DRAFT AMENDMENT ISO 13849-1:2006/DAM 1

ISO/TC **199** Secretariat: **DIN**

Voting begins on **2013-08-29** Voting terminates on **2014-01-29**

Safety of machinery — Safety-related parts of control systems —

Part 1: General principles for design

AMENDMENT 1

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —

Partie 1: Principes généraux de conception

AMENDEMENT 1

ICS 13.110

ISO/CEN PARALLEL PROCESSING

This draft has been developed within the International Organization for Standardization (ISO), and processed under the **ISO-lead** mode of collaboration as defined in the Vienna Agreement.

This draft is hereby submitted to the ISO member bodies and to the CEN member bodies for a parallel five-month enquiry.

Should this draft be accepted, a final draft, established on the basis of comments received, will be submitted to a parallel two-month approval vote in ISO and formal vote in CEN.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

COPYRIGHT PROTECTED DOCUMENT

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

Foreword

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

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

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

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

Amendment 1 to ISO 13849-1:2006 was prepared by Technical Committee ISO/TC 199, *Safety of machinery* and by Technical Committee CEN/TC 114, *Safety of machinery* in collaboration.

Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

AMENDMENT 1

Foreword

Last paragraph:

Delete reference to "ISO 13849-100" *since Part 100 had been withdrawn*

Introduction

Paragraph after listing:

Update reference "ISO 12100-1" *to* "ISO 12100"

5th paragraph:

Update reference "Council Directive 98/37/EC, The machinery Directive" *to* "Directive 2006/42/EC on machinery"

Table 1 and paragraph before Table 1:

Replace Table 1 and the paragraph before Table 1 by the following paragraph:

"IEC 62061 and this part of ISO 13849 specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these International Standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. ISO/TR 23849 gives guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery."

Add the following table headline after the new paragraph, in order to avoid the renumbering of all tables and the respective references:

"Table 1 deleted"

Scope

Replace NOTE 5 by new NOTE 5:

"NOTE 5 ISO 13849-1 covers high demand and continuous mode."

Normative references

Delete references:

*"*ISO 12100-1:2003, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology*

ISO 12100-2:2003, *Safety of machinery — Basic concepts, general principles for design — Part 2: Technical principles*

ISO 14121, *Safety of machinery — Principles of risk assessment"*

Add reference:

"ISO 12100:2010 *Safety of machinery — General principles for design — Risk assessment and risk reduction"*

3.1 Terms and definitions

Update reference by replacing "ISO 12100-1" *by* "ISO 12100"

3.1.6

Update source in NOTE by replacing "(see ISO 12100-1:2003, 3.34)" *by* "(see ISO 12100:2010, 3.36)"

3.1.10

Update source of definition by replacing "[ISO 12100-1:2003, 3.5]" *by* "[ISO 12100:2010, 3.5]"

3.1.11

Update source of definition by replacing "[ISO 12100-1:2003, 3.6]" *by* "[ISO 12100:2010, 3.6, modified]"

3.1.12

Update source of definition by replacing "[ISO 12100-1:2003, 3.9]" *by* "[ISO 12100:2010, 3.10]"

3.1.13

Update source of definition by replacing "[ISO 12100-1:2003, 3.11]" *by* "[ISO 12100:2010, 3.12]"

3.1.14

Update reference in NOTE by replacing "ISO 12100-1:2003, definition 3.12" *by* "ISO 12100:2010, definition 3.13"

3.1.15

Update source of definition by replacing "[ISO 12100-1:2003, 3.13]" *by* "[ISO 12100:2010, 3.17]"

3.1.16

Update source of definition by replacing "[ISO 12100-1:2003, 3.14]" *by* "[ISO 12100:2010, 3.15]"

3.1.17

Update source of definition by replacing "[ISO 12100-1:2003, 3.16]" *by* "[ISO 12100:2010, 3.16]"

3.1.18

Update source of definition by replacing "[ISO 12100-1:2003, 3.22]" *by* "[ISO 12100:2010, 3.23]"

3.1.19

Update source of definition by replacing "[ISO 12100-1:2003, 3.23]" *by* "[ISO 12100:2010, 3.24]"

3.1.20

Update source of definition by replacing "[ISO 12100-1:2003, 3.28]" *by* "[ISO 12100:2010, 3.30]"

3.1.27

Update reference in NOTE by replacing "ISO 12100-1:2003, definition 3.18" *by* "ISO 12100:2010, definition 3.19"

