BS EN 61508-6:2010

BSI Standards Publication

Functional safety of electrical/ electronic/programmable electronic safety related systems

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

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS EN 61508-6:2010

National foreword

This British Standard is the UK implementation of EN 61508-6:2010. It is identical to IEC 61508-6:2010. It supersedes BS EN 61508-6:2002 which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2010

ISBN 978 0 580 65448 0

ICS 13.260; 25.040.40; 29.020; 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2010.

Amendments issued since publication

Amd. No.	Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN 61508-6:2010

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61508-6

May 2010

ICS 25.040.40

Supersedes EN 61508-6:2001

English version

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

(IEC 61508-6:2010)

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3 (CEI 61508-6:2010)

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010)

This European Standard was approved by CENELEC on 2010-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

© 2010 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 61508-6:2010 E

Documents
Document Sharing Hub

Full document details: BS EN 61508-6:2010

Foreword

The text of document 65A/553/FDIS, future edition 2 of IEC 61508-6, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61508-6 on 2010-05-01.

This European Standard supersedes EN 61508-6:2001.

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

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2011-02-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-05-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61508-6:2010 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

[1] IEC 61511 series	NOTE	Harmonized in EN 61511 series (not modified).
[2] IEC 62061	NOTE	Harmonized as EN 62061.
[3] IEC 61800-5-2	NOTE	Harmonized as EN 61800-5-2.
[4] IEC 61078:2006	NOTE	Harmonized as EN 61078:2006 (not modified).
[5] IEC 61165:2006	NOTE	Harmonized as EN 61165:2006 (not modified).
[16] IEC 61131-3:2003	NOTE	Harmonized as EN 61131-3:2003 (not modified).
[18] IEC 61025:2006	NOTE	Harmonized as EN 61025:2007 (not modified).
[26] IEC 60601 series	NOTE	Harmonized in EN 60601 series (partially modified).
[27] IEC 61508-1:2010	NOTE	Harmonized as EN 61508-1:2010 (not modified).
[28] IEC 61508-5:2010	NOTE	Harmonized as EN 61508-5:2010 (not modified).
[29] IEC 61508-7:2010	NOTE	Harmonized as EN 61508-7:2010 (not modified).

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following referenced documents are indispensable for the application 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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements	EN 61508-3	2010
IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations	EN 61508-4	2010

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

CONTENTS

INTRODUCTION 8
1 Scope 10
2 Normative references 12
3 Definitions and abbreviations 12
Annex A (informative) Application of IEC 61508-2 and of IEC 61508-3 13
Annex B (informative) Example of technique for evaluating probabilities of hardware failure 21
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction – worked example 76
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems 80
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3 95
Bibliography 110

Figure 1 – Overall framework of the IEC 61508 series 11
Figure A.1 – Application of IEC 61508-2 17
Figure A.2 – Application of IEC 61508-2 (Figure A.1 *continued*) 18
Figure A.3 – Application of IEC 61508-3 20
Figure B.1 – Reliability Block Diagram of a whole safety loop 22
Figure B.2 – Example configuration for two sensor channels 26
Figure B.3 – Subsystem structure 29
Figure B.4 – 1oo1 physical block diagram 30
Figure B.5 – 1oo1 reliability block diagram 31
Figure B.6 – 1oo2 physical block diagram 32
Figure B.7 – 1oo2 reliability block diagram 32
Figure B.8 – 2oo2 physical block diagram 33
Figure B.9 – 2oo2 reliability block diagram 33
Figure B.10 – 1oo2D physical block diagram 33
Figure B.11 – 1oo2D reliability block diagram 34
Figure B.12 – 2oo3 physical block diagram 34
Figure B.13 – 2oo3 reliability block diagram 35
Figure B.14 – Architecture of an example for low demand mode of operation 40
Figure B.15 – Architecture of an example for high demand or continuous mode of operation 49
Figure B.16 – Reliability block diagram of a simple whole loop with sensors organised into 2oo3 logic 51
Figure B.17 – Simple fault tree equivalent to the reliability block diagram presented on Figure B.1 52
Figure B.18 – Equivalence fault tree / reliability block diagram 52
Figure B.19 – Instantaneous unavailability *U(t)* of single periodically tested components 54
Figure B.20 – Principle of PFD_{avg} calculations when using fault trees 55

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

Figure B.21 – Effect of staggering the tests 56
Figure B.22 – Example of complex testing pattern 56
Figure B.23 – Markov graph modelling the behaviour of a two component system 58
Figure B.24 – Principle of the multiphase Markovian modelling 59
Figure B.25 – Saw-tooth curve obtained by multiphase Markovian approach 60
Figure B.26 – Approximated Markovian model 60
Figure B.27 – Impact of failures due to the demand itself 61
Figure B.28 – Modelling of the impact of test duration 61
Figure B.29 – Multiphase Markovian model with both DD and DU failures 62
Figure B.30 – Changing logic (2oo3 to 1oo2) instead of repairing first failure 63
Figure B.31 – "Reliability" Markov graphs with an absorbing state 63
Figure B.32 – "Availability" Markov graphs without absorbing states 65
Figure B.33 – Petri net for modelling a single periodically tested component 66
Figure B.34 – Petri net to model common cause failure and repair resources 69
Figure B.35 – Using reliability block diagrams to build Petri net and auxiliary Petri net for *PFD* and *PFH* calculations 70
Figure B.36 – Simple Petri net for a single component with revealed failures and repairs 71
Figure B.37 – Example of functional and dysfunctional modelling with a formal language 72
Figure B.38 – Uncertainty propagation principle 73
Figure D.1 – Relationship of common cause failures to the failures of individual channels 82
Figure D.2 – Implementing shock model with fault trees 93

Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D, 1oo3 and 2oo3) 27
Table B.2 – Average probability of failure on demand for a proof test interval of six months and a mean time to restoration of 8 h 36
Table B.3 – Average probability of failure on demand for a proof test interval of one year and mean time to restoration of 8 h 37
Table B.4 – Average probability of failure on demand for a proof test interval of two years and a mean time to restoration of 8 h 38
Table B.5 – Average probability of failure on demand for a proof test interval of ten years and a mean time to restoration of 8 h 39
Table B.6 – Average probability of failure on demand for the sensor subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*) 40
Table B.7 – Average probability of failure on demand for the logic subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*) 41
Table B.8 – Average probability of failure on demand for the final element subsystem in the example for low demand mode of operation (one year proof test interval and 8 h *MTTR*) 41
Table B.9 – Example for a non-perfect proof test 42
Table B.10 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one month and a mean time to restoration of 8 h 45

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

Table B.11 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of three month and a mean time to restoration of 8 h 46

Table B.12 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of six month and a mean time to restoration of 8 h ..... **Error! Bookmark not defined.**

Table B.13 – Average frequency of a dangerous failure (in high demand or continuous mode of operation) for a proof test interval of one year and a mean time to restoration of 8 h ..... **Error! Bookmark not defined.**

Table B.14 – Average frequency of a dangerous failure for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*) 49

Table B.15 – Average frequency of a dangerous failure for the logic subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*) 50

Table B.16 – Average frequency of a dangerous failure for the final element subsystem in the example for high demand or continuous mode of operation (six month proof test interval and 8 h *MTTR*) 50

Table C.1 – Example calculations for diagnostic coverage and safe failure fraction 78

Table C.2 – Diagnostic coverage and effectiveness for different elements 79

Table D.1 – Scoring programmable electronics or sensors/final elements 88

Table D.2 – Value of *Z* – programmable electronics 89

Table D.3 – Value of *Z* – sensors or final elements 89

Table D.4 – Calculation of β_{int} or $\beta_{D\ int}$ 90

Table D.5 – Calculation of β for systems with levels of redundancy greater than 1oo2 91

Table D.6 – Example values for programmable electronics 92

Table E.1 – Software safety requirements specification 96

Table E.2 – Software design and development – software architecture design 97

Table E.3 – Software design and development – support tools and programming language 98

Table E.4 – Software design and development – detailed design 99

Table E.5 – Software design and development – software module testing and integration 100

Table E.6 – Programmable electronics integration (hardware and software) 100

Table E.7 – Software aspects of system safety validation 101

Table E.8 – Modification 101

Table E.9 – Software verification 102

Table E.10 – Functional safety assessment 102

Table E.11 – Software safety requirements specification 104

Table E.12 – Software design and development – software architecture design 104

Table E.13 – Software design and development – support tools and programming language 105

Table E.14 – Software design and development – detailed design 106

Table E.15 – Software design and development – software module testing and integration 106

Table E.16 – Programmable electronics integration (hardware and software) 107

Table E.17 – Software aspects of system safety validation 108

Table E.18 – Modification 108

AVA Documents
Document Sharing Hub

Full document details: BS EN 61508-6:2010

Table E.19 – Software verification 109
Table E.20 – Functional safety assessment 109

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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 International Standard 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 international standards 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 must 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 International Standard 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 international standards and in revisions of those that already exist.

This International Standard

– considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, though 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 international standards, dealing with E/E/PE safety-related systems, to be developed; the development of product and application sector international standards, 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 2 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;

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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

NOTE 4 It may 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;
– introduces systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;
– 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.

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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 software safety integrity tables specified in Annex A of IEC 61508-3 for safety integrity levels 2 and 3.

1.2 IEC 61508-1, IEC 61508-2, 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). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in IEC Guide 104 and ISO/IEC Guide 51. IEC 61508-1, IEC 61508-2, IEC 61508-3 and IEC 61508-4 are also intended for use as stand-alone publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

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.

