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

PART 6:
GUIDELINES ON THE APPLICATION OF IEC 61508-2 AND IEC 61508-3

This English-language version is derived from the original bilingual publication by leaving out all French-language pages. Missing page numbers correspond to the French-language pages.
INTERNATIONAL STANDARD  IEC 61508-6

First edition 2000-04

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 2000 Copyright - all rights reserved

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 the publisher.

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11  Telefax: +41 22 919 03 00  E-mail: inmail@iec.ch  Web: www.iec.ch

PRICE CODE  XB
For price, see current catalogue
## CONTENTS

FOREWORD ....................................................................................................................... 11
INTRODUCTION .................................................................................................................. 15

Clause
1 Scope ......................................................................................................................... ... 19
2 Normative references..................................................................................................... 23
3 Definitions and abbreviations ......................................................................................... 23

Annex A (informative)  Application of IEC 61508-2 and of IEC 61508-3 ................................ 25
A.1 General................................................................................................................. 25
A.2 Functional steps in the application of IEC 61508-2................................................ 29
A.3 Functional steps in the application of IEC 61508-3................................................ 37

Annex B (informative)  Example technique for evaluating probabilities of hardware failure ... 41
B.1 General................................................................................................................. 41
B.2 Average probability of failure on demand (for low demand mode of operation) ..... 49
B.3 Probability of failure per hour (for high demand or continuous mode of operation) .......................................................... 75
B.4 References........................................................................................................... 91

Annex C (informative)  Calculation of diagnostic coverage and safe failure fraction: worked example ................................................................................................................. .. 93

Annex D (informative)  A methodology for quantifying the effect of hardware-related common cause failures in E/E/PE systems ................................................................. 101
D.1 General............................................................................................................... 101
D.2 Brief overview ..................................................................................................... 101
D.3 Scope of the methodology................................................................................... 109
D.4 Points taken into account in the methodology ..................................................... 109
D.5 Using the \( \beta \)-factor to calculate the probability of failure in an E/E/PE safety-related system due to common cause failures ....................................................... 111
D.6 Using the tables to estimate \( \beta \)............................................................................. 113
D.7 Examples of the use of the methodology............................................................. 121
D.8 References......................................................................................................... 123

Annex E (informative)  Example applications of software safety integrity tables of IEC 61508-3 ................................................................................................................. .. 125
E.1 General............................................................................................................... 125
E.2 Example for safety integrity level 2 ..................................................................... 125
E.3 Example for safety integrity level 3 ..................................................................... 135

Bibliography ................................................................................................................... .... 145
Table B.9 – Example for a non-perfect proof test................................................................. 75
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........ 79
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..... 81
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....... 83
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........... 85
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)...................................................................................................................... 87
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)............................................................................................................................ 89
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).................................................................................................................... 89
Table C.1 – Example calculations for diagnostic coverage and safe failure fraction.............. 97
Table C.2 – Diagnostic coverage and effectiveness for different subsystems....................... 99
Table D.1 – Scoring programmable electronics or sensors/final elements......................... 115
Table D.2 – Value of Z: programmable electronics............................................................. 119
Table D.3 – Value of Z: sensors or final elements............................................................... 119
Table D.4 – Calculation of $\beta$ or $\beta_D$ ........................................................................... 121
Table D.5 – Example values for programmable electronics................................................. 123
Table E.1 – Software safety requirements specification (see 7.2 of IEC 61508-3)............... 127
Table E.2 – Software design and development: software architecture design (see 7.4.3 of IEC 61508-3).................................................................................................................. 129
Table E.3 – Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3)................................................................. 129
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).................................................................................................................. 131
Table E.5 – Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3)................................................................. 131
Table E.6 – Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3)............................................................................................... 131
Table E.7 – Software safety validation (see 7.7 of IEC 61508-3)........................................ 133
Table E.8 – Software modification (see 7.8 of IEC 61508-3)............................................. 133
Table E.9 – Software verification (see 7.9 of part 3).......................................................... 133
Table E.10 – Functional safety assessment (see clause 8 of IEC 61508-3)......................... 135
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.11</td>
<td>Software safety requirements specification (see 7.2 of IEC 61508-3)</td>
<td>137</td>
</tr>
<tr>
<td>E.12</td>
<td>Software design and development: software architecture design (see 7.4.3 of IEC 61508-3)</td>
<td>137</td>
</tr>
<tr>
<td>E.13</td>
<td>Software design and development: support tools and programming language (see 7.4.4 of IEC 61508-3)</td>
<td>139</td>
</tr>
<tr>
<td>E.14</td>
<td>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)</td>
<td>139</td>
</tr>
<tr>
<td>E.15</td>
<td>Software design and development: software module testing and integration (see 7.4.7 and 7.4.8 of IEC 61508-3)</td>
<td>141</td>
</tr>
<tr>
<td>E.16</td>
<td>Programmable electronics integration (hardware and software) (see 7.5 of IEC 61508-3)</td>
<td>141</td>
</tr>
<tr>
<td>E.17</td>
<td>Software safety validation (see 7.7 of IEC 61508-3)</td>
<td>141</td>
</tr>
<tr>
<td>E.18</td>
<td>Modification (see 7.8 of IEC 61508-3)</td>
<td>143</td>
</tr>
<tr>
<td>E.19</td>
<td>Software verification (see 7.9 of IEC 61508-3)</td>
<td>143</td>
</tr>
<tr>
<td>E.20</td>
<td>Functional safety assessment (see clause 8 of IEC 61508-3)</td>
<td>143</td>
</tr>
</tbody>
</table>
INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

1) The 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 specifications, 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.

IEC 61508-6 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:

<table>
<thead>
<tr>
<th>FDIS</th>
<th>Report on voting</th>
</tr>
</thead>
<tbody>
<tr>
<td>65A/295/FDIS</td>
<td>65A/304/RVD</td>
</tr>
</tbody>
</table>

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annexes A to E are 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 committee has decided that the contents of this publication will remain unchanged until 2005. At this date, the publication will be

• reconfirmed;
• withdrawn;
• replaced by a revised edition, or
• amended.
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.
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
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