Add new ***definition 3.1.38:***

"**3.1.38**
high demand or continuous mode
mode of operation in which the frequency of demands on a SRP/CS is greater than one per year"

3.2 Symbols and abbreviated terms

Add in Table 2:

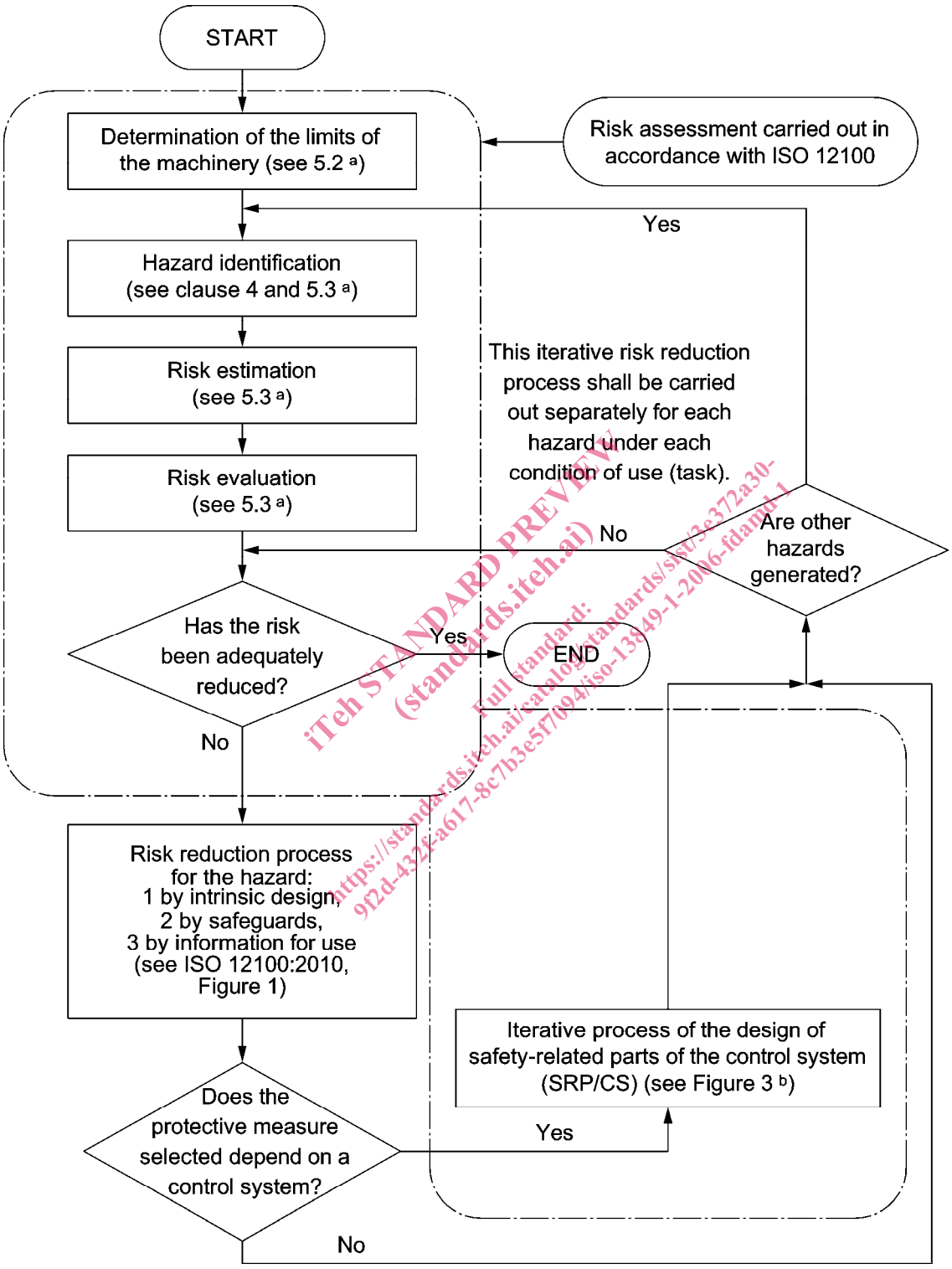
PFH_D	average probability of dangerous failure per hour	Table 3

4.1 Safety objectives in design

First paragraph:

Delete the reference "and ISO 14121" *in the first sentence.*

Replace Figure 1 with the following Figure (this new figure contains no technical modifications, but updates the references).



a Refers to ISO 12100:2010.

b Refers to this part of ISO 13849.

