



DPC: 25/30509445 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 14 March 2025

Origin: International

Latest date for receipt of comments: 07 May 2025

Project No. 2025/00341

Responsible committee: GEL/65/1 System considerations

Interested committees:

Title: Draft BS EN IEC 61508-6 Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see Functional Safety and IEC 61508).

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 07 May 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

PROJECT NUMBER: IEC 61508-6 ED3	
DATE OF CIRCULATION: 2025-03-14	CLOSING DATE FOR VOTING: 2025-06-06
SUPERSEDES DOCUMENTS: 65A/1061A/CD, 65A/1080B/CC	

IEC SC 65A : SYSTEM ASPECTS	
SECRETARIAT: United Kingdom	SECRETARY: Ms Stephanie Lavy
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 8,TC 9,TC 22,TC 31,TC 44,TC 45,TC 56,TC 61,TC 62,TC 65,SC 65B,SC 65C,SC 65E,TC 66,TC 77,TC 80,TC 108,SyC AAL,SyC SM,SC 41	HORIZONTAL FUNCTION(S):
ASPECTS CONCERNED: Safety	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING Attention IEC-CENELEC parallel voting The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE [AC/22/2007](#) OR [NEW GUIDANCE DOC](#)).

TITLE: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see Functional Safety and IEC 61508)

PROPOSED STABILITY DATE: 2027

NOTE FROM TC/SC OFFICERS: "Due to committee meetings planned at the end of May in Pisa, Italy, it is appreciated to voluntarily submit comments on this Part of the IEC 61508 series by 2025-05-12 already. Of course, there will be all comments accepted for consideration be the committee arriving within the official circulation period, but it will help the committee for starting their work on the project phase."

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
2 Normative references	11
3 Definitions and abbreviations.....	11
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3.....	12
A.1 General.....	12
A.2 Functional steps in the application of IEC 61508-2.....	14
A.3 Functional steps in the application of IEC 61508-3.....	17
A.4 Architecture considerations.....	19
A.4.1 Architecture Description Identification and Overview	20
A.4.2 Stakeholders and Concerns	20
Annex B (informative) Example of technique for evaluating probabilities of hardware failure.....	22
B.1 General.....	22
B.2 Considerations about basic probabilistic calculations	23
B.2.1 Introduction	23
B.2.2 Low demand E/E/PE safety-related system.....	23
B.2.3 Continuous or high demand mode E/E/PE safety-related system	24
B.3 Methods of calculating PFD or PFH of a system.....	25
B.3.1 Other available guidance	25
B.3.2 Reliability block diagram approach, assuming constant failure rate	26
B.3.3 Average frequency of dangerous failure (for high demand or continuous mode of operation)	45
B.4 Determination of SILs for E/E/PE Safety-Related Systems with (a) Common Functional Element(s).....	56
B.4.1 Necessity of multiple protection layers (Multi-PLs).....	56
B.4.2 Redundant channels (CHs) and multi-PLs.....	57
B.4.3 Classification of independency between (E/E/PE) safety-related systems	59
B.4.4 Illustrative example of multi-PLs with common FEs classified into Case 2-2.....	59
B.5 Safety integrity and modes of operation of the systems with analytical complexity	63
B.6 Handling uncertainties	63
B.7 References	64
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction – worked example	65
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems	69
D.1 General.....	69
D.1.1 Introduction	69
D.1.2 Brief overview.....	69
D.1.3 Defence against common cause failures	70
D.1.4 Approach adopted in the IEC 61508 series	71
D.2 Scope of the methodology.....	71

49	D.3	Points taken into account in the methodology	73
50	D.4	Using the β -factor to calculate the probability of failure in an E/E/PE safety- related system due to common cause failures	74
51			
52	D.5	Redundancy at system level estimate of β	75
53	D.6	Redundancy at PCB device level estimation of β	78
54	D.7	Estimation of β suitable for complex semiconductor	80
55	D.8	casecasecasecasecaseCaseCaseBinomial failure rate (Shock model) – CCF approach	81
56			
57	D.9	References	83
58	Annex E (informative)	Example applications of systematic capability tables of IEC 61508-3	84
59			
60	E.1	General.....	84
61	E.2	Example for safety integrity level 2	84
62	E.3	Example for safety integrity level 3	91
63	Annex F Annex F (informative)	Examples on how to include failures of the diagnostic function in the PFH / PFD _{AVG} calculation	101
64			
65	F.1	Possible approach A	101
66	F.2	Possible approach B	102
67	F.3	Possible approach C	104
68	Annex G (informative)	Failure rate estimation from field feedback, with confidence intervals	107
69			
70	G.1	Introduction.....	107
71	G.2	Assumptions for data collection.....	107
72	G.3	Assumptions and notations for parameters estimation.....	108
73	G.4	Failure rate estimation for detected failures	108
74	G.5	Failure rate estimation for undetected failures.....	109
75	G.6	Examples of failure rates estimation with upper confidence bound	111
76	Annex H	Guidance for robust safety architecture.	113
77	Bibliography		116
78			
79	Figure A.1	– Application of IEC 61508-2	16
80	Figure A.2	– Application of IEC 61508-2 (Figure A.1 <i>continued</i>).....	17
81	Figure A.3	– Application of IEC 61508-3	19
82	Figure B.1	– Reliability Block Diagram of a whole safety loop	23
83	Figure B.2	– Example configuration for two sensor channels.....	28
84	Figure B.3	– Subsystem structure	29
85	Figure B.4	– 1oo1 physical block diagram.....	31
86	Figure B.5	– 1oo1 reliability block diagram.....	31
87	Figure B.6	– 1oo2 physical block diagram	32
88	Figure B.7	– 1oo2 reliability block diagram.....	32
89	Figure B.8	– 2oo2 physical block diagram.....	33
90	Figure B.9	– 2oo2 reliability block diagram.....	33
91	Figure B.10	– 1oo2D physical block diagram.....	34
92	Figure B.11	– 1oo2D reliability block diagram	34
93	Figure B.12	– – 2oo3 physical block diagram	35
94	Figure B.13	– 2oo3 reliability block diagram.....	36
95	Figure B.14	– – Systems block diagram of biped nursing robot	37

96	Figure B.15 – – Hazardous event described by FT of multi-PLs	58
97	Figure B.16 – – Hazardous event described by FT of multi-CHs system.....	58
98	Figure B.17 – – Reliability block diagrams of typical multi-PLs to control a collision risk	
99	by biped nursing robot	60
100	Figure D.1 – Relationship of common cause failures to the failures of individual	
101	channels	71
102	Figure D.2 – Implementing shock model with fault trees.....	82
103		
104	Table B.1 – Terms used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and	
105	2oo3)	28
106	Table B.9 – Example for a non-perfect proof test	45
107	Table C.1 – Example calculations for diagnostic coverage and safe failure fraction	66
108	Table C.2 – Diagnostic coverage and effectiveness for different elements	67
109	Table D.1 – Scoring sensors/final elements	75
110	Table D.2 – Scoring Logic Subsystems	76
111	Table D.3 – Calculation of β_{DU} and β_{DD}	77
112	Table D.4 – Calculation of β for systems with levels of redundancy greater than 1oo2	78
113	Table D.5 – Example of a common cause failure analysis	79
114	Table D.6 – Additional Modifier	80
115	Table D.7 – Estimation of attributes of β -value.....	80
116	Table D.8 – Measures to quantify a β -factor.....	81
117	Table E.1 – Software safety requirements specification	85
118	Table E.2 – Software design and development – software architecture design	85
119	Table E.3 – Software design and development – support tools and programming	
120	language	87
121	Table E.4 – Software design and development – detailed design	87
122	Table E.5 – Software design and development – software module testing and	
123	integration	88
124	Table E.6 – Programmable electronics integration (hardware and software)	89
125	Table E.7 – Software aspects of system safety validation	89
126	Table E.8 – Software modification	90
127	Table E.9 – Software verification	90
128	Table E.10 – Functional safety assessment	91
129	Table E.11 – Software safety requirements specification	92
130	Table E.12 – Software design and development – software architecture design	92
131	Table E.13 – Software design and development – support tools and programming	
132	language	94
133	Table E.14 – Software design and development – detailed design	94
134	Table E.15 – Software design and development – software module testing and	
135	integration	96
136	Table E.16 – Programmable electronics integration (hardware and software)	97
137	Table E.17 – Software aspects of system safety validation	97
138	Table E.18 – Modification	98
139	Table E.19 – Software verification	99
140	Table E.20 – Software life cycle through lifecycle activities.....	99

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/
PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –****Part 6: Guidelines on the application
of IEC 61508-2 and IEC 61508-3**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC 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, IEC 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 <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61508-6 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement, control and automation.

This third edition cancels and replaces the second edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition (the following list does refer to this document; other parts do mention specific further details):

- a) Document was upgraded to the 2024 version of the ISO/IEC Directives; this does introduce a significant number of editorial changes, clause renumbering and rewording of the information provided in Notes;

- b) The following new Annexes have been created:
- i) Annex F gives examples on how to include failures of the diagnostic function in the calculation of the safety parameters;
 - ii) Annex G gives guidance on failure rate estimation from field feedback with confidence intervals.
 - iii) Annex H gives guidance on robust safety architecture.
- c) New common cause method on redundancy at PCB device level estimation of β (D.6) and for estimation of β suitable for complex semiconductor (D.7) has been added;
- d) Examples from TR 12489 have been included (Annex B).
- e) Corrections and explanations have been made related to formulas and their applicability.
- f) Various minor editorial errors have been corrected, the normative references and the bibliography has been updated.

The text of this document is based on the following documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this document is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts of the IEC 61508 series, published under the general title *Functional safety of electrical / electronic / programmable electronic safety-related systems*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
 - withdrawn,
 - replaced by a revised edition, or
 - amended.

INTRODUCTION

Systems comprised of electrical and/or electronic elements have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions.

This document sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of product and application sector documents based on the IEC 61508 series.

In most situations, safety is achieved by a number of systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy should therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this document is concerned with E/E/PE safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of applications using E/E/PE safety-related systems in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the required safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such measures to be formulated in future product and application sector documents and in revisions of those that already exist.

