored by an electronic system, a shuttle valve or a similar device, and supplemented by an accumulator or a backup pump if the primary source of oil is interrupted.

NOTE 2 This is an example of a “fail-operational” system. The safe state is to maintain the ability to steer via the secondary oil supply. The oil supply and steering control have been combined into a single safety function in this case.

A category 2M system is considered equivalent to a category 2 system with regards to the process and requirements for calculating a MPL_a from ISO 13849-1:2015 Table 6. Figure 3 is an example of a category 2M steering system, while Figure 4 shows the system as a block diagram.

7.5.3.3 Example of a category 2M hydraulic system



Key

1 steering cylinder

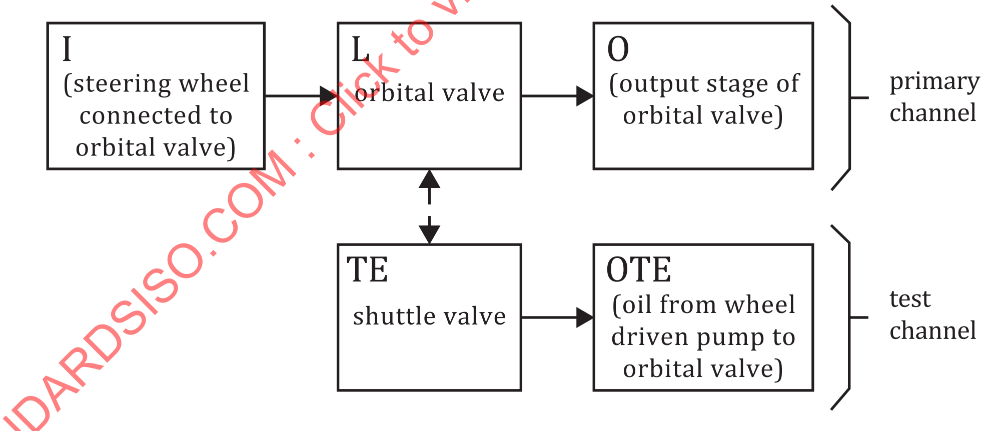
2 pump

3 shuttle valve

4 orbital valve

5 wheel driven pump

Figure 3 — Example category 2M hydraulic steering system


I
(steering wheel connected to orbital valve)
L
orbital valve
O
(output stage of orbital valve)
primary channel
TE
shuttle valve
OTE
(oil from wheel driven pump to orbital valve)
test channel

NOTE 1 The text in parenthesis denotes system features outside of the SRP/CS.

NOTE 2 The terms "ball resolver" and "shuttle valve" are interchangeable.

Figure 4 — Example of hydraulic system block diagram

7.5.4 Conflicting safety functions

In the case of conflicting safety functions, the safe states for some uncommanded applications versus failure on demand functions shall be considered. When this is the case, both failure types shall have their own safety functions, each with their own MPL_r. One of the safety functions will likely have a lower MPL_r than the other, and the safe state may be putting the machine in the safest state according to the highest MPL_r.

An example of this is a brake system on a high-speed machine, where the uncommanded application and failure on demand of the brake are both safety functions. While the higher MPL_r applies to failure on demand of the brake system, the uncommanded brake application can also be dangerous.

Because failure on demand is more dangerous, the ultimate safe state is to bring the machine to a stop. The safe state of the uncommanded activation safety function may be to stop without a command from the operator, but through the test channel; however, consideration should be given in the way the SCS brings the machine to a stop (i.e. in a way that mitigates the hazard of an uncontrolled skid).

NOTE Conflicting safety functions can be fail-operational systems.

If the MPL_r of the conflicting safety function is the same, a category 3 architecture may be used.

7.5.5 Considerations for the SRP/CS of fail-operational systems

Category 2 systems may be used for fail-operational SCS provided the response time of the fault reaction is suitably risk assessed (i.e. meet the performance level outlined in the applicable type-c standard) and is less than the demand rate.

Category 3 systems used in fail-operational applications can function as a completely redundant system. In cases where a single failure could result in conflicting outputs, redundant processing of the safety function with switching functionality between the primary and secondary channels may be used, depending on the fault state of each channel.

NOTE When such switching functionality is utilized, reducing the test frequency does not cause a reduction of diagnostic coverage as the secondary channel is not continuously operational.

An example of an SCS with continuous demand is an electro-hydraulic steering system.

7.6 Combination of SCS to achieve an overall MPL

The following can be used to combine systems in parallel; this can be useful for assessing architectures that do not match those specified for categories 1 to 4. See ISO 13849-1:2015, 6.3 for combining systems in series.

This architecture reduction applies to qualitative requirements; quantitative requirements (e.g. $MTTF_d$, DC, CCF) shall be verified separately. There shall be no common cause failures between the combined elements. An example of MPL_a reduction using series and parallel combination is shown in Figure 5.

