Technical Report

ISO/TR 13849-3

First edition
2026-03

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

Part 3: Markov model-based PFH calculation

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

Partie 3: Calcul PFH basé sur le modèle Markov

Reference number
ISO/TR 13849-3:2026(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 199, *Safety of machinery*.

A list of all parts in the ISO 13849 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document has been prepared to enhance the capabilities of the simplified procedure of ISO 13849-1:2023, 6.1.8 and Annex K, for estimating the performance level for subsystems.

By addressing the designated architectures of ISO 13849-1, the document presents an approach using Markov model-based formulas to estimate the average frequency of a dangerous failure of the safety function. As well as the simplified procedure of ISO 13849-1, the method considers the architecture, the $MTTF_D$ of channels, diagnostic coverage DC_{avg}, the common cause factor β and the mission time T_M.

Beyond the capabilities of the simplified procedure the method presented here can allow for different test rates, a mission time different from 20 years, a common cause factor different from 2 % and any $MTTF_D$ ratio of a functional channel and its related test channel. Asymmetric redundancy is supported without beforehand symmetrisation.

The formulas of this document can also be used in the context of other standards demanding the estimation of *PFH* as long as the system under assessment meets the method's underlying assumptions (see Clause 4).

ISO 13849 and IEC 62061 govern the functional safety of machinery and require the probability of failure to be determined for each safety function in terms of a quantitative estimation of the *PFH* value (average frequency of a dangerous failure of the safety function).

NOTE In IEC 62061 (as well as in IEC 61508), *PFH* is descriptively denoted as the “average frequency of a dangerous failure of the safety function”. The abbreviation *PFH* stems from the International Standard’s former denotation as the “probability of a dangerous failure per hour”.

These International Standards assist users in ascertaining the *PFH* in different ways: IEC 62061 by provision of equations for calculation of the *PFH*, ISO 13849-1 by a table and some associated formulas. Both approaches have their drawbacks. The equations in IEC 62061 fail to address single-channel tested systems in desirable depth and in some cases yield very conservative results for two-channel tested systems. The table-based solution in ISO 13849-1 lacks flexibility owing to the fixed specification of the mission time and the common cause factor (β) and entails additional overhead for asymmetrical two-channel systems. Usually, the methods in the two standards will yield *PFH* values deviating to some extent from each other.

The objective of the *PFH* equations presented and derived in this document is for the benefits of flexible solutions involving equations to be combined with the more precise modelling technique upon which the table solution is based. The *PFH* equations yield good to very good reproduction of the table values stated in ISO 13849-1:2023, Annex K, and in particular cases assume the form of equations already contained in IEC 62061. They can therefore be regarded as a further development of the instruments of both International Standards.

Markov models, which are also among the instruments considered suitable in IEC 61508-6 and IEC 61508-7, are selected exclusively as the method for analysis of the architectures studied within this document. Unlike the numerical methods (stochastic Petri nets, Monte Carlo simulation), Markov models enable equations to be derived. They are also superior to reliability block diagrams (RBDs) in their handling of mutually influencing failure processes and the reinsertion of repaired systems. The drawback of the Markov method of being able to handle only exponentially distributed processes (constant transition rates) does not provide significant detriment to the precision of the results.

Simple special cases are treated as non-standard cases of the higher-level more complex cases, enabling overall methodical coherence to be attained.

The body part of this document addresses the use of the formulas for the estimation of the *PFH* value. The definitions, variables and the basic assumptions are presented as well as the formulas.

Annex A demonstrates the application of this approach to the examples A and B in ISO 13849-1:2023, Annex I.

Annex B of this document discloses the derivation of the presented formulas based on Markov models for the different architectures.

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

Part 3: Markov model-based PFH calculation

1 Scope

This document provides formulas for the estimation of the *PFH* value of single-channel architectures as well as two-channel architectures with and without diagnostics in accordance with ISO 13849-1. The formulas presented in this document are based on Markov modelling and can be used as an alternative to the simplified procedure of ISO 13849-1 for estimating the quantifiable aspects of the performance level (see ISO 13849-1:2023, 6.1.8, Figure 12, and Annex K). They can also serve as an alternative to any other adequate method for estimating the quantifiable aspects of the performance level.

