TECHNICAL SPECIFICATION

ISO/TS 15998-2

First edition
2012-10-15

Earth-moving machinery — Machine control systems (MCS) using electronic components —

Part 2: Use and application of ISO 15998

Engins de terrassement — Systèmes de contrôle-commande utilisant des composants électroniques —

Partie 2: Utilisation et application de l'ISO 15998

Reference number
ISO/TS 15998-2:2012(E)

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

Published in Switzerland

Contents

Foreword

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

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

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

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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

ISO/TS 15998-2 was prepared by Technical Committee ISO/TC 127, *Earth-moving machinery*, Subcommittee SC 3, *Machine characteristics, electrical and electronic systems, operation and maintenance*.

ISO 15998 consists of the following parts, under the general title *Earth-moving machinery — Machine control systems (MCS) using electronic components*:

— *Performance criteria and tests for functional safety*

— *Part 2: Use and application of ISO 15998* [Technical Specification]

ISO 15998:2008, *Performance criteria and tests for functional safety*, is to become Part 1.

Introduction

The complexity inherent in electronic controls standards makes it difficult to determine even the basic levels of safety requirements. This part of ISO 15998 has been developed to assist the user of ISO 15998 by defining common earth-moving machinery features and possible failure modes with the reasonable and consistent levels of safety requirements. It will help the user to know that others will be adopting similar requirements for similar hazardous conditions.

While the first part of ISO 15998 and its reference documents are written in the abstract, this Technical Specification outlines processes in a way that relate directly to earth-moving machinery. Through its multiple examples, the user can more easily determine how to apply ISO 15998 to the different types of earth-moving machine.

Earth-moving machinery — Machine control systems (MCS) using electronic components —

Part 2: **Use and application of ISO 15998**

1 Scope

This part of ISO 15998 assists in the interpretation and application of the performance criteria and tests of functional safety for electronic machine control systems (MCS), used on earth-moving machinery, given in the first part of ISO 15998, by

— illustrating an alternative method of hazard assessment,

— providing information and application examples to illustrate compliance with ISO 15998,

— clarifying definitions, requirements and application of ISO 15998, in addressing the risk of hazardous machine movements by safety-related MCS, and

— providing guidance on the use and relationship of the normative references cited in the first part of ISO 15998.

Electronic MCS are those control systems that directly affect machine motion, i.e. propulsion (powered motion), braking, steering, attachments and working tool control systems. ISO 15998 is applicable to the mechanical failures of switches, sensors and other electronic devices and to the mechanical failure of solenoid valves such as sticking caused by debris (electronic fault monitoring of the solenoid valve function can be used if the risk assessment determines it is necessary).

Systems and ESAs (electrical/electronic subassemblies) that are ancillary to machine operation and which do not alter machine control — such as monitors, alarms, gauges, lights and wipers, as well as those portions of systems that provide feedback to the operator — are outside the scope of ISO 15998, as are purely hydraulic, pneumatic and/or mechanical MCS not using electronic/electric components, and mechanical failures such as broken axles, purely mechanical valves, tyres and similar.

2 Normative references

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

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

ISO 13849-1:2006, *Safety of machinery — Safety related parts of control systems*. Corrected by ISO 13849-1:2006/Cor 1:2009

ISO 15998:2008, *Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety*[1)]

[1)] To become ISO 15998-1.

3 Terms and definitions

For the purposes of this document, the terms, definitions and abbreviations given in the first part of ISO 15998 and the following apply.

3.1
base machine
machine with a cab or canopy and operator-protective structures if required, without equipment or attachments but possessing the necessary mounting for such equipment and attachments

[SOURCE: ISO 6016.]

3.2
equipment
set of components mounted onto the base machine that allows an attachment to perform the primary design function of the machine

[SOURCE: ISO 6016.]

3.3
attachment
assembly of components that can be mounted onto the base machine or equipment for specific use

[SOURCE: ISO 6016.]

3.4
safety integrity level
SIL
discrete level (one out of a possible three), corresponding to a range of safety integrity values, where safety integrity level 3 has the highest level of safety integrity and safety integrity level 1 has the lowest

[SOURCE: IEC 61508-4:2010, 3.5.8, modified.]

NOTE 1 The target failure measures (see Table 1).

NOTE 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the electrical/electronic/programmable electronic system safety-related systems.

NOTE 3 SIL is not a property of a system, subsystem, element or component. The correct interpretation of the phrase “SIL *n* safety-related system (where *n* is 1, 2, or 3)” is that the system is potentially capable of supporting safety functions with a safety integrity level up to *n*.

NOTE 4 SIL is most useful for manufacturers applying IEC 61508 or the risk graph presented in the first part of ISO 15998.

NOTE 5 SIL 4 is not used for EMMs (earth-moving machines).

NOTE 6 SIL Θ designates either “No requirement” or “No special safety requirement”. See Table 1 and Figure 1.

3.5
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2006, 3.1.23.]

NOTE 1 PL is most useful for manufacturers using ISO 13849.

NOTE 2 See Table 1.

3.6
required performance level
PL_r
performance level (PL) applied in order to achieve the required risk reduction for each safety function
SEE: Figures 1 and A.1

[SOURCE: ISO 13849-1:2006, 3.1.24.]

3.7
electrical/electronic subassembly
ESA
electrical and/or electronic components or set of components intended to be part of an earth-moving machine, together with any associated electrical connections and wiring, which performs one or more specialized functions

[SOURCE: ISO 13766:2006, 3.10.]

3.8
functional safety
part of the overall safety that depends on a system or equipment operating correctly in response to its inputs

[IEC/TR 61508-0, 3.1.]

NOTE 1 For example, an overtemperature protection device, using a thermal sensor in the windings of an electric motor to de-energize the motor before it can overheat, is an instance of functional safety. But providing specialized insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard).

NOTE 2 Neither safety nor functional safety can be determined without considering the systems as a whole and the environment with which they interact.

3.9
safety-related part of a control system
SRP/CS
part of a control system that responds to safety-related input signals and generates safety-related output signals

[SOURCE: ISO 13849-1:2006, 3.1.1, modified.]

NOTE The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

3.10
machine control system
MCS
system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

[SOURCE: ISO 13849-1:2006, 3.1.32.]

NOTE The machine control system can use any technology or any combination of different technologies (e.g. electrical/electronic, hydraulic, pneumatic, mechanical).

3.11
diagnostic time interval
interval between on-line tests to detect faults in the SRP/MCS

3.12
fault reaction time
time to perform the specified action to achieve or maintain a safe state

3.13
high/continuous mode
mode of operation where the frequency of demands for operation on a SRP/MCS is greater than one per year or greater than twice the frequency of the self-checking feature of the control system

3.14
process safety time
period of time between a failure occurring in the SRP/MCS and the occurrence of the hazardous event if the safety function is not performed

4 General

4.1 Other controls standards

It is strongly recommended that the user of ISO 15998 use at least one of the controls standards referenced in this part of ISO 15998. In particular, IEC 61508-1 or ISO 13849-1 provide general information and theory on electronic control system safety:

— IEC 61508-1:2010, Figure 1, outlines a process for using the IEC 61508 standards to ensure control system safety.

— ISO 13849-1:2006, Figure 1, presents an alternative flow diagram for demonstrating control system safety. Figure 3 shows risk reduction methods (which are further explained in Annex A of this document) for determining both SILs and PLrs.

See Annex B for guidance on creating the safety concept.

Manufacturers may also follow ISO 26262 (road vehicles) or ISO 25119 (agricultural machinery), making appropriate modifications to account for differences with earth-moving machinery. This allowance is to help in the transfer of technology across different industries. Manufacturers should follow one method completely as practical, except they may substitute or add appropriate clauses of IEC 61508.

4.2 Risk assessments (see 4.4 of the first part of ISO 15998)

4.2.1 SILs and PLs

Users have the option of following SIL methods such as those found in IEC 61508-5 and ISO 15998, or PL methods including those found in ISO 13849-1, ISO 25119-2 and ISO 26262-3. Regardless of whether a SIL or PL methodology is chosen, the failure rates for high/continuous demand mode operations shall demonstrate the appropriate level of safety summarized in Table 1.

NOTE 1 Table 1 is for high/continuous demand mode of operation systems. Low demand failure rates are also provided in IEC 61508-1:2010, Clause 7, and Table 2. An explanation on how to use Table 1 is provided in IEC 61508-1:2010, Clause 7, and ISO 13849-1:2006, 4.5.

NOTE 2 SIL 4 is not used for the machines covered by this part of ISO 15998, as it is not a reasonable assessment of an EMM to have a SIL 4 system requirement.

Table 1 — SIL/PL cross-reference table

SIL	**Average probability of dangerous failure per hour** (1/h)	PLr	**Average probability of dangerous failure per hour** (1/h)
—	No safety requirement	—	No safety requirement
—	No special safety requirements	a	$> 10^{-5}$ to $< 10^{-4}$
1	$> 10^{-6}$ to $< 10^{-5}$	b	$> 3 \times 10^{-6}$ to $< 10^{-5}$
		c	$> 10^{-6}$ to $< 3 \times 10^{-6}$
2	$> 10^{-7}$ to $< 10^{-6}$	d	$> 10^{-7}$ to $< 10^{-6}$
3	$> 10^{-8}$ to $< 10^{-7}$	e	$> 10^{-8}$ to $< 10^{-7}$
4	Not used for EMM	—	Not applicable

4.2.2 Risk assessment variations

Because the referenced risk assessment tools are intended as general guidance on determining SILs, it is acceptable and sometimes necessary to adjust risk assessments such as those modifications shown in Figure 1 to achieve a more straightforward correspondence between the reference methods used.

Because of complexity in using the W factor as per Annex A of the first part of ISO 15998, it is also acceptable to assume the W factor is always equal to W_2.

NOTE 1 "Θ" designates either "No requirement" or "No special safety requirement".

NOTE 2 C_4 in ISO 15998:2008, Annex A is not applicable to EMMs, as the probability of EMM involvement in the death of large number of people is negligible.

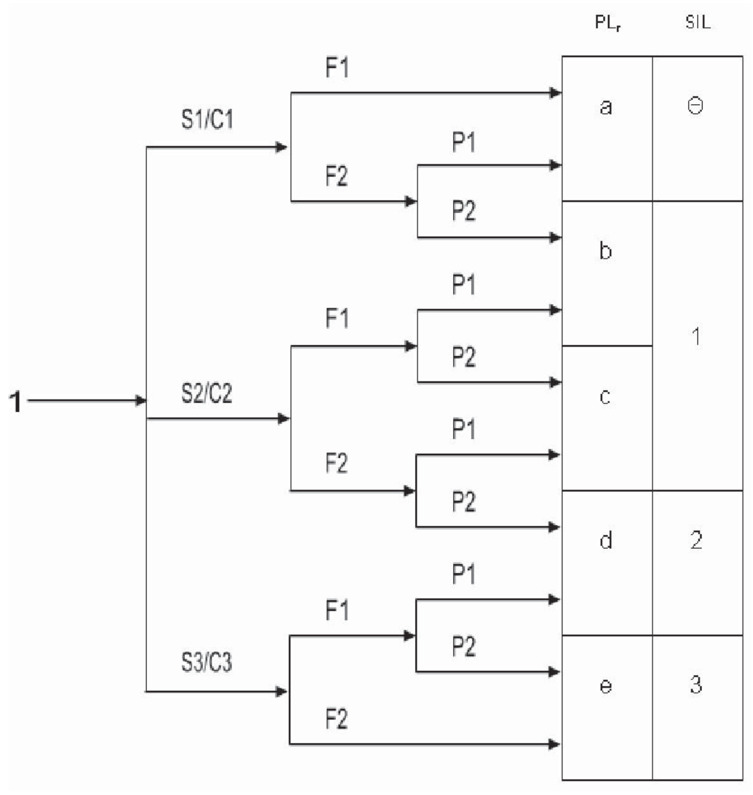


Figure 1 — Risk graph

4.2.3 Reconciling different methods

Regardless of the method used, SIL, PL_r, or equivalent, the failure rates provided in Table 1 shall be used for high/continuous demand systems. Minor adjustments may be made when failure rates do not exactly match those from other standards. Generic SILs/PLs have been established for certain machine control systems and summarized in Annex A. A risk assessment should be completed in order to specify the SIL/PL_r or similar safety requirements for the specific safety function. When risk assessment results vary significantly from the generic SILs, the user of ISO 15998 should examine them carefully to ensure that proper assumptions were made.

5 Additional guidance for safety-related machine-control systems

For ISO 15998:2008, 5.2, see Annex E for guidance.

No additional guidance is given for the remainder of Clause 5 of the first part of ISO 15998.

6 Documentation

Table B.1 (see Annex B) provides a method to summarizing the risk assessment, risk reduction and safety concept in a single spreadsheet for the purposes of organizing the documentation.

7 Test for safety-related MCS

The testing of hardware required per Clause 7 of the first part of ISO 15998, may be conducted at the machine level, system level, sensor level, switch level, harness level or solenoid level, or at the circuit board level or similar, depending upon which is most practical or preferred by the user of ISO 15998. Consideration shall be made for how machine level affects the electrical system for the environmental testing, e.g. temperature in the engine compartment, rigid and soft mounting, and so on.

Documentation from suppliers regarding performance of components is acceptable, in the absence of confirming testing by the OEM.

Annex A
(informative)

Guidelines for risk assessment

A.1 General risk assessments similar to ISO 13849-1 assessments

The ISO 13849-1 method described in this annex provides guidance in determining the PL_r and corresponding SIL associated with specific EMM forms and their SRP/MCS. For examples of other risk assessment methodologies, see Annex A of the first part of ISO 15998, ISO/TR 14121-2, ISO 25119-2, ISO 26262-3 or IEC 61508-5.

The hazard analysis should only consider reasonably foreseeable scenarios. For example, a steel tracked dozer on the highway should not be evaluated (unless the intent is to meet some unique customer requirement). Simply state that it is normally illegal to use a steel tracked dozer on the highway because of the severe road damage that would result. Each reasonable foreseeable scenario should be assessed in terms of the operator and a bystander's severity of injury, frequency and possibility of avoiding the hazard.

A.1.1 Use of risk graphs

The initial determination of the risk parameters is made without the consideration of any MCS or any safety feature integrated in the MCS to analyse the risk solely on the associated hazard. Additional guidance on how to perform a risk assessment is included in the risk parameters instructions below. The risk assessment initially assumes failure modes exist, which will cause hazardous machine behaviour. Means for mitigating those hazards are considered later in the process.

A.1.2 Severity of injury — S1, S2 and S3

Severity has 3 levels: S1 (slight — normally reversible injury), S2 (serious — normally irreversible injury or single death) and S3 (catastrophic — multiple fatalities). When selecting a severity level for a hazard, select the level that would result from the worst credible outcome of the hazard rather than the worst conceivable outcome, as this could always result in an S3. When selecting a level, also look at the immediate result without additional conditions to be present for the consequence to occur. For instance, one could imagine a tracked dozer steering right uncommanded and hitting a gas pipe line, exploding and causing multiple fatalities among bystanders. This scenario relies on many conditions to be present and is not a credible outcome of the uncommanded steering hazard. To make a decision, the usual consequences of accidents and normal healing processes should be taken into account in determining S1 and S2. For example, bruising and/or lacerations without complications would be classified as S1, whereas amputation or death would be S2.

S3 is equivalent to C_3 according to the first part of ISO 15998. This severity/consequence is defined as the "death of several people".

Another condition to consider is whether or not the EMM will be operating in traffic on public roads, a credible scenario that could result in multiple deaths (S3), whereas hazards associated with operation at a confined construction site may be one (1) level less severe (S2). When used off-road, machines are exposed to far less vehicular traffic. Therefore, machines prohibited from on-road use can reduce the severity level by one (1), compared to a similar roadable version, with respect to loss of steering or braking functionality and the associated risks of collisions with vehicular traffic.

EXAMPLE A 4WD loader that is used on-road might have a S3 for a complete loss of steering. If there is a similar loader, but it is too large for use onroad, then a lower severity level S2 might be specified for the same loss of steering condition.

Smaller machines, due to their smaller mass, impart lower forces during collision. Therefore, a compact machine's severity level relative to bystanders and vehicular traffic could be lowered by 1, when compared to a larger version in the same conditions.

A.1.3 Frequency and/or exposure times to hazard (F_1 and F_2)

A percent time of exposure can be difficult to determine when selecting between F_1 and F_2. However, the following explanation could facilitate making the right decision where doubt exists.