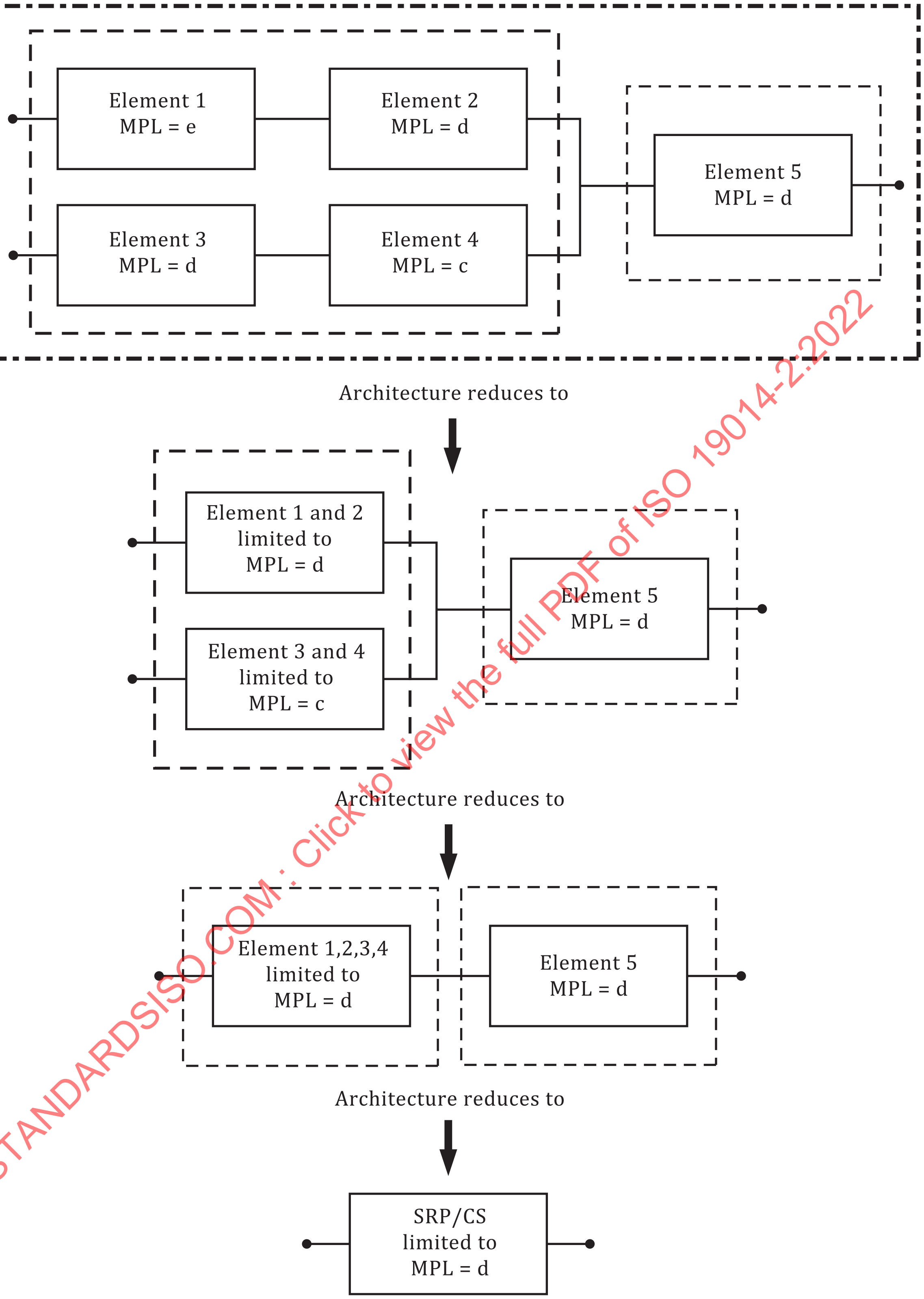


Figure 5 — Series parallel combinatorial MPL$_a$ reduction example

As an alternative to parallel-adding components, two HFT = 0 channels (category B, 1, 2) in parallel may be considered a category 3 system. The operator action to activate the two channels shall meet the requirement of AR3 in ISO 19014-1:2018, 6.5 due to the natural response of the operator, this is only valid if the two channels are truly redundant. Despite the absence of cross-monitoring between the two channels, HFT = 1 is maintained.

This process is also relevant to parallel, redundant elements in the functional blocks within the categories when added in series. Considering the blocks this way can account for, and gives credit to, the added safety margin, considering the blocks as non-redundant components, or omitting one from the calculation, does not.

8 Information for use and maintenance

8.1 General

Information for use shall be provided in accordance with ISO 12100:2010, 6.4.5.

8.2 Operator's manual

ISO 6750-1 outlines the requirements for the content of operator's manual.

In addition, the following information may be shared relative to the functional safety of EMM that meet this standard. This information could be included in manuals or in other documentation given to the end user:

- a listing of the safety functions on the machine;
- a listing of the safety-related parts of the control systems; particularly if changes to those parts could void the functional safety conformance of the machine;
- any maintenance, tests or inspection tasks that are necessary to maintain the integrity of the SCS's over the lifecycle of the machine.

It is not necessary to share the MPL or the category when these systems are being supplied as a complete SCS integrated into a machine.

Annex A
(informative)

Example systems and evaluations

A.1 General

The examples in this annex are intended to illustrate the calculation methodologies for systems of different MPL, categories, and technologies and do not necessarily reflect real systems. Thus, these examples might not align with machine performance level requirements outlined in ISO/TS 19014-5 nor do they suggest that a safe state for safety function would be appropriate on a given machine.

These examples progress from relatively simple to more complex. The examples include SCS components ranging from hydraulic only to components comprising electro-hydraulic SCS. See Table A.1 for a summary of the examples in this annex.

Table A.1 — MPL_a calculation examples presented in this annex

MPL_a	Category	Hydraulic/ hydraulic	Electric/ hydraulic	Electro-hydraulic	Parallel add
b	B			A.1 Steering	
c	1	A.2 Steering	A.3 Park brake		
c	2			A.4 Steering with automatic park brake	
d	2	A.5 Steering			
d	3			A.6 Braking	X

NOTE MTTF$_d$ values for NES/CS can be calculated through MTTF$_d$ values from the component supplier or machine manufacturer or the B_{10d} value per ISO 13849-1:2015, C.4.

A.2 Example 1 — Electro-hydraulic steering, category B

Hazardous event: failure of steering on demand.

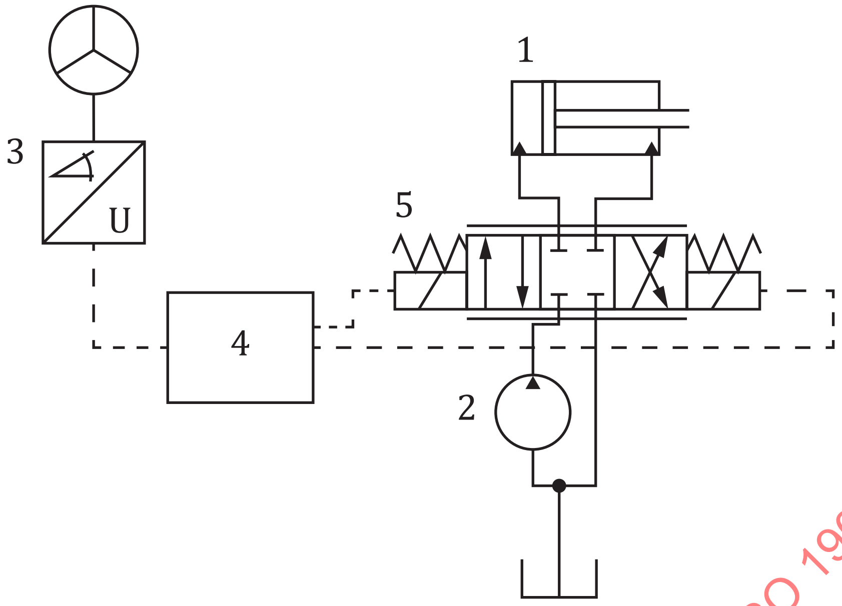
Safe state: N/A, category B has no fault reaction.

