

CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	7
2 Normative references	9
3 Definitions and abbreviations.....	9
Annex A (informative) Overview of techniques and measures for E/E/PE safety-related systems: control of random hardware failures (see IEC 61508-2).....	10
Annex B (informative) Overview of techniques and measures for E/E/PE safety related systems: avoidance of systematic failures (see IEC 61508-2 and IEC 61508-3).....	27
Annex C (informative) Overview of techniques and measures for achieving software safety integrity (see IEC 61508-3).....	54
Annex D (informative) A probabilistic approach to determining software safety integrity for pre-developed software	107
Annex E (informative) Overview of techniques and measures for design of ASICs	112
Annex F (informative) Definitions of properties of software lifecycle phases.....	126
Annex G (informative) Guidance for the development of safety-related object oriented software.....	132
Bibliography.....	134
Index	137
Figure 1 – Overall framework of IEC 61508.....	8
Table C.1 – Recommendations for specific programming languages	86
Table D.1 – Necessary history for confidence to safety integrity levels	107
Table D.2 – Probabilities of failure for low demand mode of operation	108
Table D.3 – Mean distances of two test points	109
Table D.4 – Probabilities of failure for high demand or continuous mode of operation	110
Table D.5 – Probability of testing all program properties	111
Table F.1 – Software Safety Requirements Specification	126
Table F.2 – Software design and development: software architecture design	127
Table F.3 – Software design and development: support tools and programming language.....	128
Table F.4 – Software design and development: detailed design	128
Table F.5 – Software design and development: software module testing and integration.....	129
Table F.6 – Programmable electronics integration (hardware and software).....	129
Table F.7 – Software aspects of system safety validation	130
Table F.8 – Software modification.....	130
Table F.9 – Software verification.....	131
Table F.10 – Functional safety assessment	131
Table G.1 – Object Oriented Software Architecture	132
Table G.2 – Object Oriented Detailed Design.....	133
Table G.3 – Some Oriented Detailed terms	133