

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

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

The European Standard EN 61508-6:2001 has the status of a
British Standard

ICS 25.040.40; 29.020

National foreword

This British Standard is the official English language version of EN 61508-6:2001. It is identical with IEC 61508-6:2000.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

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

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 74, an inside back cover and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments
13784	15 March 2002	Implementation of the European Standard
13839 Corr No. 1	28 March 2002	Correction to title

This British Standard, having been prepared under the direction of the Electrotechnical Sector Committee, was published under the authority of the Standards Committee and comes into effect on 15 July 2000

© BSI 28 March 2002

ISBN 0 580 36137 3

**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 61508-6:2000)

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 61508-6:2000)

Funktionale Sicherheit
sicherheitsbezogener elektrischer/
elektronischer/programmierbarer
elektronischer Systeme
Teil 6: Anwendungsrichtlinie für
IEC 61508-2 und IEC 61508-3
(IEC 61508-6:2000)

This European Standard was approved by CENELEC on 2001-07-03. 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, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

The text of the International Standard IEC 61508-6:2000, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61508-6 on 2001-07-03 without any modification.

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) 2002-08-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2004-08-01

Annexes designated "normative" are part of the body of the standard.
Annexes designated "informative" are given for information only.
In this standard, annex ZA is normative and annexes A to E are informative.
Annex ZA has been added by CENELEC.

IEC 61508 is a basic safety publication covering the functional safety of electrical, electronic and programmable electronic safety-related systems. The scope states:

"This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions. A major objective of this standard is to facilitate the development of application sector international standards by the technical committees responsible for the application sector. This will allow all the relevant factors associated with the application, to be fully taken into account and thereby meet the specific needs of the application sector. A dual objective of this standard is to enable the development of electrical/electronic/programmable electronic (E/E/PE) safety-related systems where application sector international standards may not exist".

The CENELEC Report R0BT-004, ratified by 103 BT (March 2000) accepts that some IEC standards, which today are either published or under development, are sector implementations of IEC 61508. For example:

- IEC 61511, Functional safety - Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.

The railways sector has also developed a set of European Standards (EN 50126; EN 50128 and prEN 50129).

NOTE EN 50126 and EN 50128 were based on earlier drafts of IEC 61508. prEN 50129 is based on the principles of the latest version of IEC 61508.

This list does not preclude other sector implementations of IEC 61508 which could be currently under development or published within IEC or CENELEC.

Endorsement notice

The text of the International Standard IEC 61508-6:2000 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:

IEC 61078 NOTE Harmonized as EN 61078:1993 (not modified).

IEC 61131-3 NOTE Harmonized as EN 61131-3:1993 (not modified).

CONTENTS

	Page
INTRODUCTION	8
Clause	
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
A.1 General	13
A.2 Functional steps in the application of IEC 61508-2	15
A.3 Functional steps in the application of IEC 61508-3	19
Annex B (informative) Example technique for evaluating probabilities of hardware failure ...	21
B.1 General	21
B.2 Average probability of failure on demand (for low demand mode of operation)	25
B.3 Probability of failure per hour (for high demand or continuous mode of operation)	38
B.4 References	46
Annex C (informative) Calculation of diagnostic coverage and safe failure fraction: worked example	47
Annex D (informative) A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems	51
D.1 General	51
D.2 Brief overview	51
D.3 Scope of the methodology	55
D.4 Points taken into account in the methodology	55
D.5 Using the β -factor to calculate the probability of failure in an E/E/PE safety-related system due to common cause failures	56
D.6 Using the tables to estimate β	57
D.7 Examples of the use of the methodology	61
D.8 References	62
Annex E (informative) Example applications of software safety integrity tables of IEC 61508-3	63
E.1 General	63
E.2 Example for safety integrity level 2	63
E.3 Example for safety integrity level 3	68
Annex ZA (normative) Normative references to international publications with their corresponding European publications	74
Bibliography	73