Safety function: steer as commanded.

Failure (triggering event) using test equipment (TE): N/A, category B has no test channel.

Reactions to a failure (OTE): N/A, category B has no test channel.

Figure A.1 shows a schematic of a category B electro-hydraulic steering system.



Key

1 steering cylinder
2 pump
3 steering sensor
4 ECU
5 steering valve

Figure A.1 — Scheme of electro-hydraulic steering, category B

Prepare the logic diagram.

An SCS category B electro-hydraulic steering logic diagram is shown in Figure A.2.

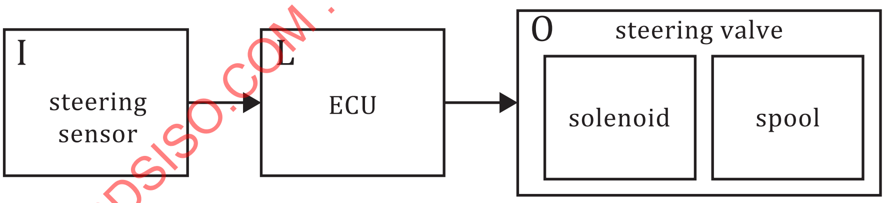


Figure A.2 — Logic diagram of electro-hydraulic steering, category B

Calculate $\mathrm{MTTF_d}$ for the system (limited to the components shown above).

Table A.2 shows the $\mathrm{MTTF_d}$ calculation by parts count for the category B electro-hydraulic steering system.

Table A.2 — Example $\mathrm{MTTF_d}$ calculation by parts count method

Part number	Part description	MTTF_i (from database) years	Dangerous failures %	$\mathrm{MTTF}_{\mathrm{d}i}$ years	$1/\mathrm{MTTF}_{\mathrm{d}i}$ 1/years	Qty	Total
1	Steering sensor	50	50	100	0,010	1	0,010
2	ECU	25	50	50	0,020	1	0,020
3	Solenoid	34	50	67	0,015	2	0,030

Table A.2 *(continued)*

Part number	Part description	MTTF$_i$ (from database) years	Dangerous failures %	MTTF$_{di}$ years	1/MTTF$_{di}$ 1/years	Qty	Total
4	Spool	75	50	150	0,007	1	0,007
$\sum(1/\text{MTTF}_{di})$							0,067
$\text{MTTF}_d = 1/\sum(1/\text{MTTF}_{di})$ in years							14,9

Identify the DC for each component.

Category B system: DC = N/A for all components.

Select MPL$_a$ from ISO 13849-1:2015, Table 6.

NOTE 1 MTTF$_d$ total = 16,7 = medium, DC = 0, category = B; therefore, the MPL$_a$ = b.

NOTE 2 The solenoid and spool can be a single assembly where the solenoid is not a serviceable component; in that case, the assembly is analysed to assign the appropriate MTTF$_d$.

A.3 Example 2 — Hydraulic/hydraulic steering, category 1

NOTE 1 To illustrate the process of calculating the MPL$_a$ of a single-channel hydraulic system, ISO 13849-2 was not used for this example. Components have been assessed as well-tried components according to ISO 13849-2.

Hazard: uncommanded steering.

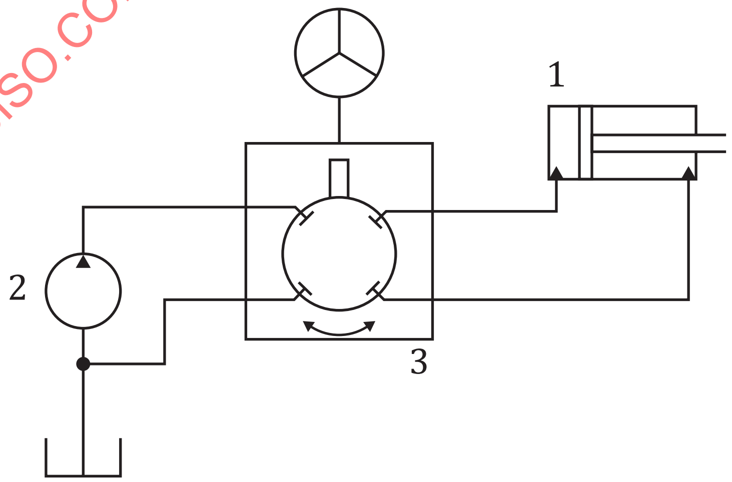
Safe state: N/A, category 1 has no fault reaction.

Safety function: steer only as commanded.

Failure (triggering event) using test equipment (TE): N/A, category 1 has no test channel.

Reactions to a failure (OTE): N/A – category 1 has no test channel.

Figure A.3 shows a schematic of a category 1 hydraulic steering system.



Key

1 steering cylinder

2 pump

3 orbital valve

Figure A.3 — Scheme of hydraulic/hydraulic steering, category 1

Prepare the logic diagram.

An SCS category 1 hydraulic steering logic diagram is shown in Figure A.4.

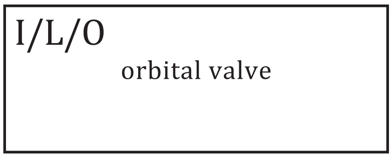


Figure A.4 — Logic diagram of hydraulic/hydraulic steering, category 1

Calculate MTTF$_d$.

Table A.3 shows the MTTF$_d$ calculation by empirical data for the category 1 hydraulic steering system.

Table A.3 — MTTF$_d$ calculation of hydraulic/hydraulic steering, category 1

Component	MTTF$_d$	DC
Orbital valve	167 year empirical data	0

Channel MTTF$_d$ = 100 years, truncated by ISO 13849-1:2015, 4.5.2.

Identify the DC for each component.

Category 1 system; DC = N/A for all components.

Select MPL$_a$ from ISO 13849-1:2015, Table 6.

