FINAL
DRAFT

AMENDMENT

ISO 13849-1:2006 FDAM 1

ISO/TC **199**

Secretariat: **DIN**

Voting begins on:
2015-03-19

Voting terminates on:
2015-05-19

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

Please see the administrative notes on page iii

Reference number
ISO 13849-1:2006/FDAM 1:2015(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

ISO/CEN PARALLEL PROCESSING

This final draft has been developed within the European Committee for Standardization (CEN), and processed under the **CEN-lead** mode of collaboration as defined in the Vienna Agreement. The final draft was established on the basis of comments received during a parallel enquiry on the draft.

This final draft is hereby submitted to the ISO member bodies and to the CEN member bodies for a parallel two-month approval vote in ISO and two-month formal vote in CEN.

Positive votes shall not be accompanied by comments.

Negative votes shall be accompanied by the relevant technical reasons.

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"

4th paragraph:

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

9th paragraph:

Delete the word "help" in the first sentence.

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

Delete NOTE 5 and substitute the last sentence of the first paragraph by:

"It applies to SRP/CS for high demand and continuous mode, regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery."

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 references:

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

ISO/TR 22100-2:2014, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*

ISO/TR 23849, *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*

IEC 62061:2012, *Safety of machinery — Functional safety of safety–related electrical, electronic and programmable electronic control systems"*

3.1 Terms and definitions

Change definition 3.1.12 as follows:

"**hazardous situation**
circumstance in which a person is exposed to at least one hazard

NOTE 1 to entry: The exposure can result in harm immediately or over a period of time.

[SOURCE: ISO 12100:2010, 3.10.]"

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

3.1.6

Update source in NOTE 1 to entry 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* "[SOURCE: ISO 12100:2010, 3.5.]"

3.1.11

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

3.1.13

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

3.1.14

Update reference in NOTE 1 to entry 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* "[SOURCE: ISO 12100:2010, 3.17.]"

3.1.16

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

3.1.17

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

3.1.18

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

3.1.19

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

3.1.20

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

3.1.27

Update reference in NOTE 1 to entry 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 or the safety related control function retains the machine in a safe state as part of normal operation

[SOURCE: IEC 62061:2012, 3.2.27, modified.]"

*Add new **definition 3.1.39:***

"**3.1.39**
proven in use
demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required performance level (PL_r)

[SOURCE: IEC 61508-4:2010, 3.8.18, modified.]"

3.2 Symbols and abbreviated terms

Add in Table 2:

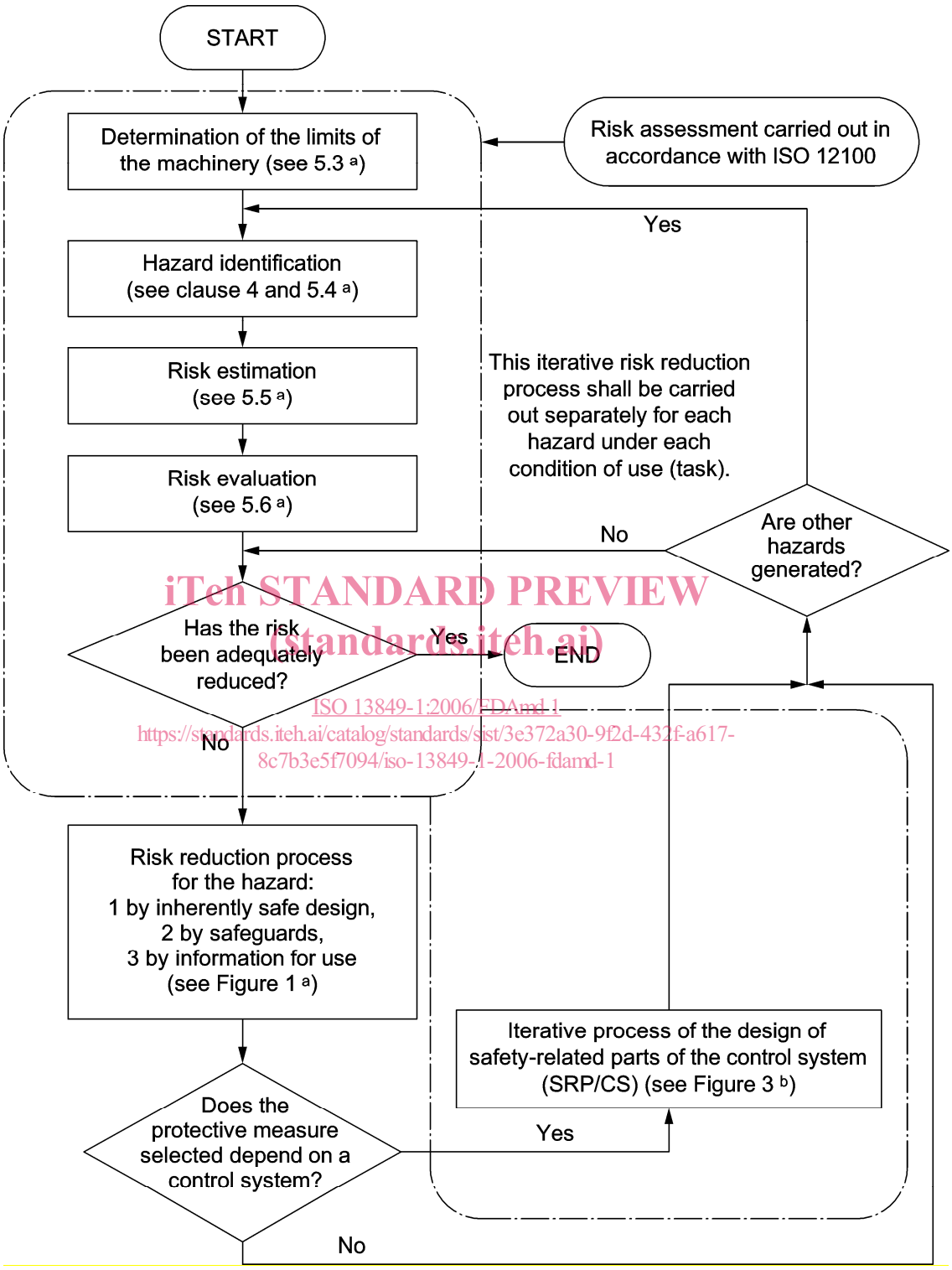
PFH_D	average probability of dangerous failure per hour	Table 3 and Table K.1
r_t	Test rate	3.1.29