4.2.1 General

First paragraph:

In order to update the references, replace first sentence with:

"The strategy for risk reduction at the machine is given in ISO 12100:2010, Clause 6."

Second paragraph:

In order to update the references, replace the three items with:

"

— hazard elimination or risk reduction by design (see ISO 12100:2010, 6.2);

— risk reduction by safeguarding and possibly complementary protective measures (see ISO 12100:2010, 6.3);

— risk reduction by the provision of information for use about the residual risk (see ISO 12100:2010, 6.4).

"

4.2.2 Contribution to the risk reduction by the control system

First paragraph, 4th sentence:

Replace the word "safeguard" *with* "interlocking guard".

Third paragraph, 2nd sentence:

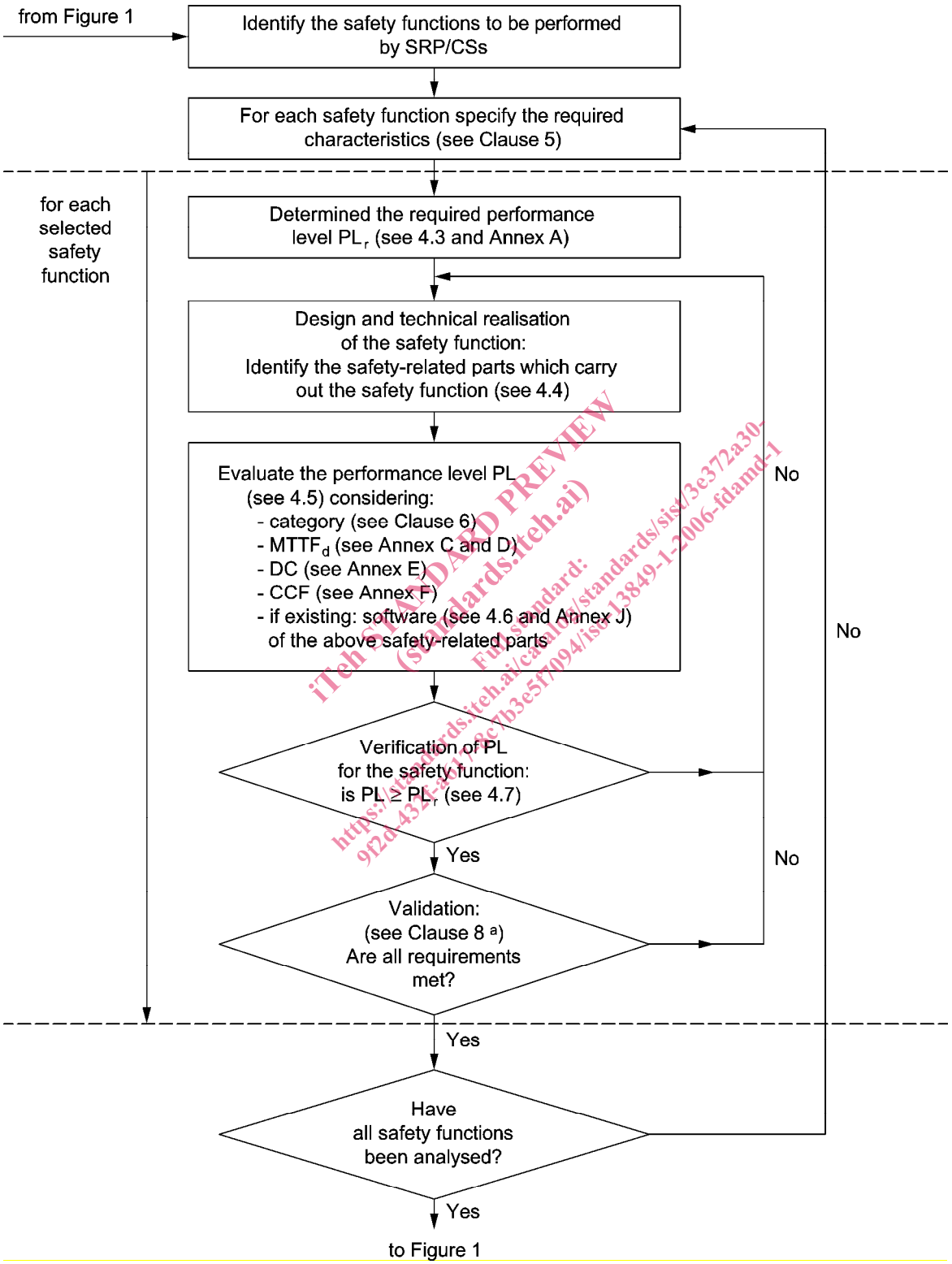
Change the sentence into "Five performance levels are set out, from the lowest PL a to the highest PL e with defined ranges of probability of a dangerous failure per hour (see Table 3)."