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

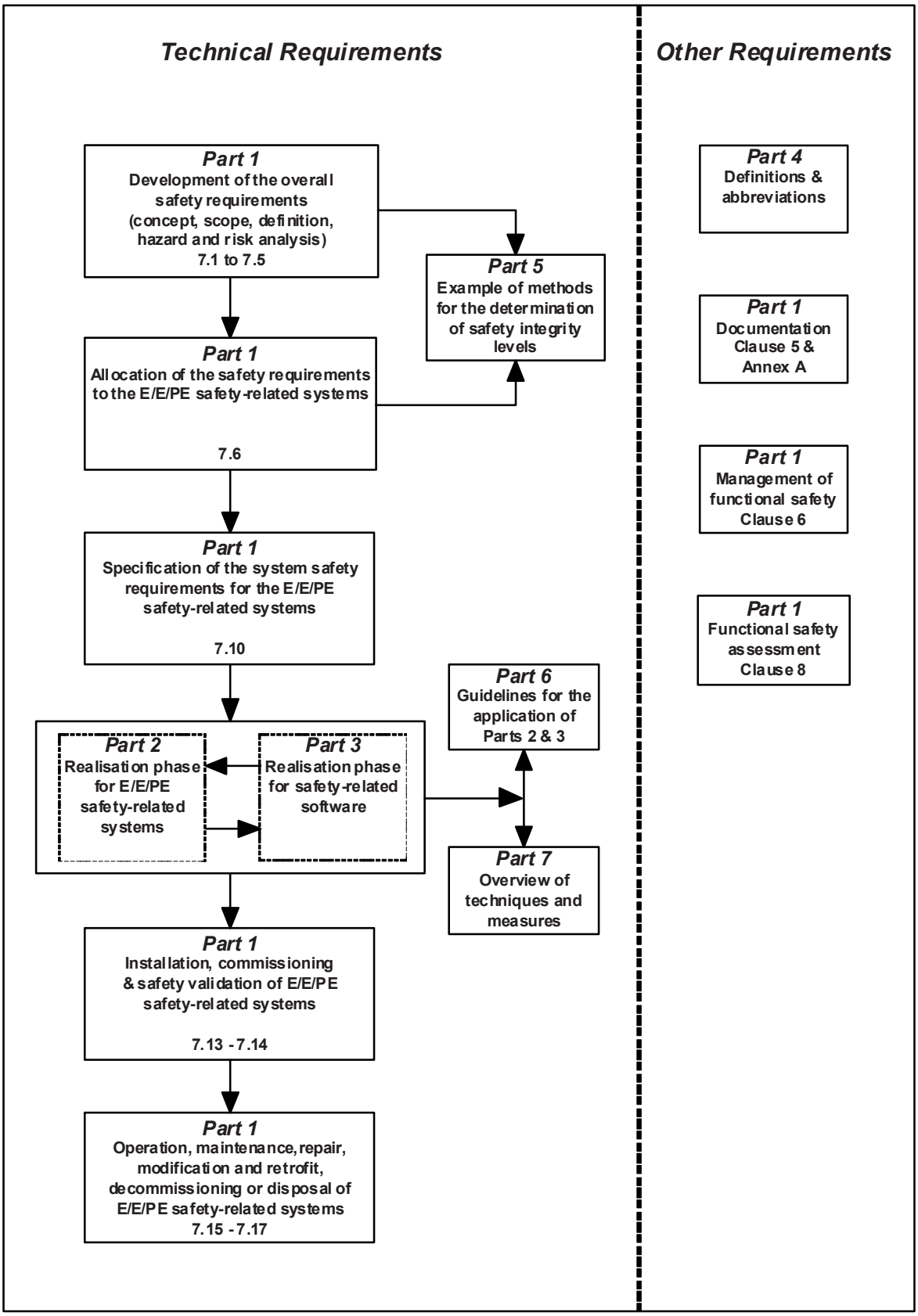

Figure 1 – Overall framework of the IEC 61508 series

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

2 Normative references

The following referenced documents are indispensable for the application 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 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:2010, *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.

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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 systems[1] 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:

– are to 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].

---

[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 61508-1).

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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, 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 techniques[4], which are graded against the safety integrity level, for the avoidance of systematic failures[5] 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 measures[6]; and
– an independent functional safety assessment[7].

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[8] 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 safety integrity for the software – both embedded (including diagnostic fault detection services) and application software. IEC 61508-3 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

---

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 or software equivalents (also called firmware), such as application-specific integrated circuits.

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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 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 may result from failures of components having a common cause due to for example similar environmental influences. The existence of such failures could 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

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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 are acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