This document

- considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE systems are used to perform safety functions;
- has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
- enables product and application sector documents, dealing with E/E/PE safety-related systems, to be developed; the development of product and application sector documents, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;
- provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
- adopts a risk-based approach by which the safety integrity requirements can be determined;
- introduces safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

NOTE 1 The standard does not specify the safety integrity level requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in

- a low demand mode of operation, the lower limit is set at an average probability of a dangerous failure on demand of 10^{-5} ;
- a high demand or a continuous mode of operation, the lower limit is set at an average frequency of a dangerous failure of 10^{-9} [h⁻¹];

NOTE 2 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 3 It can be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe. However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

1 Scope

1.1 This part of IEC 61508 contains information and guidelines on IEC 61508-2 and IEC 61508-3.

- Annex A gives a brief overview of the requirements of IEC 61508-2 and IEC 61508-3 and sets out the functional steps in their application.
- Annex B gives an example technique for calculating the probabilities of hardware failure and should be read in conjunction with 7.4.3 and Annex C of IEC 61508-2 and Annex D.
- Annex C gives a worked example of calculating diagnostic coverage and should be read in conjunction with Annex C of IEC 61508-2.
- Annex D gives a methodology for quantifying the effect of hardware-related common cause failures on the probability of failure.
- Annex E gives worked examples of the application of the systematic capability tables specified in Annex A of IEC 61508-3 for safety integrity levels 2 and 3.
- Annex F gives examples on how to include failures of the diagnostic function in the calculation of the safety parameters.
- Annex G gives guidance on how to estimate the failure rates from field feedback with confidence intervals and specifically in the context of compliance with route 2H requirements in 7.4.4.3.3 of IEC 61508-2 or route 2S requirements as stated in 7.4.9.5 of IEC 61508-2.
- Annex H gives guidance on robust safety architecture.

1.2 IEC 61508-1, IEC 61598-2, IEC 61508-3 and IEC 61508-4 are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.3 of IEC 61508-4). This document provides further information to complement these basic safety publications.

1.3 One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

1.4 Figure 1 shows the overall framework of the IEC 61508 series and indicates the role that IEC 61508-6 plays in the achievement of functional safety for E/E/PE safety-related systems.

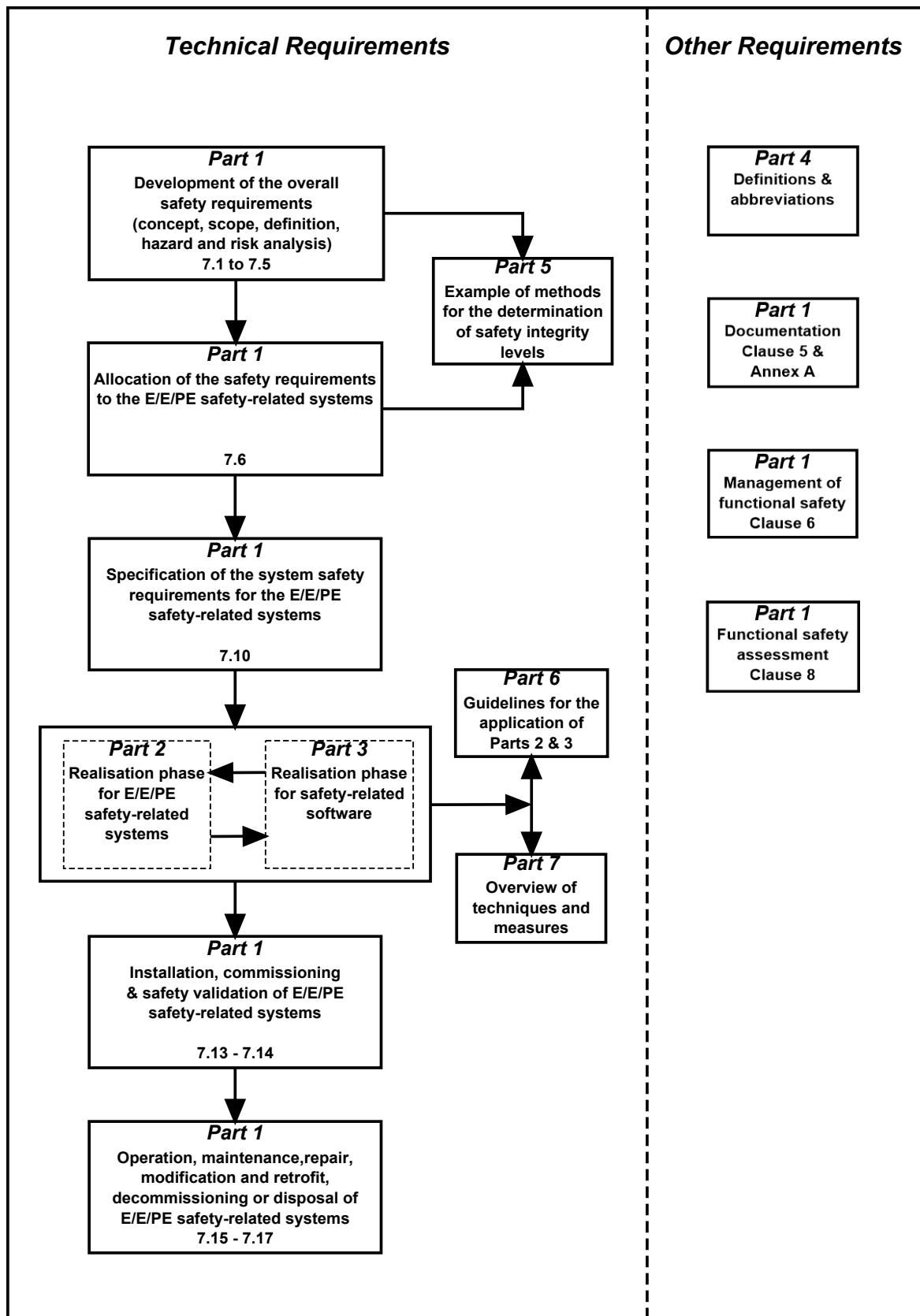


Figure 1 – Overall framework of the IEC 61508 series

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.

IEC 61508-2:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:202X, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

3 Definitions and abbreviations

For the purposes of this document, the definitions and abbreviations given in IEC 61508-4 apply.

Annex A (informative)

Application of IEC 61508-2 and of IEC 61508-3

A.1 General

Machinery, process plant and other equipment may, in the case of malfunction (for example by failures of electrical, electronic and/or programmable electronic devices), present risks to people and the environment from hazardous events such as fires, explosions, radiation overdoses, machinery traps, etc. Failures can arise from either physical faults in the device (for example causing random hardware failures), or from systematic faults (for example human errors made in the specification and design of a system cause systematic failure under some particular combination of inputs), or from some environmental condition.

IEC 61508-1 provides an overall framework based on a risk approach for the prevention and/or control of failures in electro-mechanical, electronic, or programmable electronic devices.

The overall goal is to ensure that plant and equipment can be safely automated. A key objective of this standard is to prevent:

- failures of control systems triggering other events, which in turn could lead to danger (for example fire, release of toxic materials, repeat stroke of a machine, etc.); and
- undetected failures in protection systems (for example in an emergency shut-down system), making the systems unavailable when needed for a safety action.

IEC 61508-1 requires that a hazard and risk analysis at the process/machine level is carried out to determine the amount of risk reduction necessary to meet the risk criteria for the application. Risk is based on the assessment of both the consequence (or severity) and the frequency (or probability) of the hazardous event.

IEC 61508-1 further requires that the amount of risk reduction established by the risk analysis is used to determine if one or more safety-related systems¹ are required and what safety functions (each with a specified safety integrity)² they are needed for.

IEC 61508-2 and IEC 61508-3 take the safety functions and safety integrity requirements allocated to any system, designated as a E/E/PE safety-related system, by the application of IEC 61508-1 and establish requirements for safety lifecycle activities which:

- should be applied during the specification, design and modification of the hardware and software; and
- focus on means for preventing and/or controlling random hardware and systematic failures (the E/E/PE system and software safety lifecycles)³.

IEC 61508-2 and IEC 61508-3 do not give guidance on which level of safety integrity is appropriate for a given required tolerable risk. This decision depends upon many factors,

¹ Systems necessary for functional safety and containing one or more electrical (electro-mechanical), electronic or programmable electronic (E/E/PE) devices are *designated* as E/E/PE safety-related systems and include all equipment necessary to carry out the required safety function (see 3.5.1 of IEC 61508-4).

² Safety integrity is specified as one of four discrete levels. Safety integrity level 4 is the highest and safety integrity level 1 the lowest (see 3.5.4 and 3.5.8 of IEC 61508-4).

³ To enable the requirements of this standard to be clearly structured, a decision was made to order the requirements using a development process model in which each stage follows in a defined order with little iteration (sometimes referred to as a waterfall model). However, it is stressed that any lifecycle approach can be used provided a statement of equivalence is given in the safety plan for the project (see Clause 7 of IEC 61508-4).

including the nature of the application, the extent to which other systems carry out safety functions and social and economic factors (see IEC 61508-1 and IEC 61508-5).

The requirements of IEC 61508-2 and IEC 61508-3 include:

- the application of measures and techniques⁴, which are graded against the safety integrity level, for the avoidance of systematic failures⁵ by preventative methods; and
- the control of systematic failures (including software failures) and random hardware failures by design features such as fault detection, redundancy and architectural features (for example diversity).

In IEC 61508-2, assurance that the safety integrity target has been satisfied for dangerous random hardware failures is based on:

- hardware fault tolerance requirements (see Tables 2 and 3 of IEC 61508-2); and
- the diagnostic coverage and frequency of proof tests of subsystems and components, by carrying out a reliability analysis using appropriate data.

In both IEC 61508-2 and IEC 61508-3, assurance that the safety integrity target has been satisfied for systematic failures is gained by:

- the correct application of safety management procedures;
- the use of competent staff;
- the application of the specified safety lifecycle activities, including the specified techniques and measures⁶; and
- an independent functional safety assessment⁷.

The overall goal is to ensure that remaining systematic faults, commensurate with the safety integrity level, do not cause a failure of the E/E/PE safety-related system.