F_2 should be selected if a person is frequently or continuously exposed to the hazard i.e. ≥ 10 % of the time. It is irrelevant whether the same or different persons are exposed to the hazard on successive exposures, e.g. for the use of lifts. The frequency parameter should be chosen according to the frequency and duration of access to the hazard.

Where the demand on the safety function is known by the designer, the frequency and duration of this demand can be chosen instead of the frequency and duration of access to the hazard. In this annex, the frequency of demand on the safety function is assumed to be more than once per year.

The period of exposure to the hazard should be evaluated on the basis of an average value which can be seen in relation to the total period of time over which the equipment is used. For example, if it is necessary to have workers in close proximity to the EMM during cyclic operation in order to feed and move work pieces, then F_2 should be selected. If exposure is only required from time to time, then F_1 should be selected.

In case of no other justification F_2 should be chosen if the frequency is higher than once per hour or exposure to the hazard more than 10 % of the time.

EXAMPLE 1 Operating near the edge of a cliff: the operator is most likely exposed to the edge of the cliff less than 10 % of the time so the frequency level would be F_1.

EXAMPLE 2 If operation is grading, and the steering system fails, for a motor grader this occurs most of the time, so the frequency level would be F_2.

A.1.4 Possibility of avoiding the hazard (P_1 and P_2)

When a hazardous situation occurs, P_1 should only be selected if there is a realistic chance of avoiding an accident or significantly reducing its effect; P_2 should be selected if there is almost no chance of avoiding the hazard.

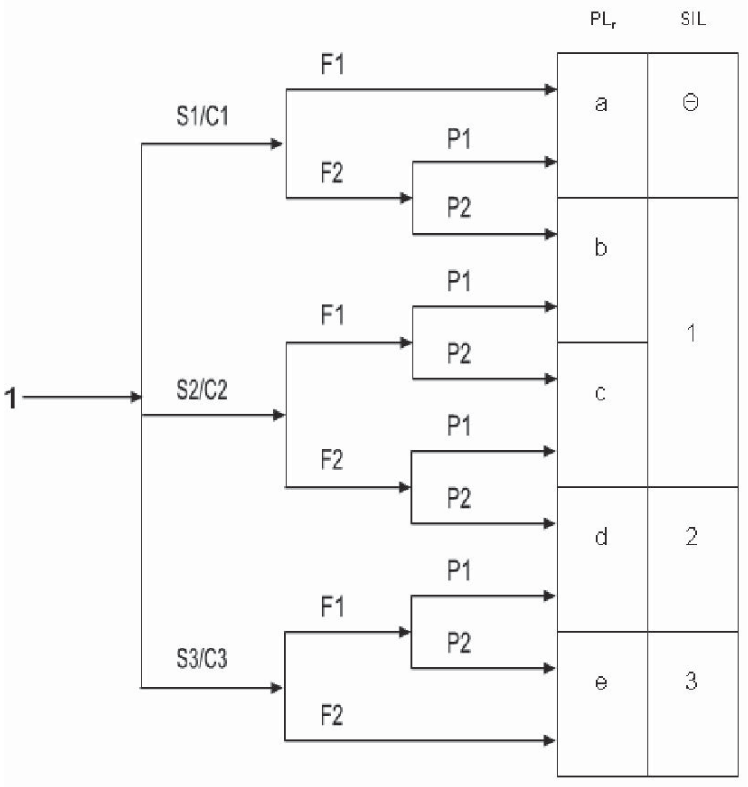
EXAMPLE A full loss of brakes on a wheel loader can initially appear to be P_2. A bucket could be lowered to stop the machine so the possibility level would drop to P_1. Lesson: when including external sources as a means of avoiding a hazard, it needs to be ensured that the design is independent of the system being evaluated. In this case, as long as the implement controls are independent from the braking system (i.e. no shared components), then dropping the bucket sufficiently mitigates the hazard risk.

It is important to know whether a hazardous situation can be recognized and avoided before leading to an accident. For example, an important consideration is whether the hazard can be directly identified by its physical characteristics, or recognized only by technical means, e.g. indicators. Other important aspects which influence the selection of parameter P include

- operation with or without jobsite supervision,
- operation by experts or non-professionals,
- speed with which the hazard arises (e.g. quickly or slowly),
- possibilities for hazard avoidance (e.g. by escaping), and
- practical safety experiences relating to the process.

The "possibility of avoiding" should not take into account design architecture to address the safety function being analysed: i.e. if analysing risks surrounding an electronic steering system, the design architecture of the electronic steering system cannot contribute to the possibility of avoiding the hazard but other independent systems (such as brakes or mechanical steering system) can.

Figure A.1 provides an example of a risk graph used to determine the required PL_r for various scenarios using the hazard analysis parameters for severity, frequency and/or exposure time and possibility of avoiding the hazard. The graph (or the alternative risk graph mentioned in 4.1.2) should be used for assessing all reasonably foreseeable scenarios for each safety function. The risk assessment method is based on ISO/TR 14121-2 (see also ISO 13849-1:2006, Annex A) and should be used in accordance with ISO 12100.



Key

1 starting point for risk estimation

S1/C_1 slight (normally reversible injury)

S2/C_2 serious (normally irreversible injury or death)

S3/C_3 death of several people

F_1 seldom-to-less-often and/or exposure time is short

F_2 frequent-to-continuous and/or exposure time is long

P_1 possible under specific conditions

P_2 scarcely possible

a–e required performance level (PLr) for MCS

Figure A.1 — Risk graph for determining PL_r for safety function

If ISO 13849 methods are used, then in applications where the SRP/CS can be considered simple, and the required performance level is a to c, a qualitative estimation of the PL may be justified in the design rationale. See also Annex E for additional guidance on using ISO 15998 methods more directly.

A.2 Guidance and examples of risk analysis for EMMs fitted with MCS for steering, propel, braking, and attachment operation for ISO 15998, ISO 13849-1 or other similar risk assessments

The hazards for the four primary operating functions of EMM examples are given to illustrate hazard identification and allocation of risk parameters. This clause is without respect to a specific control system, but is based on typical EMM forms, given a failure can occur that causes the EMM to behave in an unintended manner.

The risk graph given in ISO 13849-1, in the first part of ISO 15998 and by other risk assessment methods could indicate in some cases higher SILs/PL$_{\mathrm{r}}$s than provided by the examples and generic SILs/PL$_{\mathrm{r}}$s in this annex. However, the examples and generic SILs/PL$_{\mathrm{r}}$s do reflect state of the art available for each type of function. Furthermore, experience (e.g. accident history) indicates they are adequate and proven for each function.

The following should be considered when using the risk assessments and Tables A.1 to A.5 for EMMs.

A.2.1 Severity considerations

Severity should not be skewed by extremely unlikely events. If, for example, in 999 cases out of a 1 000, the anticipated injury would be very minor in an accident, but in one case a death is predicted, then the consequence is properly rated S1 or C_1.

A.2.2 Frequency considerations

Some machine applications can have very low frequencies of exposure, such that F_1 would not adequately describe how low the frequencies are. In those cases, it may be more appropriate not to evaluate the scenario

EXAMPLE Using a steel tracked dozer on the highway is very seldom done and is generally illegal. It is therefore not necessary to evaluate the risks associated with it.

A.2.3 Overall assessment considerations

S/C, P and F values are typically based on the consideration of a list of contributing factors that each tend to raise or lower these value partially. Table A.1 shows some of the key factors used in determining the values. After the contributors are known, the closer of the values, for example, P_1 or P_2, was selected. Risk assessments may have more resolution (e.g. ISO 25119-2) than in the examples provided here.

Examples are given for two of the various risk assessment methods. The user should select one risk assessment method for the entire control systems evaluated, to avoid conflicting results.

As speed increases, SILs/PL$_{\mathrm{r}}$ associated with steering and braking increase due to limitations of the operator in maintaining control after a failure (P). Severity also increases due to higher speeds during a collision (S/C).

Bystander presence varies significantly in some scenarios: mining sites typically have few or no bystanders, the presence of which is restricted on most mining sites. Small and medium-sized excavators and all tractor loader backhoes more often have bystanders near excavation sites. The frequency (F) should vary accordingly for bystanders.

Collisions between EMMs typically cause fewer and less severe injuries, which tends to result in lower S/C values and lower SIL/PL$_{\mathrm{r}}$ values. EMM and vehicular traffic collisions tend to have higher S/C with respect to the occupants of the vehicle.

Partial loss: it is easier to maintain control of the machine in steering and braking losses, than complete losses (P). Braking and steering maintained at 90 % operate almost normally. Steering and braking functionality at < 5 % are insufficient to prevent most accidents.

E-Stop/PB/hydraulic enable/key switch: a shutdown control’s effectiveness in avoiding an accident (P) varies significantly with machine speed. It is somewhat effective when an immediate stop works, such as for a slow-moving steel tracked machine, or stopping an attachment when a bystander is present. It is not as effective in dealing with a loss in steering at higher speeds.

When used off-road, machines are exposed to far less vehicular traffic and have a correspondingly lower S/C value. Therefore, machines prohibited from on-road use may have a SIL/PL_r one level less than a similar road-able version with respect to loss of all steering functionality and the associated risks of collisions with vehicular traffic. For example, A 4WD loader used on-road has a SIL 3/PL_r e for a complete loss of steering when there is no prior warning. For a similar loader too large for on-road use, the requirement is one level less or SIL 2/PL_rd for the same loss of steering condition.

Table A.1 — Generic SIL/PL_r risk assessments of hazard identification and risk parameter allocation for EMMs with and without MCS, using risk assessment similar to that of ISO 13849-1 or ISO 15998

Hazards to operator	**Severity of injury,** S or C	**Frequency and/or exposure time to hazard,** F	**Possibility of avoiding the hazard,** P	**Required performance level, PL_r**	**SIL**
1 – Steel tracked dozer travelling at speeds ≤ 12 km/h	N/A (not applicable)	F_2	P_1	No requirement	Θ
Uncommanded brake apply. Machine stops very abruptly.	Operator very unlikely to be injured	Machine frequently propels at speeds adequate to cause minor injuries.	Machine is provided with a seat belt, when used it significantly reduces risk of injury. The operator can use feet to brace himself. Front of cab has no sharp edges inside the zone of reach. Machine typically slips traction as it stops, reducing abruptness of the stopping.		
2 – Articulated dump truck travelling ≤ 60 km/h	S2/C_2	F_2	P_1	c	1
Uncommanded brake apply. Machine stops very abruptly.	Operator can experience significant injury during a rollover.	Machine frequently propels at speeds and payload sufficient to cause a rollover.	Machine is provided with a seat belt, when used it significantly reduces risk of injury. The operator can use feet and hands to brace himself. Front of cab has no sharp edges inside the zone of reach. Payload prevents brake from locking in most cases. Machine ROPs prevents operator from being crushed.		
3 – Rubber-tyred trencher travels < 12 km/h	N/A	F_2	P_1		Θ

Table A.1 *(continued)*

Hazards to operator	**Severity of injury,** S or C	**Frequency and/or exposure time to hazard,** F	**Possibility of avoiding the hazard,** P	**Required performance level, PL$_r$**	**SIL**
1. Machine begins to propel with F/N/R in neutral. 2. Or machine propels in opposite direction commanded. — Operator is compelled to be present in operator station — Operator has at least one primary control to stop motion.	Operator very unlikely to be injured.	Operator is normally present. Machine is frequently in neutral.	Operator can press the service brake to stop. Machine is provided with a seat belt, when used it significantly reduces risk of injury. Front of cab has no sharp edges inside the zone of reach. Machine speed is typically very slow, allowing more time for operator to respond.	No Requirement	
4 – Tractor loader backhoe travels ≤ 40 km/h	S1 or C_1	F_2	P_1	a	Θ
1. Machine begins to propel with F/N/R in neutral. 2. Or machine propels in opposite direction commanded. — Operator is compelled to be present in operator station — Operator has at least one primary control to stop motion.	Operator can experience minor reversible injury. Bumps and bruises are most likely. In very rare cases the machine can roll and the operator can fall from the operator station and suffer more severe injuries.	Operator is normally present. Machine is frequently in neutral.	Operator can press the service brake to stop. Machine is provided with a seat belt, when used it significantly reduces risk of injury. Front of cab has no sharp edges inside the zone of reach. Machine speed is typically very slow, allowing more time for operator to respond.		
5 – Articulated wheeled loader, too big for on-road use, travel speed less than 40 km/h	S2/C_2	F_1	P_1	b	1
Complete loss of all brakes for stopping. — Operator can only allow machine to coast to a stop or use attachment to stop. — Steering remains functional.	Operators can be injured due to Machine colliding with other machines. Machine can be involved in a rollover.	Loaders typically operate near obstacles including EMMs that can be hit.	Operator can steer the machine around obstacles. Machine is provided with a seat belt, when used it significantly reduces risk of injury.		
6 – Articulated wheeled loader	S2/C_2	F_1	P_2	c	1
Machine boom, bucket or other attachment moves without command. The equipment or attachment is turned-off by a disabling lever, switch or similar.	Operator can be greasing machine, or otherwise near moving parts.	Operator typically in harm's way, much less than 10 % of time.	If operator is near moving part, it can be very difficult to get away quickly enough to prevent injury.		
Hazards to bystanders	S/C	F	P	PL$_r$	SIL1
7 – Compact machine ≤ 20 km/h	S2/C_2	F_1	P_1	b	1
Machine begins to propel with F/N/R in neutral. — Operator is compelled to be present in cab. — Operator still has service brake.	Bystander can be crushed between machine and hard surface.	Bystanders close the machine and in the path less than 10 % of time.	Operator can stop the machine in the normal operating position. Operator will instinctively apply braking. Bystander can move out of machine's path		

Table A.1 *(continued)*

Hazards to operator	**Severity of injury,** S or C	**Frequency and/or exposure time to hazard,** F	**Possibility of avoiding the hazard,** P	**Required performance level, PL$_r$**	**SIL**
8 – Steel-tracked dozer travelling at speeds ≤ 12 km/h	S2/C_2	F_1	P_2	c	1
Complete loss of all brakes for stopping. — Operator can only allow machine to coast to a stop or use blade to stop. — Steering does not remain functional	Bystander can be crushed between machine and hard surface. Bystander can be run over.	Bystander is not frequently present in potential path of the machine.	There is no possibility to steer machine. Bystander can move out of machine's path in some cases. Machine speed is initially lower than most EMMs.		
9 – Tractor loader-backhoe Travelling < 40 km/h	S2/C_2	N/A	N/A		Θ
Unexpected brake apply. Machine stops very abruptly, and can skid. Steering remains functional, but is limited.	Bystander can be crushed between machine and hard surface. Bystander can be run over.	Frequency is negligible, because a bystander extremely unlikely to be in the path of a machine that is stopping faster than operator intended, even in the event of a rollover.	No further evaluation is needed.	No Requirement	
10 – Skid steer loader	S2/C_2	F_1	P_2	c	1
Machine boom or bucket or other attachment moves without command. — Operator is compelled to be in the operator station. — Operator can stop engine, to stop movement.	Bystander can be crushed between machine and hard surface. Bystander can be run over.	Bystander typically in harm's way, much less than 10 % of time.	If bystander is near moving part, it can be very difficult to get away quickly enough to prevent injury.		
Hazards to vehicular traffic	S/C	F	P	PL$_r$	SIL
11 – Articulated grader travelling ≤ 50 km/h. Machine is roadable	S3/C_3	F_2	P_2	e	3
Complete loss of primary steering and emergency steering (either steers uncommanded or not at all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering.	Vehicular traffic accident can result in multiple deaths.	Roadable motor grader is frequently roaded.	There is no possibility to steer machine. Vehicular traffic can move out of machine's path in some cases.		
12 - Articulated wheeled Loaders < 40 km/h	S3/C_3	F_1	P_2	e	3
Complete loss of primary steering and emergency steering (either steers uncommanded or not at all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering.	Potential to hit higher speed vehicle with multiple passengers	Multi-passenger vehicles in the path of machine is much less than 10 % of time.	There is no possibility to steer machine. Operator can stop the machine. Vehicle can be able to avoid the loader.		

Table A.1 *(continued)*

Hazards to operator	**Severity of injury,** S or *C*	**Frequency and/or exposure time to hazard**, *F*	**Possibility of avoiding the hazard,** *P*	**Required performance level, PL$_{\text{r}}$**	**SIL**
13 – Rigid frame haul truck, not allowed on highway < 60 km/h	S3/*C*3	N/A	N/A	N/A	N/A
Complete loss of primary steering and emergency steering (either steers uncommanded or not at all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering.	Potential to hit higher speed vehicle with multiple passengers	Neither used nor allowed onroad. Very rare risk of bus on mining site is negligible.	No further evaluation is needed.		