NOTE 2 MTTF$_d$ total = 100 = high, DC = 0, category = 1. Therefore, the MPL$_a$ =c; reference ISO 13849-1:2015, Table 6.

A.4 Example 3 — Electric/hydraulic park brake, category 1

Hazard: failure to apply park brake.

Safe state: brake applied by spring force.

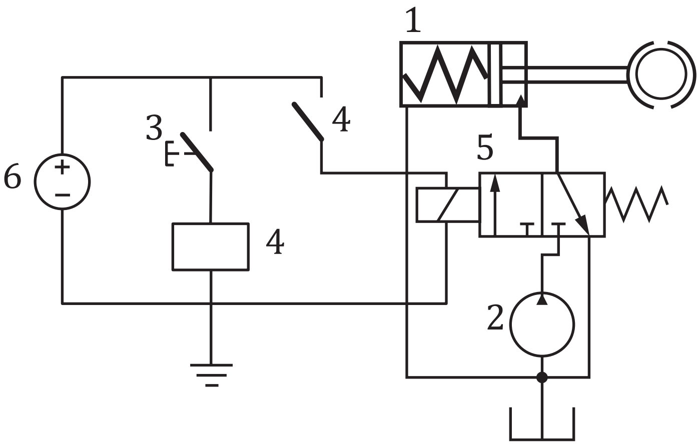
NOTE 1 This is a category 1 system because of the use of well-tried components without complex electronics.

Safety function: apply park brake when commanded. Upon loss of hydraulic or electric power the park brake will apply automatically.

Failure (triggering event) using test equipment (TE): N/A, category 1 has no test channel.

Reactions to a failure (OTE): N/A – category 1 has no test channel.

Figure A.5 shows a schematic of a category 1 electric/hydraulic park brake system.



Key

1 park brake cylinder

2 pump

3 rocker switch (in this case the rocker switch has been assessed to the requirements of ISO 13849-2 and demonstrated to meet the requirements of well-tried components)

4 relay

5 solenoid valve

6 battery source

Figure A.5 — Scheme of electric/hydraulic park brake, category 1

Prepare logic diagram.

An SCS category 1 electric/hydraulic park brake logic diagram is shown in Figure A.6.

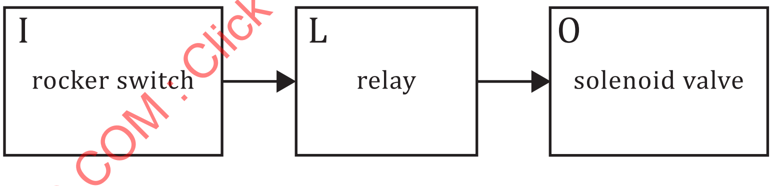


Figure A.6 — Logic diagram of electric/hydraulic park brake, category 1

Calculate MTTF_d for the system.

Table A.4 shows the MTTF_d calculation by parts count for the category 1 electric/hydraulic park brake.

Table A.4 — Example MTTF_d calculation by parts count method

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	Qty	Total
1	Rocker switch	200	50	400	0,002 5	1	0,002 5
2	Relay	200	50	400	0,002 5	1	0,002 5
3	Solenoid valve	100	50	200	0,005	1	0,005
$\sum(1/\text{MTTF}_{\text{d}i})$							0,01
$\text{MTTF}_\text{d} = 1/\sum(1/\text{MTTF}_{\text{d}i})$ in years							100

Identify the DC for each component.

DC = 0 for all components in this basic example.

Select MPL_a from ISO 13849-1:2015, Table 6.

NOTE 2 $MTTF_d$ total = 100 = high, DC = 0, category = 1 (well-tried components). Therefore, the MPL_a = c; reference ISO 13849-1:2015, Table 6.

A.5 Example 4 — Electro-hydraulic steering with automatic park brake, category 2

Hazard: uncommanded steering, failure to steer.

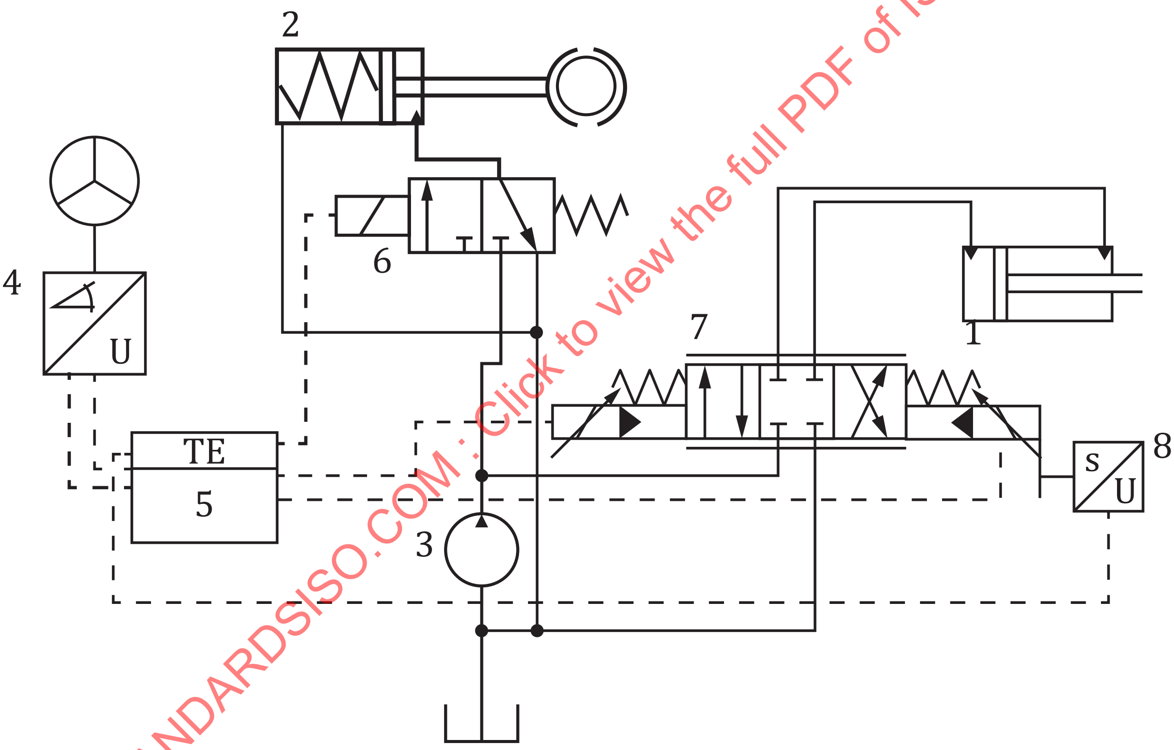
Safe state: halt machine.