IEC 61508-2 has been developed to provide requirements for achieving safety integrity in the hardware of the E/E/PE safety-related systems including sensors and final elements. Techniques and measures against both random hardware failures and systematic hardware failures are required. These involve an appropriate combination of fault avoidance and failure control measures as indicated above. Where manual action is needed for functional safety, requirements are given for the operator interface. Also diagnostic test techniques and measures, based on software and hardware (for example diversity), to detect random hardware failures are specified in IEC 61508-2.

IEC 61508-3 has been developed to provide requirements for achieving systematic capability for the software – both embedded (including diagnostic fault detection services) and application software. IEC 61508-3⁸ requires a combination of fault avoidance (quality assurance) and fault tolerance approaches (software architecture), as there is no known way to prove the absence of faults in reasonably complex safety-related software, especially the absence of specification and design faults. IEC 61508-3 requires the adoption of such software engineering principles as: top down design; modularity; verification of each phase of the development lifecycle; verified software modules and software module libraries; and clear documentation to facilitate

⁴ The required techniques and measures for each safety integrity level are shown in the tables in Annexes A and B of IEC 61508-2 and IEC 61508-3.

⁵ Systematic failures cannot usually be quantified. Causes include: specification and design faults in hardware and software; failure to take account of the environment (for example temperature); and operation-related faults (for example poor interface).

⁶ Alternative measures to those specified in the standard are acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

⁷ Independent assessment does not always imply third party assessment (see Clause 8 of IEC 61508-1).

⁸ Including fixed built-in software.

verification and validation. The different levels of software require different levels of assurance that these and related principles have been correctly applied.

The developer of the software may or may not be separate from the organization developing the whole E/E/PE system. In either case, close cooperation is needed, particularly in developing the architecture of the programmable electronics where trade-offs between hardware and software architectures need to be considered for their safety impact (see Figure 4 of IEC 61508-2).

A.2 Functional steps in the application of IEC 61508-2

The functional steps in the application of IEC 61508-2 are shown in Figures A.1 and A.2. The functional steps in the application of IEC 61508-3 are shown in Figure A.3.

Functional steps for IEC 61508-2 (see Figures A.1 and A.2) are as follows:

- a) Obtain the allocation of safety requirements (see IEC 61508-1). Update the safety planning as appropriate during E/E/PE safety-related system development.
- b) Determine the requirements for E/E/PE safety-related systems, including the safety integrity requirements, for each safety function (see 7.2 of IEC 61508-2). Allocate requirements to software and pass to software supplier and/or developer for the application of IEC 61508-3.

NOTE 1 The possibility of coincident failures in the EUC control system and E/E/PE safety-related system(s) needs to be considered at this stage (see A.5.4 of IEC 61508-5). These can result from failures of components having a common cause due to for example similar environmental influences. The existence of such failures can lead to a higher than expected residual risk unless properly addressed.

- c) Start the phase of planning for E/E/PE safety-related system safety validation (see 7.3 of IEC 61508-2).
- d) Specify the architecture (configuration) for the E/E/PE safety-related logic subsystem, sensors and final elements. Review with the software supplier/developer the hardware and software architecture and the safety implications of the trade-offs between the hardware and software (see Figure 4 of IEC 61508-2). Iterate if required.
- e) Develop a model for the hardware architecture for the E/E/PE safety-related system. Develop this model by examining each safety function separately and determine the subsystem (component) to be used to carry out this function.
- f) Establish the system parameters for each of the subsystems (components) used in the E/E/PE safety-related system. For each of the subsystems (elements), determine the following:
 - the proof test interval for failures which are not automatically revealed;
 - the mean time to restoration;
 - the diagnostic coverage (see Annex C of IEC 61508-2);
 - the probability of failure;
 - the required architectural constraints; for Route 1_H see 7.4.4.2 and Annex C of IEC 61508-2 and for Route 2_H see 7.4.4.3 of IEC 61508-2.

- g) Create a reliability model for each of the safety functions that the E/E/PE safety-related system is required to carry out.

NOTE 2 A reliability model is a mathematical formula which shows the relationship between reliability and relevant parameters relating to equipment and conditions of use.

- h) Calculate a reliability prediction for each safety function using an appropriate technique. Compare the result with the target failure measure determined in b) above and the requirements of Route 1_H (see 7.4.4.2 of IEC 61508-2) or Route 2_H (see 7.4.4.3 of IEC 61508-2). If the predicted reliability does not meet the target failure measure and/or does not meet the requirements of Route 1_H or Route 2_H, then change
 - where possible, one or more of the subsystem parameters (go back to f) above), and/or

– the hardware architecture (go back to d) above).

NOTE 3 A number of modelling methods are available and the analyst should choose which is the most appropriate (see Annex B for guidance on some methods that could be used).

- i) Implement the design of the E/E/PE safety-related system. Select measures and techniques to control systematic hardware failures, failures caused by environmental influences and operational failures (see Annex A of IEC 61508-2).
- j) Integrate the verified software (see IEC 61508-3) onto the target hardware (see 7.5 of IEC 61508-2 and Annex B of IEC 61508-2) and, in parallel, develop the procedures for users and maintenance staff to follow when operating the system (see 7.6 of IEC 61508-2 and Annex B of IEC 61508-2). Include software aspects (see A.3 f)).
- k) Together with the software developer (see 7.7 of IEC 61508-3), validate the E/E/PE system (see 7.7 of IEC 61508-2 and Annex B of IEC 61508-2).
- l) Hand over the hardware and results of the E/E/PE safety-related system safety validation to the system engineers for further integration into the overall system.
- m) If maintenance/modification of the E/E/PE safety related system is required during operational life then re-activate IEC 61508-2 as appropriate (see 7.8 of IEC 61508-2).

A number of activities run across the E/E/PE safety related system safety lifecycle. These include verification (see 7.9 of IEC 61508-2) and functional safety assessment (see Clause 8 of IEC 61508-1).

In applying the above steps the E/E/PE safety related system safety techniques and measures appropriate to the required safety integrity level are selected. To aid in this selection, tables have been formulated, ranking the various techniques/measures against the four safety integrity levels (see Annex B of IEC 61508-2). Cross-referenced to the tables is an overview of each technique and measure with references to further sources of information (see Annexes A and B of IEC 61508-7).

Annex B provides one possible technique for calculating the probabilities of hardware failure for E/E/PE safety-related systems.

NOTE 4 In applying the above steps, alternative measures to those specified in the standard can be acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

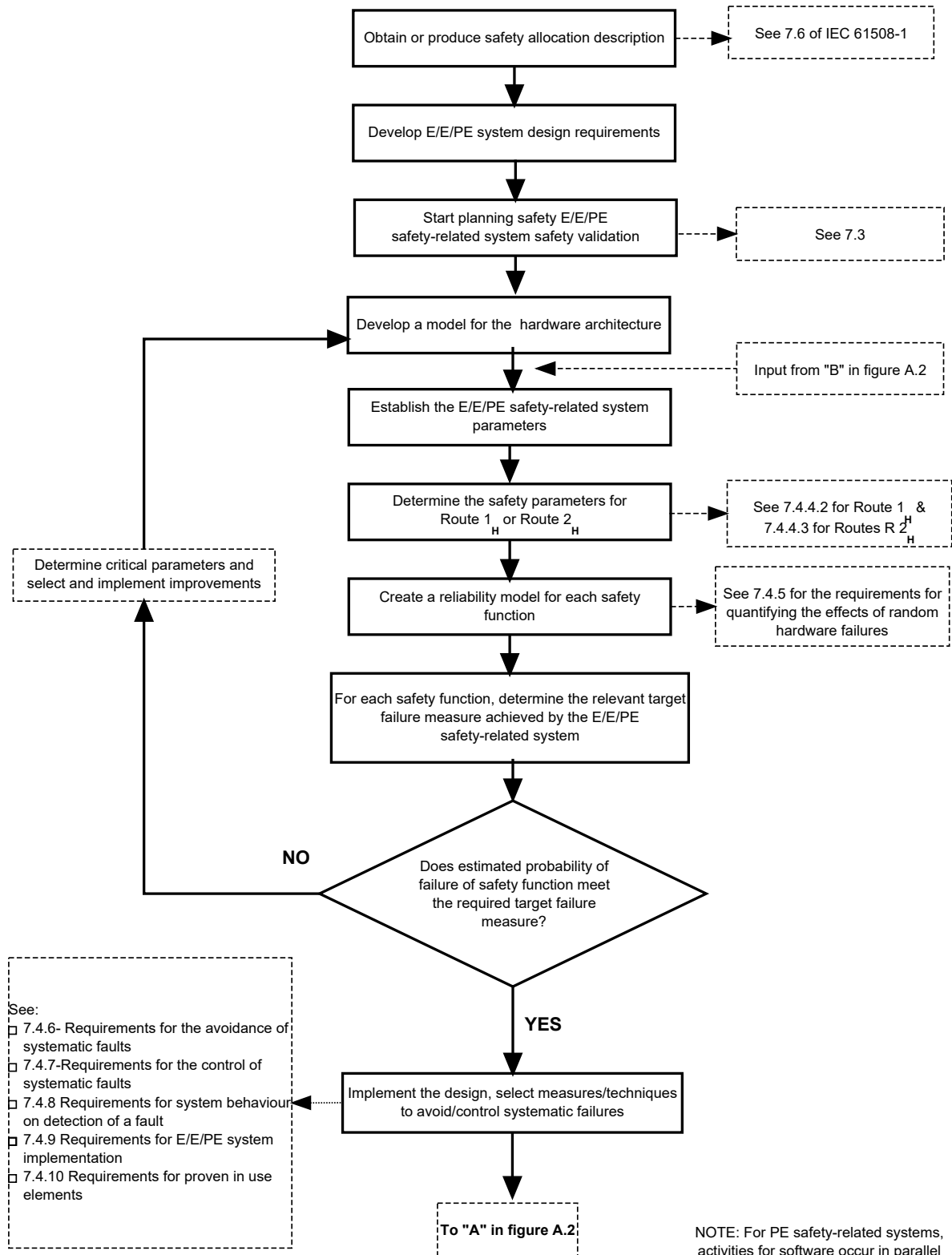
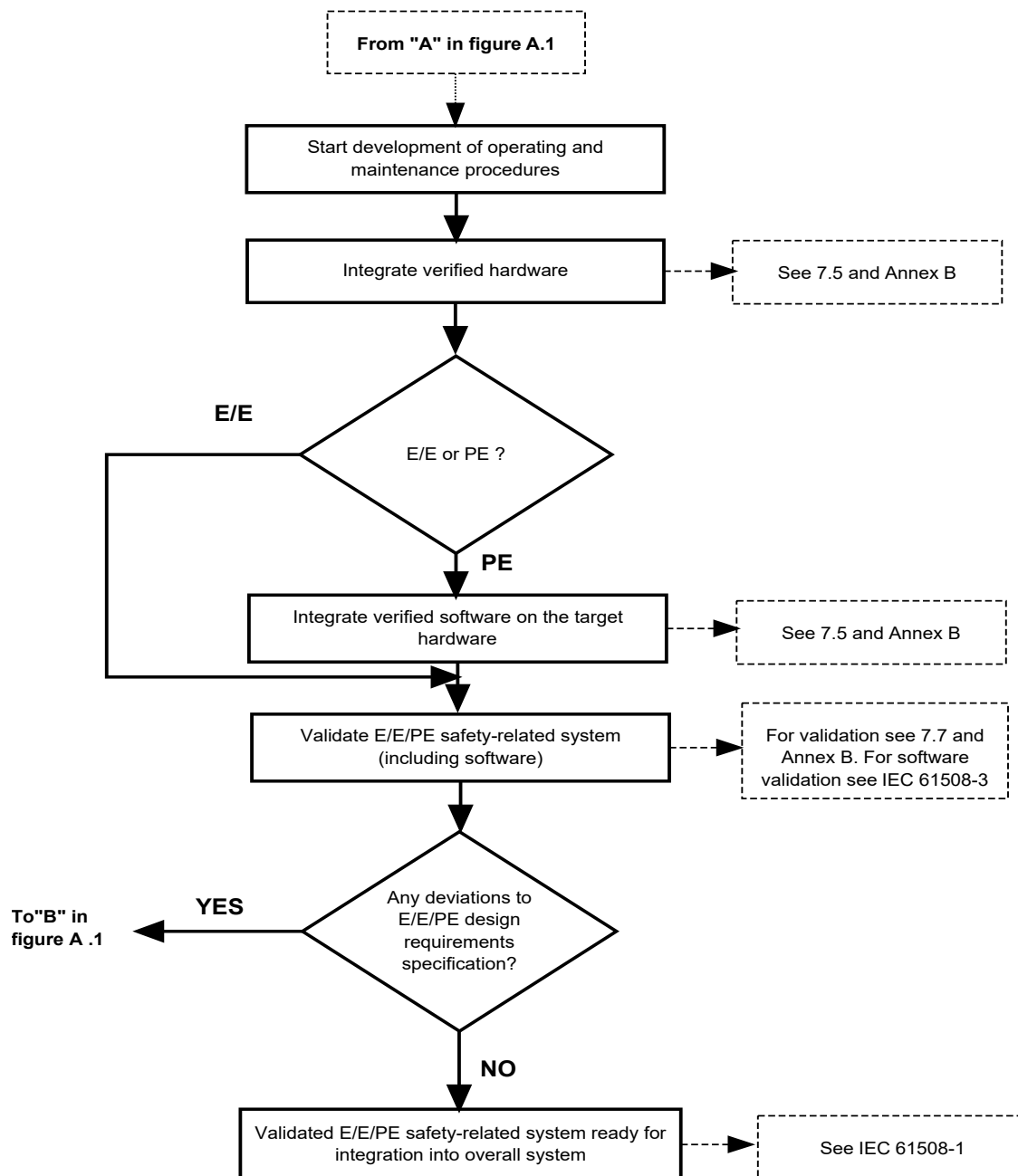


