Contents

PREFACE

ACKNOWLEDGMENTS

1. System Safety and Hazard Analysis  1
   1.1 Introduction / 1
   1.2 The Need for Hazard Analysis / 2
   1.3 System Safety Background / 3
   1.4 System Safety Overview / 4
   1.5 System Safety Process / 6
   1.6 System Safety Standards / 7
   1.7 System Safety Principles / 7
   1.8 Key Terms / 8
   1.9 Summary / 9

2. Systems  10
   2.1 System Concept / 10
   2.2 System Attributes / 12
   2.3 System Types / 13
   2.4 System Life Cycle / 13
   2.5 System Development / 15
   2.6 System Development Process / 16
   2.7 System Hierarchy / 16
   2.8 System Views / 18
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.9</td>
<td>System Development Artifacts</td>
<td>19</td>
</tr>
<tr>
<td>2.10</td>
<td>Systems Complexity and Safety</td>
<td>20</td>
</tr>
<tr>
<td>2.11</td>
<td>System Requirements</td>
<td>21</td>
</tr>
<tr>
<td>2.12</td>
<td>System Laws</td>
<td>26</td>
</tr>
<tr>
<td>2.13</td>
<td>Summary</td>
<td>26</td>
</tr>
<tr>
<td>3</td>
<td>Hazards, Mishap, and Risk</td>
<td>28</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>28</td>
</tr>
<tr>
<td>3.2</td>
<td>Hazard, Mishap, and Risk Definitions</td>
<td>29</td>
</tr>
<tr>
<td>3.3</td>
<td>Accident (Mishap) Theory</td>
<td>30</td>
</tr>
<tr>
<td>3.4</td>
<td>The Hazard–Mishap Relationship</td>
<td>31</td>
</tr>
<tr>
<td>3.5</td>
<td>Hazard Risk</td>
<td>33</td>
</tr>
<tr>
<td>3.6</td>
<td>The Components of a Hazard</td>
<td>33</td>
</tr>
<tr>
<td>3.7</td>
<td>Hazard Triangle</td>
<td>35</td>
</tr>
<tr>
<td>3.8</td>
<td>Hazard Actuation</td>
<td>35</td>
</tr>
<tr>
<td>3.9</td>
<td>Hazard Causal Factors</td>
<td>37</td>
</tr>
<tr>
<td>3.10</td>
<td>Hazard–Mishap Probability Example</td>
<td>39</td>
</tr>
<tr>
<td>3.11</td>
<td>Recognizing Hazards</td>
<td>40</td>
</tr>
<tr>
<td>3.12</td>
<td>Hazard Description</td>
<td>43</td>
</tr>
<tr>
<td>3.13</td>
<td>Hazard Theory Summary</td>
<td>43</td>
</tr>
<tr>
<td>4</td>
<td>Hazard Analysis Features</td>
<td>45</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>45</td>
</tr>
<tr>
<td>4.2</td>
<td>Types Versus Technique</td>
<td>46</td>
</tr>
<tr>
<td>4.3</td>
<td>Description of Hazard Analysis Types</td>
<td>48</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Conceptual Design Hazard Analysis Type</td>
<td>48</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Preliminary Design Hazard Analysis Type</td>
<td>49</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Detailed Design Hazard Analysis Type</td>
<td>51</td>
</tr>
<tr>
<td>4.3.4</td>
<td>System Design Hazard Analysis Type</td>
<td>52</td>
</tr>
<tr>
<td>4.3.5</td>
<td>Operations Design Hazard Analysis Type</td>
<td>53</td>
</tr>
<tr>
<td>4.3.6</td>
<td>Human Health Design Hazard Analysis Type</td>
<td>54</td>
</tr>
<tr>
<td>4.3.7</td>
<td>Requirements Design Hazard Analysis Type</td>
<td>55</td>
</tr>
<tr>
<td>4.4</td>
<td>The Timing of Hazard Analysis Types</td>
<td>57</td>
</tr>
<tr>
<td>4.5</td>
<td>The Interrelationship of Hazard Analysis Types</td>
<td>57</td>
</tr>
<tr>
<td>4.6</td>
<td>Hazard Analysis Techniques</td>
<td>59</td>
</tr>
<tr>
<td>4.7</td>
<td>Hazard Analysis Technique Attributes</td>
<td>59</td>
</tr>
<tr>
<td>4.8</td>
<td>Primary and Secondary Techniques</td>
<td>59</td>
</tr>
<tr>
<td>4.9</td>
<td>Inductive and Deductive Techniques</td>
<td>63</td>
</tr>
<tr>
<td>4.10</td>
<td>Qualitative and Quantitative Techniques</td>
<td>65</td>
</tr>
<tr>
<td>4.11</td>
<td>Summary</td>
<td>67</td>
</tr>
</tbody>
</table>
5. Hazard Recognition and Management 69
   5.1 Introduction / 69
   5.2 Hazard Analysis Tasks / 69
      5.2.1 Plan the Hazard Analysis / 70
      5.2.2 Understand the System Design / 71
      5.2.3 Acquire Hazard Analysis Tools / 71
      5.2.4 Identify Hazards / 72
      5.2.5 Validate Hazards / 72
      5.2.6 Assess Risk / 72
      5.2.7 Mitigate Risk / 72
      5.2.8 Verify Mitigation / 73
      5.2.9 Accept Risk / 73
      5.2.10 Track Hazards / 73
   5.3 Hazard Recognition / 74
      5.3.1 Hazard Recognition Introduction / 74
      5.3.2 Hazard Recognition: System Perspectives / 74
      5.3.3 Hazard Recognition: Failure Perspectives / 75
      5.3.4 Key Hazard Recognition Factors / 76
      5.3.5 Hazard Recognition Basics / 79
      5.3.6 Hazard Recognition Sources / 79
   5.4 Describing the Identified Hazard / 79
   5.5 Hazard Types by General Circumstances / 81
   5.6 Hazard Types by Analysis Category / 82
   5.7 Modelling Hazard Space / 83
      5.7.1 System Mishap Model / 84
      5.7.2 System Mishap Model Examples / 87
   5.8 Summary / 92