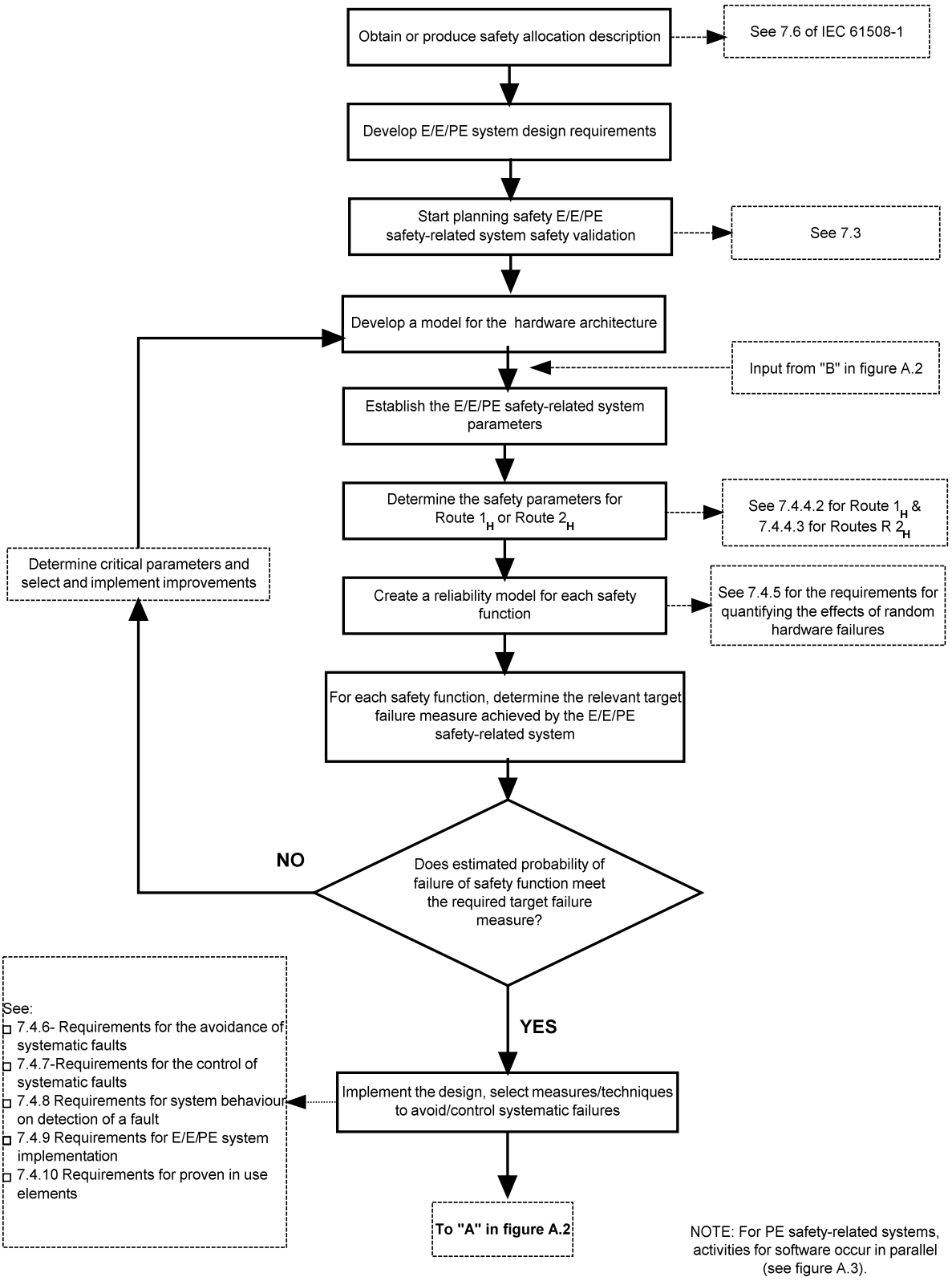

Figure A.1 – Application of IEC 61508-2

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

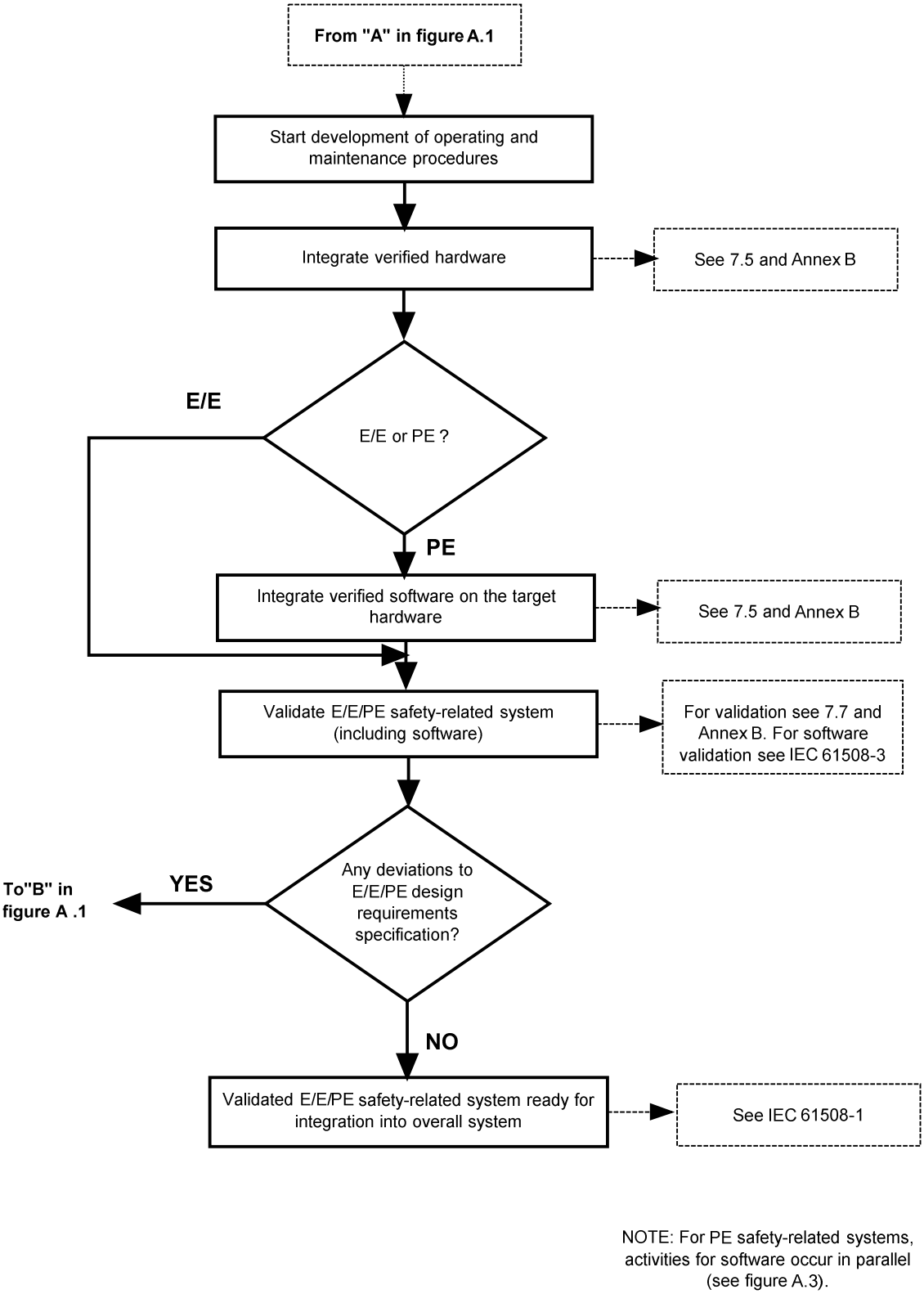

Figure A.2 – Application of IEC 61508-2 (Figure A.1 *continued*)

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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 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;

– software safety integrity level; 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 safety integrity 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 are acceptable provided justification is documented during safety planning (see Clause 6 of IEC 61508-1).