A.3 Safety integrity levels (SIL)/Performance Levels (PL$_{\text{r}}$) from generic SIL/PL$_{\text{r}}$ risk assessments

A.3.1 Tables A.2 to A.5 show comparison SIL/PL$_{\text{r}}$ values for various machine forms and operating functions based upon example risk assessments and assignment of the SIL/PL$_{\text{r}}$. These examples show the generic SILs/ PL$_{\text{r}}$s to illustrate conservative values for SRP/MCS.

A.3.2 Hazards are categorized according the operator (Op.), bystander (Bys.) and vehicular traffic (Veh.). Vehicular traffic refers to automobiles, trucks and busses encountered while transporting on or working on highways. Vehicular traffic for this chart does not refer to other EMMs found on a job site.

NOTE 1 Regional requirements for roading are not necessarily the same as the values in Tables A.2 to A.5.

NOTE 2 Maximum speed indicates maximum speed on level ground.

Depending on the situation, service personnel can be either operators or bystanders on the generic SIL/PL$_{\text{r}}$ chart. When a service person is inside the operator station, the operator hazards (Op.) from the chart generally refer to hazards associated with servicing the machine. When the service person leaves the operator station, then he is still considered an operator. If there are two individuals involved with servicing a machine, one in the operator station and one outside the operator station, then the bystander (Bys.) hazards address the service person outside the operator station.

Table A.2 — Generic SIL/PL$_r$ chart

Failure mode	Hazard cat.	Steel-tracked dozer, loader, pipelayer, scraper puller ≤ 12 km/h	Articulated rubber-tracked dozer or loader ≤ 40 km/h	Tractor loader-backhoe ≤ 40 km/h	Articulated wheeled loaders ≤ 40 km/h	Art. wheeled loader, too big for onroad use/ Undergrnd. mining loader/ Landfill compactor ≤ 40 km/h	Articulated compact wheeled loader ≤ 40 km/h
STATIONARY MACHINE							
Any movement of machine: Such as articulation, propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar begin to move uncommanded — Stationary machine — Operator is not present — Disabling devices/park brakes applied. — Engine can be running. — Attachments on ground where appropriate for machines not in use.	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	N/A	SIL 1/PL$_r$ b
Engine starts uncommanded During maintenance. —Battery disconnector is locked in position OFF	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
WORKING MACHINE							
Propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar remains stationary when commanded to move.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	SIL Θ / No requirement
PROPEL/BRAKING							
Propel speed/acceleration much higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such as the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL Θ / No requirement	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL Θ / No requirement	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	N/A	SIL 1/PL$_r$ b

Table A.2 *(continued)*

Failure mode	Hazard cat.	Steel-tracked dozer, loader, pipelayer, scraper puller ≤ 12 km/h	Articulated rubber-tracked dozer or loader ≤ 40 km/h	Tractor loader-backhoe ≤ 40 km/h	Articulated wheeled loaders ≤ 40 km/h	Art. wheeled loader, too big for onroad use/ Undergrnd. mining loader/ Landfill compactor ≤ 40 km/h	Articulated compact wheeled loader ≤ 40 km/h
Propel speed/acceleration slightly higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	SIL Θ/No requirement
Complete loss of all brakes for stopping. — Operator can only allow machine to coast to a stop or use attachment in some cases. — Steering remains functional for most wheeled machines, but not for skid steers and crawler machines.	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	N/A	SIL 2/PL_r d	SIL 2/PL_r d	SIL 2/PL_r d	N/A	SIL 1/PL_r b
Complete loss of service and secondary braking. — Operator still has at least one primary control to stop the machine, such as park brake.	Op.	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	N/A	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	N/A	SIL 1/PL_r b
Complete loss of engine/ transmission/electrical retarder. — Maintain service, secondary, and park brake functions. Without warning.	Op.	N/A	N/A	N/A	N/A	N/A	N/A
	Bys.	N/A	N/A	N/A	N/A	N/A	N/A
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
Any brake applies uncommanded by operator, potentially while propelling at full speed. — Machine skids to a stop in most conditions. — Steering is very poor.	Op.	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a
	Bys.	SIL Θ/No requirement	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a
	Veh.	N/A	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	N/A	SIL Θ/PL_r a
Swing brake release without command. — Machine can move very slowly only, due to hydraulic leakage. — Operator is not present.	Op.	N/A	N/A	N/A	N/A	N/A	N/A
	Bys.	N/A	N/A	N/A	N/A	N/A	N/A
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A

Table A.2 *(continued)*

Failure mode	Hazard cat.	Steel-tracked dozer, loader, pipelayer, scraper puller ≤ 12 km/h	Articulated rubber-tracked dozer or loader ≤ 40 km/h	Tractor loader-backhoe ≤ 40 km/h	Articulated wheeled loaders ≤ 40 km/h	Art. wheeled loader, too big for onroad use/ Undergrnd. mining loader/ Landfill compactor ≤ 40 km/h	Articulated compact wheeled loader ≤ 40 km/h
STEERING							
Complete loss of all steering (either steers uncommanded or not at all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering.	Op.	SIL Θ/PL_r a	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL Θ/PL_r a	SIL 2/PL_r d	SIL 2/PL_r d	SIL 2/PL_r d	SIL 2/PL_r d	SIL 2/PL_r d
	Veh.	N/A	SIL 3/PL_r e	SIL 3/PL_r e	SIL 3/PL_r e	N/A	SIL 3/PL_r e
Loss of normal steering while maintaining another steering system (either steers partially uncommanded or is limited in responsiveness, all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering. — Operator can switch to alternate control, such as joystick.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	N/A	SIL 2 / PL_r d	SIL 2/PL_r d	SIL 2/PL_r d	N/A	SIL 2/PL_r d
EQUIPMENT/ATTACHMENT							
Blade functions, bin dump, ripper, bucket curl, and other similar, begins to move without command. — Operator is present in operating station and can react. — The equipment or attachment is turned-off by a disabling lever, switch or similar.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	N/A	SIL 1/PL_r b	SIL 1/PL_r b	SIL Θ/PL_r a	N/A	SIL Θ/PL_r a
Rotating attachments, backhoe loader/hoe functions, excavator swing, excavator boom, excavator arm, excavator buckets which can crane, stabilizers or skid steer loader boom arm functions begin to move without command. — Operator is present in operating station and can react. — The equipment or attachment is turned-off by a disabling lever, switch or similar.	Op.	N/A	N/A	SIL Θ/No requirement	SIL Θ / No requirement	SIL Θ / No requirement	SIL Θ / No requirement
	Bys.	N/A	N/A	SIL 1/PL_r c Consider SIL 2/PLr d	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c
	Veh.	N/A	N/A	SIL 1/PL_r b	SIL 1/PL_r b	N/A	SIL 1/PL_r b

Table A.2 *(continued)*

Failure mode	Hazard cat.	Steel-tracked dozer, loader, pipelayer, scraper puller ≤ 12 km/h	Articulated rubber-tracked dozer or loader ≤ 40 km/h	Tractor loader-backhoe ≤ 40 km/h	Articulated wheeled loaders ≤ 40 km/h	Art. wheeled loader, too big for onroad use/ Undergrnd. mining loader/ Landfill compactor ≤ 40 km/h	Articulated compact wheeled loader ≤ 40 km/h
Automatic blade/bucket/bin control function is lost. Blade/bucket/bin moves randomly or in an undesirable location. — Operator assumed to be in operator station, because he is compelled to disable attachment function when exiting. — Function is only up and down, or angling. — Function is not a swing, rotate, shifting, etc.	Op.	SIL Θ/PL_r a	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL 1/PL_r b	SIL Θ/PL_r a	SIL Θ/PL_r a
	Veh.	N/A	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	N/A	SIL 1/PL_r b
Automatic blade control function is lost. Blade/bucket will not move automatically. — Function is only up and down, or angling. — Function is not a swing, rotate, side—shifting, etc.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	SIL Θ/No requirement
Quick Couplers: allows attachment to fall down uncommanded.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c
	Veh.	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement	N/A	SIL /No requirement
ENGINE							
Engine surges, with minor impact on: speed of propel, steering, braking or attachments.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	SIL Θ/No requirement

Table A.3 — Generic SIL/PL_r chart

Failure mode	Hazard cat.	Art. dump trucks ≤ 60 km/h	Undergrnd. mining truck, not allowed on highway ≤ 60 km/h	Rigid-frame haul truck, not allowed on highway ≤ 80 km/h	Crawler excavator, steel tracks not allowed on road (rubber tracks onroad) < 12 km/h	Compact crawler excavator, steel track not allowed on road (rubber tracks onroad) < 12 km/h	Large crawler excavator or shovel, > 45 t not allowed on road < 12 km/h
STATIONARY MACHINE							
Any movement of machine: Such as articulation, propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar begin to move uncommanded — Stationary machine — Operator is not present — Disabling devices/ park brakes applied. —Engine can be running. —Attachments on ground where appropriate for machines not in use.	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	SIL 1/PL_r b	N/A	N/A	N/A (SIL 1/PL_r b)	N/A (SIL 1/PL_r b)	N/A
Engine starts uncommanded during maintenance. — Battery disconnector is locked in position OFF	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
WORKING MACHINE							
Propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar remains stationary when commanded to move.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL Θ/No requirement	N/A	N/A	N/A SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A
PROPEL/BRAKING							

Table A.3 *(continued)*

Failure mode	Hazard cat.	Art. dump trucks ≤ 60 km/h	Undergrnd. mining truck, not allowed on highway ≤ 60 km/h	Rigid-frame haul truck, not allowed on highway ≤ 80 km/h	Crawler excavator, steel tracks not allowed on road (rubber tracks onroad) < 12 km/h	Compact crawler excavator, steel track not allowed on road (rubber tracks onroad) < 12 km/h	Large crawler excavator or shovel, > 45 t not allowed on road < 12 km/h
Propel speed/acceleration much higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such as the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a
	Bys.	SIL 1/PL$_r$ b	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a
	Veh.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	N/A (SIL Θ/PL$_r$ a)	N/A (SIL Θ/PL$_r$ a)	N/A
Propel speed/acceleration slightly higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	N/A
Complete loss of all brakes for stopping. — Operator can only allow machine to coast to a stop or use attachment in some cases. — Steering remains functional for most wheeled machines, but not for skid steers and crawler machines.	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL 2/PL$_r$ d	SIL 2/PL$_r$ d	SIL 2/PL$_r$ d	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	SIL 2/PL$_r$ d	N/A	N/A	N/A SIL 1/PL$_r$ b	N/A (SIL 1/PL$_r$ b)	N/A
Complete loss of service and secondary braking. —Operator still has at least one primary control to stop the machine, such as park brake.	Op.	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	N/A	N/A	N/A
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	N/A	N/A	N/A
	Veh.	SIL 1/PL$_r$ b	N/A	N/A	N/A	N/A	N/A
Complete loss of engine/transmission/electrical retarder. — Maintain service, secondary, and park brake functions. Without warning.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	N/A	N/A
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	N/A	N/A
	Veh.	SIL Θ/No requirement	N/A	N/A	N/A	N/A	N/A

Table A.3 *(continued)*

Failure mode	Hazard cat.	Art. dump trucks ≤ 60 km/h	Undergrnd. mining truck, not allowed on highway ≤ 60 km/h	Rigid-frame haul truck, not allowed on highway ≤ 80 km/h	Crawler excavator, steel tracks not allowed on road (rubber tracks onroad) < 12 km/h	Compact crawler excavator, steel track not allowed on road (rubber tracks onroad) < 12 km/h	Large crawler excavator or shovel, > 45 t not allowed on road < 12 km/h
Any brake applies uncommanded by operator, potentially while propelling at full speed. — Machine skids to a stop in most conditions. — Steering is very poor.	Op.	SIL 1/PL$_r$ c	SIL 1/PL$_r$ c	SIL 1/PL$_r$ c	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL 1/PL$_r$ b	N/A	N/A	N/A SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A
Swing brake release without command. — Machine can move very slowly only, due to hydraulic leakage. — Operator is not present.	Op.	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement	N/A
STEERING							
Complete loss of all steering (either steers uncommanded or not at all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering.	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a
	Bys.	SIL 2/PL$_r$ d	SIL 2/PL$_r$ d	SIL 2/PL$_r$ d	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a
	Veh.	SIL 3/PL$_r$ e	N/A	N/A	N/A SIL 1/PL$_r$ b	N/A SIL Θ/PL$_r$ a	N/A
Loss of normal steering while maintaining another steering system (either steers partially uncommanded or is limited in responsiveness, all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering. — Operator can switch to alternate control, such as joystick.	Op.	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	N/A	N/A	N/A
	Bys.	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	N/A	N/A	N/A
	Veh.	SIL 2/PL$_r$ d	N/A	N/A	N/A	N/A	N/A
EQUIPMENT/ATTACHMENT							
Blade functions, bin dump, ripper, bucket curl, and other similar, begins to move without command. — Operator is present in operating station and can react. — Equipment or attachment is turned-off by a disabling lever, switch or similar.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	N/A	N/A	N/A SIL 1/PL$_r$ b	N/A SIL 1/PL$_r$ b	N/A

Table A.3 *(continued)*

Failure mode	Hazard cat.	Art. dump trucks ≤ 60 km/h	Undergrnd. mining truck, not allowed on highway ≤ 60 km/h	Rigid-frame haul truck, not allowed on highway ≤ 80 km/h	Crawler excavator, steel tracks not allowed on road (rubber tracks onroad) < 12 km/h	Compact crawler excavator, steel track not allowed on road (rubber tracks onroad) < 12 km/h	Large crawler excavator or shovel, > 45 t not allowed on road < 12 km/h
Rotating attachments, backhoe loader/hoe functions, excavator swing, excavator boom, excavator arm, excavator buckets which can crane, stabilizers or skid steer loader boom arm functions begin to move without command. — Operator is present in operating station and can react. — Equipment or attachment is turned-off by a disabling lever, switch or similar.	Op.	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	N/A	N/A	N/A	SIL 1/PL_r c Consider SIL 2/PLr d	SIL 1/PL_r c Consider SIL 2/PLr d	SIL 1/PL_r c SIL Θ/No requirement for arm and boom if not used to crane
	Veh.	N/A	N/A	N/A	N/A SIL 1/PL_r b	N/A SIL 1/PL_r b	N/A
Automatic blade/bucket/bin control function is lost. Blade/bucket/bin moves randomly or in an undesirable location. — Operator assumed to be in operator station, because he is compelled to disable attachment function when exiting. — Function is only up and down, or angling. — Function is not a swing, rotate, shifting, etc.	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL Θ/PL_r a or SIL 1/PL_r b if there is a potential contacting the operator station, or other jobsite hazards.	SIL Θ/PL_r a or SIL 1/PL_r b if there is a potential contacting the operator station, or other jobsite hazards.	SIL Θ/PL_r a or SIL 1/PL_r b if there is a potential contacting the operator station, or other jobsite hazards.
	Bys.	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	SIL 1/PL_r b	N/A	N/A	N/A SIL 1/PL_r b	N/A SIL 1/PL_r b	N/A
Automatic blade control function is lost. Blade/bucket will not move automatically. — Function is only up and down, or angling. — Function is not a swing, rotate, side-shifting, etc.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL Θ/No requirement	N/A	N/A	N/A SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A
Quick couplers: allows attachment to fall down uncommanded.	Op.	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	N/A	N/A	N/A	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c
	Veh.	N/A	N/A	N/A	N/A SIL Θ/PL_r a	N/A SIL Θ/PL_r a	N/A
ENGINE							

Table A.3 *(continued)*

Failure mode	Hazard cat.	Art. dump trucks ≤ 60 km/h	Undergrnd. mining truck, not allowed on highway ≤ 60 km/h	Rigid-frame haul truck, not allowed on highway ≤ 80 km/h	Crawler excavator, steel tracks not allowed on road (rubber tracks onroad) < 12 km/h	Compact crawler excavator, steel track not allowed on road (rubber tracks onroad) < 12 km/h	Large crawler excavator or shovel, > 45 t not allowed on road < 12 km/h
Engine surges, with minor impact on: speed of propel, steering, braking or attachments.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL Θ/PL$_r$ a	N/A	N/A	N/A SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A