6. Functional Hazard Analysis 93
   6.1 FHA Introduction / 93
   6.2 FHA Background / 93
   6.3 FHA History / 94
   6.4 FHA Theory / 94
   6.5 FHA Methodology / 95
   6.6 FHA Worksheets / 96
   6.7 FHA Example 1: Aircraft Flight Functions / 99
   6.8 FHA Example 2: Aircraft Landing Gear Software / 99
   6.9 FHA Example 3: Ace Missile System / 102
   6.10 FHA Advantages and Disadvantages / 105
   6.11 Common FHA Mistakes to Avoid / 105
   6.12 FHA Summary / 108
10. System Hazard Analysis 164
10.1 SHA Introduction / 164
10.2 SHA Background / 165
10.3 SHA History / 166
10.4 SHA Theory / 166
10.5 SHA Methodology / 167
10.6 SHA Worksheet / 167
10.7 SHA Guidelines / 170
10.8 SHA Example / 172
10.9 SHA Advantages and Disadvantages / 175
10.10 Common SHA Mistakes to Avoid / 175
10.11 SHA Summary / 176

11. Operating and Support Hazard Analysis 177
11.1 O&SHA Introduction / 177
11.2 O&SHA Background / 177
11.3 O&SHA History / 178
11.4 O&SHA Definitions / 179
11.4.1 Operation / 179
11.4.2 Procedure / 179
11.4.3 Task / 179
11.5 O&SHA Theory / 180
11.6 O&SHA Methodology / 181
11.7 O&SHA Worksheet / 183
11.8 O&SHA Hazard Checklists / 185
11.9 O&SHA Support Tools / 186
11.10 O&SHA Guidelines / 187
11.11 O&SHA Examples / 188
11.11.1 Example 1 / 188
11.11.2 O&SHA Example 2 / 188
11.12 O&SHA Advantages and Disadvantages / 198
11.13 Common O&SHA Mistakes to Avoid / 198
11.14 Summary / 198