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

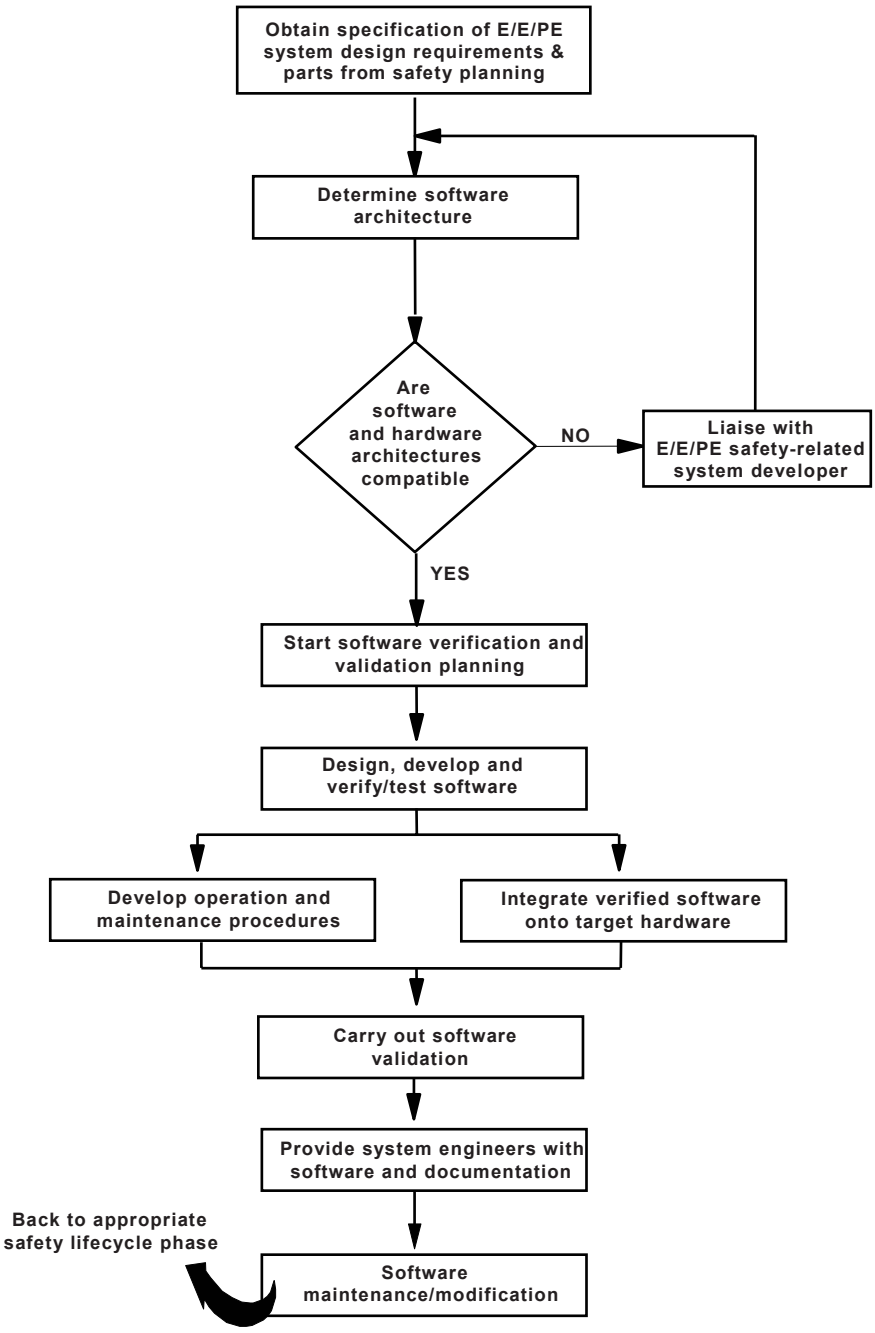

Figure A.3 – Application of IEC 61508-3

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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.

NOTE 1 System architectures stated in this part are provided by way of examples and should not 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/transitions) 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 and IEC 61078 [4]) and Fault Trees (FT) (see B.6.6.5 and B.6.6.9 of IEC 61508-7) and IEC 61025 [18] 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.6.6.6 of IEC 61508-7 and IEC 61165 [5]), Petri nets (see B.2.3.3 and B.6.6.10 of IEC 61508-7 and IEC 62551 [19]) and formal language models belong to states/transitions models. Two Markovian approaches are investigated: a simplified approach based on specific formulae (B.3) and a general approach allowing direct calculations on Markov graphs (B.5.2). For non Markovian safety systems, Monte Carlo simulations can be used instead. With present time personal computers this is achievable even for SIL 4 calculations. Subclauses B.5.3 and B.5.4 of this annex provides guidelines about handling Monte Carlo simulations (see B.6.6.8 of IEC 61508-7) on behavioural models based on Petri nets and formal languages modelling.

The simplified approach which is presented first is based on RBD graphical representations and specific Markovian formulae obtained from Taylor's developments and slightly conservative underlying hypotheses described in B.3.1.

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 underling hypotheses of any particular method are satisfied or any adjustments are required to obtain an adequate realist 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.