Safety function: apply the park brake.

Failure (triggering event) using test equipment (TE): steering solenoid position sensor.

Reactions to a failure (OTE): N/A – halt the machine using the park brake.

Figure A.7 shows a schematic of a category 2 electro-hydraulic steering system with automatic park brake.



Key

1	steering cylinder
2	park brake
3	pump
4	steering sensor
5	ECU (contains both primary and test functionality)
6	park brake valve
7	steering valve
8	spool position sensor (Note this is for fault detection if the valve does not respond as intended)

Figure A.7 — Scheme for electro-hydraulic steering with automatic park brake, category 2

Prepare block diagram.

An SCS category 2 electro-hydraulic steering system with automatic brake logic diagram is shown in Figure A.8.

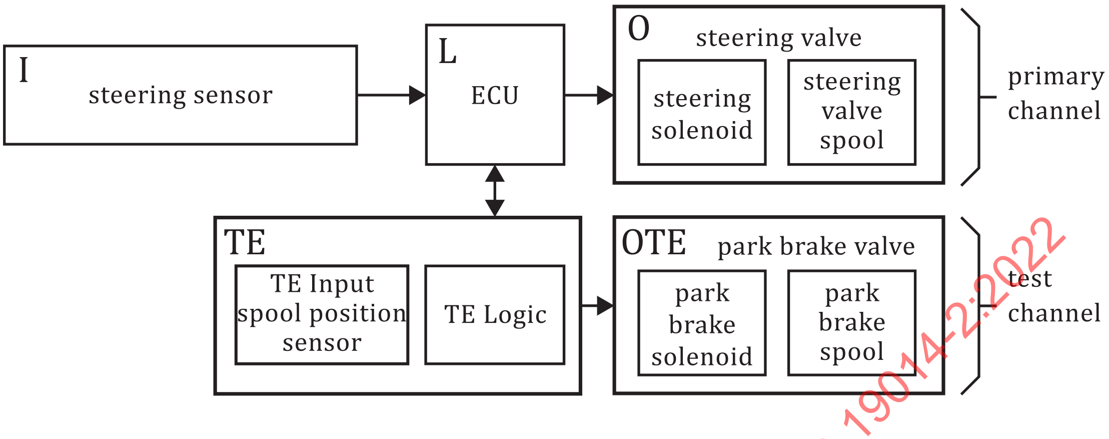


Figure A.8 — Logic diagram of electro-hydraulic steering with automatic park brake, category 2

Calculate MTTF_d for the system.

Table A.5 shows the MTTF_d calculation by parts count for the main channel and Table A.6 for the test channel of a category 2 electro-hydraulic steering system with automatic park brake.

Table A.5 — Example MTTF_d calculation by parts count method for the main channel

Part number	Part description	MTTF_i (from Mfg. data)	Dangerous failures	$\text{MTTF}_{\text{d}i}$	$1/\text{MTTF}_{\text{d}i}$	Qty	Total
		Years	%	Years	1/years		
1	Steering sensor	100	50	200	0,005 0	1	0,005 0
2	ECU (primary functionality)	50	50	100	0,010 0	1	0,010 0
3	Steering solenoid	200	50	400	0,002 5	2	0,005 0
4	Steering valve spool	75	50	150	0,006 7	1	0,006 7
$\sum(1/\text{MTTF}_{\text{d}i})$							0,026 7
$\text{MTTF}_\text{d} = 1/\sum(1/\text{MTTF}_{\text{d}i})$ in years							37,5

Table A.6 — Example MTTF_d calculation by parts count method for the test channel

Part number	Part description	MTTF_i (from Mfg. data)	Dangerous failures	$\text{MTTF}_{\text{d}i}$	$1/\text{MTTF}_{\text{d}i}$	Qty	Total
		Years	%	Years	1/years		
1	ECU (test functionality)	50	50	100	0,010	1	0,010
2	Spool position sensor	100	50	200	0,005	1	0,005
3	Park brake solenoid	100	50	200	0,005	1	0,005
4	Park brake spool						
$\sum(1/\text{MTTF}_{\text{d}i})$							0,020
$\text{MTTF}_\text{d} = 1/\sum(1/\text{MTTF}_{\text{d}i})$ in years							50,0

Identify any common cause failures.

The park brake is “spring applied and hydraulically released” requiring oil pressure to be applied to release the brake. Failure of the power supply will result in the loss of steering and will automatically apply the park brake.

Refer to Table A.7 below to score common cause failures.

Table A.7 — Common cause failure scoring

#	Measure against CCF	Score	Comment
1	**Separation/segregation**		
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creepage distances on printed-circuit boards.	**15/15**	All circuit boards are properly designed. Interconnecting harnesses are proven in use.
2	**Diversity**		
	Different technologies/design or physical principles used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, measuring of distance and pressure, digital and analogue, components of different manufacturers.	**20/20**	All electronic components are susceptible to a failure of the power supply resulting in the loss of steering. The spring applied hydraulically released park brake will automatically be applied.
3	**Design/application/experience**		
3.1	Protection against over-voltage, over-pressure, over-current, etc.	**15/15**	Battery power applied to the circuit is fused. The ECU contains an internal voltage regulator and clamping diodes.
3.2	Components used are well-tried.	**0/5**	The ECU is relatively new and untried.
4	**Assessment/analysis**		
	To avoid common cause failures in design, results of a failure mode and effect analysis are considered.	**5/5**	An FMEA was conducted.
5	**Competence/training**		
	Designers/maintainers have been trained to understand the causes and consequences of common cause failures.	**5/5**	Design and maintenance personnel have completed required training.
6	**Environmental**		
6.1	The system has been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF.	**25/25**	The system has been tested to be conformant to ISO 13766.
6.2	The requirements for immunity to all relevant environmental influences such as temperature, shock, vibration, and humidity have been considered.	**10/10**	The system has been tested to ISO 19014-3 and passed.
	Total	**95/100**	

A score above 65 is passing. Measures against common cause failure have been sufficiently applied.

