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)

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Symbols and abbreviated terms **2**

5 General requirements **3**
- 5.1 Application 3
- 5.2 Existing SCS 4

6 System design **4**
- 6.1 Overview 4
- 6.2 General requirements 4
- 6.3 Hardware design 5

7 System safety performance evaluation **6**
- 7.1 Machine performance level achieved (MPL_a) 6
- 7.2 Hardware safety evaluation 6
  - 7.2.1 General 6
  - 7.2.2 Fault consideration 6
  - 7.2.3 Fault exclusion 7
  - 7.2.4 Mean time to dangerous failure ($MTTF_d$) 7
- 7.3 Diagnostic coverage (DC) 7
  - 7.3.1 DC of ESCS 7
  - 7.3.2 DC of N/ESCS 7
- 7.4 System-level fault reduction measures of hydraulic systems based on hydraulic system robustness (HSR) 8
  - 7.4.1 General 8
  - 7.4.2 HSR score calculation 8
- 7.5 Category classifications 9
  - 7.5.1 General 9
  - 7.5.2 Category B/Category 1 12
  - 7.5.3 Category 2 14
  - 7.5.4 Conflicting safety functions 15
  - 7.5.5 Considerations for the SRP/CS of fail-operational systems 16
- 7.6 Combination of SCS to achieve an overall MPL 16

8 Information for use and maintenance **18**
- 8.1 General 18
- 8.2 Operator’s manual 18

Annex A (informative) **Example systems and evaluations** **19**

Annex B (informative) **Examples of evaluations using HSR scoring** **33**

Annex C (normative) **Compatibility with other functional safety standards** **37**

Annex D (informative) **Safety function evaluation** **38**

Annex E (normative) **Exceptions, exclusions, additions to ISO 13849-1 and ISO 13849-2** **40**

Bibliography **43**

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.

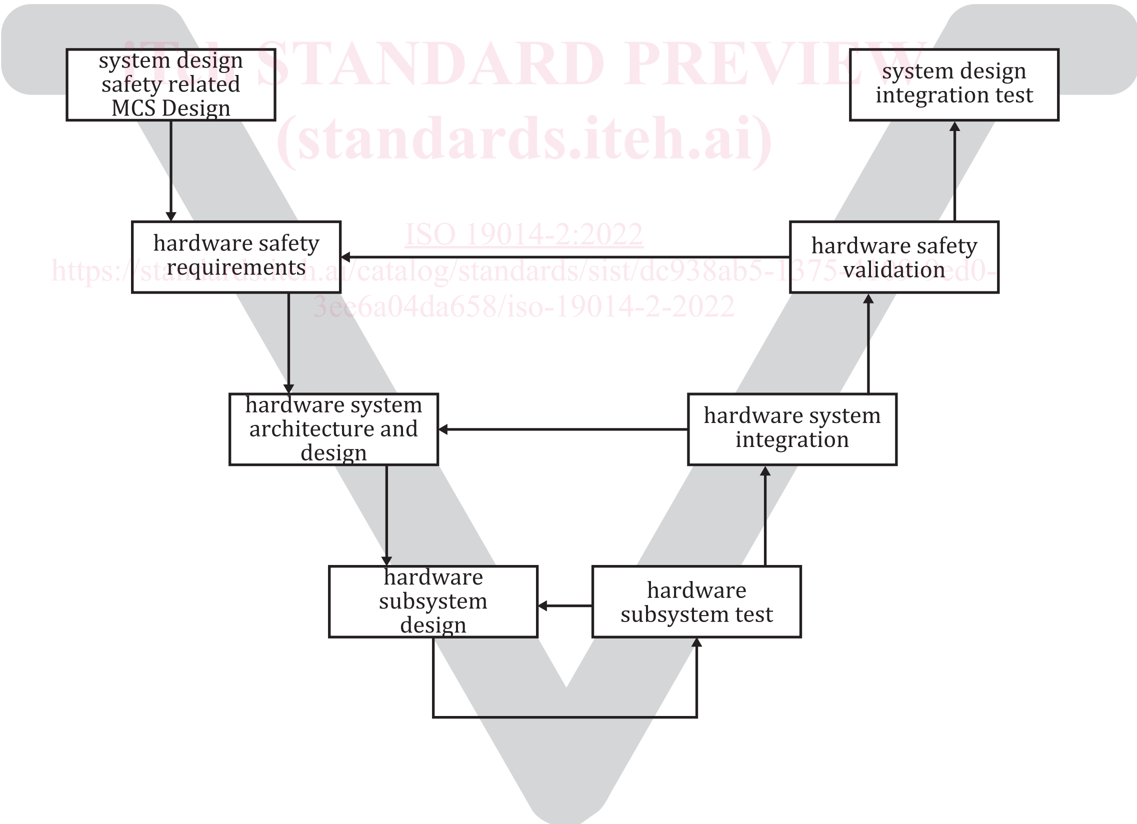

Figure 1 — Hardware development V-model

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