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

If software programmes are used to perform the calculations then the practitioner shall have an understanding of the formulae/techniques used by the software package to ensure its use is suitable for the specific application. 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).

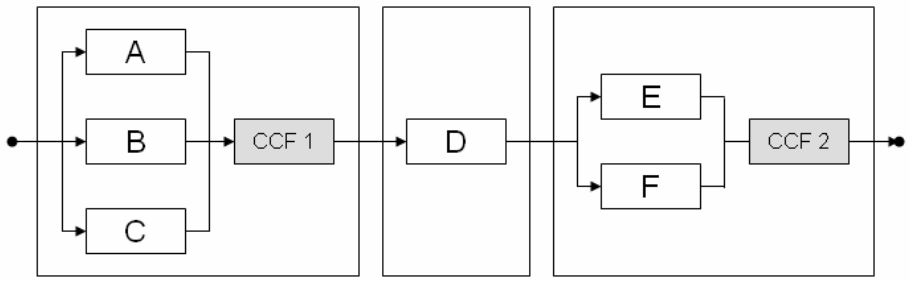

Figure B.1 – Reliability Block Diagram of a whole safety loop

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 system 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 conservative estimate 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:

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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

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} has not 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 $(\lambda_{DU}.\tau)^2/4$ when the actual result is $(\lambda_{DU}.\tau)^2/3$.

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.

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

In this case the *PFH* may be calculated by using the unreliability over the period of interest:

$$F(T):\ PFH(T) = \frac{1 - \exp\left[-\int_0^T \Lambda(t)dt\right]}{T} = \frac{F(T)}{T}$$

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

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

When the system is made of components completely and quickly repairable with constant failure and repair rates (e.g. dangerous detected failures), $\Lambda(t)$ reaches quickly an asymptotic constant value Λ_{as} and, when $PFH(T) << 1.$, we have:

$$PFH(T) = \frac{1 - \exp(-\Lambda_{as}.T)}{T} \approx \Lambda_{as} = \frac{1}{MTTF}$$

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, $\Lambda_{as,}$ introduced in B.2.3.2.

This leads to the following approximations:

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

where

MUT is the acronym for Mean Up Time;

MDT is the acronym for Mean Down Time;

MTBF is the acronym for Mean Time Between Failure; and

MTTF is the acronym for Mean Time To Failure.

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

B.2.3.4 Failure rate considerations

Several formulae above use the overall system failure rate $\Lambda(t)$. Its evaluation is not so easy and some reminders are needed.

Series structures are very simple to handle as failure rates can be added. From Figure B.1, we can write $\Lambda(t) = \Lambda^{abc}(t) + \lambda^{CCF1}(t) + \lambda^{d}(t) + \Lambda^{ef}(t) + \lambda^{CCF2}(t)$ where $\Lambda(t)$ is the overall failure rate of the E/E/PE safety-related system and $\Lambda^{abc}(t)$, $\lambda^{CCF1}(t)$, $\lambda^{d}(t)$, $\Lambda^{ef}(t)$ and $\lambda^{CCF2}(t)$ the failure rates of the five minimal cut sets.

For parallel structures this is not so simple because there are no simple relationships with individual components failure rates. For example, let us consider cut set (E, F):

1) When E and F cannot be immediately be restored (e.g. DU failures), $\Lambda^{ef}(t)$ varies continuously from 0 to λ (failure rate of E or F). An asymptotic value is reached when one of the two components is likely to have failed. This is a very slow process as this arises when t becomes larger than $1/\lambda$. This asymptotic value will be never reached in actual life if E and F are periodically proof tested with a test interval $\tau << 1/\lambda$.
2) When E and F are restored in a relatively short period of time (e.g. DD failures), $\Lambda^{ef}(t)$ goes very fast to an asymptotic value $\Lambda^{ef}_{As} = 2\lambda^2/\mu$ which can be used as an equivalent constant failure rate. It is reached when t becomes greater than two or three times the larger *MTTR* of the components. It is a particular case of the completely and quickly repairable systems discussed above.

Therefore, in the general case, evaluating the overall system failure rates imply more complex calculations than the more simple series structure.

B.3 Reliability block diagram approach, assuming constant failure rate

B.3.1 Underlying hypothesis

The calculations are based on the following 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, which are assumed to be equal;

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

NOTE 2 This assumption affects the safe failure fraction (see Annex C of IEC 61508-2), but the safe failure fraction does not 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;
– 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 1 h, the remainder being the MRT.

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

– for 1oo1 and 2oo2 voted groups 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 that part of the system under discussion, which is usually either the sensor, logic or final element subsystem;
– the abbreviated terms are described in Table B.1.

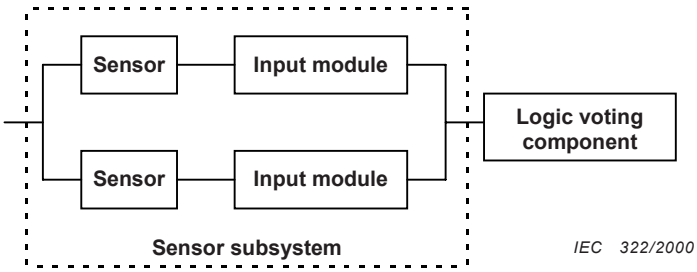

Figure B.2 – Example configuration for two sensor channels

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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