Figure A.1 – Application of IEC 61508-2



NOTE: For PE safety-related systems, activities for software occur in parallel (see figure A.3).

Figure A.2 – Application of IEC 61508-2 (Figure A.1 continued)

A.3 Functional steps in the application of IEC 61508-3

Functional steps for IEC 61508-3 (see Figure A.3) are as follows.

- a) Obtain the requirements for the E/E/PE safety-related systems and relevant parts of the safety planning (see 7.3 of IEC 61508-2). Update the safety planning as appropriate during software development.

NOTE 1 Earlier lifecycle phases can have already:

- specified the required safety functions and their associated safety integrity levels (see 7.4 and 7.5 of IEC 61508-1);
 - allocated the safety functions to designated E/E/PE safety-related systems (see 7.6 of IEC 61508-1); and
 - allocated functions to software within each E/E/PE safety-related system (see 7.2 of IEC 61508-2).
- b) Determine the software architecture for all safety functions allocated to software (see 7.4 of IEC 61508-3 and Annex A of IEC 61508-3).
- c) Review with the E/E/PE safety-related system's supplier/developer, the software and hardware architecture and the safety implications of the trade-offs between the software and hardware (see Figure 4 of IEC 61508-2). Iterate if required.
- d) Start the planning for software safety verification and validation (see 7.3 and 7.9 of IEC 61508-3).
- e) Design, develop and verify/test the software according to the:
- software safety planning;
 - systematic capability; and
 - software safety lifecycle.
- f) Complete the final software verification activity and integrate the verified software onto the target hardware (see 7.5 of IEC 61508-3), and in parallel develop the software aspects of the procedures for users and maintenance staff to follow when operating the system (see 7.6 of IEC 61508-3, and A.2 k)).
- g) Together with the hardware developer (see 7.7 of IEC 61508-2), validate the software in the integrated E/E/PE safety-related systems (see 7.7 of IEC 61508-3).
- h) Hand over the results of the software safety validation to the system engineers for further integration into the overall system.
- i) If modification of the E/E/PE safety-related system software is required during operational life then re-activate this IEC 61508-3 phase as appropriate (see 7.8 of IEC 61508-3).

A number of activities run across the software safety lifecycle. These include verification (see 7.9 of IEC 61508-3) and functional safety assessment (see Clause 8 of IEC 61508-3).

In applying the above steps, software safety techniques and measures appropriate to the required safety integrity are selected. To aid in this selection, tables have been formulated ranking the various techniques/measures against the four safety integrity levels (see Annex A of IEC 61508-3). Cross-referenced to the tables is an overview of each technique and measure with references to further sources of information (see Annex C of IEC 61508-7).

Worked examples in the application of the systematic capability tables are given in Annex E, and IEC 61508-7 includes a probabilistic approach to determining software safety integrity for pre-developed software (see Annex D of IEC 61508-7).

NOTE 2 In applying the above steps, alternative measures to those specified in the standard can be acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

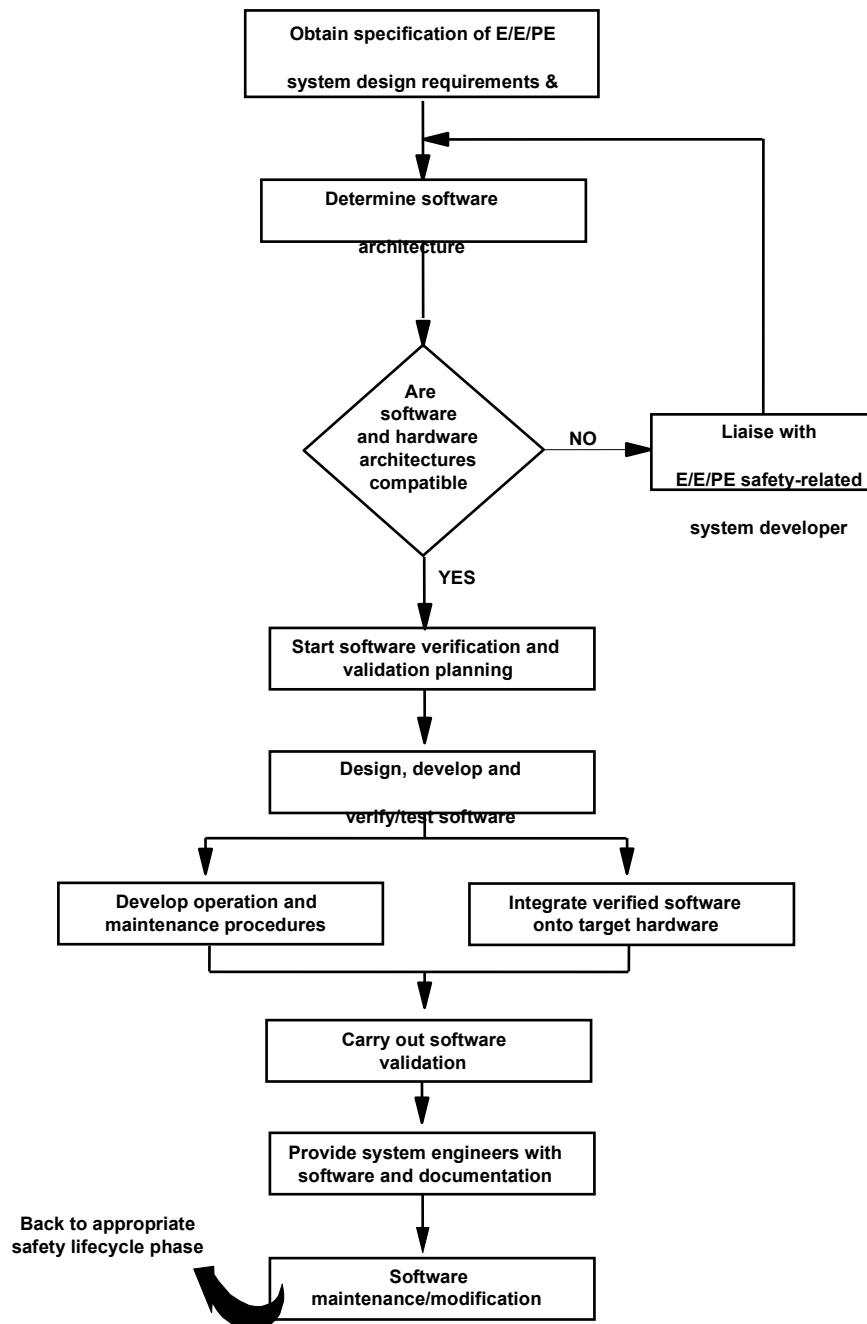


Figure A.3 – Application of IEC 61508-3

A.4 Architecture considerations

Clause A.2 identifies two steps concerning architecture specification and modelling in bullets d) and e).

