



Technology Training that Works

Practical Industrial Safety, Risk Assessment and Shutdown Systems for Industry

Contents

Preface	i	
1	Introduction	1
1.1	Definition of safety instrumentation	1
1.2	What is this book about?	2
1.3	Why is this book necessary?	2
1.4	Contents of the book	3
1.5	Introduction to hazards and risks	3
1.6	Fatal accident rate (FAR)	5
1.7	Overview of safety systems engineering (SSE)	7
1.8	Why be systematic?	8
1.9	Introduction to standards: IEC 61508 and ISA S84	11
1.10	Equipment under control	17
1.11	The safety lifecycle model and its phases (SLC phases)	18
1.12	Implications of IEC 61508 for control systems	21
1.13	Summary	22
1.14	Safety lifecycle descriptions	23
1.15	Some websites for safety systems information	28
1.16	Bibliography and sources of information	29
1.17	Guidelines on sector standards	31
2	Hazards and risk reduction	37
2.1	Introduction	37
2.2	Consider hazards under some main subjects	38
2.3	Basic hazards of chemical process	39
2.4	Introduction to hazard studies and the IEC model	42
2.5	Process control versus safety control	45
2.6	Simple and complex shut-down sequences, examples	50
2.7	Protection layers	54
2.8	Risk reduction and classification	58



Technology Training that Works

2.9	Risk reduction terms and equations	61
2.10	The concept of safety integrity level (SIL)	63
2.11	Practical exercise	66
<hr/>		
3	Hazard studies	71
<hr/>		
3.1	Introduction	71
3.2	Information as input to the SRS	71
3.3	Outline of methodologies for hazard studies 1, 2 and 3	76
3.4	Process hazard study 2	78
3.5	Risk analysis and risk reduction steps in the hazard study	79
3.6	Interfacing hazard studies to the safety life cycle	84
3.7	Evaluating SIS requirements	85
3.8	Meeting IEC requirements	88
3.9	Hazard study 3	89
3.10	Conclusions	96
3.11	Fault trees as an aid to risk assessment and the development of protection schemes	96
3.12	Hazard study 2 guidelines	102
3.13	Hazard studies for computer systems	111
3.14	Data capture checklist for the hazard study	113
<hr/>		
4	Safety requirements specifications	117
<hr/>		
4.1	Developing overall safety requirements	117
4.2	Development of the SRS	119
4.3	Documenting the SRS	125
4.4	Determining the safety integrity	132
4.5	Summary of this chapter	144
<hr/>		
5	Technology choices and the conceptual design stage	145
<hr/>		
5.1	Introduction	145
5.2	What the standards say	146
5.3	Technologies for the logic solver	149
5.4	Development of safety PLCs	161
5.5	Classification and certification	179
5.6	Summary	179
5.7	SIS architecture conventions	179



Technology Training that Works

6	Basic reliability analysis applied to safety systems	183
6.1	Introduction	183
6.2	Design process	184
6.3	Failure modes	186
6.4	Reliability formulae	188
6.5	Analysis models and methods	190
6.6	Some design considerations	200
6.7	Summary of parameters used in the reliability analysis of the safety systems	209
6.8	Some sources of reliability data for instrumentation	210
6.9	Safety performance calculation packages and reliability databases	212
7	Safety in field instruments and devices	213
7.1	Introduction	213
7.2	Objectives	214
7.3	Field devices for safety	214
7.4	Sensor types	215
7.5	Guidelines for the application of field devices	223
7.6	Design requirements for field devices	235
7.7	Technology issues	238
7.8	Summary of field devices for safety	243
8	Engineering the safety system: hardware	245
8.1	Introduction	245
8.2	Project engineering	245
8.3	Activities in box 9	248
8.4	ISA clause 7: SIS detailed design:	252
8.5	Information flow and documents at the engineering stage	258
8.6	Conclusion	259
9	Engineering the application software	261
9.1	Introduction	261
9.2	Application software activity steps	270



Technology Training that Works

10	Overall planning (IEC phases 6, 7 and 8)	273
10.1	Introduction	273
10.2	Maintenance and operations planning	274
10.3	Validation planning	278
10.4	Installation and commissioning planning	279
10.5	IEC Phase 8: installation and commissioning planning	279
10.6	Summary	282
11	Installation and commissioning (IEC phase 12)	283
11.1	Introduction	283
11.2	Factory acceptance tests	284
11.3	Installation	289
11.4	Summary	297
11.5	Documentation required for the pre-startup acceptance test	298
12	Validation, operations and management of change (IEC phases 13, 14 and 15)	299
12.1	Introduction	299
12.2	Verification, validation and functional safety assessment	299
12.3	Operations, maintenance and repair	304
12.4	Functional testing	309
12.5	Management of change	313
12.6	Summary	316
13	Justification for a safety instrumented system	317
13.1	Introduction	317
13.2	Impact of safety system failures	318
13.3	Justification	320
Appendix A	Practical exercises	327
Appendix B	Glossary	369