

Contents

Foreword	IX
Acknowledgements.....	X
1. Scope	1
2. Terms, Definitions and Acronyms	2
2.1 Terms and Definitions	2
2.2 Acronyms	4
3. Overview of IEC 61511	6
3.1 Background.....	6
3.2 Scope and Application of IEC 61511	6
3.3 Relationship between IEC 61508 and IEC 61511	7
3.4 IEC 61511	7
3.5 Lifecycle Approach	8
3.6 Potential Issues with IEC 61511-1	10
4. Legal Aspects	14
4.1 Health and Safety Legislation	14
4.2 Other Health and Safety Legislation	15
4.3 Application to Existing Installations	16
4.4 Civil Liabilities.....	17
5. Common Requirements for all Activities	18
5.1 Responsibilities	18
5.2 Competency.....	19
5.3 Planning.....	21
5.4 Verification.....	22
5.5 Validation	22
5.6 Functional Safety Assessment.....	24
5.7 Audit and Revision	27
5.8 Conformity Assessment.....	27
5.9 Management of Lifecycle Activities	28
5.10 Documentation.....	29
5.11 Change Control and Configuration Management	31

6. Requirements for Specific Activities	32
6.1 Front End Activities.....	32
6.2 Hazard and Risk Assessment and Allocation.....	33
6.3 Functional Safety Requirements	40
6.4 Application Design and Engineering	42
6.5 Integration.....	50
6.6 Equipment Procurement	57
6.7 SIS Installation.....	60
6.8 SIS Commissioning and Process Commissioning	62
6.9 Operation and Maintenance	66
6.10 Modification and Decommissioning	70
7. References.....	72
7.1 Standards Referenced.....	72
7.2 Publications Referenced	73
7.3 Further Reading.....	76
Annex A – Technology Issues.....	77
A.1 Introduction	77
A.2 Assessment and Certification.....	77
A.3 AK Certification versus SIL.....	78
A.4 SIS Architecture	78
A.5 Technologies for Logic Solvers.....	78
Annex B – Example Functional Safety Plan Overview	85
Annex C – Example Competency Scheme.....	88
C.1 Generic Competence Standard	88
C.2 Customised Competence Standard	88
C.3 Assessment Process.....	89
C.4 Competence Management System	90
Annex D – Example Supplier Safety Validation Plan	96
D.1 General.....	96
D.2 Competency	96
D.3 Modifications.....	96
D.4 Specification	97
D.5 Random Hardware Failures.....	97
D.6 Systematic Capability	97
D.7 Assessment of Modules	97
D.8 Language and Tools.....	97
D.9 Code Review and Test.....	97
D.10 Validation	97

Annex E – Reliability and Data Considerations	102
E.1 Device Reliability Data	102
E.2 Function Reliability Analysis	102
E.3 Other Factors affecting Function Reliability	104
E.4 Analysis of Failure Data.....	108
Annex F – Reliability Calculation Method	111
F.1 Terminology.....	111
F.2 Basic Reliability Model	112
F.3 Combining Elements in Series.....	113
F.4 Combining Elements in Parallel.....	114
F.5 Complex Redundancy.....	115
F.6 Mean Time Before Failure.....	116
F.7 Availability and Average Probability of Failure.....	117
F.8 Redundant Systems.....	122
F.9 Proof Testing Strategy	124
F.10 Common Cause Failures	125
F.11 General Formulae for Fault Tolerant Systems.....	126
Annex G – ALARP	129
G.1 General.....	130
G.2 Methods	131
G.3 Calibrating Risk Assessment Tools	132
G.4 Hierarchy of Controls	133
G.5 Cost Benefit Analysis.....	134
Annex H – Tolerable Risk Criteria	137
H.1 UK Legislation and Regulation.....	137
H.2 Individual Frequency of Fatality	139
H.3 Societal Risk.....	142
Annex I – Random and Systematic Failures.....	144
I.1 Random Hardware Failures	144
I.2 Systematic Failures.....	145
I.3 Consequences of Systematic Failures	146
Annex J – Complex Functional Safety	148
J.1 Introduction.....	148
J.2 The Combustion Process	151
J.3 Double Block and Vent Philosophy.....	151
J.4 Safety Function Integrity Requirements.....	152
J.5 Valve Proving Philosophy	152
J.6 Control Philosophy	153

J.7 Gas Isolation Function Failure	155
J.8 Fault Tree.....	156
J.9 Failure Assessment	157
J.10 Final Assessment.....	161
Annex K – Selection of Equipment	162
K.1 SIF Design	162
K.2 Systematic Capability Explained	163
K.3 Conformity to IEC 61508 (Route 1 and Route 2)	163
K.4 Alternative Conformity to IEC 61511 (Prior Use).....	164
K.5 Selection of Components by the User	164
K.6 Hardware Fault Tolerance.....	165
K.7 SC as applied to Synthesis of Elements.....	165
EEMUA Publication: Feedback Form	168
EEMUA Publications Catalogue	169
 Tables	
Table 1 – Application of IEC 61508 and IEC 61511	8
Table B. 1 – Example Functional Safety Plan Overview	85
Table C. 1 – Example Generic Competence Standard.....	90
Table D. 1 – Quality and Functional Safety Control Matrix.....	98
 Figures	
Figure 1 – Safety lifecycle	9
Figure 2 – Functional Safety Lifecycle showing FSA	25
Figure H. 1 – R2P2 Tolerability of Risk	138
Figure H. 2 – Company Tolerability of Risk	139
Figure H. 3 – Societal Risk	142
Figure J. 1 – Double Block and Vent	151
Figure J. 2 – Double Block and Vent Fault Tree	156