	Page
Figure 1 – Overall framework of IEC 61508	11
Figure A.1 – Application of IEC 61508-2	17
Figure A.2 – Application of IEC 61508-2 (continued)	18
Figure A.3 – Application of IEC 61508-3	20
Figure B.1 – Example configuration for two sensor channels	23
Figure B.2 – Subsystem structure	25
Figure B.3 – 1oo1 physical block diagram	26
Figure B.4 – 1oo1 reliability block diagram	26
Figure B.5 – 1oo2 physical block diagram	27
Figure B.6 – 1oo2 reliability block diagram	28
Figure B.7 – 2oo2 physical block diagram	28
Figure B.8 – 2oo2 reliability block diagram	28
Figure B.9 – 1oo2D physical block diagram	29
Figure B.10 – 1oo2D reliability block diagram	29
Figure B.11 – 2oo3 physical block diagram	30
Figure B.12 – 2oo3 reliability block diagram	30
Figure B.13 – Architecture of an example for low demand mode of operation	35
Figure B.14 – Architecture of an example for high demand or continuous mode of operation	44
Figure D.1 – Relationship of common cause failures to the failures of individual channels ..	53
 Table B.1 – Terms and their ranges used in this annex (applies to 1oo1, 1oo2, 2oo2, 1oo2D and 2oo3)	 24
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	31
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	32
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	33
Table B.5 – Average probability of failure on demand for a proof-test interval of 10 years and a mean time to restoration of 8 h	34
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)	35
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)	36
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)	36

Table B.9 – Example for a non-perfect proof test.....	38
Table B.10 – Probability of failure per hour (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.....	40
Table B.11 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of three months and a mean time to restoration of 8 h.....	41
Table B.12 – Probability of failure per hour (in high demand or continuous mode of operation) for a proof test interval of six months and a mean time to restoration of 8 h.....	42
Table B.13 – Probability of failure per hour (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.....	43
Table B.14 – Probability of failure per hour for the sensor subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR).....	44
Table B.15 – Probability of failure per hour for the logic subsystem in the example for high demand or continuous mode of operation (six month proof-test interval and 8 h MTTR).....	45
Table B.16 – Probability of failure per hour 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)	45
Table C.1 – Example calculations for diagnostic coverage and safe failure fraction	49
Table C.2 – Diagnostic coverage and effectiveness for different subsystems	50
Table D.1 – Scoring programmable electronics or sensors/final elements.....	58
Table D.2 – Value of Z: programmable electronics	60
Table D.3 – Value of Z: sensors or final elements.....	60
Table D.4 – Calculation of β or β_D	61
Table D.5 – Example values for programmable electronics.....	62
Table E.1 – Software safety requirements specification (see 7.2 of IEC 61508-3).....	64
Table E.2 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3).....	65
Table E.3 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3)	65
Table E.4 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding)	66
Table E.5 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3).....	66
Table E.6 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3).....	66
Table E.7 – Software safety validation (see 7.7 of IEC 61508-3)	67
Table E.8 – Software modification (see 7.8 of IEC 61508-3)	67
Table E.9 – Software verification (see 7.9 of part 3)	67
Table E.10 – Functional safety assessment (see clause 8 of IEC 61508-3)	68

	Page
Table E.11 – Software safety requirements specification (see 7.2 of IEC 61508-3)	69
Table E.12 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3)	69
Table E.13 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3)	70
Table E.14 – Software design and development: detailed design (see 7.4.5 and 7.4.6 of IEC 61508-3) (this includes software system design, software module design and coding)	70
Table E.15 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3)	71
Table E.16 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3)	71
Table E.17 – Software safety validation (see 7.7 of IEC 61508-3)	71
Table E.18 – Modification (see 7.8 of IEC 61508-3)	72
Table E.19 – Software verification (see 7.9 of IEC 61508-3)	72
Table E.20 – Functional safety assessment (see clause 8 of IEC 61508-3)	72

INTRODUCTION

Systems comprised of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems (PESs)) 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 those 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 components (electrical/ electronic/programmable electronic systems (E/E/PESs)) 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 application sector standards.

