

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

BASIC SAFETY PUBLICATION

PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

**Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques  
programmables relatifs à la sécurité –  
Partie 3: Prescriptions concernant les logiciels**

<https://standards.iteh.ai/en/standards/iec/5638b9f8-e2eb-486d-8e3c-bd0550a44fc2/iec-61508-3-1998>



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 1998 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland  
Email: [inmail@iec.ch](mailto:inmail@iec.ch)  
Web: [www.iec.ch](http://www.iec.ch)

### About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

### About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: [www.iec.ch/searchpub](http://www.iec.ch/searchpub)

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: [www.electropedia.org](http://www.electropedia.org)

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: [www.iec.ch/webstore/custserv](http://www.iec.ch/webstore/custserv)

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: [csc@iec.ch](mailto:csc@iec.ch)  
Tel.: +41 22 919 02 11  
Fax: +41 22 919 03 00

### A propos de la CEI

La Commission Electrotechnique internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

### A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: [www.iec.ch/searchpub/cur\\_fut-f.htm](http://www.iec.ch/searchpub/cur_fut-f.htm)

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,...). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: [www.iec.ch/online\\_news/justpub](http://www.iec.ch/online_news/justpub)

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: [www.electropedia.org](http://www.electropedia.org)

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: [www.iec.ch/webstore/custserv/custserv\\_entry-f.htm](http://www.iec.ch/webstore/custserv/custserv_entry-f.htm)

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:

Email: [csc@iec.ch](mailto:csc@iec.ch)  
Tél.: +41 22 919 02 11  
Fax: +41 22 919 03 00

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

BASIC SAFETY PUBLICATION  
PUBLICATION FONDAMENTALE DE SÉCURITÉ

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

**Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques  
programmables relatifs à la sécurité –  
Partie 3: Prescriptions concernant les logiciels**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE  
CODE PRIX



## CONTENTS

	Page
FOREWORD .....	4
INTRODUCTION .....	5
Clause	
1 Scope .....	7
2 Normative references .....	10
3 Definitions and abbreviations .....	10
4 Conformance to this standard .....	10
5 Documentation .....	10
6 Software quality management system .....	11
6.1 Objectives .....	11
6.2 Requirements .....	11
7 Software safety lifecycle requirements .....	12
7.1 General .....	12
7.2 Software safety requirements specification .....	18
7.3 Software safety validation planning .....	20
7.4 Software design and development .....	22
7.5 Programmable electronics integration (hardware and software) .....	28
7.6 Software operation and modification procedures .....	29
7.7 Software safety validation .....	29
7.8 Software modification .....	31
7.9 Software verification .....	33
8 Functional safety assessment .....	37
Annex A (normative) Guide to the selection of techniques and measures .....	38
Annex B (normative) Detailed tables .....	44
Annex C (informative) Bibliography .....	48
Tables	
1 Software safety lifecycle: overview .....	15
A.1 Software safety requirements specification (see 7.2) .....	39
A.2 Software design and development: software architecture design (see 7.4.3) .....	39
A.3 Software design and development: support tools and programming language (see 7.4.4) .....	40
A.4 Software design and development: detailed design (see 7.4.5 and 7.4.6) .....	40

Table	Page
A.5 Software design and development: software module testing and integration (see 7.4.7 and 7.4.8) .....	41
A.6 Programmable electronics integration (hardware and software) (see 7.5) .....	41
A.7 Software safety validation (see 7.7) .....	41
A.8 Modification (see 7.8) .....	42
A.9 Software verification (see 7.9) .....	42
A.10 Functional safety assessment (see clause 8) .....	43
B.1 Design and coding standards (referenced by table A.4) .....	44
B.2 Dynamic analysis and testing (referenced by tables A.5 and A.9) .....	44
B.3 Functional and black-box testing (referenced by tables A.5, A.6 and A.7) .....	45
B.4 Failure analysis (referenced by table A.10) .....	45
B.5 Modelling (referenced by table A.7) .....	45
B.6 Performance testing (referenced by tables A.5 and A.6) .....	46
B.7 Semi-formal methods (referenced by tables A.1, A.2 and A.4) .....	46
B.8 Static analysis (referenced by table A.9) .....	46
B.9 Modular approach (referenced by table A.4) .....	47
<b>Figures</b>	
1 Overall framework of this standard .....	9
2 E/E/PES safety lifecycle (in realisation phase) .....	13
3 Software safety lifecycle (in realisation phase) .....	13
4 Relationship between and scope of IEC 61508-2 and 61508-3 .....	14
5 Software safety integrity and the development lifecycle (the V-model) .....	14
6 Relationship between the hardware and software architectures of programmable electronics .....	18

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

## Part 3: Software requirements

### FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-3 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

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

FDIS	Report on voting
65A/269/FDIS	65A/277/RVD

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

Annexes A and B form an integral part of this standard.  
Annex C is for information only.