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 references/wordings):



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 paragraph with:

"The strategy for risk reduction at the machine is given in ISO 12100:2010, 6.1, and further guidance is given in ISO 12100:2010, 6.2 (inherent design measures) and 6.3 (safeguarding and complementary protective measures). This strategy covers the whole life cycle of the machine."

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"

Add the following Note after the first paragraph:

"Note: There is no need to apply this strategy of risk reduction on non-safety related parts of control systems or purely functional elements of a machine (see ISO TR 22100-2:2014, clause 3)."

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)."

Add the following paragraph before table 3:

"In order to achieve a PL, beside quantifiable aspects, it is also necessary to satisfy requirements related to qualitative aspects of PL (see 4.5).

Table 3:

Change the title of the second column into "Average probability of dangerous failure per hour (PFH_D) 1/h".

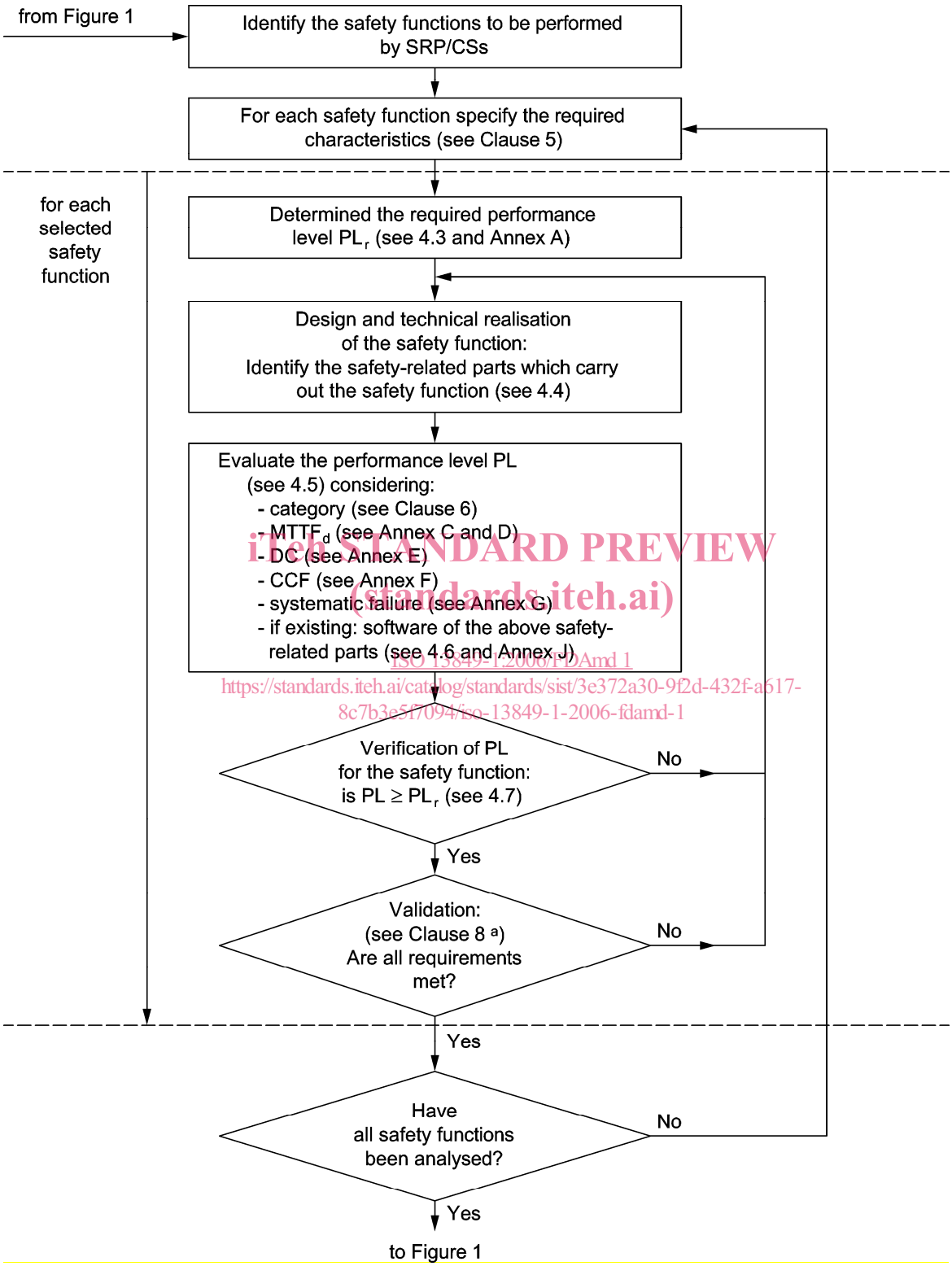
Delete the Note in the table.

