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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Engins de terrassement — Systèmes de contrôle-commande utilisant des composants électroniques —
Partie 2: Utilisation et application de l'ISO 15998

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

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

© ISO 2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO 2012 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

© ISO 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1e-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

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.

 © ISO 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

© ISO 2012 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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).

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3425eb1c-d324-468e-94dd-b7ff77edf18a/iso-ts-15998-2-2012

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.

© ISO 2012 – All rights reserved

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

[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 0 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.

© ISO 2012 – All rights reserved

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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-87ff77fedf18/iso-ts-15998-2-2012

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

© ISO 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedff8/iso-ts-15998-2-2012

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.

© ISO 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7877fedf18/iso-ts-15998-2-2012

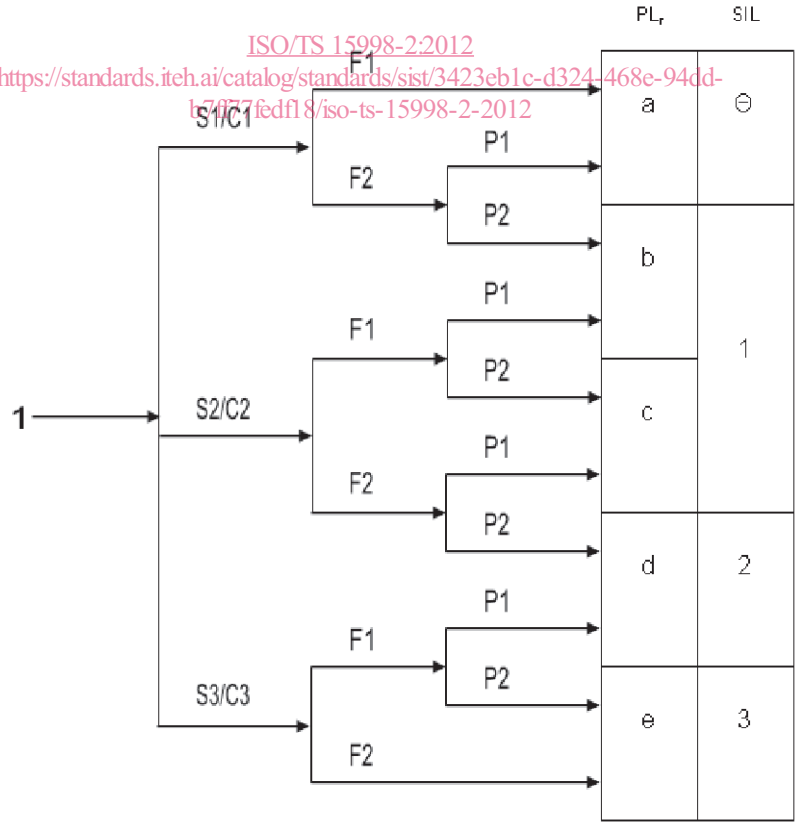


Figure 1 — Risk graph

© ISO 2012 – All rights reserved

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7f77fedff8/iso-ts-15998-2-2012

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

 © ISO 2012 – All rights reserved

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7877fed0 8f/iso-ts-15998-2-2012

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.

© ISO 2012 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423eb1c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

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

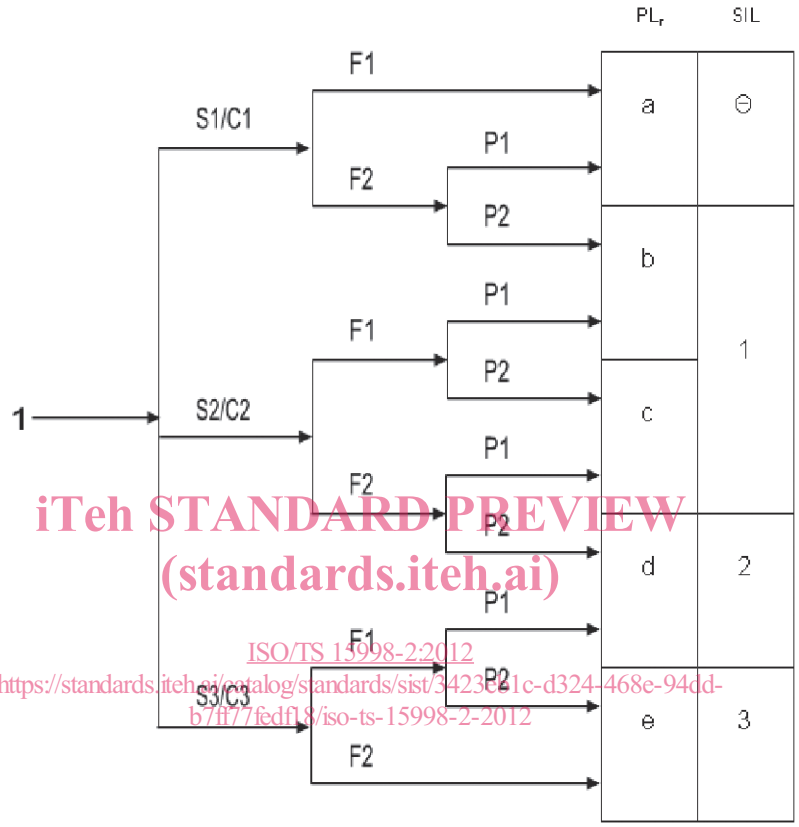
— practical safety experiences relating to the process.

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

 © ISO 2012 – All rights reserved

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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/TS 15998-2:2012
https://standards.iteh.ai/catalog/standards/sist/3423e21c-d324-468e-94dd-b7ff77fedf18/iso-ts-15998-2-2012

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.

© ISO 2012 – All rights reserved