The following guidance provides information about the content and the formalisation of architecture descriptions on a general level. It is derived from requirements of IEC/ISO 15288 [28] and ISO/IEC 42010 [40].

Similar considerations can be applied to software architectures (see Clause A.3 bullet b).

A.4.1 Architecture Description Identification and Overview

- An Architecture Description identifies the E/EPE safety related system whose architecture is being expressed.
- When an E/E/PE safety related system is designed to implement one or more E/E/PE safety related functions, the Architecture Description includes all elements implementing all the concerned E/E/PE safety related functions.
- An Architecture Description includes supplementary information as determined by the project or organisation producing it.

Examples of this information might be: authors, reviewers, approving authority, issuing organization; change history; configuration management information; context; date of issue and status; glossary; overview; references; scope; summary; and version control information.

- An Architecture Description includes the results of any architecture evaluations conducted on this architecture. This is the analysed alternative architectures and the rationale for the choice of the specified and implemented one.

An example is the rationale for the choice of connecting sensing elements on different logic solvers than the one performing the logic of concerned E/E/PE safety related function.

A.4.2 Stakeholders and Concerns

- An Architecture Description identifies the stakeholders of the system whose concerns are considered fundamental to the architecture (i.e., "architecturally significant"). E.g. in process industries architectures have to answer the double concern of industrial safety and Occupational Health and Safety which leads to the presence of emergency push-buttons.

When identifying stakeholders, the following can usefully be considered and included when applicable: users of the system; operators of the system; acquirers of the system; owners of the system; suppliers of the system; developers of the system; builders of the system; maintainers of the system.

- An Architecture Description identifies the concerns considered fundamental to the architecture of the system.

When identifying concerns, the following can usefully be considered and included when applicable: the purposes of the system; the suitability of the architecture for achieving the system's purposes; the feasibility of constructing and deploying the system; the potential risks and impacts of the system to its stakeholders throughout its life cycle; maintainability and evolvability of the system.

- An Architecture Description associates each identified concern with the identified stakeholders having that concern. E.g. it is clearly known why a pushbutton is present in an automatic function.

A.4.3 Architecture Views in an Architecture Description

- An Architecture Description includes each architecture viewpoint used therein.
- Each identified concern should be framed by at least one viewpoint. This is so that all identified concerns are covered.

"A viewpoint **frames** a concern" when the viewpoint gives the architect the means to express that concern. e.g., the formalism of control graphs and bond graphs frames concerns about software structure and dependencies, ~~whereas other notations, such as UML use case diagrams, would less be helpful for modelling these concerns.~~ Associating concerns with viewpoints contributes to architects "using the right tool for the job" when modelling the architecture.

- Each architecture viewpoint is specified by:

- the concerns framed by this viewpoint;
- the stakeholders interested in this viewpoint;

- the *model kinds* used in this viewpoint;

A **model kind** captures conventions for a type of modelling. To adequate frame a set of concerns, a viewpoint can use one or more model kinds. E.g. sequence function charts and block diagrams are conventions adapted to different concerns.

- For each model kind that is part of the viewpoint, the languages, notations, conventions, modelling techniques, analytical methods and/or other operations useful on models of this kind;

- References to sources on this viewpoint in the literature or previous work.

In addition, a viewpoint might define any of the following to aid the architect:

- Correspondence rules, criteria and methods for checking completeness (of views) or consistency (between views). This is a very important aspect for Functional Safety Assessment;

- Methods for evaluation or analysis of views;

- Methods, heuristics, metrics, patterns, design rules or guidelines, best practices and examples to aid in view creation and synthesis.

- An Architecture Description includes exactly one architecture view for each architecture viewpoint used.

- Each architecture view adheres to the conventions specified by its governing viewpoint.

- Each architecture view includes:

- identifying and supplementary information as specified by the organisation and/or project;

- identification of its governing viewpoint;

- one or more architecture models that address all of the concerns framed by its governing viewpoint; and cover the whole system from that viewpoint. Each model:

- includes version identification as specified by the organization or project;
 - identifies its governing model kind and adheres to the conventions of that model kind;
 - may be a part of more than one architecture view.

- a record of any known issues within a view with respect to its governing viewpoint. (Such as unresolved issues, known conflicts, etc.)

As an example an “architecture functional view” can show the hierarchized organisation of the safety functions down to the element safety functions.

Annex B (informative)

Example of technique for evaluating probabilities of hardware failure

B.1 General

This annex provides possible techniques for calculating the probabilities of hardware failure for E/E/PE safety-related systems installed in accordance with IEC 61508-1, IEC 61508-2 and IEC 61508-3. The information provided is informative in nature and should not be interpreted as the only evaluation techniques that might be used. It does, however, provide both a relatively simple approach for assessing the capability of E/E/PE safety-related systems and guidelines to use alternative techniques derived from the classical reliability calculations techniques. This Annex does not provide any guidance on meeting Architectural Constraints.

NOTE 1 System architectures stated in this part are provided by way of examples and cannot be considered exhaustive as there are many other architectures that may be used.

NOTE 2 See ISA-TR84.00.02-2002 [17] in the Bibliography.

A number of reliability techniques are more or less straightforwardly usable for the analysis of hardware safety integrity of E/E/PE safety-related systems. Classically, they are sorted according to the two following point of views:

- static (Boolean) versus dynamic (states/transition) models;
- analytical versus Monte Carlo simulation calculations.

Boolean models encompass all models describing the static logical links between the elementary failures and the whole system failure. Reliability Block Diagrams (RBD) (see C.6.4 of IEC 61508-7 IEC 6 and Fault Trees (FT) (see B.6.5.5 and B.6.5.9 of IEC 61508-7) IEC 6 belong to Boolean models.

States/transitions models encompass all models describing how the system behaves (jumps from states to states) according to arising events (failures, repairs, tests, etc.). Markovian (see B.6.5.6 of IEC 61508-7 IEC 6), Petri nets (see B.6.5.10 of IEC 61508-7 IEC 6) and formal language models belong to states/transitions models. Monte Carlo simulations can be used (see B.6.5.8 of IEC 61508-7).

All these methods can be used for the majority of safety related systems and, when deciding which technique to use on any particular application, it is very important that the user of a particular technique is competent in using the technique and this may be more important than the technique which is actually used. It is the responsibility of the analyst to verify that the underlying hypotheses of any particular method are satisfied, or any adjustments are required to obtain an adequate realistic conservative result. In case of poor reliability data or dominant common cause failure, it may be sufficient to use the simplest model / techniques. Whether the loss of accuracy is significant can only be determined in the particular circumstances. See Part 3, H.3.1 Tool usage and qualification planning.

If software programmes are used to perform the calculations then the practitioner should have an understanding of the formulae/techniques used by the software package to ensure its use is suitable for the specific application, and IEC 61508-6. The practitioner should also verify the software package by checking its output with some manual calculated test cases.

Where a failure of the EUC control system places a demand on the E/E/PE safety-related system, then the probability of a hazardous event occurring also depends on the probability of failure of the EUC control system. In that situation, it is necessary to consider the possibility of co-incident failure of components in the EUC control system and the E/E/PE safety-related system due to common cause failure mechanisms. The existence of such failures could lead to a higher than expected residual risk unless properly addressed.

B.2 Considerations about basic probabilistic calculations

B.2.1 Introduction

The reliability block diagram (RBD) on Figure B.1 is representing a safety loop made of three sensors (A, B, C), one logic solver (D), two final elements (E, F), and common cause failures (CCF).

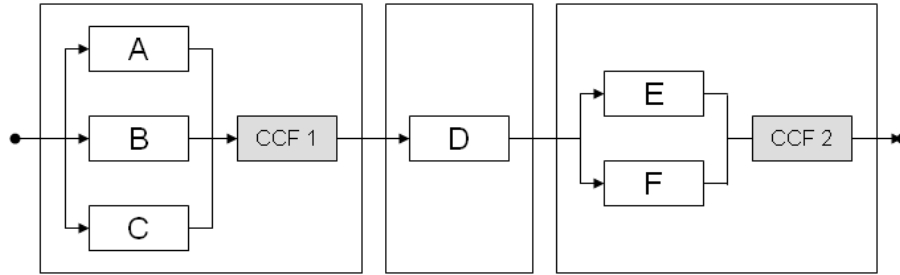


Figure B.1 – Reliability Block Diagram of a whole safety loop

This facilitates the identification of five failure combinations leading to the E/E/PE safety-related system failure. Each of them is a so-called minimal cut set:

- (A, B, C) is a triple failure;
- (E, F) is a double failure;
- (D) (CCF1) (CCF2) are single failures.

B.2.2 Low demand E/E/PE safety-related system

When a E/E/PE safety-related system is used in low demand mode, the standard requires that its PFD_{avg} (i.e. its average unavailability) be assessed. This is simply the ratio $MDT(T)/T$ where $MDT(T)$ is the mean down time over the period $[0, T]$ of the E/E/PE safety-related system.

For safety systems the probability of failure is, normally, very low and the probability to have two minimal cut sets at the same time is negligible. Therefore, the sum of the mean down times due to each cut sets gives a reasonable approximation of the mean down time of the whole system. From Figure B.1 we find:

$$MDT \approx MDT^{ABC} + MDT^D + MDT^{EF}$$

Dividing by T gives:

$$PFD_{avg} \approx PFD_{avg}^{ABC} + PFD_{avg}^D + PFD_{avg}^{EF}$$

Therefore, for parts in series, PFD_{avg} calculations are very similar to those performed with ordinary probabilities when they are very small compared to 1.

However for parallel parts where multiple failure are required before the loss of the function like (E, F), it is clear that MDT^{EF} may not be calculated straightforwardly from MDT^E and MDT^F : The (E,F) system's MDT has to be calculated as

$$MDT^{EF} = \int_0^T PFD^E(t) PFD^F(t) dt$$

Therefore, ordinary probabilistic calculations (additions and multiplications) are no longer valid for PFD_{avg} calculations (integrals) of parts in parallel. PFD_{avg} doesn't have the same properties as a genuine probability and its assimilation with a genuine probability is likely to lead to non conservative results. In particular, it is not possible to obtain the PFD_{avg} of an E/E/PE safety-related system just by combining in a conventional way the $PFD_{avg,i}$ of its components. As this is sometimes encouraged by commercial Boolean software packages, analysts should be vigilant to avoid such non conservative calculations which are undesirable when dealing with safety.