Fourth paragraph, below Table 3:

Replace "(see ISO 14121)" *with* "(see ISO 12100)"

Figure 3:

Change the reference by replacing at the bottom of Figure 3 "To Figure 1 (ISO 12100)" *with* "To Figure 1"



a ISO 13849-2 provides additional help for the validation.

4.5.1 Performance level PL

Replace NOTE 2 by the following new NOTE 2:

"NOTE 2 For the design of complex control systems, such as PES designed to perform safety functions, the application of other relevant standards can be appropriate (e.g. IEC 61508 or IEC 61496)."

Add the following new paragraph below Table 4:

"Although there is correspondence between the PLs of this standard and SILs of standards IEC 61508 and IEC 62061 it is allowed to use either standard but it is not permissible to mix the requirements of ISO 13849-1 and IEC 61508/IEC 62061 (see also ISO/TR 23849) when designing safety-related parts of control systems (SRP/CS)."

4.5.2 Mean time to dangerous failure of each channel ($MTTF_d$)

Second paragraph:

Add new NOTE:

"NOTE In order to combine more than 3 subsystems (SRP/CS) in Category 4 the maximum MTTFd value is increased to 2500 years for each subsystem (SRP/CS). This is because in Category 4 the other quantifiable aspects, structure and DC, are at their maximum point and this allows the series combination of more than 3 subsystems (SRP/CS) with Category 4 and achieve PL e in accordance to Clause 6.3."

4.5.3 Diagnostic coverage (DC)

Add new NOTE below Table 6:

"NOTE Examples of estimation of the diagnostic coverage (DC) is given in Annex E."

4.5.4 Simplified procedure for estimating PL

Replace headline of clause 4.5.4 with:

"4.5.4 Simplified procedure for estimating the quantifiable aspects of PL (PFH_D)"

Fifth paragraph:

Update the reference by replacing "(see ISO 12100-1:2003, Annex A)" *with* "(see ISO 12100:2010, Annex A)"

Replace the 3rd indent (page 19) with:

— for category 2, demand rate ≤ 1/100 test rate; or testing occurs immediately upon demand of the safety function and the overall time to detect the fault and to bring the machine to a non-hazardous condition (usually to stop the machine) is shorter than the time to reach the hazard (see also ISO 13855);

Replace the 4th indent (page 19) by:

— for category 2, $MTTF_{d,TE}$ is greater than one half of $MTTF_{d,L}$.

7th paragraph of page 19:

Update the reference by replacing "(see also ISO 12100-2:2003, Clause 3 and IEC 60204-1:2000)" *with* "(see also ISO 12100:2010, Clause 3 and IEC 60204-1:2005)"

4.6.2 Safety-related embedded software (SRESW)

Change in listing on page 22 (2nd listing in clause 4.6.2) in the 6th indent "separation in non-safety-related software" *to* "separation from non-safety-related software"

Add at the end of clause 4.6.2, below NOTE 2, the following new paragraph:

"For components for which SRESW requirements are not fulfilled, e.g. non safety rated PLCs, these components may be used under the following alternative conditions:

— the SRP/CS is limited to PL a or b and uses category B, 2 or 3;

— the SRP/CS is limited to PL c or d and uses two components for two channels in category 2 or 3 and the two components use diverse embedded software or diverse technologies and an appropriate safety related application software (see 4.6.3), so that failure detection fulfils the required DC (e. g. cross monitoring);

— the SRP/CS is limited to PL c or d and uses two components for two channels in category 2 or 3 and uses two diverse application software channels so that failure detection fulfils the required DC (e. g. cross monitoring)."

4.8 Ergonomics aspects of design

First paragraph:

Replace "ISO 12100-2" *with* "ISO 12100" *and* "IEC 60204-1:2000, Clause 10" *with* "IEC 60204-1:2005, Clause 10"

Third paragraph:

Update the reference by replacing "ISO 12100-2:2003, 4.8" *with* "ISO 12100:2010, 6.2.8"