Table A.4 — Generic SIL/PL$_r$ chart

Failure mode	Hazard cat.	Wheeled excavator, roadable ≤ 25 km/h	Wheeled excavator, non-roadable or roadable ≤ 40 km/h	Wheeled excavator, non-roadable ≤ 12 km/h	Articulated motor grader, roadable ≤ 50 km/h	Articulated grader, too big for public road use, typically used in mining ≤ 50 km/h	Skid steer loader and all-terrain track loaders, steel-track not allowed onroad; rubber-tracks onroad < 25 km/h
STATIONARY MACHINE							
Any movement of machine: Such as articulation, propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar begin to move uncommanded — Stationary machine — Operator is not present — Disabling devices/park brakes applied. —Engine can be running. — Attachments on ground where appropriate for machines not in use.	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	SIL 1/PL$_r$ b	N/A SIL 1/PL$_r$ b	N/A	SIL 1/PL$_r$ b	N/A	N/A SIL 1/PL$_r$ b
Engine starts uncommanded During maintenance. — Battery disconnector is locked in position OFF	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
WORKING MACHINE							

Table A.4 *(continued)*

Failure mode	Hazard cat.	Wheeled excavator, roadable ≤ 25 km/h	Wheeled excavator, non-roadable or roadable ≤ 40 km/h	Wheeled excavator, non-roadable ≤ 12 km/h	Articulated motor grader, roadable ≤ 50 km/h	Articulated grader, too big for public road use, typically used in mining ≤ 50 km/h	Skid steer loader and all-terrain track loaders, steel-track not allowed onroad; rubber-tracks onroad < 25 km/h
Propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar remains stationary when commanded to move.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL Θ/No requirement	SIL Θ/No requirement	N/A	SIL Θ/No requirement	N/A	N/A SIL Θ/No requirement
PROPEL/BRAKING							
Propel speed/acceleration much higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such as the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	SIL 1/PL_r b	N/A SIL 1/PL_r b	N/A	SIL 1/PL_r b	N/A	N/A SIL 1/PL_r b
Propel speed/acceleration slightly higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	N/A SIL Θ/No requirement	N/A	SIL Θ/No requirement	N/A	N/A SIL Θ/No requirement
Complete loss of all brakes for stopping. — Operator can only allow machine to coast to a stop or use attachment in some cases. — Steering remains functional for most wheeled machines, but not for skid steers and crawler machines.	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	SIL 1/PL_r b	N/A SIL 2/PL_r d	N/A	SIL 2/PL_r d	N/A	N/A SIL 1/PL_r b

Table A.4 *(continued)*

Failure mode	Hazard cat.	Wheeled excavator, roadable ≤ 25 km/h	Wheeled excavator, non-roadable or roadable ≤ 40 km/h	Wheeled excavator, non-roadable ≤ 12 km/h	Articulated motor grader, roadable ≤ 50 km/h	Articulated grader, too big for public road use, typically used in mining ≤ 50 km/h	Skid steer loader and all-terrain track loaders, steel-track not allowed onroad; rubber-tracks onroad < 25 km/h
Complete loss of service and secondary braking. — Operator still has at least one primary control to stop the machine, such as park brake.	Op.	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	SIL 1/PL_r b	SIL 1/PL_r b	N/A	SIL 1/PL_r b	N/A	N/A SIL 1/PL_r b
Complete loss of engine/transmission/electrical retarder. — Maintain service, secondary, and park brake functions. Without warning.	Op.	N/A	N/A	N/A	N/A	N/A	N/A
	Bys.	N/A	N/A	N/A	N/A	N/A	N/A
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
Any brake applies uncommanded by operator, potentially while propelling at full speed. — Machine skids to a stop in most conditions. — Steering is very poor.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/PL_r a	SIL Θ/PL_r a	SIL Θ/PL_r a
	Veh.	SIL Θ/PL_r a	N/A SIL Θ/PL_r a	N/A	SIL Θ/PL_r a	N/A	N/A SIL Θ/PL_r a
Swing brake release without command. — Machine can move very slowly only, due to hydraulic leakage. — Operator is not present.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	N/A	N/A
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	N/A	N/A
	Veh.	SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A	N/A	N/A	N/A
STEERING							
Complete loss of all steering (either steers uncommanded or not at all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering.	Op.	SIL Θ/PL_r a	SIL 1/PL_r b	SIL Θ/PL_r a	SIL 1/PL_r b	SIL 1/PL_r b	SIL Θ/PL_r a
	Bys.	SIL 1/PL_r b	SIL 2/PL_r d	SIL Θ/PL_r a	SIL 2/PL_r d	SIL 2/PL_r d	SIL 1/PL_r b
	Veh.	SIL 2/PL_r d	N/A SIL 3/PL_r e	N/A	SIL 3/PL_r e	N/A	N/A SIL 2/PL_r d

Table A.4 *(continued)*

Failure mode	Hazard cat.	Wheeled excavator, roadable ≤ 25 km/h	Wheeled excavator, non-roadable or roadable ≤ 40 km/h	Wheeled excavator, non-roadable ≤ 12 km/h	Articulated motor grader, roadable ≤ 50 km/h	Articulated grader, too big for public road use, typically used in mining ≤ 50 km/h	Skid steer loader and all-terrain track loaders, steel-track not allowed onroad; rubber-tracks onroad < 25 km/h
Loss of normal steering while maintaining another steering system (either steers partially uncommanded or is limited in responsiveness, all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering. — Operator can switch to alternate control, such as joystick.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/PL$_r$ a	SIL 1/PL$_r$ b	SIL Θ/PL$_r$ a	SIL 1/PL$_r$ b	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a
	Veh.	SIL 1/PL$_r$ b	N/A SIL 2/PL$_r$ d	N/A	SIL 2/PL$_r$ d	N/A	N/A SIL 1/PL$_r$ b
EQUIPMENT/ATTACHMENT							
Blade functions, bin dump, ripper, bucket curl, and other similar, begins to move without command. — Operator is present in operating station and can react. — Equipment or attachment is turned- off by a disabling lever, switch or similar.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	SIL 1/PL$_r$ b	N/A SIL 1/PL$_r$ b	N/A	SIL 1/PL$_r$ b	N/A	N/A SIL 1/PL$_r$ b
Rotating attachments, backhoe loader/hoe functions, excavator swing, excavator boom, excavator arm, excavator buckets which can crane, stabilizers or skid steer loader boom arm functions begin to move without command. — Operator is present in operating station and can react. — Equipment or attachment is turned-off by a disabling lever, switch or similar.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	N/A	SIL Θ/No requirement. SIL 1/PL$_r$ c for boom while exiting
	Bys.	SIL 1/PL$_r$ c Consider SIL 2/PLr d	SIL 1/PL$_r$ c Consider SIL 2/PLr d	SIL 1/PL$_r$ c Consider SIL 2/PLr d	N/A	N/A	SIL 1/PL$_r$ c
	Veh.	SIL 1/PL$_r$ c	N/A SIL 1/PL$_r$ c	N/A	N/A	N/A	N/A SIL 1/PL$_r$ b

Table A.4 *(continued)*

Failure mode	Hazard cat.	Wheeled excavator, roadable ≤ 25 km/h	Wheeled excavator, non-roadable or roadable ≤ 40 km/h	Wheeled excavator, non-roadable ≤ 12 km/h	Articulated motor grader, roadable ≤ 50 km/h	Articulated grader, too big for public road use, typically used in mining ≤ 50 km/h	Skid steer loader and all-terrain track loaders, steel-track not allowed onroad; rubber-tracks onroad < 25 km/h
Automatic blade/bucket/bin control function is lost. Blade/bucket/bin moves randomly or in an undesirable location. — Operator assumed to be in operator station, because he is compelled to disable attachment function when exiting. — Function is only up and down, or angling. — Function is not a swing, rotate, shifting, etc.	Op.	SIL Θ/No requirement, or SIL 1/PL_rb, if there is a potential contacting the operator station, or other jobsite hazards.	SIL Θ/No requirementor SIL 1/PL_rb, if there is a potential contacting the operator station, or other jobsite hazards.	SIL Θ/No requirement or SIL 1/PL_rb, if there is a potential contacting the operator station, or other jobsite hazards.	SIL 1/PL_r b	SIL 1/PL_r b	SIL Θ/No requirement. SIL 1/PL_rc for boom while exiting
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PLr b
	Veh.	SIL 1/PL_r b	SIL 1/PL_r b	N/A	SIL 1/PL_r b	N/A	N/A (SIL 1/PL_r b)
Automatic blade control function is lost. Blade/bucket will not move automatically. — Function is only up and down, or angling. — Function is not a swing, rotate, side-shifting, etc.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A	SIL Θ/No requirement	N/A	N/A SIL Θ/No requirement
Quick couplers: allows attachment to fall down uncommanded.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	N/A	SIL Θ/No requirement
	Bys.	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c	N/A	N/A	SIL 1/PL_r c
	Veh.	SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A	N/A	N/A	N/A SIL Θ/No requirement
ENGINE							
Engine surges, with minor impact on: speed of propel, steering, braking or attachments.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	SIL Θ/No requirement	N/A SIL Θ/No requirement	N/A	SIL Θ/No requirement	N/A	N/A SIL Θ/No requirement

Table A.5 — Generic SIL/PL_r chart

Failure mode	Hazard cat.	Crawler trencher < 12 km/h	Rubber-tyred trencher < 12 km/h	Walk-behind horizontal directional drill < 12 km/h	Ride-on horizontal directional drill < 12 km/h	Wheeled tractor scraper, roadable ≤ 40 km/h	Self-propelled roller, road-able < 12 km/h
STATIONARY MACHINE							
Any movement of machine: such as articulation, propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar begin to move uncommanded — Stationary machine — Operator is not present — Disabling devices/park brakes applied. — Engine can be running. — Attachments on ground where appropriate for machines not in use.	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	N/A	SIL 1/PL_r b	N/A	N/A SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
Engine starts uncommanded During maintenance. — Battery disconnector is locked in position OFF.	Op.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
WORKING MACHINE							
Propel, boom, bucket, arm, blade, dumper bin, excavator swing, raising and lower functions and other similar, rotating functions such as drilling, sawing, mowing, auging, and similar remains stationary when commanded to move.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement
PROPEL/BRAKING							
Propel speed/acceleration much higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such as the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL 1/PL_r b	SIL Θ/No requirement
	Veh.	N/A	SIL 1/PL_r b	N/A	N/A	SIL 1/PL_r b	SIL 1/PL_r b

Table A.5 *(continued)*

Failure mode	Hazard cat.	Crawler trencher < 12 km/h	Rubber-tyred trencher < 12 km/h	Walk-behind horizontal directional drill < 12 km/h	Ride-on horizontal directional drill < 12 km/h	Wheeled tractor scraper, roadable ≤ 40 km/h	Self-propelled roller, roadable < 12 km/h
Propel speed/acceleration slightly higher than commanded. — Driving near a location where there could be a collision or where bystanders are present. — Operator can stop propel using service brakes or other similar device, such the F/N/R. — Service brake capacity is adequate for the increase stopping force needed.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement
Complete loss of all brakes for stopping. — Operator can only allow machine to coast to a stop or use attachment in some cases. — Steering remains functional for most wheeled machines, but not for skid steers and crawler machines.	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 2/PL$_r$ d	SIL 2/PL$_r$ d
	Veh.	N/A	SIL 1/PL$_r$ b	N/A	N/A	SIL 2/PL$_r$ d	SIL 2/PL$_r$ d
Complete loss of service and secondary braking. — Operator still has at least one primary control to stop the machine, such as park brake.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	SIL 1/PL$_r$ b	N/A	N/A	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
Complete loss of engine/ transmission/ electrical retarder. Maintain service, secondary, and park brake functions. Without warning.	Op.	N/A	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	N/A	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	N/A	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement
Any brake applies uncommanded by operator, potentially while propelling at full speed. — Machine skids to a stop in most conditions. Steering is very poor.	Op.	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL Θ/PL$_r$ a	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	SIL 1/PL$_r$ b	N/A	N/A	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
Swing brake release without command. — Machine can move very slowly only, due to hydraulic leakage. — Operator is not present.	Op.	N/A	N/A	N/A	N/A	N/A	N/A
	Bys.	N/A	N/A	N/A	N/A	N/A	N/A
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
STEERING							

Table A.5 *(continued)*

Failure mode	Hazard cat.	Crawler trencher < 12 km/h	Rubber-tyred trencher < 12 km/h	Walk-behind horizontal directional drill < 12 km/h	Ride-on horizontal directional drill < 12 km/h	Wheeled tractor scraper, roadable ≤ 40 km/h	Self-propelled roller, roadable < 12 km/h
Complete loss of all steering (either steers uncommanded or not at all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL 1/PL_r b	SIL 1/PL_r b
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL 2/PL_r d	SIL 2/PL_r d
	Veh.	N/A	SIL 1/PL_r b	N/A	N/A	SIL 3/PL_r e	SIL 3/PL_r e
Loss of normal steering while maintaining another steering system (either steers partially uncommanded or is limited in responsiveness, all while propelling). — Operator has braking to stop the machine. — Operator is not warned prior to loss of steering. — Operator can switch to alternate control, such as joystick.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL 1/PL_r b	SIL 1/PL_r b
	Veh.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL 2/PL_r d	SIL 2/PL_r d
EQUIPMENT/ATTACHMENT							
Blade functions, bin dump, ripper, bucket curl, and other similar, begins to move without command. — Operator is present in operating station and can react. — Equipment or attachment is turned— off by a disabling lever, switch or similar.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A
	Bys.	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	SIL 1/PL_r b	N/A
	Veh.	N/A	N/A	N/A	N/A	SIL 1/PL_r b	N/A
Rotating attachments, backhoe loader — hoe functions, excavator swing, excavator boom, excavator arm, excavator buckets which can crane, stabilizers or skid steer loader boom arm functions begin to move without command. — Operator is present in operating station and can react. — Equipment or attachment is turned- off by a disabling lever, switch or similar.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	N/A	SIL Θ/No requirement
	Bys.	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c	SIL 1/PL_r c	N/A	N/A
	Veh.	N/A	SIL 1/PL_r b	N/A	N/A	N/A	N/A

Table A.5 *(continued)*

Failure mode	Hazard cat.	Crawler trencher < 12 km/h	Rubber-tyred trencher < 12 km/h	Walk-behind horizontal directional drill < 12 km/h	Ride-on horizontal directional drill < 12 km/h	Wheeled tractor scraper, roadable ≤ 40 km/h	Self-propelled roller, roadable < 12 km/h
Automatic blade/bucket/bin control function is lost. — Blade/bucket/bin moves randomly or in an undesirable location. — Operator assumed to be in operator station, because he is compelled to disable attachment function when exiting. — Function is only up and down, or angling. — Function is not a swing, rotate, shifting, etc.	Op.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Bys.	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
	Veh.	N/A	SIL 1/PL$_r$ b	N/A	N/A	SIL 1/PL$_r$ b	SIL 1/PL$_r$ b
Automatic blade control function is lost. Blade/bucket will not move automatically. — Function is only up and down, or angling. — Function is not a swing, rotate, side- shifting, etc.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement
Quick couplers: allows attachment to fall down uncommanded.	Op.	N/A	N/A	N/A	N/A	N/A	N/A
	Bys.	N/A	N/A	N/A	N/A	N/A	N/A
	Veh.	N/A	N/A	N/A	N/A	N/A	N/A
ENGINE							
Engine surges, with minor impact on: speed of propel, steering, braking or attachments.	Op.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Bys.	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement	SIL Θ/No requirement
	Veh.	N/A	SIL Θ/No requirement	N/A	N/A	SIL Θ/No requirement	SIL Θ/No requirement

Example SILs/PLrs were determined from risk assessments of worst-case hazards associated with the given machine form. It is recommended that specific risk assessments be conducted using Annex A of the first part of ISO 15998, for different machine forms, special applications or other special considerations.

A.3.3 The schematics in Figures A.2 to A.5 are example configurations demonstrating systems that are consistent with the generic SILs/PL$_r$s of Tables A.2 to A.5 . Other configurations are, of course, possible.