In most situations, safety is achieved by a number of protective 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 electrical/ electronic/programmable electronic (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 E/E/PES applications in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the exact prescription of safety measures is dependent on many factors specific to the application. This International Standard, by being generic, will enable such a prescription to be formulated in future application sector international standards.

This International Standard

- considers all relevant overall, E/E/PES and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PESs 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 application sector international standards, dealing with safety-related E/E/PESs, to be developed; the development of application sector international standards, within the framework of this International 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;
- uses 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;

- adopts a risk-based approach for the determination of the safety integrity level requirements;
- sets numerical target failure measures for E/E/PE safety-related systems which are linked to the safety integrity levels;
- sets a lower limit on the target failure measures, in a dangerous mode of failure, that can be claimed for 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 failure of 10^{-5} to perform its design function on demand,
 - a high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

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

- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not rely on the concept of fail-safe, which may be of value when the failure modes are well-defined and the level of complexity is relatively low – the concept of fail-safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

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 3.4.4 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 IEC/ISO Guide 51. IEC 61508 is also intended for use as a stand-alone standard.

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 do not apply unless specifically referred to or included in the publications prepared by those technical committees.

NOTE In the USA and Canada, until the proposed process sector implementation of IEC 61508 (i.e. IEC 61511) is published as an international standard, existing national process safety standards based on IEC 61508 (i.e. ANSI/ISA S84.01-1996) can be applied to the process sector instead of IEC 61508.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of this standard and indicates the role that IEC 61508-6 plays in the achievement of functional safety for E/E/PE safety-related systems.