Abbre-viation	Term (units)	Parameter ranges in Tables B.2 to B.5 and B.10 to B.13
T_1	Proof test interval (hour)	One month (730 h)[1] Three months (2 190 h)[1] Six months (4 380 h) One year (8 760 h) Two years (17 520 h)[2] Ten years (87 600 h)[2]
MTTR	Mean time to restoration (hour)	8 h NOTE MTTR = MRT = 8 hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT.
MRT	Mean repair time (hour)	8 h NOTE MTTR = MRT = 8 hours is based on the assumption that the time to detect a dangerous failure, based on automatic detection, is << MRT
DC	Diagnostic coverage (expressed as a fraction in the equations and as a percentage elsewhere)	0 % 60 % 90 % 99 %
β	The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere) (Tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta_D$)	2 % 10 % 20 %
β_D	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) (Tables B.2 to B.5 and B.10 to B.13 assume $\beta = 2 \times \beta_D$)	1 % 5 % 10 %
λ_{DU}	Dangerous Undetected failure rate (per hour) of a channel in a subsystem	$0{,}05 \times 10^{-6}$ $0{,}25 \times 10^{-6}$ $0{,}5 \times 10^{-6}$ $2{,}5 \times 10^{-6}$ 5×10^{-6} 25×10^{-6}
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	

AVA Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

Abbre-viation	Term (units)	Parameter ranges in Tables B.2 to B.5 and B.10 to B.13
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 (per hour) of a channel in a subsystem	
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal to 0,5 λ (assumes 50 % dangerous failures and 50 % safe failures)	
λ_{DD}	Detected dangerous failure rate (per hour) 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 (per hour) 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 (per hour) 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 (hour) 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 (hour) 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 (hour) 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 (hour) for 1oo2D architecture (this is the combined down time for all the channels in the voted group)	
T_2	Interval between demands (h)	
K	Fraction of the success of the autotest circuit in the 1oo2D system	
PTC	Proof Test Coverage	

[1] High demand or continuous mode only.

[2] Low demand mode only.

B.3.2 Average probability of failure on demand (for low demand mode of operation)

B.3.2.1 Procedure for calculations

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):

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

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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.

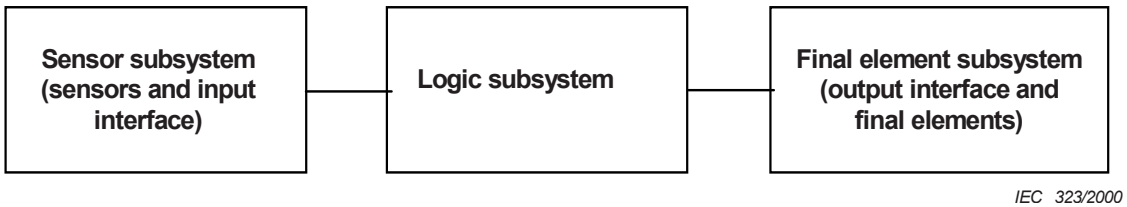

Figure B.3 – Subsystem structure

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.

a) 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.

b) Refer to the relevant table from Tables B.2 to B.5 which are for six-month, one-year, two-year and 10-year proof test intervals. These tables also assume an 8 h mean time to restoration for each failure once it has been revealed.

c) For each voted group in the subsystem, select from the relevant table of Tables B.2 to B.5:

– architecture (for example, 2oo3);

– diagnostic coverage of each channel (for example, 60 %);

– the dangerous failure rate (per hour), λ_D, of each channel (for example, $2{,}5 \times 10^{-06}$);

– the common cause failure β-factors, β and β_D, for the interaction between the channels in the voted group (for example, 2 % and 1 % respectively).

NOTE 1 It is assumed that every channel in the voted group has the same diagnostic coverage and failure rate (see Table B.1).

NOTE 2 It is assumed in Tables B.2 to B.5 (and in Tables B.10 to B.13) that the β-factor in the absence of diagnostic tests (also used for undetected dangerous failures in the presence of diagnostic tests), β, is 2 times the β-factor for failures detected by the diagnostic tests, β_D.

d) Obtain, from the relevant table from Tables B.2 to B.5, the average probability of failure on demand for the voted group.

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:

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

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

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

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_2, then the equivalent single value for the *MDT* is:

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

and

$$MDT_E = \frac{\lambda_1}{\lambda_T}\left(\frac{T_1}{2}\right) + \frac{\lambda_2}{\lambda_T}\left(\frac{T_2}{2}\right)$$

B.3.2.2 Architectures for low demand mode of operation

NOTE 1 This subclause should 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.3.1.

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

B.3.2.2.1 1oo1

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

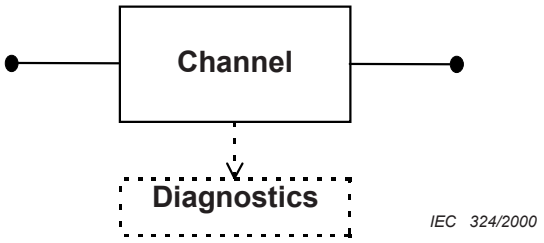

Figure B.4 – 1oo1 physical block diagram

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

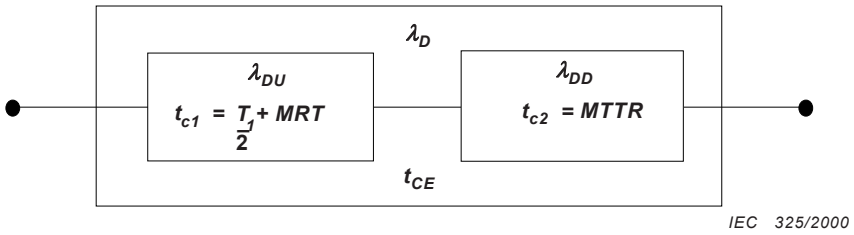

Figure B.5 – 1oo1 reliability block diagram

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:

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

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

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

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

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

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

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

B.3.2.2.2 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.

