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 It supersedes BS EN 61508-6:2002 which is withdrawn.

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

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

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

© BSI 2010

ISBN 978 0 580 65448 0
ICS 13.260; 25.040.40; 29.020; 35.020

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

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

Amendments issued since publication

<table>
<thead>
<tr>
<th>Amd. No.</th>
<th>Date</th>
<th>Text affected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This is a preview of "BS EN 61508-6:2010". Click here to purchase the full version from the ANSI store.
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)
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– latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2013-05-01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:

### 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.

<table>
<thead>
<tr>
<th>Publication</th>
<th>Year</th>
<th>Title</th>
<th>EN/HD</th>
<th>Year</th>
</tr>
</thead>
</table>
## CONTENTS

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

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