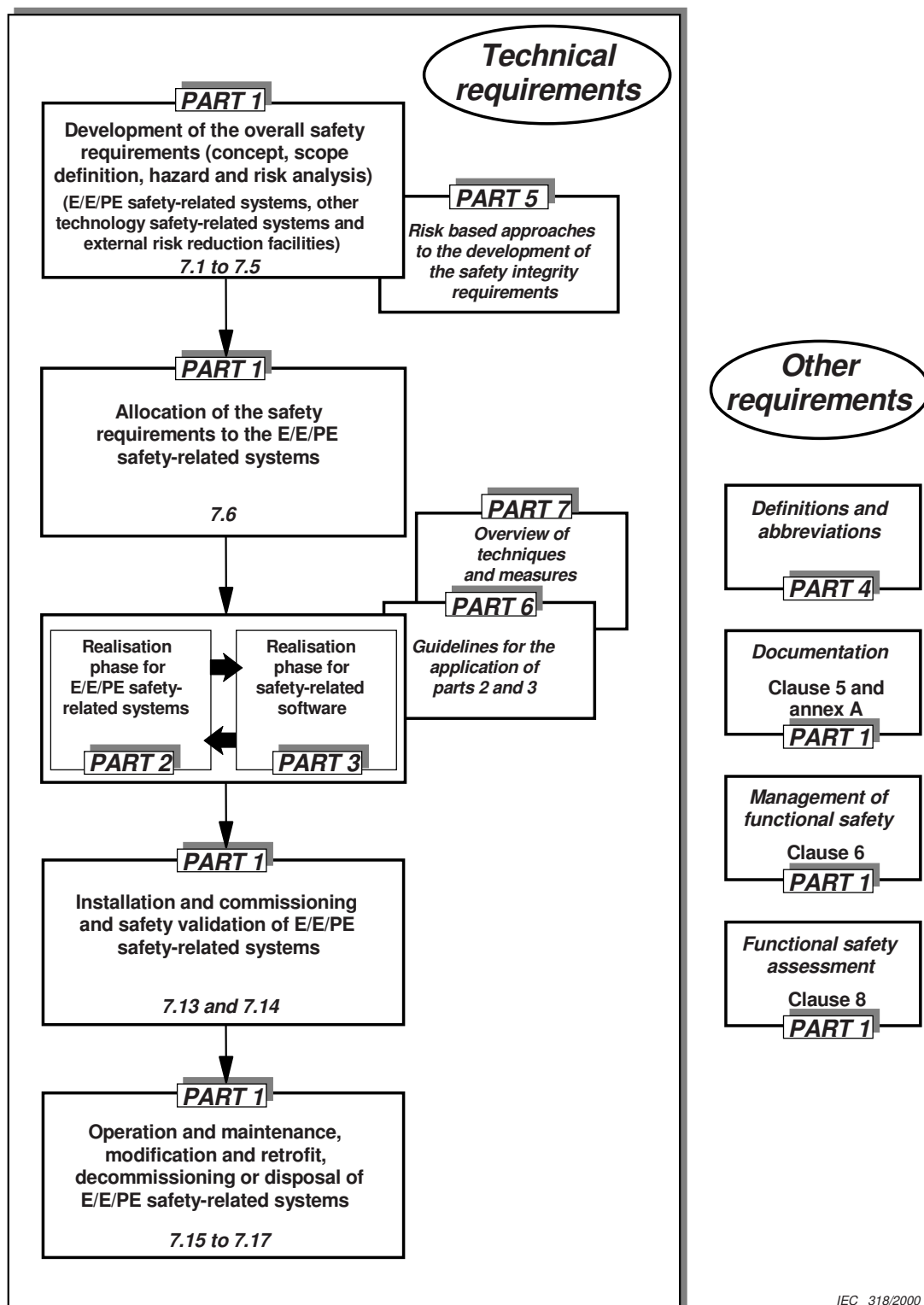


Figure 1 – Overall framework of IEC 61508

IEC 318/2000

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 61508. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of IEC 61508 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC Guide 104:1997, *Guide to the drafting of safety standards and the rôle of committees with safety pilot functions and safety group functions*

IEC/ISO Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

3 Definitions and abbreviations

For the purpose of this standard, 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 electro-mechanical, 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/PES 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 3.4.1 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 7.6.2.9 of IEC 61508-1).

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 6 of IEC 61508-1).

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 ¹⁾, which are graded against the safety integrity level, for the avoidance of systematic failures ²⁾ 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 ³⁾; and
- an independent functional safety assessment ⁴⁾.

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 ⁵⁾ 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.

1) 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.

2) 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).

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

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

5) Including fixed built-in software or software equivalents (also called firmware), such as application-specific integrated circuits.

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 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/PES. 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/PES development.
- b) Determine the requirements for E/E/PES safety, 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 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 7.5.2.4 of IEC 61508-1). 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/PES safety validation (see 7.3 of IEC 61508-2).
- d) Specify the architecture (configuration) for the E/E/PES 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 (components), 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);