Fourth paragraph, below Table 3:

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

Figure 3:

Replace Figure 3 by the following Figure (some clarification of the big box in the middle):



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

Figure 4:

Change the key for figure 4 into:

"**Key**

I input (e.g. limit switch, sensor, AOPD)
L logic
O output (e.g. valve, contactor, current converter)
1 initiation event (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD)
2 machine actuator (e.g. motor, cylinder)"

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:

"When a safety related control function is designed using one or more SRP/CS, each SRP/CS shall be designed either according to ISO 13849-1 or according to IEC 62061/ IEC 61508 (see also ISO/TR 23849) although there is correspondence between the PLs of this standard and the SILs of standards IEC 61508 and IEC 62061. SRP/CSs can be combined according to 6.3."

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

Second paragraph:

Change the second paragraph as follows and add a new NOTE:

"For each SRP/CS (subsystem) according to table 5, the maximum value of $MTTF_D$ for each channel is 100 years. For Category 4 SRP/CS (subsystems) the maximum value of $MTTF_D$ for each channel is increased to 2500 years.

NOTE This higher value is justified 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)

2nd paragraph:

Change the second paragraph as follows:

"For the estimation of DC, in most cases, failure mode and effects analysis (FMEA, see IEC 60812) or similar methods can be used. In this case, all relevant faults and/or failure modes should be considered. For a simplified approach to estimating DC, see Annex E."

Add a new NOTE below Table 6:

"NOTE Examples of estimation of the diagnostic coverage (DC) are 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"

2nd Paragraph:

Change the first sentence into:

"This clause describes a simplified procedure for estimating the quantifiable aspects of PL of a SRP/CS based on designated architectures."

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 by:

"— for category 2, demand rate ≤ 1/100 test rate (see also Note in Annex K); or testing occurs immediately upon demand of the safety function and the overall time to detect the fault and to bring the machine to a 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 by:

"— for category 2, $MTTF_D$ of the testing channel is greater than one half of $MTTF_D$ of the functional channel."

Delete the Note after the 4th indent.

9th paragraph:

Change the paragraph into:

"For SRP/CS with software, the requirements of 4.6 shall be applied."

12th paragraph:

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)"

Add the following new paragraph as 4.5.5:

"

4.5.5 Description of the output part of the SRP/CS by category

If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application–specific reliability data is available, the machine manufacturer may evaluate the quantifiable aspects of the PL without any $MTTF_D$-calculation.

For such cases, the safety-related performance level (PL) is implemented by the architecture, the diagnostic and the measures against CCF.

Table 8 shows the relationship between achievable PL (corresponding to Figure 5) and categories. PL a and PL b can be implemented with Cat. B. PL c can be implemented with Cat. 1 or Cat. 2, if well-tried components and well-tried safety principles are used.

When implementing an PL c safety function with Cat.1, the T_{10D} values of safety-relevant components that are not monitored in the process, are determined. This T_{10D} values can be determined based on proven in use data by machine manufacturer.

The $MTTF_D$ of the test channel in Cat. 2 shall at least be 10 years.

PL d can be implemented with Cat. 3 if well-tried components and well-tried safety principles are used. PL e can be implemented with Cat. 4, if well-tried components and well-tried safety principles are used.

Basically: In the implementation of the safety function with Cat. 2, Cat. 3 or Cat. 4 common-cause failures (CCF) and a sufficient diagnostic coverage (DC) have to be considered (low, medium for Cat. 2 and 3, high for Cat. 4).

In this case the calculation of the DC_{avg} is reduced to the arithmetic mean value of all components individuals DCs in the functional channel.

Table 1 — PL and PFH_D as worst case estimation based on category, DC_{avg}, and use of well-tried components

	PFH_D (1/h)	Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL a	2*10-5	●	O	O	O	O
PL b	5*10-6	●	O	O	O	O
PL c	1,7*10-6	-	●2*	●1*	O	O
PL d	2,9*10-7	-	-	-	●1*	O
PL e	4,7*10-8	-	-	-	-	●1*
●	Applied category is recommended					
O	Applied category is optional					
-	Category is not allowed					