EXAMPLE For a redundant (1oo2) channel with a dangerous undetected failure rate λ_{DU} with a proof test interval τ , an incorrect probability model calculation could give $(\lambda_{DU} \cdot \tau)^2/4$ when the actual result is $(\lambda_{DU} \cdot \tau)^2/3$.

Calculations may be performed analytically or by using Monte Carlo simulation. This annex describes how to do that by using conventional reliability models based on Boolean (RBD or Fault-trees) or, states/transitions models (Markov, Petri nets, etc.).

B.2.3 Continuous or high demand mode E/E/PE safety-related system

B.2.3.1 General PFH formula

When an E/E/PE safety-related system is used in continuous or high demand mode, the standard requires the calculation of its PFH (i.e. its average frequency of dangerous failure). This is the average of the so called unconditional failure intensity (also called failure frequency) $w(t)$ over the period of interest:

$$PFH(T) = \frac{1}{T} \int_0^T w(t) dt$$

Where the E/E/PE safety-related system is working in continuous mode and is the ultimate safety barrier, then the overall safety-related system failure will lead directly to a potentially hazardous situation. Hence for failures that cause the loss of the overall safety function no overall safety-related system repair can be considered in the calculations. However, if the failure of the overall safety-related system does not lead directly to the potential hazard due to some other safety barrier or equipment failure then it may be possible to consider the detection and repair of the safety-related system in its risk reduction calculation.

B.2.3.2 Un-reliability case (e.g. single barrier working in continuous mode)

This case is relevant when E/E/PE safety-related system working in continuous mode is the ultimate safety barrier. Therefore a potential hazard can occur as soon as it is failing. No overall system failures are acceptable over the period of interest.

In this case the PFH may be calculated by using the failure rate over the period of interest:

$$PFH(T) = \frac{\int_0^T \Lambda(t) dt}{T} = \Lambda_{avg}$$

The overall system failure rate, $\Lambda(t)$, may be time dependent or constant.

When it is time dependant, we have: $PFH(T) = \frac{1 - \exp(-\Lambda_{avg} \cdot T)}{T} \approx \Lambda_{avg}$

When the system is made of components completely and quickly repairable with constant failure and repair rates (*if not constant failure rate the exponential cannot be applied*) (e.g. dangerous detected failures), $\Lambda(t)$ reaches quickly an asymptotic constant value Λ_{as} and, when

$PFH(T) \ll 1$, we have: $PFH(T) = \frac{1 - \exp(-\Lambda_{as} \cdot T)}{T} \approx \Lambda_{as} = \frac{1}{MTTF}$

λ_{as} exists only when the E/E/PE safety-related system working in continuous mode comprises only safe and DD failures (i.e. quickly detected and repaired). No repair of failures that can directly cause the overall failure of the safety function can be considered. For a redundant configuration where it is relevant to consider proof tests, then the asymptotic failure rate is not relevant and the previous equations have to be used. It is the job of the analyst to verify which case is relevant

B.2.3.3 Unavailability case (e.g. multiple safety barriers)

When the E/E/PE safety-related system working in continuous mode is not the ultimate barrier, its failures only increase the demand frequency on other safety barriers, or when it is working in the high demand mode, such that it is possible to detect (automatically or manually) and repair a fault that could cause the direct loss of the safety function within the expected demand period. In this case its overall failures can be repaired and *PFH* may be calculated from the availability, $A(t)$, and from the conditional failure intensity, $\lambda_v(t)$, of the system.

Again, when the system is made of components completely and quickly repairable (i.e. when, in any degraded situation, there is an high probability to come back quickly to a good working state), $\lambda_v(t)$ reaches quickly its asymptotic value, λ_{vas} , which, in addition, is also a good approximation of the true asymptotic overall system failure rate, λ_{as} , introduced in B.2.3.2.

This leads to the following approximations:

$$PFH = \frac{1}{MUT} = \frac{1}{MTTF} \approx \frac{1}{MTBF}$$

where

MUT is the acronym for Mean Up Time;

MTBF is the acronym for Mean Time Between Failure; and

MTTF is the acronym for Mean Time To Failure.

B.3 Methods of calculating PFD or PFH of a system

B.3.1 Other available guidance

For general guidance on reliability expressions and methods see EN 61703:2016 'Mathematical expressions for reliability, availability, maintainability and maintenance support terms'.

There are various methods available to calculate the PFD or PFH of a system, such as Analytical formulae (associated with Reliability block diagrams (RBD)), Boolean, Markovian, Petri net, and Monte Carlo. These methods are described in CEN Technical report CEN ISO / TR12489: 2013, 'Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems'. This Technical report covers all the above-mentioned methods and provides typical examples, however it primarily focus on Low Demand systems and its coverage for the analytical RBD approach is very limited.

Therefore, for guidance on all the methods, other than the analytical RBD, reference should be made to the CEN Technical Report. For the Analytical RBD approach the following guidance is provided. Examples for Low Demand systems given in B.3 have been taken from CEN Technical report so the numerical values obtained can be compared with using some of the other methods.

The following standards describe in detail the terms and techniques used in this clause:

- IEC 61025:2006 Fault tree analysis (FTA), RBD
- IEC 61078:2016 Reliability block diagrams

- IEC 61703:2016, for Mathematical expressions for reliability, availability, maintainability and maintenance support terms.

B.3.2 Reliability block diagram approach, assuming constant failure rate

B.3.2.1 Underlying hypothesis

The calculations are based on the following conditions and assumptions:

- the resulting average probability of failure on demand for the system is less than 10^{-1} , or the resultant average frequency of dangerous failure for the system is less than 10^{-5} h^{-1}

NOTE 1 This assumption means that the E/E/PE safety-related system is within the scope of IEC 61508 series and within the SIL 1 band (see Tables 2 and 3 of IEC 61508-1).

- component failure rates are constant over the life of the system;
- the sensor (input) subsystem comprises the actual sensor(s) and any other components and wiring, up to but not including the component(s) where the signals are first combined by voting or other processing (for example for two sensor channels, the configuration would be as shown in Figure B.2);
- the logic subsystem comprises the component(s) where the signals are first combined, and all other components up to and including where final signal(s) are presented to the final element subsystem;
- the final element (output) subsystem comprises all the components and wiring which process the final signal(s) from the logic subsystem including the final actuating component(s);
- the hardware failure rates used as inputs to the calculations and tables are for a single channel of the subsystem (for example, if 2oo3 sensors are used, the failure rate is for a single sensor and the effect of 2oo3 is calculated separately);
- the channels in a voted group all have the same failure rates and diagnostic coverage;
- the overall hardware failure rate of a channel of the subsystem is the sum of the dangerous failure rate and safe failure rate for that channel,;

NOTE 2 This assumption affects the safe failure fraction (see Annex C of IEC 61508-2), but the safe failure fraction cannot affect the calculated values for probability of failure given in this annex.

- for each safety function, there is perfect proof testing and repair (i.e. all failures that remain undetected are detected by the proof test), but for the effects of a non-perfect proof test see B.3.2.5;
- the proof test interval is at least an order of magnitude greater than the MRT;
- for each subsystem there is a single proof test interval and MRT;
- the expected interval between demands is at least an order of magnitude greater than the proof test interval;
- the expected mean time to repair a detected fault is at least a magnitude greater than the diagnostic test interval.
- the system are used where there is a defined safe state for the system
- for all subsystems operating in low demand mode of operation, and for 1oo2, 1oo2D, 1oo3 and 2oo3, voted groups operating in high demand or continuous mode of operation, the fraction of failures specified by the diagnostic coverage is both detected and repaired within the MTTR used to determine hardware safety integrity requirements;

EXAMPLE If a MTTR of 8 h is assumed, this includes the diagnostic test interval which is typically less than 10 minutes the remainder being the MRT.

NOTE 3 For 1oo2, 1oo2D, 1oo3 and 2oo3 voted groups, it can be assumed that any repair is on-line. Configuring an E/E/PE safety-related system, so that on any detected fault the EUC can be put into a safe state, improves the average probability of failure on demand. The degree of improvement can depend on the diagnostic coverage.

- for 1oo1 operating in high demand or continuous mode of operation, the E/E/PE safety-related system always achieves a safe state after detecting a dangerous fault; to achieve this, the expected interval between demands is at least an order of magnitude greater than the diagnostic test intervals, or the sum of the diagnostic test intervals and the time to achieve a safe state is less than the process safety time;

NOTE 4 For process safety time see 3.6.20 of IEC 61508-4.

- when a power supply failure removes power from a de-energize-to-trip E/E/PE safety-related system and initiates a system trip to a safe state, the power supply does not affect the average probability of failure on demand of the E/E/PE safety-related system; if the system is energized to trip, or the power supply has failure modes that can cause unsafe operation of the E/E/PE safety-related system, the power supply should be included in the evaluation;
- where the term channel is used, it is limited to only one path of the system under discussion;
- The product of the failure rate multiplied by the associated average down time should be $\ll 1$.
- During proof testing the EUC is either in a safe state or alternative safety measures are in place (see Part 2, 7.4.8.1);
- For a system undetected fault occurring between proof tests on a simplex system it is assumed that on average this will occur halfway between two proof test periods, for a duplex system which experience two undetected faults these, on average, will occur at one third and two thirds between proof tests and for triple system, on average, will occur at one quarter, one half and three quarters between proof tests.
- For a safety function operating in low demand mode of operation, on detection of a dangerous fault occurring on a:
 - a) single channel system: it is assumed that on the detection of a dangerous fault it is: reported but no change to the output state takes place; and, the fault is detected and repaired within the MTTR.
 - b) dual channel system: it is assumed that on the occurrence of the first channel dangerous fault: the system remains online whilst the channel is repaired within the MTTR and; if there is a second detected dangerous failure this will, on average, occur halfway through the MTTR of the first channel;
 - c) triple channel system voting 1oo3, with repair online: the system remains online whilst the channel is repaired within the MTTR and; if after a first detected fault, there are a further two detected faults, these will, on average, occur one third and two thirds during the MTTR of the first detected fault;
- For the above configurations, if the dangerous detected fault is configured to put the EUC into a safe state within the process safety time, then λ_{DD} can be treated the same as a safe failure. Therefore, the same equation can be used but with setting λ_{DD} to zero.
- If any of the dangerous detected failures are unable to meet the above criteria, then these failures should be included in dangerous undetected.
- For a safety function operating in high demand or continuous mode of operation, the system on detection of dangerous fault occurring on;
- A single channel system: it is assumed that the system is configured to put the EUC into a safe state within the process safety time.
- If any of the dangerous detected failures are unable to meet the criteria then these failures should be included in dangerous undetected.
- For all redundant configurations: there are two solutions provided;
- on the detection of a dangerous fault, it is reported but would not change the output state, and;

- 903 – on the detection of a dangerous fault, it the EUC is put into a safe state within the process
- 904 safety time.
- 905 – If any of the dangerous detected failures are unable to meet the criteria then these failures
- 906 should be included in dangerous undetected.
- 907 – Should any of the above assumptions be invalid then alternative modelling maybe required.
- 908 – the abbreviated terms are described in Table B.1.