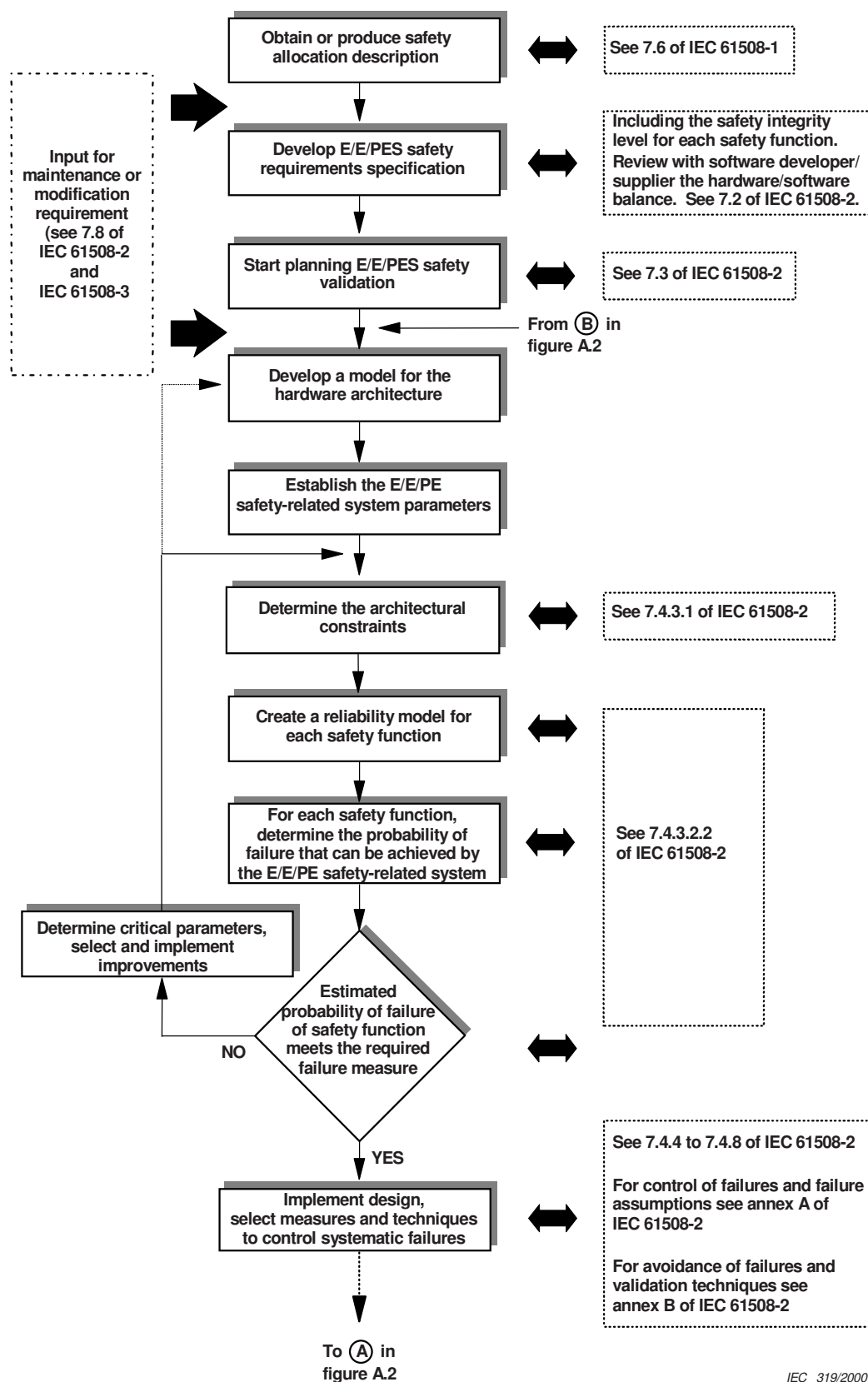
- the probability of failure; and
 - the safe failure fraction (see annex C of IEC 61508-2).
- g) Determine the architectural constraints (see tables 2 and 3 of IEC 61508-2).
- h) Create a reliability model for each of the safety functions that the E/E/PE safety-related system is required to carry out.
- NOTE A reliability model is a mathematical formula which shows the relationship between reliability and relevant parameters relating to equipment and conditions of use.
- i) 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 tables 2 and 3 of IEC 61508-2 (see 7.4.3.1 of IEC 61508-2). If the predicted reliability does not meet the target failure measure and/or does not meet the requirements of tables 2 and 3 of IEC 61508-2, 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 A number of modelling methods are available and the analyst should choose which is the most appropriate (see 7.4.3.2.2 note 9 of IEC 61508-2 for a list of some methods that could be used).
- j) 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).
- k) 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)).
- l) Together with the software developer (see 7.7 of IEC 61508-3), validate the E/E/PES (see 7.7 of IEC 61508-2 and annex B of IEC 61508-2).
- m) Hand over the hardware and results of the E/E/PES safety validation to the system engineers for further integration into the overall system.
- n) If maintenance/modification of the E/E/PES 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/PES 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/PES 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.