Identify any fault exclusions.

The harness components used in this system are well-tried and proven in use, see ISO 13849-2:2012, Table D.4. A quality control system is used during production. The harnesses routing is reviewed for quality as part of the design and manufacturing process. All power circuits are fused. All control functions are individually tested at the end of the assembly line. The interconnecting harnesses can reasonably be fault-excluded as it is very unlikely that a harness fault will lead to a hazardous failure.

Identify the DC_{avg} for the system.

a. Identify all dangerous failure modes for each component.

b. Identify all dangerous failure modes that can be diagnosed.

c. Use the formula from ISO 13849-1:2015 Annex E to calculate DC.

Table A.8 shows the calculation of the DC_{avg} for the category 2 electro-hydraulic steering system with automatic park brake.

Table A.8 — Calculating DC_{avg} for the system

Part Number	Part description	Detectable?	Dangerous failure?	DC_{part} %	$MTTF_d$ years	$DC/MTTF_d$	$1/MTTF_d$
1	Steering sensor			90	200	0,45	0,005
	fails in range	yes	yes				
	fails out of range	yes	yes				
2	ECU			60	100	0,6	0,01
	control processor stops	no	yes				
	output driver fails	yes	yes				
	input gate fails	yes	yes				
3	Steering solenoid 1			90	400	0,225	0,002 5
	coil opens	yes	yes				
	coil shorts	yes	yes				
4	Steering solenoid 2			90	400	0,225	0,002 5
	coil opens	yes	yes				
	coil shorts	yes	yes				
5	Steering valve spool			99	150	0,66	0,006 666 67
	fails in range	yes	yes				
	fails out of range	yes	yes				
						2,16	0,026 666 67
	DC_{avg} (%)						81

$$d_{\text{avg}} = \frac{\frac{d_1}{m_1}+\frac{d_2}{m_2}+\ldots+\frac{d_n}{m_n}}{\frac{1}{m_1}+\frac{1}{m_2}+\ldots+\frac{1}{m_n}}$$

$$= \frac{\left(90/200\right)+\left(60/100\right)+2\times\left(90/400\right)+\left(99/150\right)}{\left(1/200\right)+\left(1/100\right)+2\times\left(1/400\right)+\left(1/150\right)}$$

$$= 81\ \%$$

where

d_n is the diagnostic coverage DC of the n^{th} component:

m_n is the mean time to dangerous failure MTTF_d of the n^{th} component.

In this example, the MPL_a is selected from ISO 13849-1:2015, Table 6.

NOTE MTTF_d total = 37,5 = High, DC = low, category = 2; therefore, MPL_a = c.

A.6 Example 5 — Hydraulic steering system, category 2M

Hazard: failure to steer.

Safe state: steer with secondary oil.

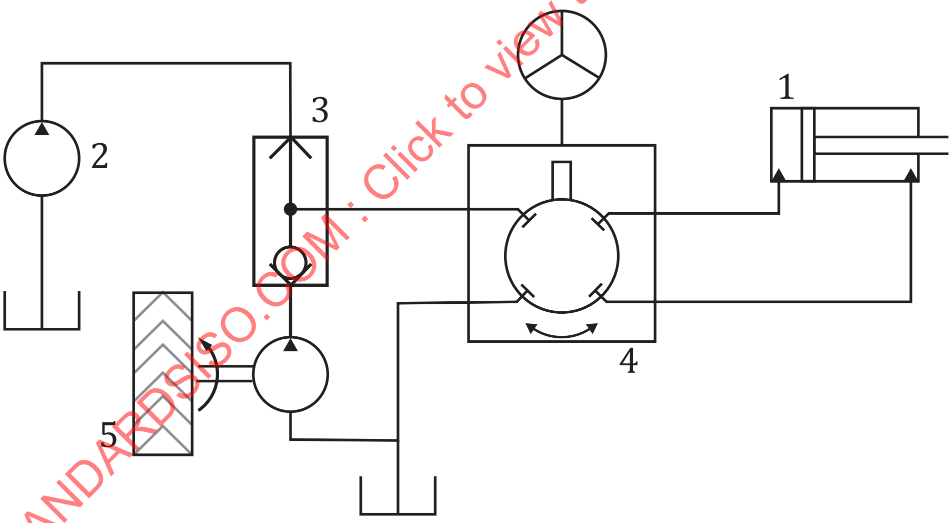
Safety function: steer as commanded.

Failure (triggering event) using test equipment (TE): use oil from secondary source upon loss of oil from primary source. All other faults are fault excluded per ISO 13849-2:2015 and mitigated through non-control system means.

Reactions to a failure (OTE): Steer with secondary oil.

NOTE When a component is fault excluded it is not necessary to calculate the MTTF_d for that component. However, the MTTF_d calculation has been included below in Table A.9 to demonstrate the process.

Figure A.9 shows a schematic of a category 2M hydraulic steering system.



Key

1 steering cylinder

2 pump

3 shuttle valve

4 orbital valve

5 wheel driven pump

Figure A.9 — Scheme of hydraulic steering system, category 2M

Prepare logic diagram.

An SCS category 2M hydraulic steering system logic diagram is shown in Figure A.10.

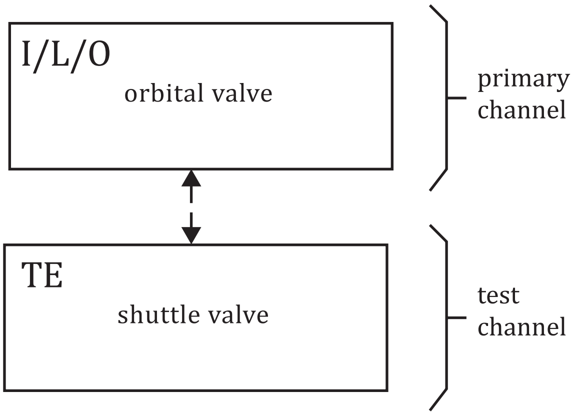


Figure A.10 — Logic diagram of hydraulic steering system, category 2M

Calculate MTTF_d for the system.

Table A.9 shows the MTTF_d calculation by parts count for the main channel and Table A.10 for the test channel of a category 2M hydraulic steering system.