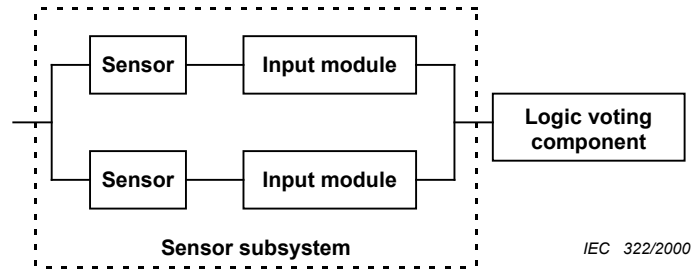


Figure B.2 – Example configuration for two sensor channels

**Table B.1 – Terms used in this annex
(applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and 2oo3)**

Abbreviation	Term (units)
T_1	Proof test interval (h)
$MTTR$	Mean time to restoration (h)
MRT	Mean repair time (h)
DC	Diagnostic coverage (expressed as a fraction in the equations and as a percentage elsewhere)
β_{DU}	The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)
β_{DD}	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)
PFD_G	Average probability of failure on demand for the group of voted channels (If the sensor, logic or final element subsystem comprises of only one voted group, then PFD_G is equivalent to PFD_S , PFD_L or PFD_{FE} respectively)
PFD_S	Average probability of failure on demand for the sensor subsystem
PFD_L	Average probability of failure on demand for the logic subsystem
PFD_{FE}	Average probability of failure on demand for the final element subsystem
PFD_{SYS}	Average probability of failure on demand of a safety function for the E/E/PE safety-related system
PFH_G	Average frequency of dangerous failure for the group of voted channels (if the sensor, logic or final element subsystem comprises of only one voted group, then PFH_G is equivalent to PFH_S , PFH_L or PFH_{FE} respectively)
PFH_S	Average frequency of dangerous failure for the sensor subsystem
PFH_L	Average frequency of dangerous failure for the logic subsystem
PFH_{FE}	Average frequency of dangerous failure for the final element subsystem
PFH_{SYS}	Average frequency of dangerous failure of a safety function for the E/E/PE safety-related system
λ	Total failure rate of a channel in a subsystem

Abbreviation	Term (units)
λ_D	Dangerous failure rate of a channel in a subsystem
λ_{DD}	Detected dangerous failure rate of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)
λ_{DU}	Undetected dangerous failure rate of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)
λ_{SD}	Detected safe failure rate of a channel in a subsystem (this is the sum of all the detected safe failure rates within the channel of the subsystem)
t_{CE}	Channel equivalent mean down time for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem)
t_{GE}	Voted group equivalent mean down time for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)
t_{CE}'	Channel equivalent mean down time for 1oo2D architecture (this is the combined down time for all the components in the channel of the subsystem)
t_{GE}'	Voted group equivalent mean down time for 1oo2D architecture (this is the combined down time for all the channels in the voted group)
T_2	Interval between demands or maintenance overhaul
K	Fraction of the success of the autotest circuit in the 1oo2D system
PTC	Proof Test Coverage
Note to table Dangerous failures that are detected and negated prior to dangerously influencing the operation of the safety function by a channel can be categorised as SD failures rather than DD failures.	

B.3.2.2 Average probability of failure on demand (for low demand mode of operation)

The average probability of failure on demand of a safety function for the E/E/PE safety-related system is determined by calculating and combining the average probability of failure on demand for all the subsystems which together implement the safety function. Since in this annex the probabilities are small, this can be expressed by the following (see Figure B.3):

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

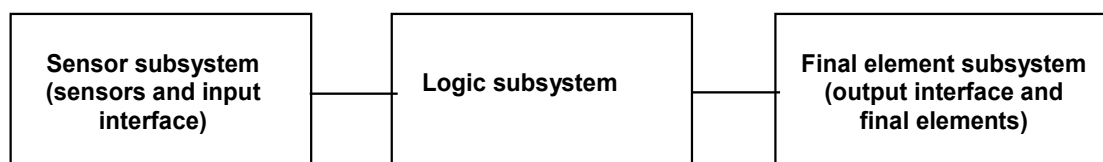
where

PFD_{SYS} is the average probability of failure on demand of a safety function for the E/E/PE safety-related system;

PFD_S is the average probability of failure on demand for the sensor subsystem;

PFD_L is the average probability of failure on demand for the logic subsystem; and

PFD_{FE} is the average probability of failure on demand for the final element subsystem.



IEC 323/2000

Figure B.3 – Subsystem structure

To determine the average probability of failure on demand for each of the subsystems, the following procedure should be adhered to for each subsystem in turn.

- d) Draw the block diagram showing the sensor subsystem (input) components, logic subsystem components or final element subsystem (output) components. For example, sensor subsystem components may be sensors, barriers, input conditioning circuits; logic subsystem components may be processors and scanning devices; and final element subsystem components may be output conditioning circuits, barriers and actuators. Represent each subsystem as one or more 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 or 2oo3 voted groups.
- e) If the safety function depends on more than one voted group of sensors or actuators, the combined average probability of failure on demand of the sensor or final element subsystem, PFD_S or PFD_{FE} , is given in the following equations, where PFD_{Gi} and PFD_{Gj} is the average probability of failure on demand for each voted group of sensors and final elements respectively:

$$PFD_S = \sum_i PFD_{Gi}$$

$$PFD_{FE} = \sum_j PFD_{Gj}$$

The formula used in all the equations for both PFD and system failure rate are all a function of component failure rate and mean down time (MDT). Where there are a number of elements in the system and it is required to calculate the combined elements overall PFD or system failure rate, then it is often necessary to use a single value for the MDT in the equations. However each element may have different failure detection mechanisms with different MDT and different elements may have different MDT values for the same failure mechanisms, in which case it is necessary to calculate a single value for the MDT which can represent all the elements in the path. This can be accomplished by considering the total paths overall failure rate then proportioning the individual MDT 's equivalent to their failure rate contribution to the total failure rate under consideration.

As an example, if there are two elements in series but one with a proof test, T_1 , and the other with a proof test, $T_{1.1}$, then the equivalent single value for the MDT is:

$$\lambda_T = \lambda_1 + \lambda_2$$

and

$$MDT_E = \frac{\lambda_1}{\lambda_T} \left(\frac{T_1}{2} \right) + \frac{\lambda_2}{\lambda_T} \left(\frac{T_{1.1}}{2} \right)$$

B.3.2.3 Architectures for low demand mode of operation

The use of MTTR in these equations assumes that the diagnostic test interval is very small compared with the repair time. If this is not the case then the diagnostic test interval (say T) should be treated the same as the Proof Test interval, e.g. for a simplex element the MTTR becomes $T/2 + MRT$.

NOTE 1 This subclause can be read sequentially, since equations which are valid for several architectures are only stated where they are first used.

NOTE 2 The equations are based on the assumptions listed in B.3.2.1.

NOTE 3 The following examples are typical configurations and are not intended to be exhaustive.

B.3.2.3.1 1oo1

This architecture consists of a single channel, where any dangerous failure leads to a failure of the safety function when a demand arises.

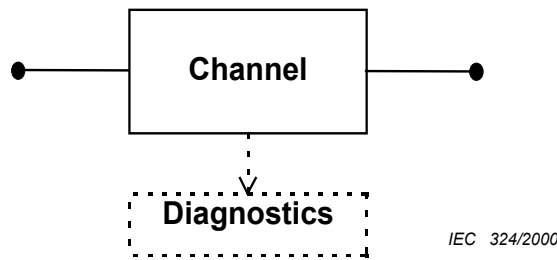


Figure B.4 – 1oo1 physical block diagram

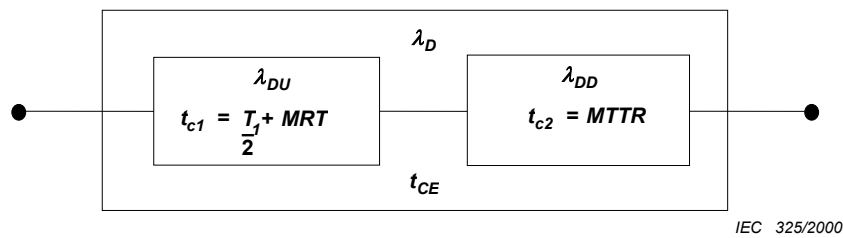


Figure B.5 – 1oo1 reliability block diagram

Figures B.4 and B.5 contain the relevant block diagrams. The dangerous failure rate for the channel is given by

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

Figure B.5 shows that the channel can be considered to comprise of two components, one with a dangerous failure rate λ_{DU} resulting from undetected failures and the other with a dangerous failure rate λ_{DD} resulting from detected failures. It is possible to calculate the channel equivalent mean down time t_{CE} , adding the individual down times from both components, t_{c1} and t_{c2} , in direct proportion to each component's contribution to the probability of failure of the channel:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

In the equations for t_{CE} and t_{GE} the strict algebraic formulae would have λ_{DU} as $(1-\beta_{DU})\lambda_{DU}$ and λ_{DD} as $(1-\beta_{DD})\lambda_{DD}$ and λ_D as $((1-\beta_{DU})\lambda_{DU} + (1-\beta_{DD})\lambda_{DD})$, however since these are ratios the slightly simplified formulae given for t_{CE} and t_{GE} introduce very little differences, particularly when considered against the uncertainty of the numerical values of λ .