NOTE Different estimation methods can vary in the resulting *PFH* values due to their nature. A certain variation is usually the consequence of different modelling approaches and unavoidable simplifications specific to the method.

Other requirements of ISO 13849-1, e.g. on categories or software, are not addressed by this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 13849-1, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13849-1 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.2 Symbols and abbreviated terms

The definition of parameters related to the quantitative estimation of the *PFH* value, such as mean time to dangerous failure $MTTF_D$, diagnostic coverage *DC*, common cause factor β mission time T_M, etc., can be found in ISO 13849-1:2023, Clause 3.

With only a few exceptions, all variables used in this document are listed in Table 1 below.

NOTE Within this document components with mechanical wear are concisely addressed as wearing elements or wearing parts.

Table 1 — Used variables and locations of their appearance

Variable	Pre-ferred unit	Description	Use (selection)
$B_{10D\,E}$	–	Number of working cycles by which 10 % of the wearing elements E have failed dangerously	Formulas (5), (6), (B.1), (B.4), (B.5)
C_N	–	Auxiliary variable used for two-channel systems	Formulas (31), (B.102)
C_P	–	Auxiliary variable used for two-channel systems	Formulas (30), (B.101)
DC	–	Diagnostic coverage of the functional channel of a single-channel system or a symmetrical two-channel system	Figures 3, 4, 9, B.2, B.3; Formulas (11), (13), (14), (15), (17), (18), (38), (B.47), (B.49), (B.50), (B.51), (B.54), (B.55), (B.125), (B.126)
DC_A	–	Diagnostic coverage of channel A of a two-channel system	Figures 6, 7, (B.14), (B.15); Formulas (20), (22), (24), (32), (36), (39), (B.65), (B.66), (B.99)
$\overline{DC}_A$	–	Generalized diagnostic coverage of channel A of a two-channel system with consideration of the test interval of the channel	Formulas (24), (26), (37), (B.64), (B.65), (B.122), (B.123)
DC_B	–	Diagnostic coverage of channel B of a two-channel system	Figures 6, 7, (B.14), (B.15); Formulas (21), (23), (25), (33), (36), (39), (B.68), (B.69), (B.100)
$\overline{DC}_B$	–	Generalized diagnostic coverage of channel B of a two-channel system with consideration of the test interval of the channel	Formulas (25), (27), (37), (B.67), (B.68), (B.122), (B.123)
DC_{CH}	–	Diagnostic coverage of channel CH	Formula (4)
DC_i $i = 1 \ldots n$	–	Diagnostic coverage of element *i* of channel CH	Figure 1, Formula (4)
E	–	Element or wearing element	Formulas (5), (6), (B.1), (B.2), (B.3), (B.4), (B.5)
E_i $i = 1 \ldots n$	–	Element *i* of channel CH	Figure 1, Formulas (1), (2), (3), (4)
d_{op}	d/a	Mean annual number of operation days of a wearing element	Formula (7)
h_{op}	h/d	Mean daily number of operation hours of a wearing element	Formula (7)
L_A	h^{-1}	Auxiliary variable used for two-channel systems	Figures B.21, B.22; Formulas (19), (20), (22), (26), (28), (29), (30), (31), (32), (34), (B.66), (B.94), (B.95), (B.98), (B.99), (B101), (B102), (B104), (B.106)
L_B	h^{-1}	Auxiliary variable used for two-channel systems	Figures B.21, B.22; Formulas (19), (21), (23), (27), (28), (29), (30), (31), (33), (35), (B.69), (B.94), (B.95), (B.98), (B.100), (B.101), (B.102), (B.105), (B.107)
L_α	h^{-1}	Auxiliary variable used for single-channel systems	Formulas (B.30), (B.32), (B.34)