Table A.9 — Example MTTF_d calculation by parts count method for the main channel

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	Qty	Total
1	Orbital valve	200	50	400	0,002 5	1	0,002 5
$\sum(1/\text{MTTF}_{\text{d}i})$							0,002 5
$\text{MTTF}_\text{d} = 1/\sum(1/\text{MTTF}_{\text{d}i})$ in years							400

Table A.10 — Example MTTF_d calculation by parts count method for the test channel

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	Qty	Total
1	Shuttle valve	100	50	200	0,005	1	0,005
$\sum(1/\text{MTTF}_{\text{d}i})$							0,005
$\text{MTTF}_\text{d} = 1/\sum(1/\text{MTTF}_{\text{d}i})$ in years							200

The main channel MTTF_d = 100 years, truncated by ISO 13849-1:2015, 4.5.2.

Identify the DC for each component.

DC = 99 % due to the continuous monitoring provided by the shuttle valve of the primary channel to perform its function.

Select MPL_a from ISO 13849-1:2015, Table 6.

MTTF_d total = 100 = high, DC = high, category = 2M; therefore, the MPL_a = d; reference ISO 13849-1:2015, Table 6.

A.7 Example 6 — Electro-Hydraulic service braking, category 3

Dual channel brake system with analogue pedal sensor and end of travel switch.

The circuit below demonstrates the combination of a redundant braking system that increases the MPL_a by adding the two circuits in parallel.

Hazard: failure to brake.

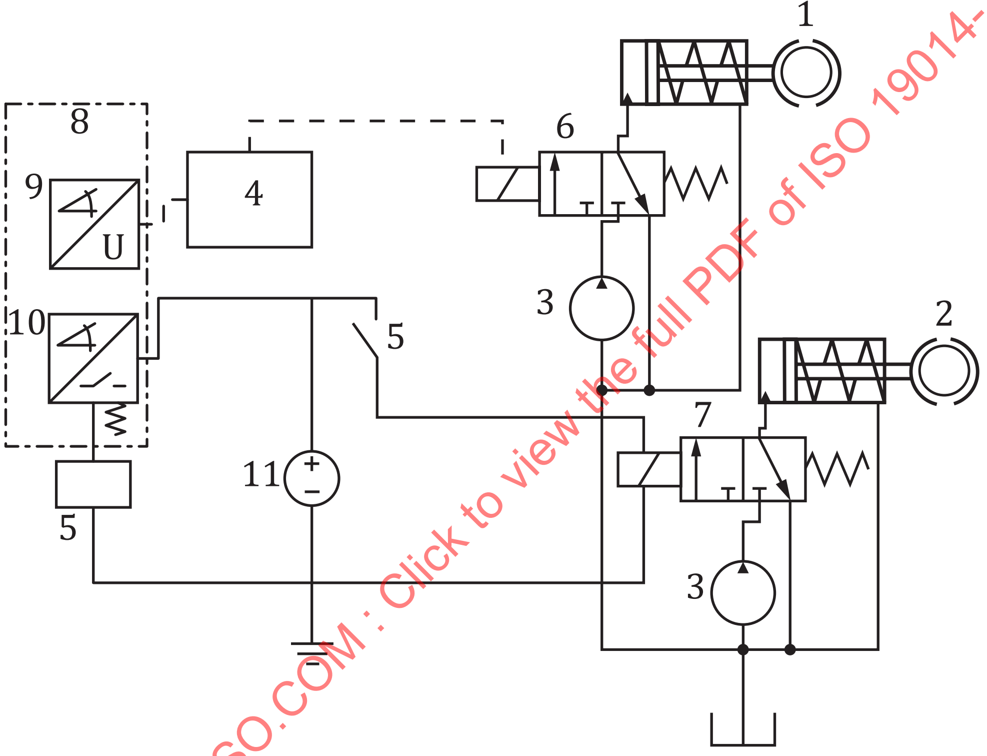
Safe state: brake when commanded.

Safety function: brake with secondary channel.

Failure (triggering event) using test equipment (TE): the brake pedal contains an end-of-travel switch actuating the secondary brake channel if the primary channel fails.

Reactions to a failure (OTE): brake with secondary channel triggered by an end of travel switch.

Figure A.11 shows a schematic of a category 3 electro-hydraulic service brake system.



Key

1 primary brake cylinder
2 secondary brake cylinder
3 pump
4 ECU
5 brake relay
6 primary brake solenoid valve
7 secondary brake solenoid valve
8 brake pedal
9 pedal sensor
10 end of travel switch
11 battery source

Figure A.11 — Scheme of electro-hydraulic service braking category 3

Calculate the MTTF_d for each channel.

For this example, MTTF values could have been obtained from the manufacturer.

Table A.11 shows the MTTF$_d$ calculation by parts count for the primary brake system.

Table A.11 — Example MTTF$_d$ calculation by parts count method

Part number	Part description	MTTF$_i$ (from database)	Dangerous failures	MTTF$_{di}$	1/MTTF$_{di}$	Qty	Total
		years	%	years	1/years		
1	Pedal sensor	200	50	400	0,002 5	1	0,002 5
2	ECU	50	50	100	0,010	1	0,010
3	Primary brake solenoid valve	200	50	400	0,002 5	1	0,002 5
∑(1/MTTF$_{di}$)							0,015
MTTF$_d$ = 1/∑(1/MTTF$_{di}$) in years							66,7

Table A.12 shows the MTTF$_d$ calculation by parts count for the secondary brake system.

Table A.12 — Example MTTF$_d$ calculation by parts count method

Part number	Part description	MTTF$_i$ (from database)	Dangerous failures	MTTF$_{di}$	1/MTTF$_{di}$	Qty	Total
		years	%	years	1/years		
1	End of travel switch	200	50	400	0,002 5	1	0,002 5
2	Relay	200	50	400	0,002 5	1	0,002 5
3	Secondary brake solenoid valve	100	50	200	0,005	1	0,005
∑(1/MTTF$_{di}$)							0,010
MTTF$_d$= 1/∑(1/MTTF$_{di}$) in years							100

Establish the MPL$_a$ of both circuits.

The primary brake circuit MPL$_a$ = c from a similar analysis in the example above.

The secondary brake circuit is a category 1 circuit with High MTTF$_d$ with MPL$_a$ = c.

Identify the total MPL$_a$ for the combined circuit.

