



Technology Training that Works

Practical Safety Instrumentation & Emergency Shutdown Systems for Process Industries

Contents

1	Overview of safety instrumented systems	1
1.1	Summary of contents	1
1.2	Introduction and objectives	2
1.3	Safety system basics	4
1.4	Risk reduction and safety integrity	7
1.5	Protection layers	12
1.6	Safety management principles	16
1.7	The legal framework for process safety	25
1.8	New standards	33
1.9	The safety lifecycle	40
1.10	Setting SIL targets	43
1.11	Meeting SIL targets	49
1.12	Safety reliability versus availability for production	53
1.13	Introduction to safety PLCs	55
1.14	The cost of ownership	58
1.15	Management of functional safety	63
1.16	Conclusion of the overview chapter	66
2	Introduction to IEC 61511 and the safety lifecycle	67
2.1	Summary	67
2.2	Introduction	67
2.3	Safety Life Cycles (SLC)	68
2.4	IEC 61511 safety life cycle	72
2.5	Conclusions	83



Technology Training that Works

3	Hazop methods and hazard analysis for defining risk reduction requirements	85
3.1	Summary	85
3.2	Introduction	86
3.3	Background	87
3.4	The process hazard study lifecycle	88
3.5	Lifecycle models for hazard studies	91
3.6	Methodologies for hazard study 1	92
3.7	Process hazard study 2	95
3.8	Guideword diagrams and hazard summary table	98
3.9	Risk analysis and risk reduction measures	99
3.10	Practical example of hazard 2 application	103
3.11	Interfacing hazard studies to the IEC 61511 SLC	103
3.12	Evaluating SIS requirements	104
3.13	Software tools for PHA	105
3.14	Introduction to Hazop	105
3.15	Overview of HAZOP method	107
3.16	Points to note on the examination procedure	126
4	Principles of risk reduction & safety allocations	149
4.1	Summary	149
4.2	Introduction	150
4.3	Learning Objectives	150
4.4	Deciding risk reduction targets	152
4.5	Layers of protection and the allocation of safety functions	153
4.6	Alarms, and do they qualify as safeguards?	157
4.7	Principles of risk reduction	162
4.8	The quantitative method for SIL determination	168
4.9	Deciding between demand mode and continuous mode	169
4.10	Practical exercise	171
4.11	The conceptual design phase	171



Technology Training that Works

4.12	Conclusion to the allocations phase	172
4.13	Preparing the safety requirements specification	172
4.14	Conclusions on the safety allocations and requirements phases	181
5	Practical SIL determination methods based on IEC 61511	191
5.1	Summary	191
5.2	Introduction	191
5.3	Introduction to part 3 of IEC 61511	193
5.4	Semi quantitative method for SIL	194
5.5	The safety layer matrix (Annex C)	195
5.6	Risk graph methods (Annexes D and E)	197
5.7	Software tools using risk graphs	208
5.8	Practical exercises in SIL determination	208
5.9	Conclusions	208
6	Practical SIS configurations for safety and availability targets	209
6.1	Summary	209
6.2	Introduction	209
6.3	The design process	210
6.4	Safety reliability versus availability for production	214
6.5	Architectures and fault tolerance concepts	215
6.6	Identification of sub-systems	217
6.7	Architectures needed to meet SIL ratings	222
6.8	Implications for equipment selection and costs	224
6.9	Conclusions	227
7	Practical selection of sensors and actuators for safety duties	229
7.1	Summary	229
7.2	Introduction	229



Technology Training that Works

7.3	Field devices for safety	231
7.4	Sensor types	232
7.5	Guidelines for application of field devices	240
7.6	Qualification requirements for field devices	249
7.7	Instrument Selection	251
7.8	Technology issues	253
7.9	Summary of field devices for safety	259
<hr/>		
8	Practical reliability analysis methods to IEC 61511	261
<hr/>		
8.1	Summary	261
8.2	Introduction	261
8.3	Introduction to reliability analysis	263
8.4	Failure modes	266
8.5	Reliability formulae	268
8.6	Analysis models and methods	270
8.7	Some design considerations	279
8.8	Markov models	285
8.9	Reliability calculation software tools	288
8.10	Summary	289
<hr/>		
9	Design and selection of safety controllers	291
<hr/>		
9.1	Summary	291
9.2	Introduction	291
9.3	Technologies for the logic solver	292
9.4	Development of safety PLCs	304
9.5	Characteristics of safety PLCs	309
9.6	The alternative approach of IEC 61511	318
9.7	Developments in safety control technology	320
9.8	Classification and certification	327
9.9	Choosing the logic server	327
9.9	Summary	329



Technology Training that Works

10	Practical system integration and application software for safety controllers	331
10.1	Summary	331
10.2	Introduction	332
10.3	The problem with software	333
10.4	End user position	334
10.5	Basics of the software life cycle	335
10.6	Application software	337
10.7	Programming tools	340
10.8	IEC 61511 application software safety life cycle	341
10.9	Application software activity steps	345
10.10	Factory Acceptance Tests	345
10.11	Test facilities in development systems	350
10.12	Summary of software engineering	352
11	Practical documentation and validation of safety systems	353
11.1	Summary	353
11.2	Introduction and purpose	353
11.3	Documentation schedule for an SIS project	355
11.4	Document format examples	361
11.5	Verification, validation and functional safety assessment	371
11.6	Installation through to validation	374
11.7	Validation	379
11.8	Training of technicians and operators	381
11.9	Handover to operations	381
11.10	Conclusions	382
12	Diagnostics and proof testing of safety instrumentation	385
12.1	Summary	385
12.2	Introduction	385
12.3	Proof testing	386



Technology Training that Works

12.4	Diagnostics	395
12.5	Valve diagnostic methods	396
12.6	Improving the PFD values and optimizing test intervals	403
12.7	Conclusions	406
12.8	Appendix: Proof test interval calculation	406

Appendices	409
-------------------	------------

Appendix A: Glossary of terms and abbreviations used in safety-instrumented systems	409
Appendix B: Overview of the SLC based on table 1 of IEC 61508 part 1	417
Appendix C: References and sources of information	421
Appendix D: Guidelines on sector standards	427
Appendix E: Sources of reliability data and calculation packages	433
Appendix F: Summary of parameters used in the reliability analysis of safety systems	437
Appendix G: Composite safety integrity levels table	439
Appendix H: Hazard studies for computer systems	441
Practical exercises	445
Practical solutions	493