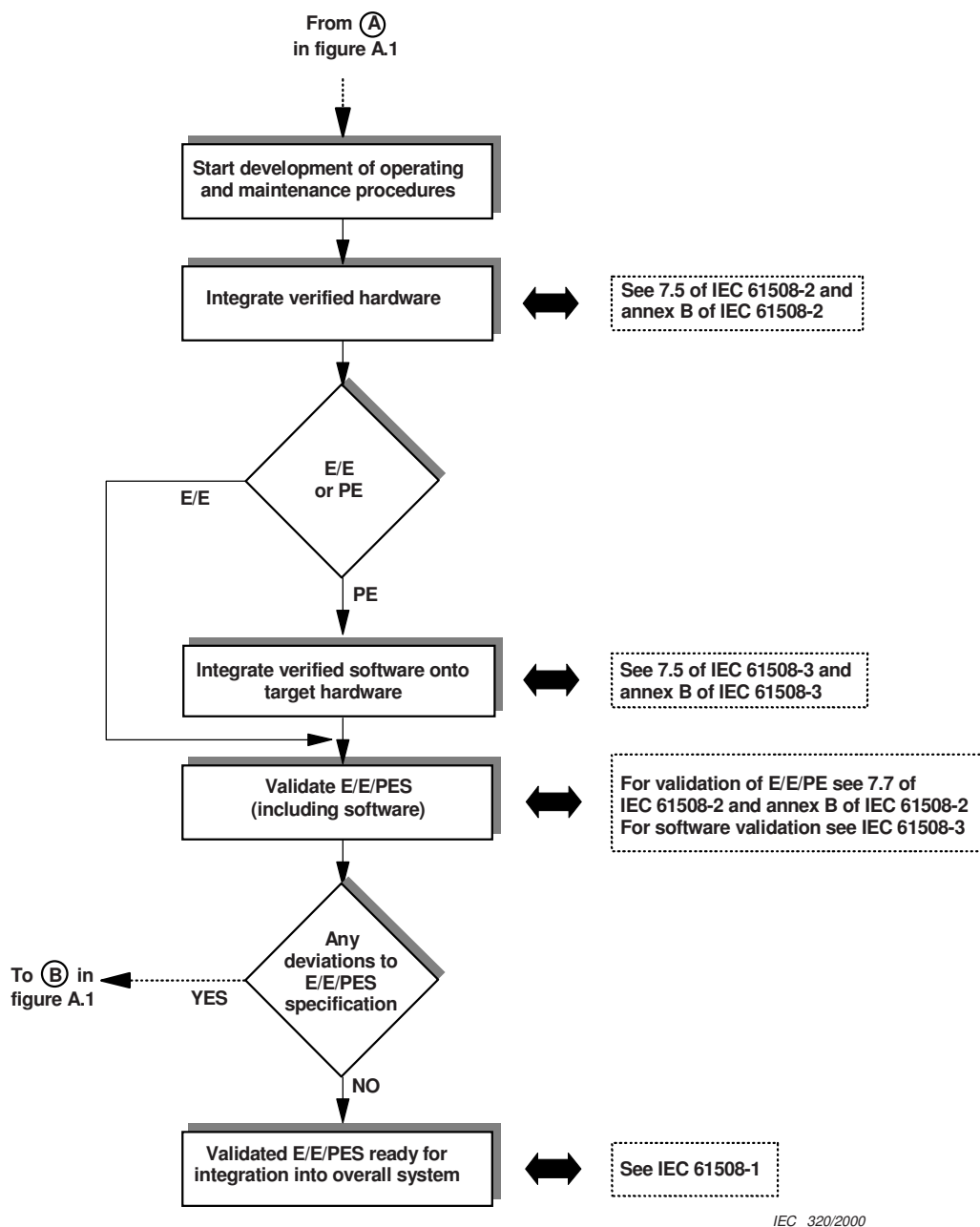
NOTE In applying the above steps, alternative measures to those specified in the standard are acceptable provided justification is documented during safety planning (see clause 6 of IEC 61508-1).