The parallel addition of two MPL$_a$= c circuits results in an increase of MPL$_a$ to d.

SRP/CS: (MPL$_a$=c +$_{\text{parallel}}$ MPL$_a$=c) = MPL$_a$=d.

Prepare a logic diagram identifying the SCS.

The logic diagram for a category 3 electro-hydraulic service brake is shown in Figure A.12.

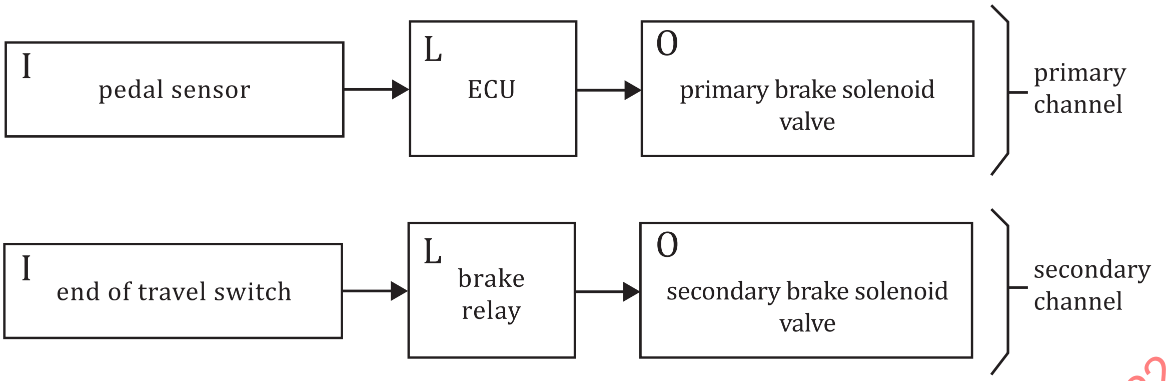


Figure A.12 — Logic diagram of electro-hydraulic service braking category 3

Annex B
(informative)

Examples of evaluations using HSR scoring

B.1 Wheel loader hydraulic steering circuit

The circuit below demonstrates the use of HSR to establish a MPL_a=d for an all hydraulic SCS. The steering wheel controls an orbital valve that provides pressure to a hydraulic cylinder used to steer a machine.

Hazard: failure to steer, uncommanded steering.

Safe state: maintain steering function.

Safety function: steer the machine only as commanded.

Failure (triggering event) using test equipment (TE): shuttle valve detects which of the main steering supply pressure or ground speed driven pump pressure is highest.

Reactions to a failure (OTE): shuttle valve will supply highest pressure to the orbital valve.

Fault exclusions:

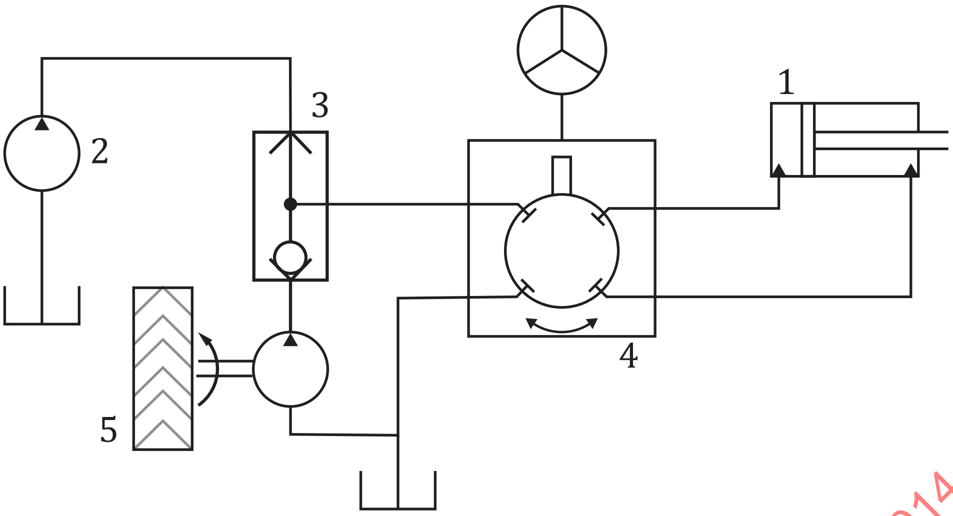
All hydraulic components meet the conditions for the following fault exclusions per ISO 13849-2:2012, Annex C where appropriate:

- change of switching times;
- non-switching or incomplete switching;
- spontaneous change of the initial switching position;
- leakage;
- bursting of the valve housing or breakage of the moving components as well as breakage / fracture of the monitoring or housing screws;
- for proportional valves: hydraulic faults which cause uncontrolled behaviour;
- for shuttle valves: simultaneous closing of both input connections.

NOTE 1 Hosing and connectors similarly meet the requirements for fault exclusion, however those fault exclusions are not specifically listed here.

NOTE 2 Justification supporting the argument for fault exclusion is part of the necessary documentation supporting an MPL claim.

Figure B.1 shows a schematic of an orbital valve steering system.



Key

1 steering cylinder

2 pump

3 shuttle valve

4 orbital valve

5 wheel driven pump

Figure B.1 — Scheme of orbital valve steering system

HSR Scoring for the orbital valve steering system is as shown in Table B.1.

Table B.1 — HSR scoring for orbital valve steering system

Criteria	Possible score	System score	Include in *q* (yes/no)
Over dimensioning (e.g. enough spool clearance, straightness and cylindricity)	+10	+10	No
Countermeasures for spool adherence, spinning	+10	+10	No
Countermeasures for objectionable hydraulic input (e.g. instantaneous high pressure to both ports of hydraulic motor)	+10	+10	No
Secondary energy source (e.g. having pilot accumulator) or failsafe design when loss of energy source.	+20	+20	No
Slowly or stepwise progressive fault (e.g. decrease steering assist force before significant fault)	+10	+10	No
Hose burst mitigation (e.g. piercing debris)	+10	+10	No
System designed to maintain required cleanliness	+10	+10	No
Countermeasures for cavitation caused by aeration in hydraulic oil	+10	+10	No
Countermeasures for pressure transfer problems caused by aeration in hydraulic oil (e.g. air vent circuit)	+10	0	Yes
Total score		90	

Calculation of the HSR score.

t = 90 (sum of "System score" column)