IEC 61508 consists of the following parts, under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems*:

- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

The contents of the corrigendum of April 1999 have been included in this copy.

## 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 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 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 use 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.

Withhold

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

IEC 61508-3:1998

<https://standards.iteh.ai/doc/iec/5638b9f8-e2eb-486d-8e3c-bd0550a44fc2/iec-61508-3-1998>



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

## Part 3: Software requirements

### 1 Scope

1.1 This part of IEC 61508

- a) is intended to be utilised only after a thorough understanding of IEC 61508-1 and IEC 61508-2;
- b) applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. Such software is termed safety-related software.
  - Safety-related software includes operating systems, system software, software in communication networks, human-computer interface functions, support tools and firmware as well as application programs.
  - Application programs include high level programs, low level programs and special purpose programs in limited variability languages (see 3.2.7 of IEC 61508-4).
- c) requires that the software safety functions and software safety integrity levels are specified.

NOTE 1 – If this has already been done as part of the specification of the E/E/PE safety-related systems (see 7.2 of IEC 61508-2), then it does not have to be repeated in this part.

NOTE 2 – Specifying the software safety functions and software safety integrity levels is an iterative procedure; see figures 2 and 6.

NOTE 3 – See clause 5 and annex A of IEC 61508-1 for documentation structure. The documentation structure may take account of company procedures, and of the working practices of specific application sectors.

- d) establishes requirements for safety lifecycle phases and activities which shall be applied during the design and development of the safety-related software (the software safety lifecycle model). These requirements include the application of measures and techniques, which are graded against the safety integrity level, for the avoidance of and control of faults and failures in the software.
- e) provides requirements for information relating to the software safety validation to be passed to the organisation carrying out the E/E/PES integration.
- f) provides requirements for the preparation of information and procedures concerning software needed by the user for the operation and maintenance of the E/E/PE safety-related system.
- g) provides requirements to be met by the organisation carrying out modifications to safety-related software.
- h) provides, in conjunction with IEC 61508-1 and IEC 61508-2, requirements for support tools such as development and design tools, language translators, testing and debugging tools, configuration management tools.

NOTE 4 – Figures 4 and 6 show the relationship between IEC 61508-2 and IEC 61508-3.

**1.2** Parts 1, 2, 3 and 4 of this standard 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 part 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*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications.

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.

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 in the USA and Canada, 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.

**1.3** Figure 1 shows the overall framework of parts 1 to 7 IEC 61508, and indicates the role that IEC 61508-3 plays in the achievement of functional safety for E/E/PE safety-related systems. Annex A of IEC 61508-6 describes the application of IEC 61508-2 and IEC 61508-3.

iTeh Standards  
(<https://standards.itih.ai>)  
Document Preview

IEC 61508-3:1998

<https://standards.itih.ai/standards/iec/5638b9f8-e2eb-486d-8e3c-bd0550a44fc2/iec-61508-3-1998>

