

Index

- Accident scenario, 225
- ALARP, 467
- Amelioration, 425
- Analysis Techniques
 - Barrier analysis, 335–351
 - Bent pin analysis, 353–364
 - Cause consequence analysis, 383–395
 - Common cause failure analysis, 397–422
 - Definition of, 31
 - Event tree analysis, 223–234
 - Failure mode and effects analysis, 235–259
 - Fault hazard analysis, 261–269
 - Fault tree analysis, 183–221
 - Functional hazard analysis, 271–289
 - HAZOP analysis, 365–381
 - Health hazard assessment, 155–168
 - Markov analysis, 317–333
 - MORT analysis, 423–430
 - Operating & support hazard analysis, 131–153
 - Petri net analysis, 307–316
 - Preliminary hazard analysis, 73–93
 - Preliminary hazard list, 55–72
 - Safety requirements/criteria analysis, 169–181
 - Sneak circuit analysis, 291–306
 - Software safety assessment, 431–449
 - Subsystem hazard analysis, 95–114
 - System hazard analysis, 115–129
- Analysis Types
 - Conceptual design hazard analysis type, 34
 - Definition of, 31
 - Detailed design hazard analysis type, 37
 - Health design hazard analysis type, 41
 - Operations design hazard analysis type, 40
 - Preliminary design hazard analysis type, 35
 - Requirements design hazard analysis type, 42
 - System design hazard analysis type, 38
- AND gate, 190
- Approximation formulas (fault tree), 201, 202
- As low as reasonably practical, 467
- Barrier, 337, 343
- Barrier analysis, 335–351
- Bent pin, 354, 355
- Bent pin analysis, 353–364
- Bottom-up analysis, 49
- Cable failure matrix analysis, 353
- Cascading failure, 401
- Cause consequence analysis, 383–395
- Combinatorial model, 319
- Commercial off the shelf, 468
- Common cause failure, 397, 400
- Common cause failure analysis, 397–422
- Common mode failure, 400
- Common mode failure analysis, 398

- Conceptual design hazard analysis type, 34
- COTS, 468
- Critical item list, 238
- Cut set, 191

- Deductive, 48
- Dependent event, 399
- Detailed design hazard analysis type, 37
- Deterministic process, 319
- Development lifecycle, 11
- Dynamic fault tree analysis, 218

- Energy trace and barrier analysis, 335
- Engineering development lifecycle model, 11
- Event tree, 223
- Event tree analysis, 223–234

- Failure, 237
- Failure cause, 238
- Failure effect, 238
- Failure mode, 237
- Failure mode and effects analysis, 235–259
- Failure mode effects and criticality analysis, 235
- Fault, 238
- Fault hazard analysis, 261–269
- Fault tree, 183
- Fault tree analysis, 183–221
- Fault tree approximation formulas, 201, 202
- Firmware, 433
- FMEA, 235–259
- FMECA, 235
- FTA, 183–221
- Function, 6
- Functional dependency gate, 218
- Functional flow diagram, 83
- Functional hazard analysis, 271–289
- Functional model, 241

- Guide word, 372

- Hazard, 15
- Hazard actuation, 19, 20
- Hazard barrier, 337, 343
- Hazard causal factor, 14, 18, 21
- Hazard checklist, 25, 62, 483
- Hazard components, 17
- Hazard example, 18
- Hazard mitigation, 475
- Hazard theory, 15
- Hazard triangle, 17
- Hazardous element, 17
- HAZOP analysis, 365–381

- Health design hazard analysis type, 41
- Health hazard assessment, 155–168
- HHA, 155–168

- Indenture level, 238
- Indentured equipment list, 83
- Indentured task list, 135, 136
- Independent event, 399
- Inductive, 48
- Initiating event, 225
- Initiating mechanism, 17
- Inhibit gate, 190
- Interlock, 474
- Intermittent failure, 243

- Less than adequate, 425

- Markov analysis, 317–333
- Minimal cut set, 191
- Mishap, 14
- Mishap risk, 16
- Mitigation, 475
- MORT analysis, 423–430
- Mutually exclusive event, 401

- NDI, 475
- Non developmental item, 475

- O&SHA, 131–153
- Operating & support hazard analysis, 131–153
- Operational sequence diagram, 141, 142
- Operations design hazard analysis type, 40
- OR gate, 190

- Petri net analysis, 307–316
- PHA, 73–93
- PHA worksheet, 79
- PHL, 55–72
- PHL worksheet, 61
- Pivotal event, 225
- Preliminary design hazard analysis type, 35
- Preliminary hazard analysis, 73–93
- Preliminary hazard list, 55–72
- Probabilistic risk assessment, 52, 385, 476
- Process FMEA, 242
- Product FMEA, 242

- Qualitative analysis, 51
- Quantitative analysis, 51

- Reachability, 309, 312
- Requirements design hazard analysis type, 42

- Residual risk, 477
- Risk, 15, 17
- Risk assessment, 478
- Risk mitigation, 475
- Risk priority number, 238

- Safety critical, 478
- Safety critical function, 478
- Safety critical function thread, 123,124
- Safety requirements/criteria analysis, 169–181
- SCA, 291–306
- SHA, 115–129
- SHRI, 435, 438
- Sneak, 293
- Sneak circuit, 291
- Sneak circuit analysis, 291–306
- Sneak label, 299, 300
- Sneak indicator, 300, 301
- Sneak path, 299, 300
- Sneak timing, 299, 300
- Software, 433
- Software FMEA, 243
- Software hazard risk index, 435, 438
- Software safety assessment, 431–449
- SRCA, 169–181
- SSHA, 95–114

- SSP, 481
- SSPP, 481
- State, 319
- State transition diagram, 319
- Stochastic process, 319
- Structural model, 241
- Subsystem, 480
- Subsystem hazard analysis, 95–114
- System, 6, 481
- System attributes, 7
- System design hazard analysis type, 38
- System function, 6
- System hazard analysis, 115–129
- System lifecycle, 9
- System safety, 3, 481
- System safety process, 4
- System safety program, 481
- System safety program plan, 481
- System safety requirement, 73

- Target/threat, 17
- Top-down analysis, 49
- Top level mishap
- Total risk, 482

- Validation, 482
- Verification, 482