For every architecture, the detected dangerous failure rate and the undetected dangerous failure rate are given by

$$\lambda_{DU} = \lambda_D(1 - DC); \quad \lambda_{DD} = \lambda_D DC$$

It should be noted that the use of MTTR in these equations assumes that the diagnostic test interval is very small compared with the repair time. If this is not the case then the diagnostic test interval (say T_2) should be treated the same as the Proof Test interval, e.g. for a simplex element the MTTR becomes $T_2/2 + MRT$.

For a channel with down time t_{CE} resulting from dangerous failures

$$PFD = 1 - e^{-\lambda_D t_{CE}} \approx \lambda_D t_{CE} \quad \text{since } \lambda_D t_{CE} \ll 1$$

Hence, for a 1oo1 architecture, the average probability of failure on demand is

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

B.3.2.3.2 1oo2

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be a dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

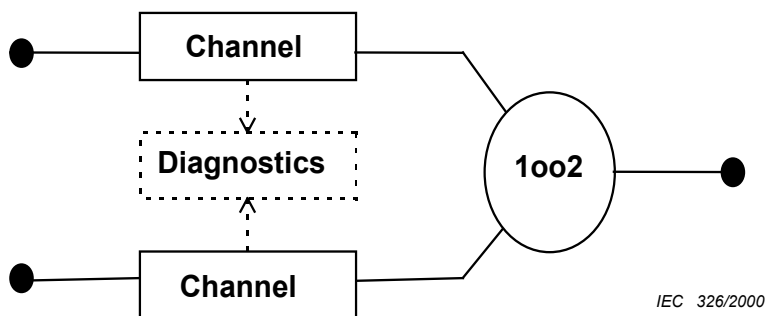


Figure B.6 – 1oo2 physical block diagram

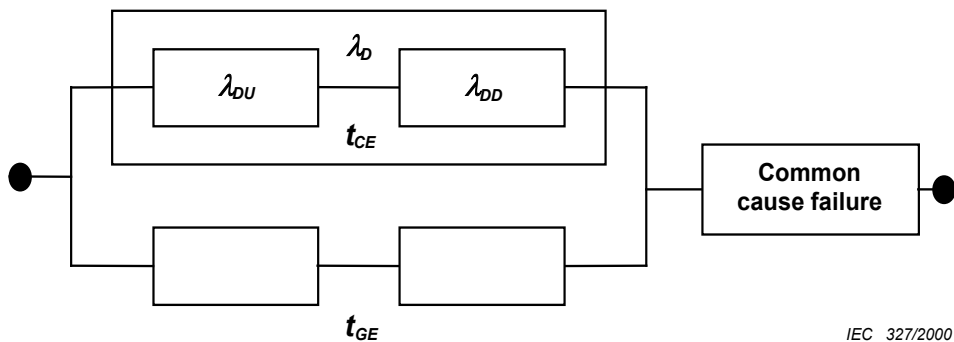


Figure B.7 – 1oo2 reliability block diagram

Figures B.6 and B.7 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.3.1, but now it is necessary to also calculate the system equivalent down time t_{GE} , which is given by

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T_i}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR / 2$$

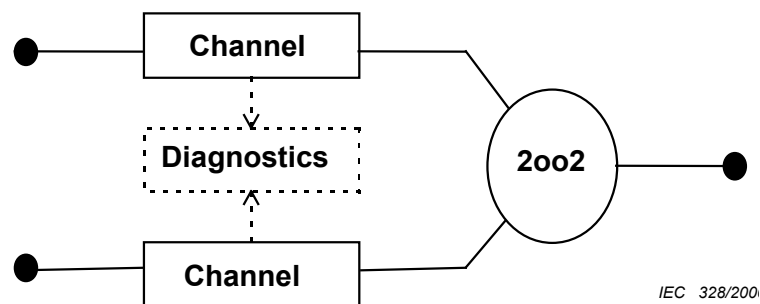
In the equations for t_{CE} and t_{GE} the strict algebraic formulae would have λ_{DU} as $(1-\beta_{DU})\lambda_{DU}$ and λ_{DD} as $(1-\beta_{DD})\lambda_{DD}$ and λ_D as $((1-\beta_{DU})\lambda_{DU} + (1-\beta_{DD})\lambda_{DD})$, however since these are ratios the slightly simplified formulae given for t_{CE} and t_{GE} introduce very little differences, particularly when considered against the uncertainty of the numerical values of λ .

The average probability of failure on demand for the architecture is

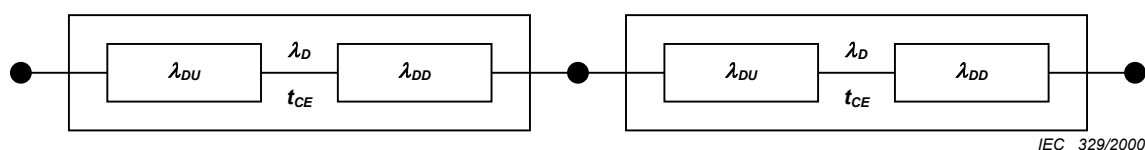
$$PFD_G = 2((1 - \beta_{DD})\lambda_{DD} + (1 - \beta_{DU})\lambda_{DU})^2 t_{CE} t_{GE} + \beta_{DD}\lambda_{DD}MTTR + \beta_{DU}\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

1018 B.3.2.3.3 2oo2

1019 This architecture consists of two channels connected in parallel so that both channels need to
 1020 demand the safety function before it can take place. It is assumed that any diagnostic testing
 1021 would only report the faults found and would not change any output states or change the output
 1022 voting.



1024 Figure B.8 – 2oo2 physical block diagram



1026 Figure B.9 – 2oo2 reliability block diagram

1027 Figures B.8 and B.9 contain the relevant block diagrams. The value of t_{CE} is as given in
 1028 B.3.2.3.1.1, and the average probability of failure on demand for the architecture is

$$1029 PFD_G = 2\lambda_D t_{CE}$$

1030 B.3.2.3.4 1oo2D

1031 This architecture consists of two active channels connected in parallel. During normal operation,
 1032 both channels need to demand the safety function before it can take place, e.g., 2oo2. In
 1033 addition, if diagnostic tests in either channel, (which consist of two monitoring channels, one
 1034 per active channel), detect a fault, **either safe or dangerous**, then the output voting is adapted
 1035 so that the overall output state then follows that given by the other non- faulty channel. If the
 1036 diagnostic tests find faults in both channels or a discrepancy that cannot be allocated to either
 1037 channel, then the **overall** output state goes to the safe state (i.e. safety function activated).

1038 In order to detect a discrepancy between the channels, either channel can determine the state
 1039 of the other channel via a means independent of the other channel, **the discrepancy monitoring**
 1040 **is only active provide there is no channel fault detected**. The channel 1oo2D comparison / switch
 1041 over / vote adaption mechanism, may not be 100 % effective and **the output may remain in the**
 1042 **2oo2 voting arrangement even though one channel has signalled a detected fault or an**
 1043 **unresolved discrepancy between the channels has been signalled**. The parameter K represents
 1044 the **fraction of expected correct functioning of this channel comparison / switching mechanism**.

1045 **The discrepancy diagnostics needs to react within process safety time for low demand, high**
 1046 **demand or continuous mode.**

There may be other implementations of the design for 1oo2D in which case the following equation would have to be modified because the assumptions underlying the reliability model have changed.

NOTE 1 The parameter K and its associated term can be determined by an FMEA.

NOTE 2 The “D” in “1oo2D” can have different interpretations including “Degradation” or “Extensive self diagnostics”. The key issue is to understand the functionality of the diagnostics”.

Note 3 There can be also a 2oo2D configuration which is similar to the 1oo2D but does not include the discrepancy diagnostic monitoring between the two channels.

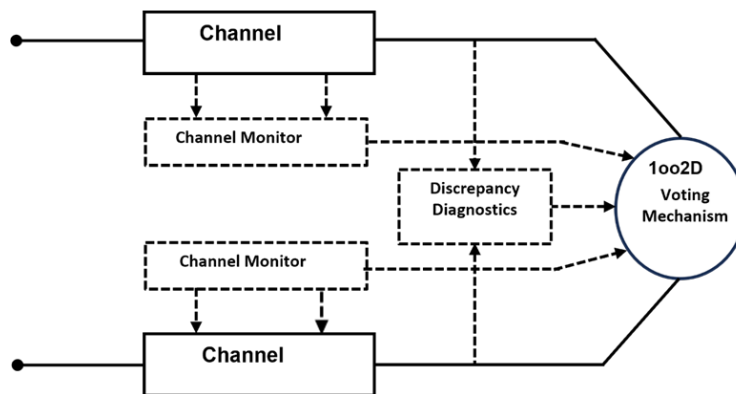


Figure B.10 – 1oo2D physical block diagram

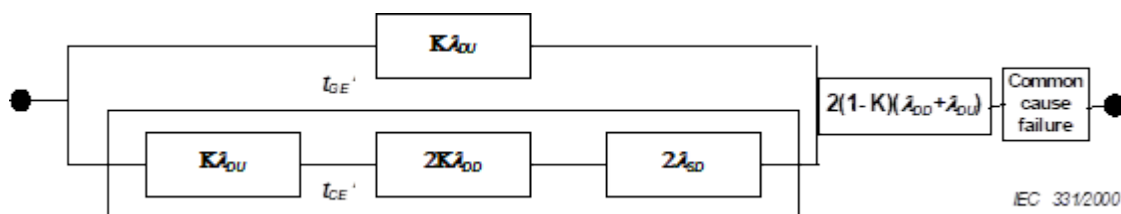


Figure B.11 – 1oo2D reliability block diagram

The detected safe failure rate for every channel is given by

$$\lambda_{SD} = \lambda_S DC$$

Figures B.10 and B.11 contain the relevant block diagrams. The values of the equivalent mean down times differ from those given for the other architectures in B.3.2.3.1 and B.3.2.3.2 and hence are labelled t_{CE}' and t_{GE}' . Their values are given by