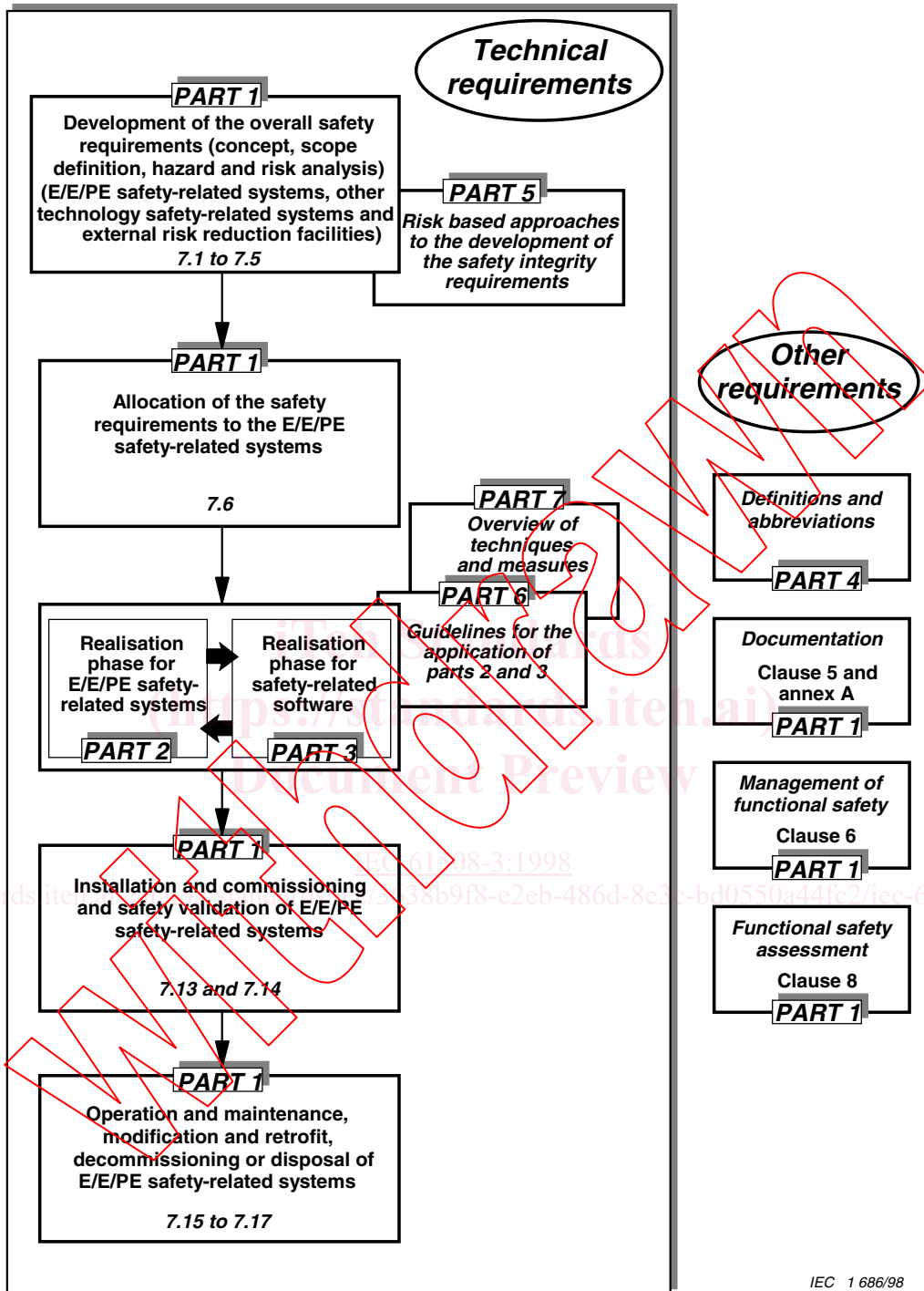


Figure 1 – Overall framework of this standard

## 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 61508. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and 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. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 61508-1:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, — *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electrical/programmable electronic safety-related systems* <sup>1)</sup>

IEC 61508-4:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations of terms*

IEC 61508-5:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6: —, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 6: Guidelines on the application of parts 2 and 3* <sup>1)</sup>

IEC 61508-7: —, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures* <sup>1)</sup>

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

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

## 3 Definitions and abbreviations

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

## 4 Conformance to this standard

The requirements for conformance to this standard are given in clause 4 of IEC 61508-1.

## 5 Documentation

The objectives and requirements for documentation are given in clause 5 of IEC 61508-1.

---

<sup>1)</sup> To be published.

## 6 Software quality management system

### 6.1 Objectives

The objectives are as detailed in 6.1 of IEC 61508-1.

### 6.2 Requirements

**6.2.1** The requirements are as detailed in 6.2 of IEC 61508-1 with the following additional requirements.

**6.2.2** The functional safety planning shall define the strategy for the software procurement, development, integration, verification, validation and modification to the extent required by the safety integrity level of the E/E/PE safety related system.