12. Health Hazard Analysis 199
12.1 HHA Introduction / 199
12.2 HHA Background / 199
12.3 HHA History / 200
12.4 HHA Theory / 200
15.5.1 FT Building Blocks / 245
15.5.2 FT Definitions / 247
15.5.3 FT Construction: Basics / 248
15.5.4 FT Construction: Advanced / 251
15.5.5 FT Construction Rules / 252
15.6 Functional Block Diagrams / 253
15.7 FT Cut Sets / 254
15.8 MOCUS Algorithm / 254
15.9 Bottom-Up Algorithm / 256
15.10 FT Mathematics / 256
  15.10.1 Probability of Success / 256
  15.10.2 Probability of Failure / 256
  15.10.3 Boolean Rules for FTA / 256
  15.10.4 AND Gate Probability Expansion / 257
  15.10.5 OR Gate Probability Expansion / 257
  15.10.6 FT Probability Expansion / 257
  15.10.7 Inclusion–Exclusion Approximation / 257
15.11 Probability / 258
15.12 Importance Measures / 259
  15.12.1 Cut Set Importance / 260
  15.12.2 Fussell–Vesely Importance / 260
  15.12.3 Risk Reduction Worth / 261
  15.12.4 Risk Achievement Worth / 261
  15.12.5 Birnbaum’s Importance Measure / 261
15.13 FT Example 1 / 262
15.14 FT Example 2 / 262
15.15 FT Example 3 / 271
15.16 Phase- and Time-Dependent FTA / 271
15.17 Dynamic FTA / 274
15.18 FTA Advantages and Disadvantages / 275
15.19 Common FTA Mistakes to Avoid / 276
15.20 Summary / 276

16. Failure Mode and Effects Analysis / 278
  16.1 FMEA Introduction / 278
  16.2 FMEA Background / 278
  16.3 FMEA History / 279
  16.4 FMEA Definitions / 280
  16.5 FMEA Theory / 281
     16.5.1 FMEA Structural and Functional Models / 283
     16.5.2 FMEA Product and Process FMEA / 283
# 16. FMEA

16.5.3 FMEA Functional Failure Modes / 283
16.5.4 FMEA Hardware Failure Modes / 284
16.5.5 FMEA Software Failure Modes / 285
16.5.6 Quantitative Data Sources / 286

16.6 Methodology / 286
16.7 FMEA Worksheet / 289
16.8 FMEA Example 1: Hardware Product FMEA / 292
16.9 FMEA Example 3: Functional FMEA / 292
16.10 FMEA Level of Detail / 295
16.11 FMEA Advantages and Disadvantages / 298
16.12 Common FMEA Mistakes to Avoid / 298
16.13 FMEA Summary / 298

# 17. Hazard and Operability (HAZOP) Analysis

17.1 Introduction / 300
17.2 HAZOP Analysis Background / 301
17.3 HAZOP History / 301
17.4 HAZOP Theory / 302
17.5 HAZOP Methodology / 303
  17.5.1 Design Representations / 305
  17.5.2 System Parameters / 305
  17.5.3 Guide Words / 306
  17.5.4 Deviation from Design Intent / 307
17.6 HAZOP Worksheet / 309
17.7 HAZOP Example 1 / 310
17.8 HAZOP Example 2 / 311
17.9 HAZOP Advantages and Disadvantages / 311
17.10 Common HAZOP Analysis Mistakes to Avoid / 313
17.11 HAZOP Summary / 313