IEC 319/2000

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

Figure A.1 – Application of IEC 61508-2



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

Figure A.2 – Application of IEC 61508-2 (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 Earlier lifecycle phases have already

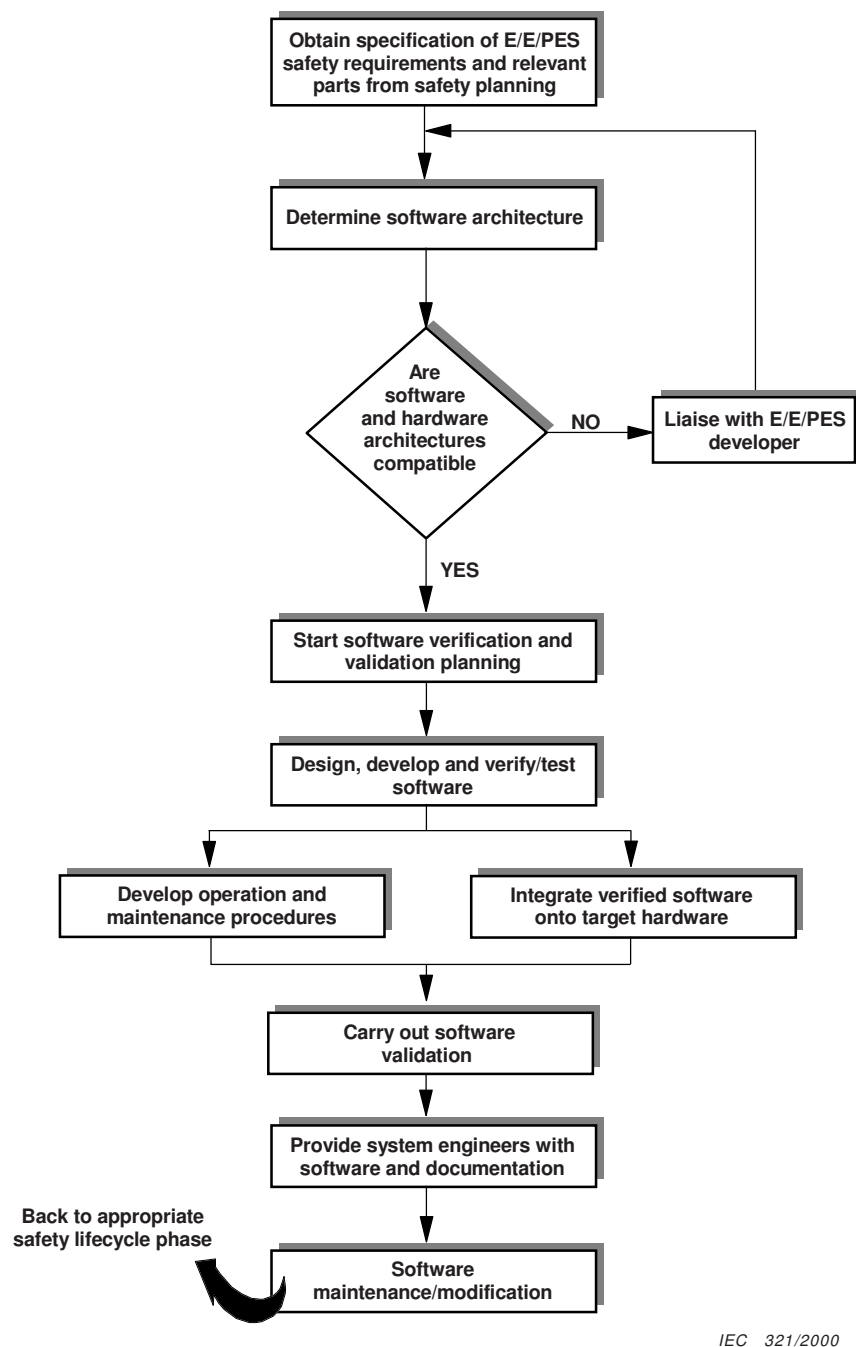
- specified the required safety functions and their associated safety integrity levels (see 7.4 and 7.5 of IEC 61508-1);
 - allocated the safety functions to designated E/E/PE safety-related systems (see 7.6 of IEC 61508-1); and
 - allocated functions to software within each E/E/PE safety-related system (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/PES 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/PES 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 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).