NOTE 1 FIT = $10^{-9}\ h^{-1}$

Table 1 *(continued)*

Variable	Pre-ferred unit	Description	Use (selection)
L_β	h^{-1}	Auxiliary variable used for single-channel systems	Formulas (B.30), (B.33), (B.34)
L_θ	h^{-1}	Auxiliary variable used for single-channel systems	Formulas (B.30), (B.31), (B.34)
L_1	h^{-1}	Auxiliary variable used for two-channel systems	Formulas (28), (B.94)
L_2	h^{-1}	Auxiliary variable used for two-channel systems	Formulas (29), (B.95)
$MTTF_{D\,CH}$	a	Mean time to dangerous failure of channel CH	Formulas (2), (3)
$MTTF_{D\,E}$	a	Mean time to dangerous failure of the wearing element E	Formula (B.5)
$MTTF_{D\,Ei}$ $i = 1 \ldots n$	a	Mean time to dangerous failure of the element *i* of channel CH	Formulas (2), (3)
n_{op}	h^{-1}, a^{-1}	Operating frequency (number of operations per time unit) of the wearing element E; in case of intermittent operation: mean operating frequency based on a time span of one year	Formulas (5), (6), (7), (B.1), (B.4), (B.5)
$P_{A\,DD}$	–	Mean probability of the state “A DD”	Formula (B.59)
$p_{A\,DU}$	–	Instantaneous probability of the state “A DU”	Formula (B.92)
$P_{A\,DU\,2}$	–	Mean probability of the state “A DU 2”	Formula (B.60)
$p_{B\,DU}$	–	Instantaneous probability of the state “B DU”	Formula (B.93)
PFH	h^{-1}	Average frequency of a dangerous failure per hour NOTE PFH is seen as the mean value over time of the frequency of the unmet demands upon the safety function (frequency of unsuccessful attempts, frequency of malfunction).	Figures B.3, B.15; Formulas (10), (11), (13), (14), (15), (16), (17), (18), (19), (36), (37), (38), (39), (40), (B.34), (B.35), (B.47), (B.49), (B.50), (B.51), (B.52), (B.54), (B.55), (B.97), (B.98), (B.119), (B.120), (B.121), (B.122), (B.123), (B.124), (B.125), (B.126), (B.127), (B.128), (B.135)
pfh	h^{-1}	Instantaneous value of the frequency of a dangerous failure (instantaneous value of the *PFH*)	Formulas (B.29), (B.30), (B.34), (B.96), (B.97)
PFH_{NT}	h^{-1}	*PFH* of a single-channel, untested system (see *PFH*)	Formulas (B.38), (B.39), (B.40)
PFH_{TOT}	h^{-1}	*PFH* of a single-channel, time-optimal tested system (see *PFH*)	Formulas (B.37), (B.39), (B.40)
PFH_i $i = 1 \ldots n$ or $i = 1 \ldots 5$	h^{-1}	*PFH* contribution of subsystem *i* of a series arrangement of *n* subsystems or *PFH* component *i* of a two-channel system in simplified analysis (see *PFH*)	Formulas (10), (B.114), (B.115), (B.116), (B.117), (B.118), (B.119)
P_{FPN}	–	Mean probability of the state “FPN” (flow partitioning node)	Figure B.7; Formulas (B.10), (B.12)
p_{FPN}	–	Instantaneous probability of the state “FPN” (flow partitioning node)	Figure B.7; Formulas (B.6), (B.7), (B.8), (B.9), (B.10), (B.11)
p_i $i = 1 \ldots 3$	–	Instantaneous probability of the state *i*	Formulas (B.19), (B.20), (B.23), (B.24), (B.70), (B.71), (B.72), (B.76), (B.77), (B.78)
NOTE 1 FIT = 10^{-9} h^{-1}			

Table 1 *(continued)*

Variable	Pre-ferred unit	Description	Use (selection)
p_{INT}	–	Instantaneous probability of the state "INT"	Figure B.27; Formulas (B.108), (B.109), (B.110), (B.111)
$p_{M\,D}$	–	Instantaneous probability of the state "M D" of a single-channel system	Formulas (B.28), (B.29)
p_{OK}	–	Instantaneous probability of the state "OK" of a single-channel system	Formulas (B.27), (B.29)
P_{OK}	–	Mean probability of the state "OK" of a two-channel system	Formulas (B.59), (B.60), (B.61)
r_d	h^{-1}	Demand rate upon the safety function	Figures B.3, B.12, B.15; Formulas (11), (12), (14), (17), (B.15), (B.16), (B.17), (B.18), (B.35), (B.36), (B.41), (B.45), (B.46), (B.47), (B.50), (B.54)
r_r	h^{-1}	Repair rate	Figures B.3, B.15
r_t	h^{-1}	Test rate of the functional channel of a single-channel system or a symmetrical two-channel system	Figures 3, 4, 9, B.2, B.3, B.12; Formulas (11), (12), (14), (17), (B.15), (B.16), (B.17), (B.29), (B.35), (B.36), (B.41), (B.45), (B.46), (B.47), (B.50), (B.54), (B.126)
r_{ti} $i = 1 \ldots n$	h^{-1}	Test rate of element *i* of channel CH	Figure 1
r_{tA}	h^{-1}	Test rate of channel A of a two-channel system	Figures 6, B.14, B.15; Formulas (22), (24), (B.57), (B.124)
r_{tB}	h^{-1}	Test rate of channel B of a two-channel system	Figures 6, B.14, B.15; Formulas (23), (25), (B.58), (B.124)
T	h	Test interval of a symmetrical two-channel system; clearing interval of the flow partitioning node "FPN" or the state "INT"	Figures 9, B.7, B.27; Formulas (38), (B.10), (B.11), (B.12), (B.13), (B.14), (B.15), (B.111), (B.113), (B.125)
$T_{10D\,E}$	h, a	Time until 10 % of the wearing elements E have failed dangerously	Formulas (6), (B.1), (B.2), (B.3)
T_A	h	Test interval of channel A of a two-channel system	Figures 6, 7, B.14, B.16, B.18, B.24; Formulas (20), (24), (36), (B.57), (B.59), (B.61), (B.62), (B.64), (B.65), (B.66), (B.114), (B.120), (B.121)
T_B	h	Test interval of channel B of a two-channel system	Figures 6, 7, B.14, B.16, B.24; Formulas (21), (25), (36), (B.58), (B.63), (B.67), (B.68), (B.69), (B116), (B.120), (B.121)
t_{cycle}	s	Cycle time of a wearing element	Formula (7)
NOTE 1 FIT = $10^{-9}\ h^{-1}$			

Table 1 *(continued)*

Variable	Pre-ferred unit	Description	Use (selection)
T_M	h, a	Mission time; if a proof test according to IEC 62061:2021, 3.2.47, is implemented, the proof test interval supersedes T_M.	Formulas (11), (13), (17), (18), (19), (20), (21), (22), (23), (24), (25), (36), (37), (38), (39), (40), (B.34), (B.35), (B.37), (B.47), (B.49), (B.54), (B.55), (B.60), (B.61), (B.62), (B.63), (B.65), (B.66), (B.68), (B.69), (B.97), (B.98), (B.99), (B.100), (B.115), (B.117), (B.120), (B.121), (B.122), (B.123), (B.124), (B.125), (B.126), (B.127), (B.128), (B.135)
$TRTE$	–	Time-related test efficiency on a single-channel tested system	Figure B.13; Formulas (12), (B.41), (B.45), (B.46)
β	–	Common cause factor, constituting a quantitative dimension for the common cause failures of two channels (single-channel system: functional channel F and test channel M; two-channel system: channels A and B)	Figures 3, 6, 7, 8, 9, B.1; B.2, B.14; Formulas (8), (9), (38)
Δt	h, a	Period of time for which the mean operation frequency n_{op} of a wearing element is calculated (typically one year) or Small time interval used for limit calculation	Formulas (7) Formulas (B.6), (B.7)
Λ_1	h^{-1}	Failure-induced absolute inflow rate to the flow partitioning node “FPN”	Figure B.7; Formulas (B.6), (B.7), (B.8), (B.9), (B.10), (B.11), (B.12)
Λ_2	h^{-1}	Failure-induced absolute outflow rate from the flow partitioning node “FPN” or from the state “INT”	Figures B.7, B.27; Formulas (B.12), (B.111), (B.113)
Λ_3	h^{-1}	Absolute outflow rate from the flow partitioning node “FPN” caused by periodic clearing	Figure B.7; Formulas (B.11), (B.12)
λ_1	h^{-1}, FIT	Failure-induced nominal inflow rate to the flow partitioning node “FPN” or to the intermediate state “INT”	Figures B.7, B.27; Formulas (B.13), (B.14), (B.108), (B.110), (B.111), (B.113)
λ_2	h^{-1}, FIT	Failure-induced nominal outflow rate from the flow partitioning node “FPN” or from the intermediate state “INT”	Figures B.7, B.27; Formulas (B.6), (B.7), (B.8), (B.9), (B.10), (B.11), (B.12), (B.13), (B.14), (B.108), (B.110), (B.111), (B.113)
λ_A	h^{-1}, FIT	Failure-induced nominal outflow rate from the flow partitioning node “FPN”	Figures B.7, B.8, B.9, B.12; Formulas (B.13), (B.16), (B.29), (B.32), (B.33)
NOTE 1 FIT = 10^{-9} h^{-1}			