NOTE – The philosophy of this approach is to use the functional safety planning as an opportunity to customise this standard to take account of the varying safety integrity which is required in the E/E/PE safety-related system components. 7.4.2.8 of part 3 should be taken into account when E/E/PE safety-related system components of differing safety integrity levels are to be used together.

#### 6.2.3 Software configuration management should

- a) apply administrative and technical controls throughout the software safety lifecycle, in order to manage software changes and thus ensure that the specified requirements for software safety continue to be satisfied;
- b) guarantee that all necessary operations have been carried out to demonstrate that the required software safety integrity has been achieved;
- c) maintain accurately and with unique identification all configuration items which are necessary to maintain the integrity of the E/E/PE safety-related system. Configuration items include at least the following: safety analysis and requirements; software specification and design documents; software source code modules; test plans and results; pre-existing software components and packages which are to be incorporated into the E/E/PE safety-related system; all tools and development environments which are used to create or test, or carry out any action on, the software of the E/E/PE safety-related system;
- d) apply change-control procedures to prevent unauthorized modifications; to document modification requests; to analyse the impact of a proposed modification, and to approve or reject the request; to document the details of, and the authorisation for, all approved modifications; to establish configuration baseline at appropriate points in the software development, and to document the (partial) integration testing which justifies the baseline (see 7.8); to guarantee the composition of, and the building of, all software baselines (including the rebuilding of earlier baselines);

NOTE 1 – Management decision and authority is needed to guide and enforce the use of administrative and technical controls.

- e) document the following information to permit a subsequent audit: configuration status, release status, the justification for and approval of all modifications, and the details of the modification;
- f) formally document the release of safety-related software. Master copies of the software and all associated documentation should be kept to permit maintenance and modification throughout the operational lifetime of the released software.

NOTE 2 – For further information on configuration management, see ISO/IEC 12207.

## 7 Software safety lifecycle requirements

### 7.1 General

#### 7.1.1 Objective

The objective of the requirements of this subclause is to structure the development of the software into defined phases and activities (see table 1 and figures 2 to 5).

#### 7.1.2 Requirements

**7.1.2.1** A safety lifecycle for the development of software shall be selected and specified during safety planning in accordance with clause 6 of IEC 61508-1.

NOTE – A safety lifecycle model which satisfies the requirements of clause 7 of IEC 61508-1 may be suitably customised for the particular needs of the project or organisation.

**7.1.2.2** Quality and safety assurance procedures shall be integrated into safety lifecycle activities.

**7.1.2.3** Each phase of the software safety lifecycle shall be divided into elementary activities with the scope, inputs and outputs specified for each phase.

NOTE 1 – For further information on lifecycle phases, see ISO/IEC 12207

NOTE 2 – Clause 5 of IEC 61508-1 considers the outputs from the safety lifecycle phases. In the development of some E/E/PE safety-related systems, the output from some safety lifecycle phases may be a distinct document, while the documented outputs from several phases may be merged. The essential requirement is that the output of the safety lifecycle phase be fit for its intended purpose. In simple developments, some safety lifecycle phases may also be merged (see 7.4.5).

**7.1.2.4** Provided that the software safety lifecycle satisfies the requirements of figure 3 and table 1, it is acceptable to tailor the depth, number and work-size of the phases of the V-model (see figure 5) to take account of the safety integrity and the complexity of the project.

NOTE – The full list of lifecycle phases in table 1 is suitable for large newly developed systems. In small systems, it might be appropriate, for example, to merge the phases of software system design and architectural design.

**7.1.2.5** It is acceptable to order the software project differently from the organization of this standard (i.e. use another software safety lifecycle model), provided all the objectives and requirements of this clause are met.

**7.1.2.6** For each lifecycle phase, appropriate techniques and measures shall be used. Annexes A and B (guide to the selection of techniques and measures) give recommendations. Selecting techniques from annexes A and B does not guarantee by itself that the required safety integrity will be achieved.

**7.1.2.7** The results of the activities in the software safety lifecycle shall be documented (see clause 5).

**7.1.2.8** If at any stage of the software safety lifecycle, a change is required pertaining to an earlier lifecycle phase, then that earlier safety lifecycle phase and the following phases shall be repeated.