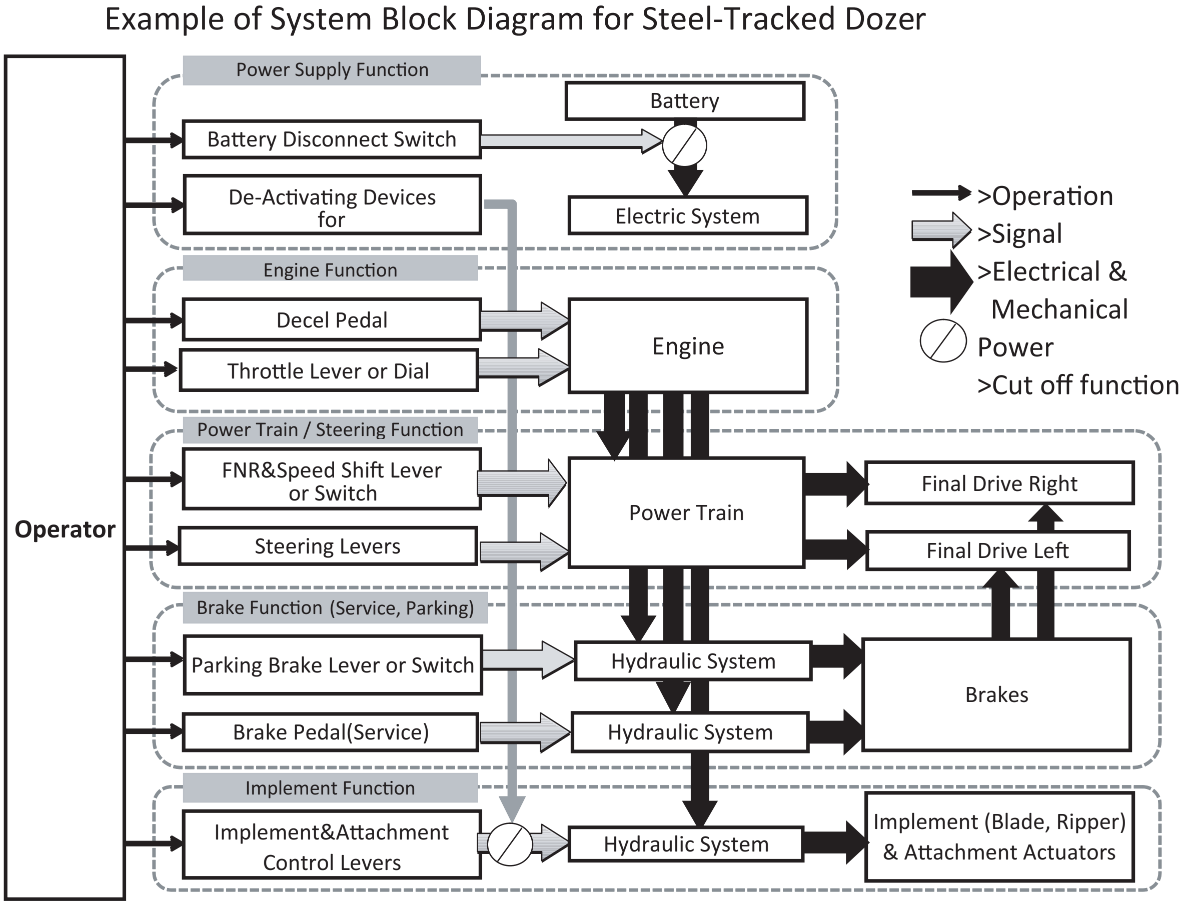

Example of System Block Diagram for Steel-Tracked Dozer
Power Supply Function
Battery
Battery Disconnect Switch
De-Activating Devices for
Electric System
>Operation
>Signal
>Electrical & Mechanical Power
>Cut off function
Engine Function
Decel Pedal
Throttle Lever or Dial
Engine
Power Train / Steering Function
FNR&Speed Shift Lever or Switch
Steering Levers
Power Train
Final Drive Right
Final Drive Left
Operator
Brake Function (Service, Parking)
Parking Brake Lever or Switch
Hydraulic System
Brake Pedal(Service)
Hydraulic System
Brakes
Implement Function
Implement&Attachment Control Levers
Hydraulic System
Implement (Blade, Ripper) & Attachment Actuators

Figure A.2 — Steel-tracked crawler dozer

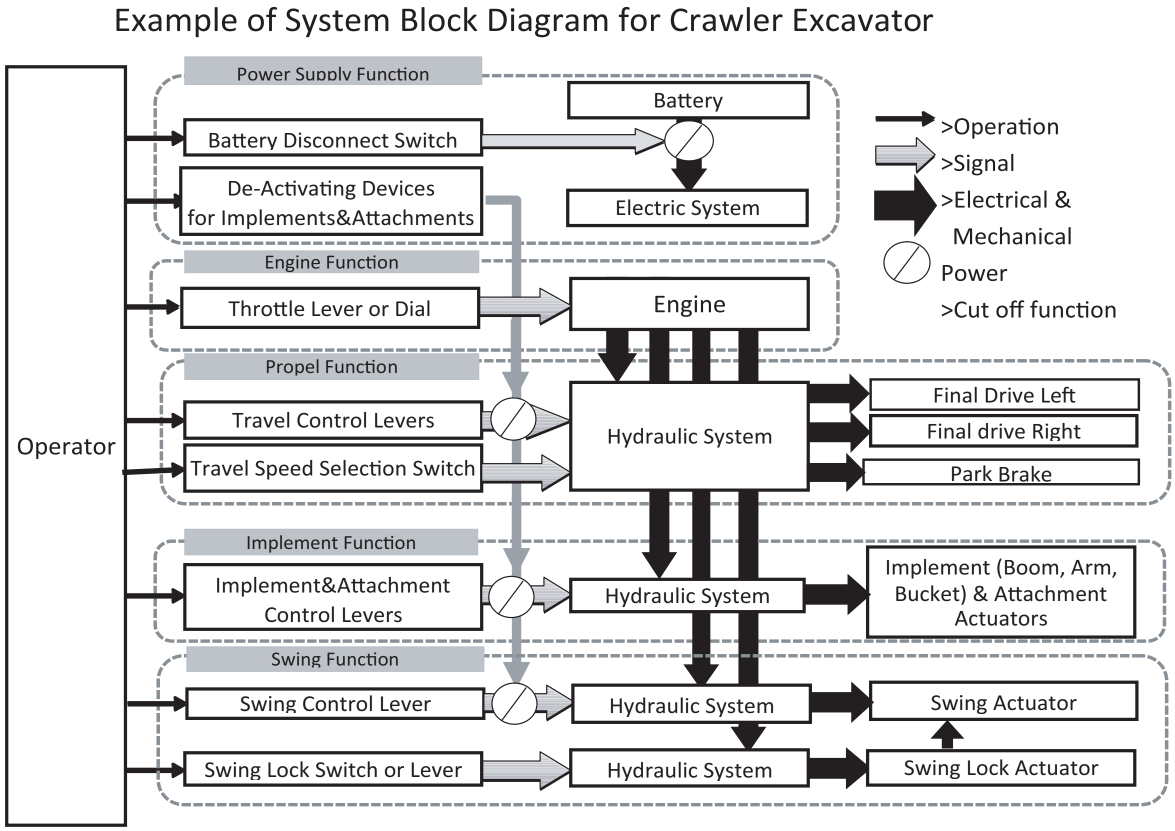


Figure A.3 — Steel-tracked crawler excavator

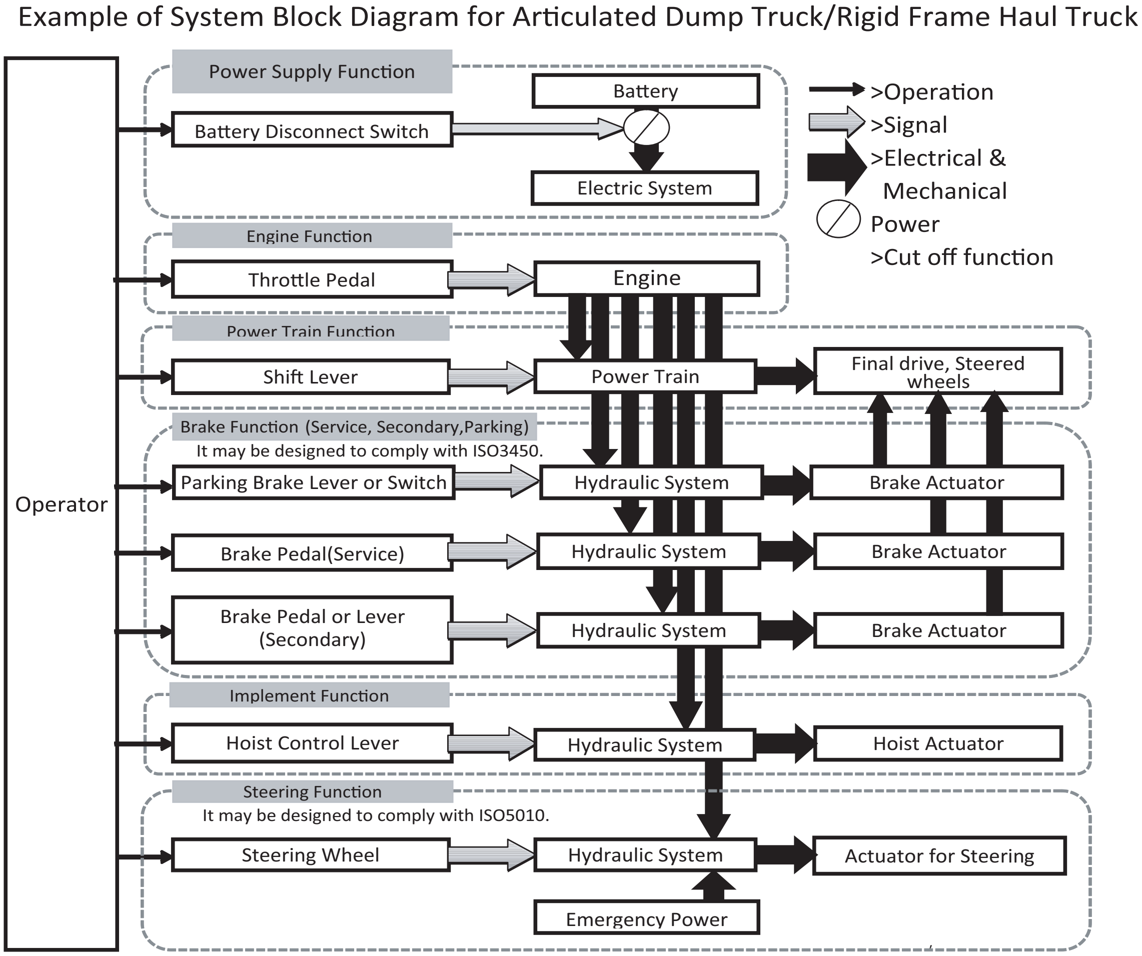


Figure A.4 — Articulated dump truck/rigid-frame haul truck

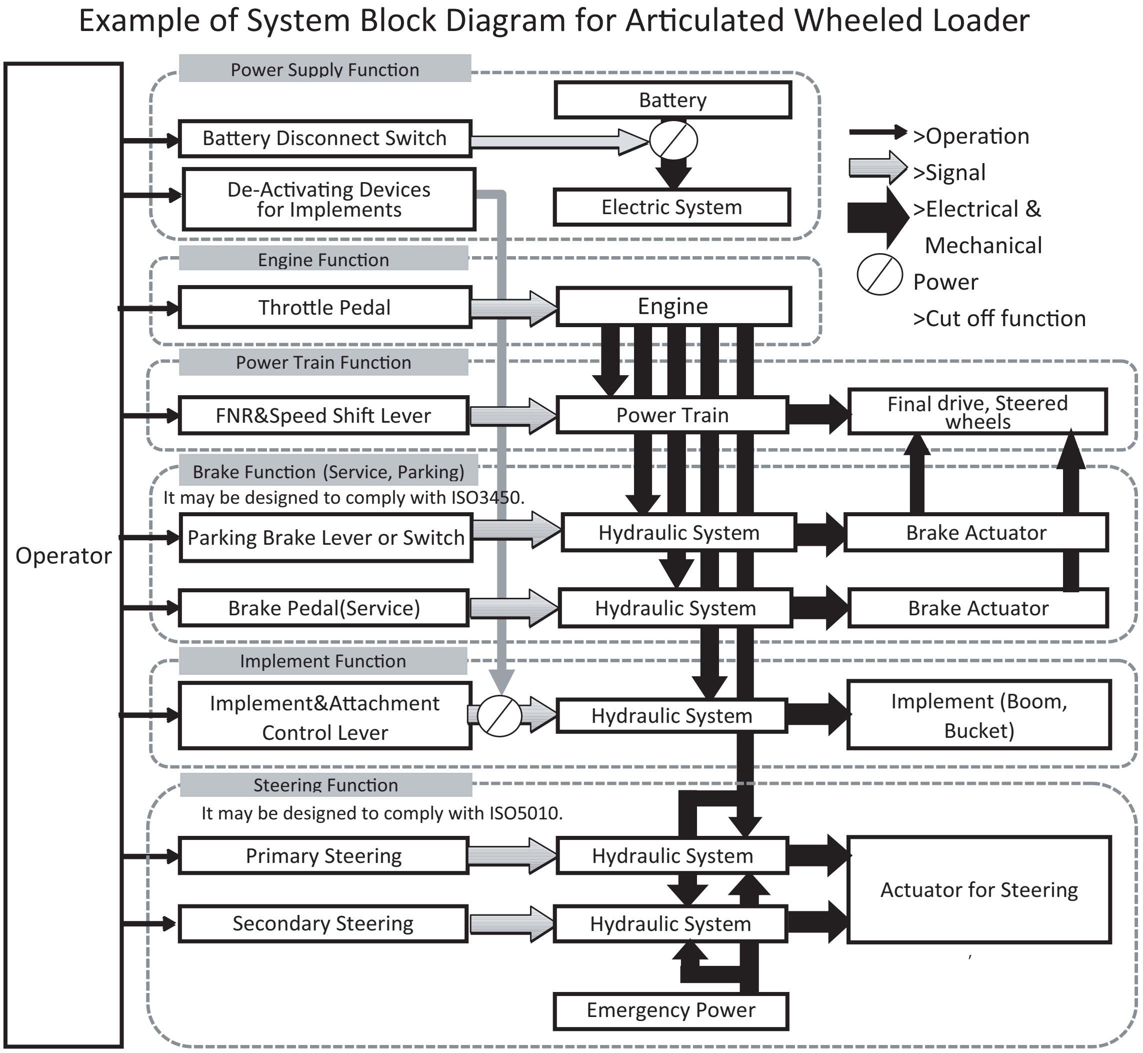


Figure A.5 — Articulated wheeled loader

A.4 Contributions to the risk reduction of the MCS

Various methods can be used for the reduction of hazards (see, for example, ISO 13849-1:2006, 4.2). For construction equipment, the following rules may be used directly in the risk assessment, but could require further analysis. The failed portions of a control system, such as braking, steering, propel or attachment control, can have the risks mitigated by using the methods below. The overall SIL/PL_r remains at the same higher level, but certain combinations of features allow parts of the system to have lesser requirements.

NOTE 1 Combinations of lower SIL/PL_r systems can be combined electronically in ways not described below. IEC 61508-6:2010, Annex B, addresses these, in which case the control system as a whole remains at the higher SIL/PL_r.

NOTE 2 The difference between a SIL 1/PL_rb and SIL 2/PL_rd system is that the reliability of SIL 2 is effectively 10 times more reliable with respect to the undesirable failure mode.

A.4.1 Redundant control systems

Operators can change control actuators to prevent accidents. Machines with redundant controls that approximately mimic the function of each other may lower the SIL/PL_r by one for each of the sub-systems making up the total system (provided the particular failure mode in question does not result in both primary controls failing simultaneously.)

EXAMPLE 1 A full loss of service and secondary braking is SIL 2/PL$_r$ d for an articulated dump truck. If there is a park brake with dynamic stopping capability per ISO 3450, then the requirement of the service brake can be lowered to SIL 1/PL b.

EXAMPLE 2 A full loss of all steering (e.g. of normal and emergency steering power sources) is SIL 3/PL$_r$ e for most wheeled machines used onroad to >25 km/h. A machine can have a mechanical/hydraulic steering wheel system as a primary steering system and an additional electro-hydraulic joystick steering system. In this case, it is acceptable for the joystick electrical control system requirement to be SIL 2/PL d if these steering systems comply with ISO 5010. It is the combination of the individual steering systems of lesser SILs/PLs working together that provides an overall SIL 3/PL$_r$ e system.

EXAMPLE 3 If there is an additional method of steering — such as when both an electro-hydraulic joystick steering system and a mechanical/hydraulic steering wheel system are primary steering systems — then it is acceptable that the requirement be SIL 2/PL d with respect to the joystick electrical control system(s), if these steering systems comply with ISO 5010. It is the combination of the individual steering systems of lesser SILs/PLs working together that provides an overall SIL 3/PL$_r$ e system.

A.4.2 Advance warning

Failure modes which occur with adequate warning time to safely stop a machine, thereby reducing the hazardous condition, can lower the SIL/PL$_r$ by one level for the control system (provided the particular failure mode in question will not result in both the function and the warning failing simultaneously).