IEC 321/2000

Figure A.3 – Application of IEC 61508-3

Annex B (informative)

Example technique for evaluating probabilities of hardware failure

B.1 General

This annex provides one possible technique 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 technique that might be used. It does, however, provide a relatively simple approach for assessing the capability of E/E/PE safety-related systems.

NOTE 1 Other techniques are described for example in ANSI/ISA S84.01-1996, Application of safety instrumented systems for the process industries.

There are a number of techniques available for the analysis of hardware safety integrity for E/E/PE safety-related systems. Two of the more common techniques are reliability block diagrams (see C.6.5 of IEC 61508-7) and Markov models (see C.6.4 of IEC 61508-7). Both methods, if correctly applied, yield similar results, but in the case of complex programmable electronic subsystems (for example where multiple channel cross-voting and automatic testing are employed) there may be some loss of accuracy when reliability block diagrams are used compared to Markov models.

This loss of accuracy may not be significant in the context of the complete E/E/PE safety-related system and when the accuracy of the reliability data used in the analysis is taken into account. For example, field devices often predominate in the analysis of the hardware safety integrity for E/E/PE safety-related systems. Whether the loss of accuracy is significant can only be determined in the particular circumstances. In the case of complex programmable electronic subsystems, reliability block diagrams give results with more pessimistic hardware safety integrity values than Markov models (i.e. reliability block diagrams give a higher probability of failure). This annex uses reliability block diagrams.

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.

The calculations are based on the following assumptions:

- the resulting average probability of failure on demand for the subsystem is less than 10^{-1} , or the resultant probability of failure per hour for the subsystem is less than 10^{-5} ;
- 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.1);

- 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;

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.2.5;
- the proof test interval is at least an order of magnitude greater than the diagnostic test interval;
- for each subsystem there is a single proof test interval and mean time to restoration;

NOTE 3 The mean time to restoration is defined in 7.4.3.2.2, note 5 of IEC 61508-2 as including the time taken to detect a failure. In this annex, the single assumed value of mean time to restoration for both detected and undetected failures includes the diagnostic test interval but not the proof test interval. For undetected failures, the mean time to restoration used in the calculations should not include the diagnostic test interval, but since the mean time to restoration is always added to the proof test interval, which is at least an order of magnitude greater than the diagnostic test interval, the error is not significant.

- multiple repair teams are available to work on all known failures;
- the expected interval between demands is at least an order of magnitude greater than the mean time to restoration;
- for all subsystems operating in low demand mode of operation, and for 1oo2, 1oo2D 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 mean time to restoration used to determine hardware safety integrity requirements;

EXAMPLE If a mean time to restoration of 8 h is assumed, this includes the diagnostic test interval which is typically less than 1 h, the remainder being the actual repair time.

NOTE 4 For 1oo2, 1oo2D 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 5 The process safety time is defined in 7.4.3.2.5 of IEC 61508-2 as the period of time between a failure occurring in the EUC or the EUC control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed.