EESTI STANDARD EVS-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

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION
EVS

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
Käesolev Eesti standard EVS-EN 61508-6:2010 sisaldab Euroopa standardi EN 61508-6:2010 ingliskeelset teksti.	This Estonian standard EVS-EN 61508-6:2010 consists of the English text of the European standard EN 61508-6:2010.
Standard on kinnitatud Eesti Standardikeskuse 31.08.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 31.08.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Euroopa standardimisorganisatsioonide poolt rahvuslikele liikmetele Euroopa standardi teksti kättesaadavaks tegemise kuupäev on 28.05.2010.	Date of Availability of the European standard text 28.05.2010.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

ICS 25.040.40

Võtmesõnad: control, diagnosis (medical), management, medicine, policy, process measuring and contr, programmable, reliability, reliability assurance, safety, safety devices, safety engineering, safety requirements, safety systems, specification (approval), specifications, use

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

Ref. No. EN 61508-6:2010 E

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).

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

CONTENTS

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;

- 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.

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.

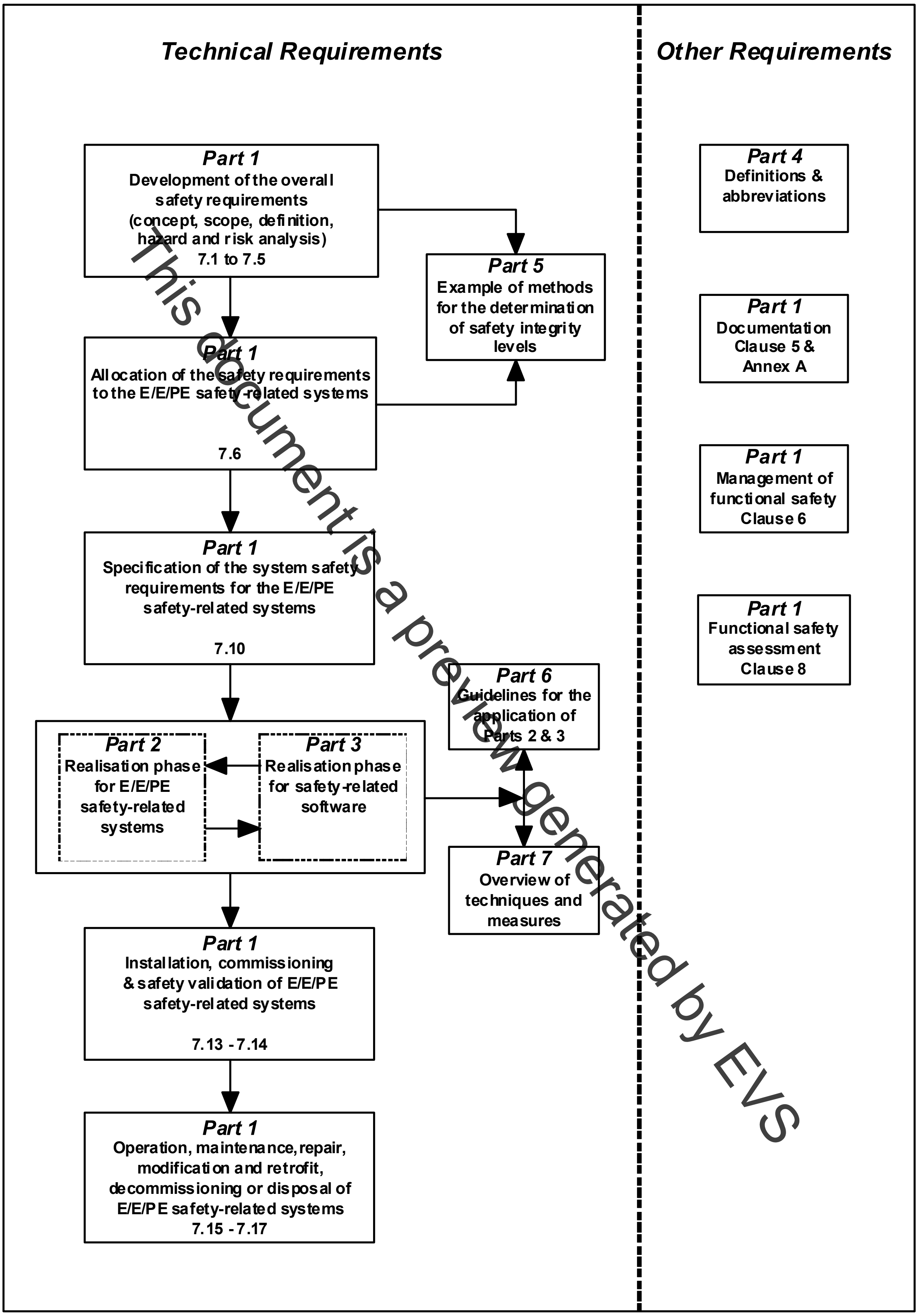
Technical Requirements
Other Requirements
Part 1
Development of the overall safety requirements (concept, scope, definition, hazard and risk analysis)
7.1 to 7.5
Part 5
Example of methods for the determination of safety integrity levels
Part 1
Allocation of the safety requirements to the E/E/PE safety-related systems
7.6
Part 1
Specification of the system safety requirements for the E/E/PE safety-related systems
7.10
Part 6
Guidelines for the application of Parts 2 & 3
Part 2
Realisation phase for E/E/PE safety-related systems
Part 3
Realisation phase for safety-related software
Part 7
Overview of techniques and measures
Part 1
Installation, commissioning & safety validation of E/E/PE safety-related systems
7.13 - 7.14
Part 1
Operation, maintenance, repair, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
7.15 - 7.17
Part 4
Definitions & abbreviations
Part 1
Documentation
Clause 5 & Annex A
Part 1
Management of functional safety
Clause 6
Part 1
Functional safety assessment
Clause 8

Figure 1 – Overall framework of the IEC 61508 series

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.