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

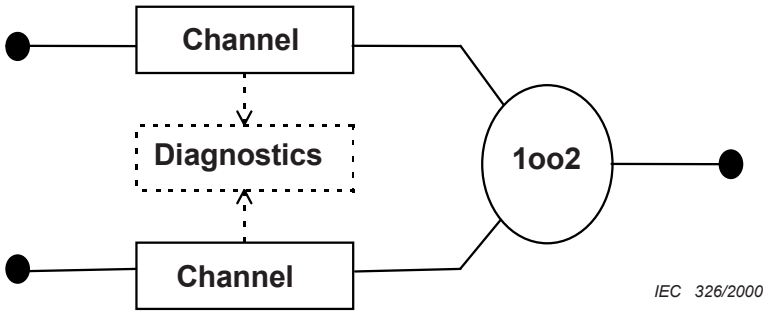

Figure B.6 – 1oo2 physical block diagram

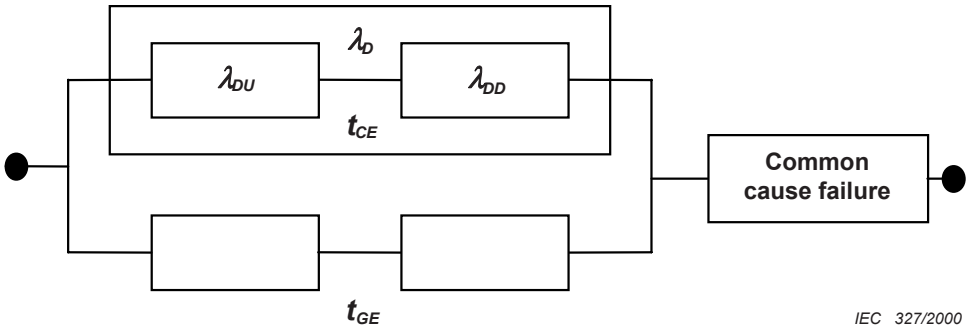

Figure B.7 – 1oo2 reliability block diagram

Figures B.6 and B.7 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1, but now it is necessary to also calculate the system equivalent down time t_{GE}, which is given by

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

The average probability of failure on demand for the architecture is

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

B.3.2.2.3 2oo2

This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. 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.

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010

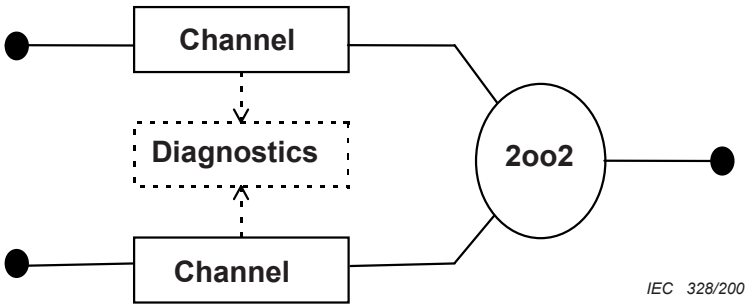

Figure B.8 – 2oo2 physical block diagram

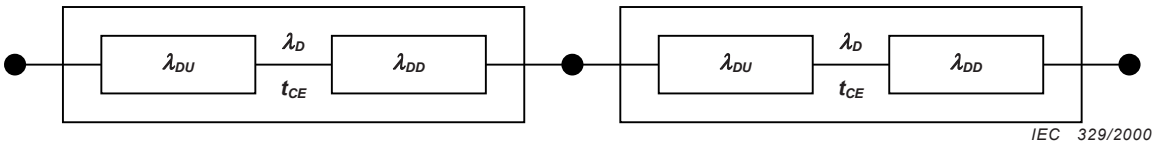

Figure B.9 – 2oo2 reliability block diagram

Figures B.8 and B.9 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1, and the average probability of failure on demand for the architecture is

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

B.3.2.2.4 1oo2D

This architecture consists of two channels connected in parallel. During normal operation, both channels need to demand the safety function before it can take place. In addition, if the diagnostic tests in either channel detect a fault then the output voting is adapted so that the overall output state then follows that given by the other channel. If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated to either channel, then the output goes to the safe state. In order to detect a discrepancy between the channels, either channel can determine the state of the other channel via a means independent of the other channel. The channel comparison / switch over mechanism may not be 100 % efficient therefore K represents the efficiency of this inter-channel comparison / switch mechanism, i.e. the output may remain on the 2oo2 voting even with one channel detected as faulty.

NOTE The parameter K will need to be determined by an FMEA.

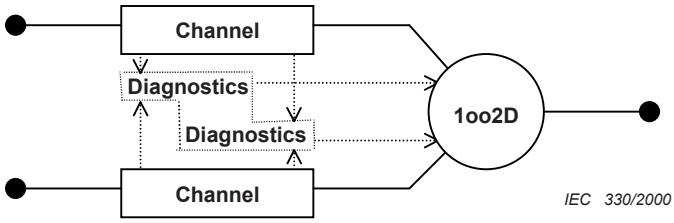

Figure B.10 – 1oo2D physical block diagram

Documents
Document Sharing Hub
Full document details: BS EN 61508-6:2010