EXAMPLE A full loss of primary and emergency steering is SIL 3/PL$_r$ e for wheeled machines used onroad. If there is a warning in time to allow the operator to steer safely to a stop, then the steering control system by itself need only be designed to SIL 2/PL d.

A.4.3 Disablement

Disabling a control, either automatically or through a compulsory action of the operator, can significantly reduce the risk of uncommanded motion when the operator leaves the operator station; therefore the SIL/PL$_r$ of the basic control can be less by one with respect to injuries to persons standing on the ground and at risk from un-commanded motion.

EXAMPLE If a fault in a SIL 1/PL$_r$ b basic propel system is detected by another monitoring system that is capable of transitioning safely to a neutral condition, then the overall system is SIL 1, but the “basic” portion of the propel and monitoring systems may each be a SIL Θ/PL a/(where each system’s failure rates are less than one failure/10^4 h of operation).

A.4.4 Countering

Some failure modes of a control system are such that the operator can stop an uncommanded movement in one direction by applying a command in the opposite direction. Countering can significantly reduce the risk of uncommanded motion, provided there is also a method of positively disabling the control, such as a park brake or hydraulic enable.

EXAMPLE If the neutral point of a controller shifts away from the centre point on a variable input device, the operator can move the input device in the opposite direction to counter the fault. A more specific example would be on a skid steer where the propel system may fluctuate depending on the sensor input (or the slope of the worksite). This can make it is necessary to command a small amount of propulsion to hold the machine stationary. Movement of the machine when the propel control is in neutral is still SIL 1/PL$_r$ b for the overall controls system, but the sensor failure mode is not considered SIL 1/PL$_r$ b, but rather SIL Θ/PL a. Similarly, if the boom on the machine drifts down due to sensor drift (or hydraulic leakage) it is also SIL Θ/PL a. The presumption in both cases is that the operator will be able to adjust to these situations, and has the option of locking the machine to prevent them occurring.

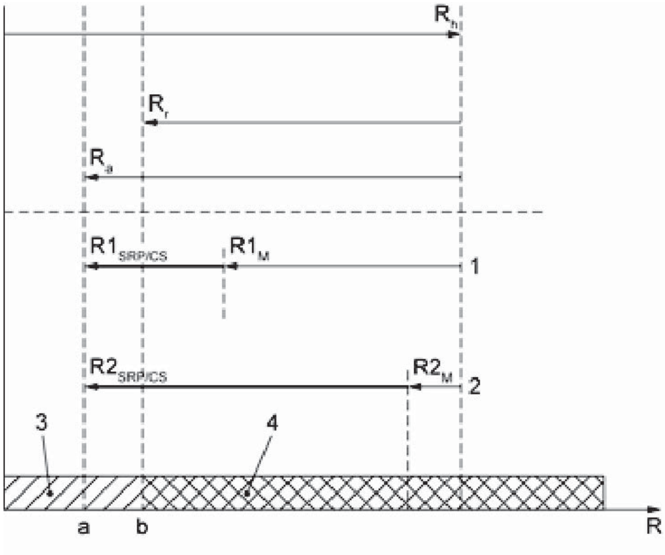
A.5 Risk reduction chart

Several methods can be used to determine if the SRP/MCS specifications fulfil the safety concept as defined from the SIL and associated PL_r level. These methods are defined in detail within the normative references of ISO 15998.

The strategy for risk reduction for SRP/MCS covers the whole life cycle of the machine and includes the safety concept. The hazard analysis and risk reduction process for a machine requires that hazards be eliminated or reduced through a hierarchy of measures:

A.5.1 Risk reduction process used to achieve tolerable risk (adequately reduced risk)

One significant method associated with the safety concept is the risk reduction process. Risk reduction can be achieved by applying various protective measures — both SRP/MCS and non-MCS — with the end result of achieving a safe condition (see Figure A.6).



Key

R_h	for a specific hazardous situation, the risk before protective measures are applied
R_r	risk reduction required from protective measures
R_a	actual risk reduction achieved with protective measures
1	solution 1: important part of risk reduction due to protective measures other than MCS (e.g. mechanical measures), small part of risk reduction due to SRP/MCS
2	solution 2: important part of risk reduction due to the SRP/MCS (e.g. interlocks), small part of risk reduction due to protective measures other than MCS (e.g. mechanical measures)
3	adequately reduced risk
4	inadequately reduced risk
R	risk
$R1_{SRP/CS}$ $R2_{SRP/CS}$	risk reduction from the safety function carried out by the SRP/MCS
$R1_M$, $R2_M$	risk reduction from protective measures other than SRP/MCS (e.g. mechanical measures)

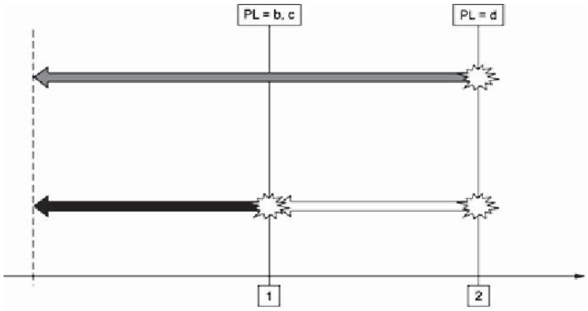
[a] Residual risk obtained by solutions 1 or 2.

[b] Adequately reduced risk.

Figure A.6 — Overview of risk reduction process for each hazardous situation

Another way to illustrate this concept is with a non-electrical MCS braking system and a combined braking system with mechanical and electric-hydraulic MCS, as in Table A.6.

Table A.6 — Examples of risk reduction for braking systems

Tolerable risk	
	**Examples**
	Non-electrical braking system(s)
	Completely redundant secondary braking system with additional dynamic parking brake as backup to secondary brakes
	Combination of E/H park and secondary brake and primary non-electrical braking system
	Proven common components for EH PB/secondary brakes.
	Risk represented as SIL

In the illustration of Table A.6, the risk assessment determined a SIL 2/PL_r d level was required regardless of the type of MCS. The machine is fitted with a traditional non-electric braking system in compliance with a C-type level safety standard — here, ISO 3450 (shown in grey). The non-electric braking system is triple redundant and provides a safe state for any single failure resulting in a PL that exceeds the SIL 2/PL_r d.

The second system (in black and white) comprises electric/hydraulic (E/H) secondary and park brake systems and a non-electrical primary braking system. This combination also provides triple redundancy and provides a safe state for any single failure resulting in a combined PL that exceeds the SIL 2/PL_r d. The EH portion of the system is evaluated as having SIL 1/PL_r b performance and consists of proven-in-use components.

EMMs are commonly fitted with similar redundant systems for steering. A similar example could be offered for a combined steering system comprised of a EH steering system having a SIL 1/PL b performance and mechanical-hydraulic redundant steering system having SIL 2/PL d performance. The combination of both of these systems is additive and would result in a SIL 3/PL_r e performance level.

A.5.2 Risk reduction via an operator protection device

The risks associated with exiting the operator station of a skid steer loader having the boom lower are SIL 1/PL_r c. If there is an interlock, such as a lap bar, that positively disables the hydraulic system (i.e. locks the position of the boom regardless of the basic control system, while exiting the operator station), then the combination of the two separate systems basic and lap bar disabling, can meet the SIL 1/PL_r c requirements. The basic control of the boom relative to the operator could then have a lower SIL Θ/No requirement design.

NOTE The risk of injury to the bystander is not lessened by the lap bar and is SIL 1/PL b. Therefore, the full reduction for the basic portion of the control cannot be realized unless other provisions of the design address the hazards to the bystander.

Annex B
(informative)

Guidance for describing the ISO 15998 safety concept

Table B.1 presents an example describing the safety concept for a wheeled loader propel transmission controlled by a MCU and the operator's electronic directional control shifter. As one portion of the process, this information would be used to demonstrate the compliance of the safety-related transmission MCS and electronic control shifter with ISO 15998:2008, 4.2, bullet one, 4.3, 4.4, 4.5, 4.7, 5.2, 5.3, 5.4 and 5.5 (and the corresponding sections of ISO 15998-1). Each SRP/MCS for the wheeled loader would need a similar safety concept description. Diagrams and schematics would be required in most actual systems, but have been omitted here for the sake of brevity.

Table B.1 — Wheeled loader — Propel direction MCS — Example

Safety concept description elements from ISO 15998:2008 [ISO 15998-1]	**E/E/PE system being described — Example — Transmission MCU**	
4.2 [First bullet point] a list of all system units used by the safety related functions	**Transmission:** power shift, torque converter Solenoids to control transmission gear and direction F/N/R (forward/neutral/reverse) lever to input direction, made up of three switches Harnesses to electrically connect the system Electrical power supply — Alternator and battery	
4.3 Description of basic function	**F/N/R direction is three digital inputs:**	
	a) Forward signal (F)	0,0–0,5 V = not in F, 4,5–5,0 V = F
	b) Neutral signal (N)	0,0–0,5 V = not in N, 4,5–5,0 V = N
	c) Reverse signal (R)	0,0–0,5 V = not in N, 4,5–5,0 V = N
	Output direction solenoids	
	Forward solenoid Reverse solenoid	0,0 V = N or R, 24 V = F 0,0 V = N or F, 24 V = R
	Open loop system Loader can be in forward, neutral or reverse. There are four speeds in forward, three in reverse. Maximum speed is 40 km/h.	
4.4 Risk analysis and assessment	The risk assessment indicates the machine propelling while operator commanding N, is SIL1/PL_r b.	

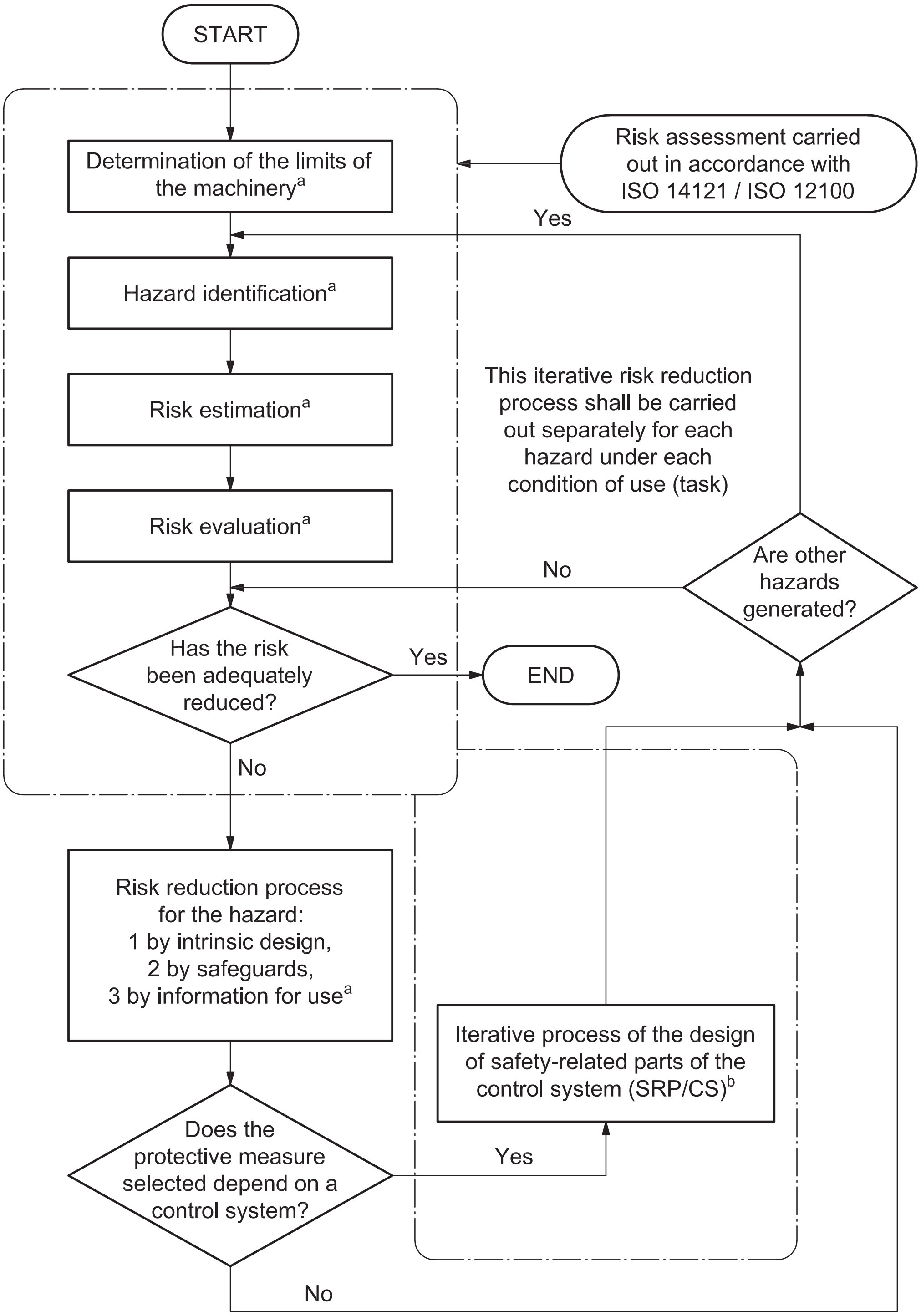
Table B.1 *(continued)*

Safety concept description elements from ISO 15998:2008 [ISO 15998-1]	E/E/PE system being described — Example — Transmission MCU
4.5 Performance criteria for the safety concept	**Redundancy** F/N/R input sensors must agree to be a valid state. If F input = 4,5–5,0 V, then N and R must both be at 0,0–0,5 V. If N input = 4,5–5,0 V, then F and R must both be at 0,0–0,5 V. If R input = 4,5–5,0 V, then N and F must both be at 0,0–0,5 V. Fault detection If F/N/R input signals are not in a valid state for more than 50 ms, then a fault is detected. Whenever any of the F/N/R input is (<0,0 V) or between (0,5 and 4,5 V) or > 5,0 V, then fault is detected. **Safe state** — When F/N/R fault is detected, transmission controller removes all power to Forward and Reverse solenoids. — Loss of power to overall machine, transmission controller, F/N/R, or solenoids, results in machine returning to Neutral FTA/FMEA/Risk assessments (not included) indicate automatically returning to N on a loader is low risk. Operator will still have fully functioning braking systems. A test harness is attached for the F/N/R, which can simulate all valid conditions, and fault conditions related to redundancy, and invalid voltage ranges. FTA/FMEA/Risk assessments (not included) indicate that shifting immediately to N on a loader is low risk. No transition is needed. Operator will still have fully functioning braking systems. Towing provisions are provided in the operator's manual, to allow removal machine from the work site.
4.7 Emergency stop function	Emergency stop is not required per the safety concept. None-the-less, the machine is provided with an emergency stop function, via the key switch, which has the capability of returning the machine to N in all conditions at any time.
5.2 Fault avoidance and fault control	Analysis per 5.2 is to be performed, as system is SIL 1/PL_r b on the transmission controller.
5.3 Requirements for programmable electronic systems (PES)	Software will be developed according to SIL1/PL_r b.
5.4 Malfunction or failure of the electronic components used in the machine-control systems	**Safe state** — When F/N/R fault is detected, transmission controller removes all power to F and R solenoids. —Loss of power to overall machine, transmission controller, F/N/R, or solenoids, results in machine returning to neutral FTA/FMEA/Risk assessments (not included) indicate that shifting immediately to N on a loader is low risk. No transition is needed. Operator will still have fully functioning braking systems.
5.5 Restart-up procedure	Once the machine has entered N because of a faulted condition, it remains in N until a valid N command is received at the transmission controller. After a valid N is received, the machine is then capable to once again shift to F or R per the operator's command.