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).

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.

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

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).

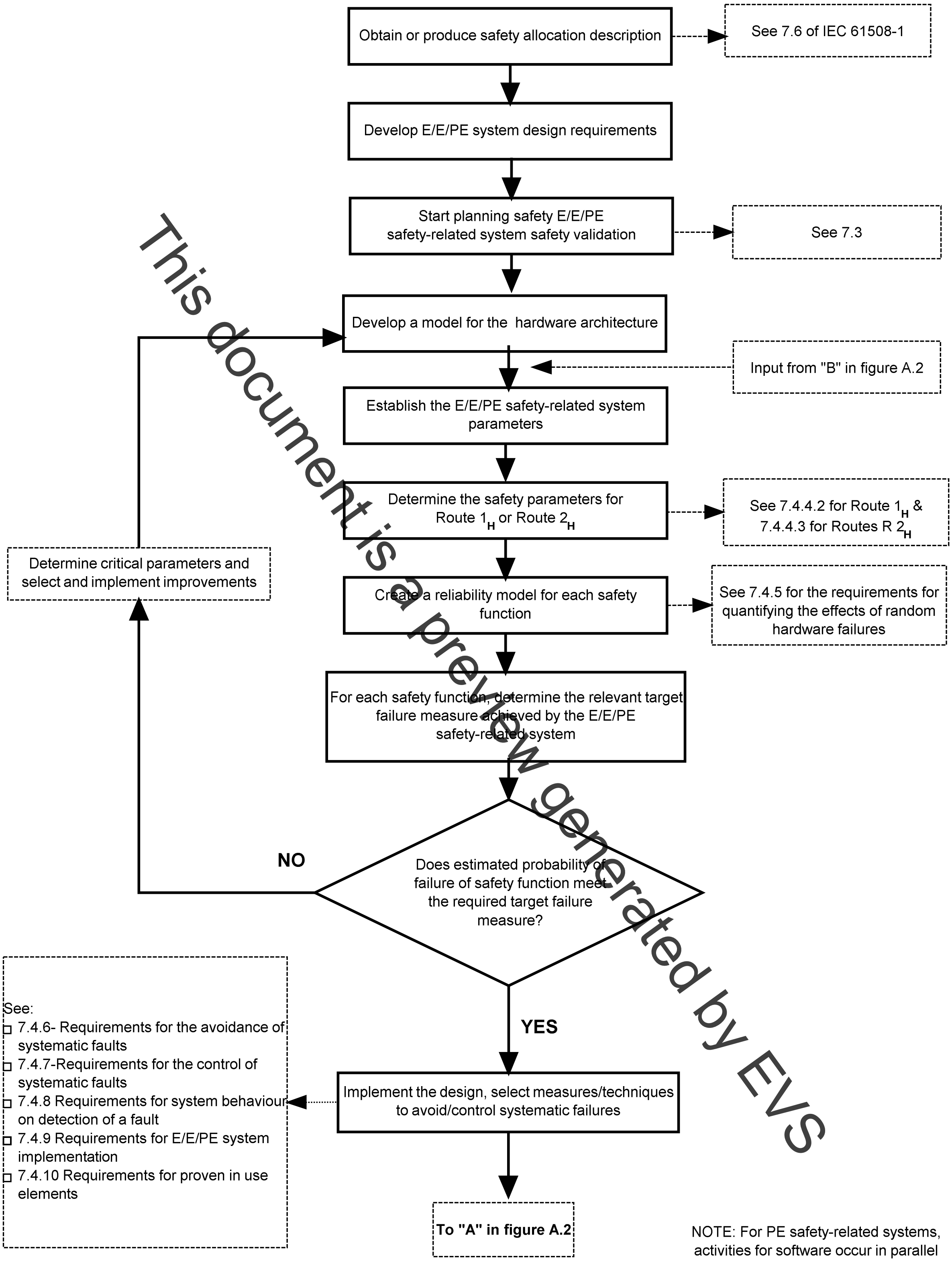
Obtain or produce safety allocation description
See 7.6 of IEC 61508-1
Develop E/E/PE system design requirements
Start planning safety E/E/PE safety-related system safety validation
See 7.3
Develop a model for the hardware architecture
Input from "B" in figure A.2
Establish the E/E/PE safety-related system parameters
Determine the safety parameters for Route 1H or Route 2H
See 7.4.4.2 for Route 1H & 7.4.4.3 for Routes R 2H
Determine critical parameters and select and implement improvements
Create a reliability model for each safety function
See 7.4.5 for the requirements for quantifying the effects of random hardware failures
For each safety function, determine the relevant target failure measure achieved by the E/E/PE safety-related system
NO
Does estimated probability of failure of safety function meet the required target failure measure?
YES
See:
□ 7.4.6- Requirements for the avoidance of systematic faults
□ 7.4.7-Requirements for the control of systematic faults
□ 7.4.8 Requirements for system behaviour on detection of a fault
□ 7.4.9 Requirements for E/E/PE system implementation
□ 7.4.10 Requirements for proven in use elements
Implement the design, select measures/techniques to avoid/control systematic failures
To "A" in figure A.2
NOTE: For PE safety-related systems, activities for software occur in parallel (see figure A.3).

Figure A.1 – Application of IEC 61508-2