# 18. Event Tree Analysis (ETA)

18.1 ETA Introduction / 316
18.2 ETA Background / 316
18.3 ETA History / 317
18.4 ETA Definitions / 317
18.5 ETA Theory / 318
18.6 ETA Methodology / 320
18.7 ETA Worksheet / 323
18.8 ETA Example 1 / 323
18.9 ETA Example 2 / 323
18.10 ETA Example 3 / 324
18.11 ETA Example 4 / 324
18.12 ETA Advantages and Disadvantages / 324
18.13 Common ETA Mistakes to Avoid / 325
18.14 Summary / 326

19. **Cause—Consequence Analysis** / 327

19.1 Introduction / 327
19.2 CCA Background / 327
19.3 CCA History / 328
19.4 CCA Definitions / 328
19.5 CCA Theory / 329
19.6 CCA Methodology / 330
19.7 CCD Symbols / 331
19.8 CCA Worksheet / 332
19.9 CCA Example 1: Three-Component Parallel System / 332
19.10 CCA Example 2: Gas Pipeline System / 333
19.10.1 Reducing Repeated Events / 335
19.11 CCA Advantages and Disadvantages / 337
19.12 Common CCA Mistakes to Avoid / 338
19.13 Summary / 338

20. **Common Cause Failure Analysis** / 339

20.1 Introduction / 339
20.2 CCFA Background / 340
20.3 CCFA History / 340
20.4 CCFA Definitions / 341
20.4.1 Independent Event / 341
20.4.2 Dependent Event / 341
20.4.3 Independence (in Design) / 341
20.4.4 Dependence (in Design) / 341
20.4.5 Common Cause Failure / 342
20.4.6 Common Mode Failure / 342
20.4.7 Cascading Failure / 343
20.4.8 Mutually Exclusive Events / 343
20.4.9 CCF Root Cause / 343
20.4.10 CCF Coupling Factor / 343
20.4.11 Common Cause Component Group / 343
20.5 CCFA Theory / 344
20.6 CCFA Methodology / 346
20.6.1 CCFA Process Step 2: Initial System Fault Tree Model / 347
20.6.2 CCFA Process Step 3: Common Cause Screening / 348
20.6.3 CCFA Process Step 4: Detailed CCF Analysis / 351
20.7 CCF Defense Mechanisms / 354
20.8 CCFA Example / 354
20.9 CCFA Models / 358
20.10 CCFA Advantages and Disadvantages / 359
20.11 Common CCFA Mistakes to Avoid / 360
20.12 Summary / 361

21. Software Hazard Analysis 363

21.1 SwHA Introduction / 363
21.2 SwHA Background / 364
21.3 SwHA History / 365
21.4 SwHA Theory / 365
21.5 SwHA Methodology / 366
21.6 SwHA Worksheet / 367
21.7 Software Criticality Level / 368
21.8 SwHA Example / 369
21.9 Software Fault Tree Analysis / 376
21.10 SwHA Advantages and Disadvantages / 377
21.11 SwHA Mistakes to Avoid / 379
21.12 SwHA Summary / 379

22. Process Hazard Analysis 381

22.1 PHA Introduction / 381
22.2 PHA Background / 381
22.3 PHA History / 382
22.4 Processing Mishaps / 382
22.5 Process Safety Management / 383
22.6 PHA Theory / 384
22.7 PHA Methodology / 385
22.8 PHA Worksheet / 386
22.9 Supporting Notes / 387
22.10 PHA Advantages and Disadvantages / 388
22.11 Common PHA Mistakes to Avoid / 389
22.12 Summary / 389

23. Test Hazard Analysis 390

23.1 THA Introduction / 390
23.2 THA Background / 390
23.3 THA History / 391
23.4 THA Theory / 391
23.5 THA Methodology / 393
23.6 THA Worksheet / 394
23.7 THA Considerations / 395
  23.7.1 Verification / 395
  23.7.2 Validation / 395
23.8 Testing in the System Development Life Cycle / 396
23.9 Types of Testing / 397
  23.9.1 Standard Development Test Types / 397
  23.9.2 Performance Tests / 397
  23.9.3 Software Performance Tests / 397
  23.9.4 Special Safety-Related Testing / 398
23.10 THA Safety Goals / 398
23.11 THA Advantages and Disadvantages / 404
23.12 Common THA Mistakes to Avoid / 404
23.13 Summary / 404

24. Fault Hazard Analysis 406

  24.1 FHA Introduction / 406
  24.2 FHA Background / 406
  24.3 FHA History / 407
  24.4 FHA Theory / 407
  24.5 FHA Methodology / 408
  24.6 FHA Worksheet / 410
  24.7 FHA Example / 411
  24.8 FHA Advantages and Disadvantages / 414
  24.9 Common FHA Mistakes to Avoid / 414
  24.10 Summary / 414

25. Sneak Circuit Analysis 416

  25.1 SCA Introduction / 416
  25.2 SCA Background / 417
  25.3 SCA History / 418
  25.4 SCA Definitions / 418
  25.5 SCA Theory / 419
  25.6 SCA Methodology / 419
    25.6.1 Step 1: Acquire Data / 420
    25.6.2 Step 2: Code Data / 421
    25.6.3 Step 3: Process Data / 421
    25.6.4 Step 4: Produce Network Trees / 422
25.6.5 Step 5: Identify Topographs / 422
25.6.6 Step 6: Perform Analysis / 423
25.6.7 Step 7: Generate SCA Report / 424

25.7 Example 1: Sneak Path / 424
25.8 Example 2: Sneak Label / 425
25.9 Example 3: Sneak Indicator / 425
25.10 Example Sneak Clues / 425
25.11 Software Sneak Circuit Analysis / 425
25.12 SCA Advantages and Disadvantages / 428
25.13 Common SCA Mistakes to Avoid / 428
25.14 Summary / 429

26. Markov Analysis / 430

26.1 MA Introduction / 430
26.2 MA Background / 430
26.3 MA History / 431
26.4 MA Definitions / 431
26.5 MA Theory / 432
26.6 MA Methodology / 434
   26.6.1 State Transition Diagram Construction / 434
   26.6.2 State Equation Construction / 436
26.7 MA Examples / 438
   26.7.1 Markov Chain / 438
   26.7.2 Markov Model of Two-Component Series System with No Repair / 438
   26.7.3 Markov Model of Two-Component Parallel System with No Repair / 439
   26.7.4 Markov Model of Two-Component Parallel System with Component Repair / 439
   26.7.5 Markov Model of Two-Component Parallel System with Component/System Repair / 440
   26.7.6 Markov Model of Two-Component Parallel System with Sequencing / 440
26.8 MA and FTA Comparisons / 441
26.9 MA Advantages and Disadvantages / 442
26.10 Common MA Mistakes to Avoid / 445
26.11 Summary / 445

27. Petri Net Analysis / 446

27.1 PNA Introduction / 446
27.2 PNA Background / 447
27.3 PNA History / 447
27.4 PNA Definitions / 448
27.5 PNA Theory / 448
27.6 PNA Methodology / 452
27.7 PNA Example / 452
27.8 PNA Advantages and Disadvantages / 453
27.9 Common PNA Mistakes to Avoid / 454
27.10 Summary / 454

28. Barrier Analysis / 456

28.1 BA Introduction / 456
28.2 BA Background / 456
28.3 BA History / 457
28.4 BA Definitions / 457
28.4.1 Energy Source / 458
28.4.2 Energy Path / 458
28.4.3 Energy Barrier / 458
28.5 BA Theory / 458
28.6 BA Methodology / 459
28.6.1 Example Checklist of Energy Sources for BA / 460
28.6.2 BA Considerations / 463
28.7 BA Worksheet / 465
28.8 BA Example / 467
28.9 BA Advantages and Disadvantages / 469
28.10 Common Barrier Analysis Mistakes to Avoid / 469
28.11 Summary / 470