Table 1 *(continued)*

Variable	Pre-ferred unit	Description	Use (selection)
λ_{AD}	h^{-1}, FIT	Dangerous failure rate of channel A of a two-channel system	Figures 6, 7, 8, B.14, B.15, B.18B.26; Formulas (19), (20), (22), (26), (28), (29), (30), (31), (32), (34), (36), (37), (39), (40), (B.59), (B.61), (B.62), (B.64), (B.66), (B.91), (B.92), (B.93), (B.94), (B.95), (B.96), (B.97), (B.98), (B.99), (B.101), (B.102), (B.114), (B.115), (B.116), (B117), (B.120), (B.121), (B.122), (B.123), (B.124), (B.127), (B.128), (B.135)
$\lambda_{AD\ SER\text{-}free}$	h^{-1}, FIT	As λ_{AD}, but without the component caused by soft errors	Formulas (8), (B.103)
$\lambda_{A\ SI}$	h^{-1}, FIT	Surrogate inflow rate to the state “A DU 2” of a two-channel system	Figures B.18, B.19, B.20; Formulas (B.60), (B.61), (B.62), (B.64)
λ_{B}	h^{-1}, FIT	Nominal outflow rate from the flow partitioning node “FPN” caused by periodic clearing	Figures B.7, B.8, B.9, B.12; Formulas (B.14), (B.17), (B.29), (B.32), (B.33)
λ_{BD}	h^{-1}, FIT	Dangerous failure rate of channel B of a two-channel system	Figures 6, 7, 8, B.14, B.15, (B.26); Formulas (19), (21), (23), (27), (28), (29), (30), (31), (33), (35), (36), (37), (39), (40), (B.63), (B.67), (B.69), (B.91), (B.92), (B.93), (B.94), (B.95), (B.96), (B.97), (B.98), (B.100), (B.101), (B.102), (B.114), (B.115), (B.116), (B117), (B.120), (B.121), (B.122), (B.123), (B.124), (B.127), (B.128), (B.135)
$\lambda_{BD\ SER\text{-}free}$	h^{-1}, FIT	As λ_{BD}, but without the component caused by soft errors	Formulas (8), (B.103)
$\lambda_{B\ SI}$	h^{-1}, FIT	Surrogate inflow rate to the state “B DU 2” of a two-channel system	Figures B.19, B.20; Formulas (B.63), (B.67)
λ_{CC}	h^{-1}, FIT	Common cause failure rate	Figure B.1; Formulas (8), (9), (B.48), (B.103),
λ_{CHD}	h^{-1}, FIT	Dangerous failure rate of channel CH	Formula (1)
λ_{D}	h^{-1}, FIT	Dangerous failure rate of each of the functional channels of a symmetrical two-channel system	Figure 9; Formulas (38), (B.125), (B.126)
$\lambda_{D\ SER\text{-}free}$	h^{-1}, FIT	As λ_{D}, but without the component caused by soft errors	Formulas (38), (B.125), (B.126)
λ_{ED}	h^{-1}, FIT	Constant surrogate dangerous failure rate over time for the wearing element E	Formulas (5), (B.2), (B.3), (B.4)
λ_{EiD} $i = 1 \ldots n$	h^{-1}, FIT	Dangerous failure rate of the element *i* of channel CH comprising *n* Elements	Figure 1; Formulas (1), (2), (3)
NOTE 1 FIT = $10^{-9}\ h^{-1}$			

Table 1 *(continued)*

Variable	Preferred unit	Description	Use (selection)
λ_{FD}	h^{-1}, FIT	Dangerous failure rate of the functional channel F of a single-channel system; dangerous failure results in loss of the safety function	Figures 3, 4, 5, B.2, B.3, B.6, B.11, B.12; Formulas (11), (13), (14), (15), (16), (17), (18), (B.16), (B.17), (B.35), (B.47), (B.49), (B.50), (B.51), (B.52), (B.54), (B.55)
$\lambda_{FD\ SER\text{-}free}$	h^{-1}, FIT	As λ_{FD}, but without the component caused by soft errors	Formulas (9), (B.48)
λ_{ij} $i = 1 \ldots 3$ $j = 1 \ldots 3$	h^{-1}, FIT	Transition rate from state *i* to state *j*	Figures B.10, B.23; Formulas (B.19), (B.20), (B.70), (B.71), (B.72)
λ_{MD}	h^{-1}, FIT	Dangerous failure rate of the test channel M of a single-channel system; dangerous failure results in loss of the diagnostics function	Figures 3, B.2, B.3, B.6, B.11, B.12; Formulas (11), (13), (17), (18), (B.16), (B.17), (B.35), (B.47), (B.49), (B.54), (B.55)
$\lambda_{MD\ SER\text{-}free}$	h^{-1}, FIT	As λ_{MD}, but without the component caused by soft errors	Formulas (9), (B.48)
NOTE 1 FIT = 10^{-9} h^{-1}			

The significance of variables not listed in Table 1 is evident directly from the context.

4 Basic assumptions

Any modelling requires assumptions used by the model. The models discussed here, and their assumptions are adjusted specifically to the typical boundary conditions of machine control systems. The following basic assumptions generally apply throughout this document:

— Implementation of the safety functions with a logical series arrangement comprising discrete subsystems in which the *PFH* of each subsystem is calculated separately.

— Use of the following subsystem architectures:

  — Single-channel untested system (1oo1, designated architecture of categories B and 1);

  — Single-channel tested system (1oo1D, designated architecture of category 2);

  — Two-channel untested system (1oo2);

  — Two-channel tested system (1oo2D, designated architecture of categories 3 and 4).

— No redundancy for increasing of the availability.

— Demand rate upon the safety function $r_d \geq 1/a$. In terms of IEC 61508 this includes $r_d = 1/a$, high demand mode of operation and continuous mode of operation.

— In the case of diagnostics, test intervals not greater than the mission time.

NOTE 1 Setting the test interval of a channel to the mission time means one test at the end of the mission time which is equivalent to no diagnostics for that channel. Commonly test intervals greater than one year are not regarded as acceptable.

— Repair following detection of failure by diagnostics (automatic or manual as per specification).

— Repair following a hazardous event.

NOTE 2 In principle, consideration of the repair following a hazardous event also necessitates consideration of the demand upon the safety function. It is found however that the demand rate needs be considered during calculation of the *PFH* only in the case of certain 1oo1D applications.

— The reciprocals of the mean repair time (*MRT*) and the mean time to restoration (*MTTR*) are substantially greater than the dangerous channel failure rates.

— Where a proof test (not usual in the machinery sector) is implemented: setting of the mission time T_M to the length of the proof-test interval.

— Ignoring rates of failure to safety.

NOTE 3 This constitutes estimation on the safe side and permits simpler models and equations. It also prevents non-guaranteed failures to safety from causing a mathematical improvement in *PFH*.

— Real component behaviour is idealized.

— Constant failure rates of channels over time; it follows that the $MTTF_D$ (mean time to dangerous failure) is equal to the reciprocal of the dangerous failure rate ($MTTF_D = 1/\lambda_D$).

NOTE 4 The mission time of wearing parts is limited to T_{10D} (corresponding to B_{10D} working cycles). Use of a surrogate failure rate (substitute $MTTF_D$) assumed to be constant over time is thus justified as an acceptable approximation; see Clause 6 and Annex B.2.

— No systematic failures included in the PFH calculation.

NOTE 5 The *PFH* calculation addresses random hardware failures only. The important aspect of systematic failures is addressed by following the relevant requirements of ISO 13849-1.

— *PFH* is seen as the mean value over time of the frequency of the unmet demands upon the safety function (frequency of unsuccessful attempts, frequency of malfunction).

NOTE 6 The frequency of the unmet demands at worst is equal to the hazard rate. For high or continuous demand mode, i.e. the modes of operation addressed by this document, the hazard rate conforms with the unconditional failure intensity upon which the definition of the *PFH* in IEC 61508 is based.

NOTE 7 In conjunction with the potential scale of harm, this frequency is essential to the residual risk despite implementation of the safety function.

— Perfect repair, where applicable: perfect proof test.

NOTE 8 It is assumed that following repair, both function blocks are intact and have the original failure rate for the remaining mission time. In the context of the general assumption of constant failure rates over time, this means that a function block that has not failed at the time of repair need not necessarily be replaced, but only checked for its proper function.

5 Channels

5.1 General

In the block diagrams of the models described here, channels are shown as discrete function blocks. A distinction is drawn between functional channels and test channels.

5.2 Functional channel

A functional channel performs the safety function when required or continuously. In the two-channel tested systems described here (1oo2D), each functional channel also has the purpose of diagnostics of the other functional channel, either by performing the full diagnostics function, or by serving as a sensor or actuator in it.

NOTE Effective diagnostics requires both detection of the failure and performance of the predefined safety-oriented action.

Loss of the ability to perform the safety function or the test function is described as a dangerous failure of the functional channel. Use of a suitable system architecture can prevent the dangerous failure of a functional channel from leading to a dangerous system failure (loss of the safety function).

5.3 Test channel

A test channel tests, at certain times or continually, the ability of a functional channel to perform the safety function. Loss of this test function does not of itself lead to failure of the safety function. To obviate the need for an additional term, it is nevertheless described as dangerous failure of the test channel, since with regard to the test channel it constitutes the least favourable form of failure in safety terms.

5.4 Channel comprising elements connected logically in series

Functional channels and test channels often consist of elements arranged logically in series, as shown in Figure 1. A channel CH comprising n elements then suffers dangerous failure when at least one of its elements E_1 ... E_n fails dangerously.

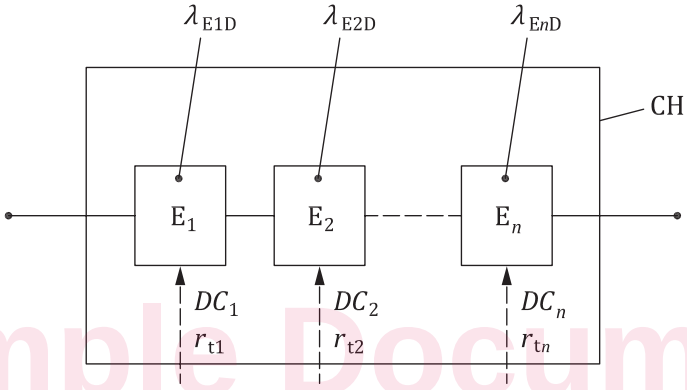

Figure 1 — Channel CH consisting of *n* elements

The dangerous failure rate of the channel can then be calculated by means of the equation:

$$\lambda_{CHD} = \lambda_{E1D} + \lambda_{E2D} + \ldots + \lambda_{EnD} \tag{1}$$

ISO 13849-1 uses the mean time to dangerous failure ($MTTF_D$) instead of the dangerous failure rate. ISO 13849-1 and this document assume all failure rates of single elements and complete channels to be constant over time. Therefore, the following applies for an element E_i or, respectively, for a channel CH:

$$MTTF_{D\,Ei} = \frac{1}{\lambda_{EiD}}, \quad MTTF_{D\,CH} = \frac{1}{\lambda_{CHD}} \tag{2}$$

and, conversely

$$\lambda_{EiD} = \frac{1}{MTTF_{D\,Ei}}, \quad \lambda_{CHD} = \frac{1}{MTTF_{D\,CH}} \tag{3}$$

Therefore, within ISO 13849-1, $MTTF_D$ can be regarded as a synonym of the reciprocal of the dangerous failure rate λ_D. Nevertheless, it is important to note that Formula (2) and Formula (3) are valid only in case of failure rates which are constant over time.

In a functional channel for which diagnostics is implemented, the diagnostics can differ between the individual elements. The diagnostic coverage of an element with a high failure rate then has a greater effect for the channel as a whole than the diagnostic coverage of an element with a low failure rate. The mean diagnostic coverage for the channel can therefore be computed as the sum of all weighted element diagnostic