Annex C
(informative)

Example of compliance with ISO 15998

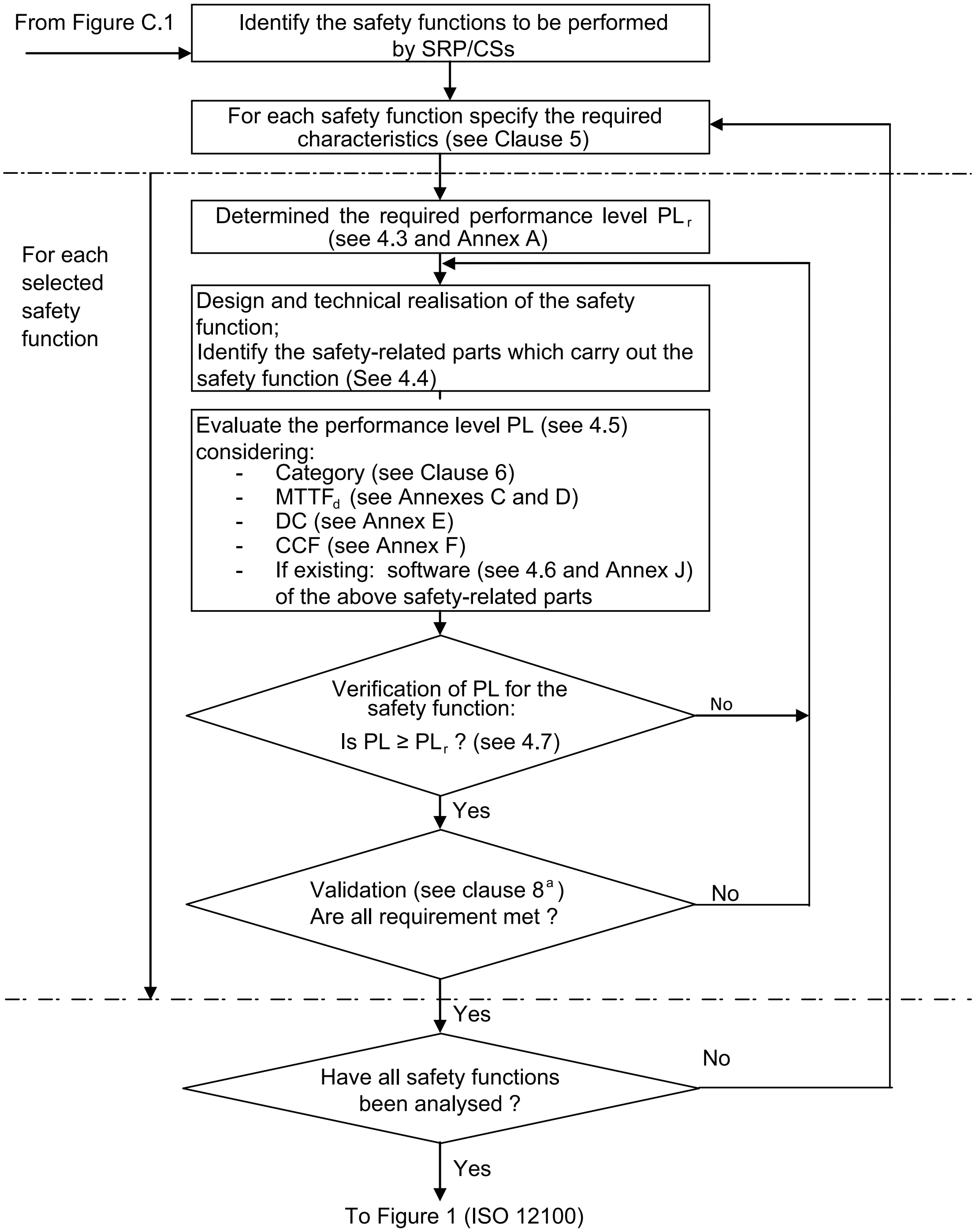
This annex summarizes one path to compliance with ISO 15998 for EMMs (earth-moving machines), using flowcharts from ISO 13849-1. See also ISO 12100 (and, for another option, IEC 61508-1:2010, Figure 2).


START
Determination of the limits of the machinery[a]
Risk assessment carried out in accordance with ISO 14121 / ISO 12100
Yes
Hazard identification[a]
Risk estimation[a]
This iterative risk reduction process shall be carried out separately for each hazard under each condition of use (task)
Risk evaluation[a]
No
Are other hazards generated?
Has the risk been adequately reduced?
Yes
END
No
Risk reduction process for the hazard:
1 by intrinsic design,
2 by safeguards,
3 by information for use[a]
Iterative process of the design of safety-related parts of the control system (SRP/CS)[b]
Does the protective measure selected depend on a control system?
Yes
No

[a] See ISO 12100.

[b] See Figure C.2 (ISO 13849-1:2006, Figure 3).

Figure C.1 — Summary process map for ISO 15998 compliance (ISO 13849-1:2006, Figure 1)


From Figure C.1
Identify the safety functions to be performed by SRP/CSs
For each safety function specify the required characteristics (see Clause 5)
For each selected safety function
Determined the required performance level PL_r (see 4.3 and Annex A)
Design and technical realisation of the safety function;
Identify the safety-related parts which carry out the safety function (See 4.4)
Evaluate the performance level PL (see 4.5) considering:
- Category (see Clause 6)
- $MTTF_d$ (see Annexes C and D)
- DC (see Annex E)
- CCF (see Annex F)
- If existing: software (see 4.6 and Annex J) of the above safety-related parts
Verification of PL for the safety function:
Is PL ≥ PL_r ? (see 4.7)
No
Yes
Validation (see clause 8[a])
Are all requirement met ?
No
Yes
Have all safety functions been analysed ?
No
Yes
To Figure 1 (ISO 12100)

Cross-references in the diagram are to ISO 13849-1:2006.

Figure C.2 — Summary process map — Iterative process for design of safety-related parts of control systems (SRP/CS) (ISO 13849-1:2006, Figure 3)

Annex D
(informative)

EMM example for complying with ISO 15998

Table D.1 — ISO 15998 verification checklist — Example

ISO 15998-1:2008/ISO 15998-1 — General requirements	Function	Completed – Yes/No/%	Compliance and verification criteria
4.2 Description of the SRP/MCS contains the following:			See below.
4.2.1 List of all system units (i.e. Control unit of transmission) used by the safety-related functions.	Product design		List of all safety-related controllers for the machine — use machine electronic specification.
4.2.2 Schematic layout of the connection devices (i.e. Wiring) and system units (i.e. controllers), representing the safety-related functions of the MCS.	Product design		Technical manual — hydraulic and electrical schematics for the machine.
4.2.3 Electrical system connection illustrated in a suitable way (i.e. circuit diagram) and shall unambiguously classify each connection device (e.g. wires) in relation to the system units (e.g. By terminal identification).	Product design		Technical manual — electrical schematics for the machine and wiring installation drawings.
4.2.4 System units (control units) marked by an identification code (e.g. numbers, symbols, characters), so that the correlation between the illustration of the system and the MCS installed in the machine can be verified.	Product design		Wiring installation drawings.
4.2.5 By using the identification code, the system units are in agreement with the documentation with regard to the basic function, safety concept and interfaces.	Product design		Wiring installation drawings with connections identified.
4.2.6 System description also includes requirements for the environmental conditions during the intended operation of the machine:	Product design		Specifications for machine, and software, hardware and MCS requirement documents
— Climatic conditions (temperature, humidity	Product design		Same as above.
— Mechanical conditions (vibration, shock)	Product design		Same as above.
— Corrosion conditions (salt spray, gas pollution)	Product design		Same as above.
— Electrical conditions (over- and under-voltage)	Product design		Same as above.
— Electromagnetic conditions	Product design		Same as above.
— Power-source-voltage fluctuation	Product design		Same as above.
4.3 Basic function of the MCS specified in a short description, which may be supported by graphical tools, such as functional schematic or block diagrams, to contain the following:	Product design		Specifications for machine, software, hardware and MCS requirement documents; block diagram with functional descriptions of each block; circuit diagram for external connection and description of external signals.
4.3.1 Enumeration of the input types and values of the MCS.	Product design		MCS requirement documents.
4.3.2 Enumeration of the controlled output types and values of the MCS.	Product design		MCS requirements documents.
4.3.3. Open-loop and closed-loop control objectives and data/sensors used.	Product design		MCS requirements documents.
4.3.4 Permissible operating and adjusting ranges.	Product design		MCS requirements documents.

Table D.1 *(continued)*

ISO 15998-1:2008/ISO 15998-1 — General requirements	Function	Completed – Yes/No/%	Compliance and verification criteria
4.4 Risk analysis and assessment of the MCS shall be carried out using the systems description in accordance with 4.2 to evaluate the hazards.	Product design and product verification		Use ISO 13849-1:2006, Tables A.2–A.5: generic SIL/$\mathrm{PL_r}$ chart from risk assessments or equivalent.
4.5 Performance criteria for basic concept and system function specified by the manufacturer for the safety concept of the machine taken into account during development and production of the MCS. The safety concept includes all measures which provide for safe operation beyond the standard operation. These are to be listed in a generally understandable way, such as in the following examples:	Product design and product verification		MCS requirements documents including safety concept. All relevant FMEAs to verify the safety concept.
— Redundancy			MCS requirements documents
— Fault-detection procedures			MCS requirements documents
— *Safe state*, a safe state may initiate, for example, an emergency motion function [reduced system performance or substitute function(s), automatic shift into a substituting function along with indication to the operator (i.e. alarms, indicators, derated performance)].			MCS requirements documents
4.6.1 Environmental conditions in which the machines are used the basis for the specification of the MCS.	Product verification		General specifications for machine, and software, hardware and MCS requirements documents
4.6.2 Environment temperature and humidity	Product verification		Comply with internal company product verification test methods and procedures for electrical and electronic components and systems which exceed those of the first part of ISO 15998.
4.6.3 Degree of protection (IP code)	Product verification		Comply with internal verification tests for electrical and electronic components and systems
4.6.4 EMC	Product verification		Comply with ISO 13766 and internal company EMC testing criteria which exceed those of the first part of ISO 15998 and ISO 13766.
4.6.5 Mechanical vibration	Product verification		Comply with internal verification tests for electrical and electronic components and systems
4.6.5 Mechanical shock	Product verification		Comply with internal verification tests for electrical and electronic components and systems.
5.1 MCS that have a minimum SIL 1/$\mathrm{PL_r}$ b or equivalent (SIL 1–3/$\mathrm{PL_r}$ b–e) fulfil the following additional requirement in accordance with the risk assessment:	Product design and product verification		Comply with both parts of ISO 15998.
5.2 Fault avoidance and fault control	Product design and product verification		MSC specification including fault avoidance and fault control as defined in Clause 5 of this part of ISO 15998 (as per 5.3, 5.4 and 5.5 of this table). Certification of quality assurance program for the manufacturer per ISO 9001 to ISO 9004 or equivalent.
5.3 Requirements for programmable electronic systems (PES) have the software developed and validated according to appropriate measures (e.g. IEC 61508-3 or ISO 13849-1:2006).	Product design and product verification		Comply with internal company — embedded software documentation specification for the software requirements specification; internal company — machine system software evaluation for validation
5.4 Malfunction or failures of the electronic components used in the MCS — entering of the safe state achieved in the case of the malfunction or failure of the electronic components used on the MCS, in accordance with risk assessment.	Product design and product verification		MCS requirements documents including safety concept and safe state. (loader examples in Table D.1)
5.5 Restart-up procedures — automatic restart-up in the case of a fault that disappears not allowed unless the evaluation of the risk assessment demonstrates safe operation can be maintained.	Product design and product verification		MCS requirements documents including description of the safety concept and safe state.

Table D.1 *(continued)*

ISO 15998-1:2008/ISO 15998-1 — General requirements	Function	Completed – Yes/No/%	Compliance and verification criteria
6 Documentation — manufacturer retains, according to the manufacturer’s record retention policy, all relevant documents for the general safety requirements of the MCS in accordance with Clause 4 of the first part of ISO 15998 .	Product design and product verification		Listed above in 4.2 to 4.6.5.
7.1 Tests give in 7.2 are intended to meet the general requirements for SRP/MCS. However, alternative means for verification are also permitted. Tests may be performance at the system unit level (e.g. sub-assembly) of the MCS and sequentially.	Product verification		Verification testing according to Clause 7 of the first part of ISO 15998 (see specifics below).
7.2 Tests for SRP/MCS — test content: test of basic functions per clauses 4.2 and 4.3; entering of safe-state test (see 5.4); functional test at operating temperature and humidity per 4.6.2 and 7.2.2; EMC test per 4.6.4; shock and vibration tests per 4.6.5, 7.2.3, 7.2.4.	Product verification		Internal company verification tests and formal test requirements for electrical and electronic components and systems; internal company procedures for machine-level electrical functional checkout; internal company procedures for machine system software evaluation; product safety and compliance functional verification of compliance with ISO 13766 and the first part of ISO 15998
7.2.2 Test of the functioning of the SRP/MCS at environmental temperature and humidity given in 7.2.2, while meeting the performance requirements given in 4.6.2, of the first part of ISO 15998.	Product verification		Comply with internal company product verification test methods and procedures for electrical and electronic components and systems which exceed the criteria of the first part of ISO 15998-1. Retain test requirements that were met.
7.2.3 Vibration test should be performed with components of MSC in the same position and with the same mountings as those fitted on the machine.	Product Verification		Same as above.
7.2.4 Shock test should be performed either in accordance with the manufacturer’s specifications or using guidance of IEC 60068-2-27.	Product Verification		Same as above.
7.2.5 Additional functional tests for SRP/MCS. Shall conduct simple software functional test and an expanded functional test in accordance with IEC 61508-7. NOTE Alternative means for verification are permitted besides those of IEC 61508.	Product Verification		Comply with product verification tests and formal test reports for machine-level electrical functional checkout.

Annex E
(informative)

Qualitative proposal for control of random hardware failures

E.1 Purpose

The purpose of this annex is to describe how IEC 61508-2:2010, Annex A can be used in order to demonstrate compliance with 5.2 of the first part of ISO 15998, *Fault avoidance and fault control for random hardware failures originating during machine life/operation*.

The method proposed relies mainly on qualitative arguments and does not require the calculation of diagnostic coverage or safe failure fraction as specified in IEC 61508-2:2010, Annex C, as that is not a normative element of ISO 15998.

This annex applies to SRP/MCS implementing safety function operating in the high/continuous mode.

E.2 Safe failure fraction (SFF)

The SFF for the subsystem results from

— the type of subsystem (type A or type B according to IEC 61508-2:2010):

> 7.4.4.1.2 An element can be regarded as type A if, for the components required to achieve the safety function,
>
> a) the failure modes of all constituent components are well defined,
>
> b) the behaviour of the element under fault conditions can be completely determined, and
>
> c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met (see 7.4.9.3 to 7.4.9.5).
>
> 7.4.4.1.3 An element shall be regarded as type B if, for the components required to achieve the safety function,
>
> a) the failure mode of at least one constituent component is not well defined,
>
> b) the behaviour of the element under fault conditions cannot be completely determined, or
>
> c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.9.3 to 7.4.9.5).
>
> NOTE This means that if at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.

[SOURCE: IEC 61508-2:2010.]

— the required SIL for the safety-related function,

— the redundancy level of the hardware architecture which determines the hardware fault tolerance.

EXAMPLE SRP/MCS: SIL1/PLr b, safe state de-energized, process safety time 500 ms. Subsystem: program sequence (of a microcontroller). Subsystem type: B (complex electronic). Subsystem hardware fault tolerance: 0 (single microcontroller, no redundancy in the SRP/MCS). Minimum required safe failure fraction: 60 % (low).

E.3 Fault control

E.3.1 Documentation

In order to apply the method the following has to be available:

- a description of the machine-control system according to 4.2 of the first part of ISO 15998;
- a description of the basic function according to 4.3 of the first part of ISO 15998;
- a risk analysis and assessment according to 4.4 of the first part of ISO 15998 including the required Safety Integrity Levels for the safety functions of the SRP/MCS;
- a description of the “safe states” for the safety functions of the SRP/MCS according to 4.5 of the first part of ISO 15998, and including information about the “process safety times” of the safety functions.

The method gives guidance to the selection of measures in order to control random hardware failures originating during machine life/operation. Therefore, it contributes to the documentation of the safety concept according to 4.5 and 5.2 of the first part of ISO 15998.

E.3.2 Hardware architecture

In order to apply the method the list of all system units of the SRP/MCS according to 4.2 of the first part of ISO 15998, shall be detailed down to subsystems fitting with IEC 61508-2:2010, Tables A.2 to A.14. See Table E.1.

Table E.1 — Hardware architecture

Table A.2	Electrical components
Table A.3	Electronic components
Table A.4	Processing units
Table A.5	Invariable memory ranges
Table A.6	Variable memory ranges
Table A.7	I/O units and interface
Table A.8	Data paths
Table A.9	Power supply
Table A.10	Program sequence
Table A.11	Clock
Table A.12	Communication and mass-storage
Table A.13	Sensors
Table A.14	Final elements

E.3.3 Architectural constraints

For every subsystem of the SRP/MCS system list, the architectural constraints according to IEC 61508-2:2010, Table 2 and Table 3 (see Tables E.2 and E.3, below) is to be used in order to determine the minimum safe failure fraction required for the subsystem.

Table E.2 — Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	**1**	**2**
< 60 %	SIL 1/PL$_r$ b/c	SIL 2/PL$_r$ d	SIL 3/PL$_r$ e
60 % ≤ 90 %	SIL 2/PL$_r$ d	SIL 3/PL$_r$ e	
90 % ≤ 99 %	SIL 3/PL$_r$ e		
≥ 99 %	SIL 3/PL$_r$ e		

[SOURCE: IEC 61508-2:2010.]

Table E.3 — Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	**1**	**2**
< 60 %	Not Allowed	SIL 1/PL$_r$ b/c	SIL 2/PL$_r$ d
60 % ≤ 90 %	SIL 1/PL$_r$ b/c	SIL 2/PL$_r$ d	SIL 3/PL$_r$ e
90 % ≤ 99 %	SIL 2/PL$_r$ d	SIL 3/PL$_r$ e	
≥ 99 %	SIL 3/PL$_r$ e		

NOTE 1 This table, in association with 7.4.4.2.1 and 7.4.4.2.2, is used for the determination of the maximum SIL that can be claimed for a subsystem given the fault tolerance of the subsystem and the SFF to the elements used.

For general application to any subsystem see 7.4.4.2.1.

For application to subsystems comprising elements that meet the specific requirements of 7.4.4.2.2. To claim that a subsystem meets a specified SIL directly from this table it will be necessary to meet all the requirements of 7.4.4.2.2.

NOTE 2 This table in association with 7.4.4.2.1 and 7.4.4.2.2 can also be used:

For the determination of the hardware fault tolerance requirements for a subsystem given the required SIL of the safety function and the SFFs of the elements to be used.

For the determination of the SFF requirements for elements given the required SIL of the safety function and the hardware fault tolerance of the subsystem.

NOTE 3 The requirements in 7.4.4.2.3 and 7.4.4.2.4 are based on the data specified in this table and Table 2.

NOTE 4 See Annex C for details of how to calculate safe failure fraction.

NOTE 5 When using 7.4.4.2.1 for the combination of type B elements, with a hardware fault tolerance of 1, in which both elements have a safe failure fraction of less than 60 %, the maximum allowable safety integrity level for a safety function carried out by the combination is SIL 1.

[SOURCE: IEC 61508-2:2010.]

E.3.4 Selection of techniques and measures to control random hardware failures during operation

The techniques and measures for controlling random hardware failures after system installation are to be selected from IEC 61508-2:2010, Annex A for every subsystem of the SRP/MCS.

The techniques and measures are to be selected so as the maximum diagnostic coverage considered achievable of IEC 61508-2:2010 in Tables A.2 to A.14 equals or exceeds the minimum required safe failure fraction due to the architectural constraints.

The techniques and measures are to be selected in accordance to the definition of the safe states of the safety functions, and the diagnostic test interval is to meet the requirements of 4.5.

EXAMPLE SRP/MCS: SIL1/PL$_r$ b, safe state de-energized, process safety time 500ms. Subsystem: program sequence (of a microcontroller). Subsystem type: B (complex electronic). Subsystem hardware fault tolerance: 0 (single microcontroller, no redundancy in the SRP/MCS). Minimum required safe failure fraction: 60 % (low). Selected diagnostic technique/measure: watchdog with separate time base and time-window. Maximum diagnostic coverage considered achievable: 90 % (medium). Additional timing requirement: diagnostic time interval + fault reaction < 500ms.

Table E.4 — Program sequence (watch-dog)

Diagnostic technique/measure	See IEC 61508-7	Maximum diagnostic coverage considered achievable	Notes
Watch-dog with separate time base without time-window	A.9.1	Low	
Watch-dog with separate time base and time-window	A.9.2	Medium	
Logical monitoring of program sequence	A.9.3	Medium	Depends on the quality of the monitoring.
Combination of temporal and logical monitoring of programme sequences	A.9.4	High	
Temporal monitoring with online check	A.9.5	Medium	
NOTE 1 This table does not replace any of the requirements of Annex C. NOTE 2 The requirements of Annex C are relevant for the determination of diagnostic coverage. NOTE 3 For general notes concerning this table, see the text preceding Table A.1.			

As

a) the maximum diagnostic coverage considered achievable: 90 % (medium) exceeds the minimum required safe failure fraction: 60 % (low),

b) the selected technique permits to reach the “safe state” de-energized,

c) the timing requirements of 4.5 are specified,

the selected technique *Watchdog with separate time base and time-window* is adequate in order to control random hardware failures during operation of the subsystem ”program sequence”.

E.3.5 Diagnostic test interval and fault reaction

E.3.5.1 Hardware fault tolerance more than zero

The requirements of IEC 61508-2:2010, 7.4.5.4:

> 7.4.5.4 The diagnostic test interval of any subsystem:
>
> — having a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mod of operation; or

> — which is implementing a safety function, or part of a safety function, operating in low demand mode of operation.
>
> Shall be such that the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

[SOURCE: IEC 61508-2:2010.]

are replaced by the following requirement:

The diagnostic test interval of any subsystem having a hardware fault tolerance of more than zero is to be less than 24 h.

E.3.6 Hardware fault tolerance of zero

The requirements of IEC 61508-2:2010, 7.4.5.3 are applicable:

> 7.4.5.3 When quantifying the effect of random hardware failures of a subsystem, having a hardware fault tolerance of 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation, credit shall only be taken for the diagnostics if:
>
> — the sum of the diagnostic test interval and the time to perform the specified action to achieve or maintain a safe state is less than the process safety time; or
>
> — in high demand mode of operation the ratio of the diagnostic test rate to the demand rate equals or exceeds 100.

[SOURCE: IEC 61508-2:2010.]

Annex F
(informative)

Architecture

The architecture of the control system should be selected based on the method selected by the user of ISO 15998. The following International Standards provide examples which may be used addressing mean time to failure consideration:

- ISO 13849-1:2006, Clause 6;
- IEC 61508-6:2010, Annex B;
- ISO 25119-2:2010, Annex A;
- ISO 26262;
- IEC 62061:2005, Clause 6.

Annex G
(informative)

Realized design to meet determined SIL or PLr levels

G.1 General

This annex is concerned with the determination that the realized design meets the determined SIL or PL_r levels. SILs should be re-evaluated to PLs in order to use references in ISO 13849-1. The realized design is to have the following quantifiable aspects determined:

- $MTTF_d$ ISO 13849-1:2006, Annex C;
- diagnostic coverage ISO 13849-1:2006, Annex E;
- common cause failure analysis ISO 13849-1:2006, Annex F;
- category of the system.

G.2 $MTTF_d$ determination

$MTTF_d$ = MTTF/percent of dangerous failures.

- Use manufacturer's data
- Use data handbooks, e.g.:
  - MIL-HDBK-217F
  - IEC/TR 62380 (formerly RDF 2000)
  - FIDES Guide
  - Advanced Logistics Development MTBF calculator
  - EPRD – Electronic Parts Reliability Data (RAC-STD-6100), Reliability Analysis Centre
  - NNPRD-95 – Non-electronic Parts Reliability Data (RAC-STD-6200) Reliability Analysis Centre
  - Software tools designed to access the above databases
  - A manufacturer (OEM or ESA supplier) may rely upon field data, to determine the $MTTF_d$, instead of calculations offered in this section
  - Siemens: SN 29500 – Failure rates of components

In many reliability calculations and the MIL standards the common assumption is that $MTTF_d$ = 2* MTTF; if mean time to failure is 50 years then mean time to dangerous failure is 100 years. It is possible to evaluate the failure mode of each component and determine the percent of the failures that are dangerous

$$MTTF_d = \frac{\text{MTTF}}{\text{percent dangerous failures}}$$

If the B10 life is available the following may be used again assuming 50 % of the failures are dangerous:

B10d approximately 2B10

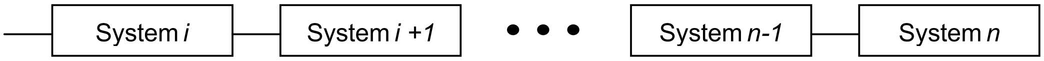
$$\mathrm{MTTFd} = \frac{\mathrm{B10d}}{(0{,}1 * \mathrm{nop})}$$

$$\mathrm{nop} = \mathrm{dop} * \mathrm{hop} * \frac{3600\mathrm{s/h}}{\mathrm{tcycle}}$$

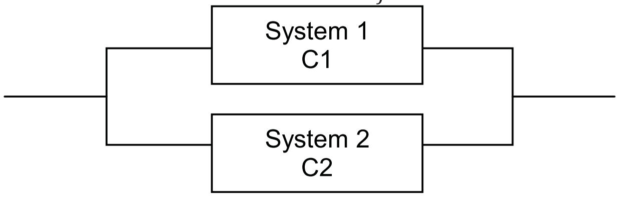
where

nop	is the number of operations;
hop	is the mean operation in hours per day;
dop	is the mean operation in days per year;
tcycle	is the mean time between the beginning of two successive cycles of the component in seconds.

The following is to be utilized to calculate MTTF$_\mathrm{d}$ in series and parallel systems:

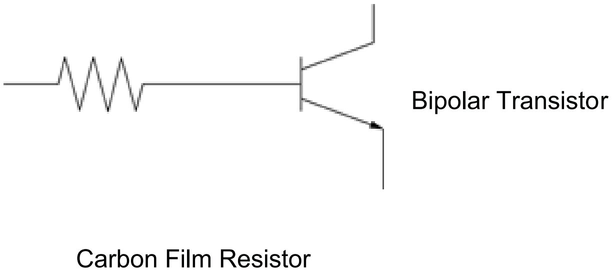


$$\frac{1}{\mathrm{MTTF_d}} = \sum_{i=1}^{N} \frac{1}{\mathrm{MTTF}_{\mathrm{d}i}} = \sum_{j=1}^{N} \frac{1}{\mathrm{MTTF}_{\mathrm{d}j}}$$



$$\mathrm{MTTF_d} = \frac{2}{3}\left[\mathrm{MTTF}_{\mathrm{d}C1} + \mathrm{MTTF}_{\mathrm{d}C2} - \frac{1}{\frac{1}{\mathrm{MTTF}_{\mathrm{d}C1}} + \frac{1}{\mathrm{MTTF}_{\mathrm{d}C2}}}\right]$$

The following is an example of a simple circuit:



Component	**MTTF** (years)	**MTTF$_\mathrm{d}$** (years)	**1/MTTF$_\mathrm{d}$**
Bipolar transistor	34 247	68 494	1.46E-05
Resistor	114 155	22 8310	4.380E-06

1/MTTF$_\mathrm{d}$ = 1/MTTF$_\mathrm{d}$(resistor) + 1/MTTF$_\mathrm{d}$(transistor)

1/MTTF$_\mathrm{d}$ = 1/68 494 + 1/228 310

MTTF$_\mathrm{d}$ = 52 687 years

This exercise will be required for each of the components and interconnect devices in the system under analysis.

The following table provides a denotation for each channel based on the $\mathrm{MTTF_d}$. In the simple example above the $\mathrm{MTTF_d}$ would be denoted as High.

$\mathrm{MTTF_d}$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $\mathrm{MTTF_d}$ < 10 years
Medium	10 years ≤ $\mathrm{MTTF_d}$ < 30 years
High	30 years ≤ $\mathrm{MTTF_d}$ ≤ 100 years

NOTE 1 The choice of the $\mathrm{MTTF_d}$ ranges of each channel is based on failure rates found in the field as state-of-the-art, forming a kind of logarithmic scale fitting to the logarithmic PL scale. An $\mathrm{MTTF_d}$ value of each channel less than three years is not expected to be found for real SRP/CS since this would mean that after one year about 30 % of all systems on the market will fail and will need to be replaced. An $\mathrm{MTTF_d}$ value of each channel greater than 100 years is not acceptable because SRP/CS for high risks should not depend on the reliability of components alone. To reinforce the SRP/CS against systematic and random failure, additional means such as redundancy and testing should be required. To be practicable, the number of ranges was restricted to three. The limitation of MTTFd of each channel values to a maximum of 100 years refers to the single channel of the SR/CS which carries out the safety function. Higher $\mathrm{MTTF_d}$ values can be used for single components (see Table D.1).

NOTE 2 The indicated borders of this table are assumed within an accuracy of 5 %.

[SOURCE: ISO 13849-1:2006, Table 5.]

G.3 Diagnostic coverage

The average diagnostic coverage is that ratio of detected dangerous failures to the total number of dangerous failures as follows. $\mathrm{DC_{avg}}$ is to be calculated for the entire channel:

$$\mathrm{DC_{avg}} = \frac{\dfrac{\mathrm{DC_1}}{\mathrm{MTTF_{d1}}} + \dfrac{\mathrm{DC_2}}{\mathrm{MTTF_{d2}}} + \ldots + \dfrac{\mathrm{DC_N}}{\mathrm{MTTF_{dN}}}}{\dfrac{1}{\mathrm{MTTF_{d1}}} + \dfrac{1}{\mathrm{MTTF_{d2}}} + \ldots + \dfrac{1}{\mathrm{MTTF_{dN}}}}$$

ISO 13849-1:2006, Annex E provides examples and estimates of DC.

Upon completion of the $\mathrm{DC_{avg}}$ analysis, the following table is to be used to establish a denotation for each channel.

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

NOTE 1 For SRP/CS consisting of several parts an average value $\mathrm{DC_{avg}}$ for DC is used in Figure 5, Clause 6 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 %, and 99 % also established in other standards (e.g. IEC 61508) dealing with diagnostic coverage of tests. Investigations show that (1 – DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 – DC) for the key values 60 %, 90 %, and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called “none”. A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated borders of this table are assumed within an accuracy of 5 %.

[SOURCE: ISO 13849-1:2006, Table 6.]

G.4 Common cause failure

A common cause failure (CCF) is a single failure point that results in a failure in 2 or more channels. IEC 61508-6:2010, Annex D provides a comprehensive procedure for measures against CCF. ISO 13849-1 provides a summary method in order to quantify CCF.

No.	Measure against CCF	Score
1	**Separation/Segregation**	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog, Components of different manufactures.	20
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, etc.	15
3.2	Components used are well-tried.	5
4	**Assessment/analysis**	
	Are the results of a failure mode and effect analysis taken into account to avoid common cause failures in design?	5
5	**Competence/training**	
	Have designers/maintainers been trained to understand the causes and consequences of common cause failures?	5
6	**Environmental**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electrical systems, both aspects should be considered.	25
6.2	Other influences Have the requirements for immunity to all relevant environmental influences such as temperature, shock, vibration, humidity (e.g. as specified in relevant standards) been considered?	10
	Total	**[max. achievable 100]**

Total score	Measures for avoiding CCF[a]
65 or better	Meets the requirements
Less than 65	Process failed = > choose additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

[SOURCE: ISO 13849-1:2006, Table 6.]

G.5 Category of system

Upon completion of the SIL or PL analysis the following table should be reviewed. The design realization may be guided by experience and a category of each channel may be selected based on initial expectations of the design.

Figure G.1 utilizes the category of system, DC_{avg}, and $MTTF_d$ in order to determine the maximum PL level attainable for the design. Since the SIL and PL are known it may direct the design realization toward a specific category. See also ISO 13849-12006, 6.2 for the details and capabilities of each category of design.

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	none	none	low	medium	low	medium	high
$MTTF_d$ of each channel:							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

[SOURCE: ISO 13849-1:2006, Table 7.]

Bibliography

[1] ISO 3450:2011, *Earth-moving machinery — Wheeled or high-speed rubber-tracked machines — Performance requirements and test procedures for brake systems*

[2] ISO 5010:2007, *Earth-moving machinery — Rubber tyred machines — Steering requirements*

[3] ISO 9001:2008, *Quality Management Systems — Requirements*

[4] ISO 9004:2009, *Managing for the sustained success of an organization — A quality management approach*

[5] ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

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

[7] ISO/TR 14121-2:2007, *Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods*

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

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

[10] ISO 25119-4:2010, *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems — Part 4: Production, operation, modification and supporting processes*

[11] ISO 26262:2011 (all parts), *Road vehicles — Functional safety*

[12] IEC 60068-2-27:2008, *Environmental testing — Part 2-27: Tests — Test Ea and guidance: Shock*

[13] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

[15] MIL-HDBK-217F: 1995, *Reliability Prediction Of Electronic Equipment*

[16] IEC/TR 62380:2004, *Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment*

[17] Guide FIDES 2009, Issue A

[18] Advanced Logistics Development MTBF calculator

ICS 53.100

Price based on 58 pages