29. Bent Pin Analysis / 471

29.1 BPA Introduction / 471
29.2 BPA Background / 471
29.3 BPA History / 472
29.4 BPA Theory / 472
29.5 BPA Methodology / 474
29.6 BPA Worksheet / 474
29.7 BPA Example / 476
29.8 BPA Advantages and Disadvantages / 478
29.9 Common BPA Mistakes to Avoid / 478
29.10 Summary / 482

30. Management Oversight Risk Tree Analysis / 483

30.1 Introduction To MORT Analysis / 483
30.2 MORT Background / 483
30.3 MORT History / 484
30.4 MORT Theory / 484
30.5 MORT Methodology / 485
30.6 MORT Analysis Worksheet / 486
30.7 MORT Advantages and Disadvantages / 487
30.8 Common MORT Analysis Mistakes to Avoid / 489
30.9 MORT Summary / 489

31. Job Hazard Analysis 490
31.1 JHA Introduction / 490
31.2 JHA Background / 491
31.3 JHA History / 492
31.4 JHA Theory / 492
31.5 JHA Methodology / 493
31.6 JHA Worksheet / 497
31.7 Example Hazard Checklist / 499
31.8 JHA Tool / 501
31.9 JHA Example / 502
31.10 JHA Advantages and Disadvantages / 502
31.11 Common JHA Mistakes to Avoid / 505
31.12 Summary / 505

32. Threat Hazard Analysis 506
32.1 THA Introduction / 506
32.2 THA Background / 506
32.3 THA History / 507
32.4 THA Theory / 507
32.5 THA Methodology / 509
   32.5.1 Cradle-to-Grave Sequences / 509
   32.5.2 Threat Scenarios / 510
   32.5.3 Characterization of Environments / 511
   32.5.4 Threats / 511
32.6 THA Worksheet / 511
32.7 THA Example / 515
32.8 THA Advantages and Disadvantages / 518
32.9 Common THA Mistakes to Avoid / 518
32.10 Summary / 518

33. System of Systems Hazard Analysis 520
33.1 SoSHA Introduction / 520
33.2 SoSHA Background / 521
33.3 SoSHA History / 522
33.4 SoS Theory / 522
33.5 SoS Safety and Hazards / 526
33.6 SoSHA Tools / 528
   33.6.1 SMM / 528
   33.6.2 SoS Component System Matrix / 530
33.7 SoSHA Methodology / 531
33.8 SoSHA Example / 533
33.9 SoSHA Worksheet / 534
33.10 SoSHA Guidelines / 535
33.11 SoSHA Advantages and Disadvantages / 535
33.12 Common SoSHA Mistakes to Avoid / 535
33.13 Summary / 536

34. Summary 537

34.1 Tenets of Hazard Analysis / 537
34.2 Description of Tenets / 538
   34.2.1 Hazards and Mishaps are Not Chance Events;
       Hazards Lead to Mishaps If Left Unchecked / 538
   34.2.2 Hazards are Created During System Design and Exist
       with the Design / 538
   34.2.3 Hazards are Comprised of Three Components: HA,
       IMs, and TTO / 539
   34.2.4 Many Hazards Cannot be Eliminated due to the Hazard
       Sources that are Required by the System / 540
   34.2.5 Hazards Present Risk; Risk is the Metric for Measuring the
       Criticality or Danger Level of a Hazard / 541
   34.2.6 Hazards can be Modified via Design Methods, which in
       Turn can Reduce Risk / 541
   34.2.7 Hazard Analysis is the Key to Preventing Mishaps;
       Hazard Identification and Mitigation Reduce Mishap Risk / 543
   34.2.8 The System Mishap Model is an Effective Hazard
       Analysis Tool / 543
   34.2.9 Hazard Analysis and Hazard Descriptions can
       Easily Become Abused, Confused, and/or Misused / 544
   34.2.10 Utilizing More than One Hazard Analysis Technique is
       Recommended / 544
   34.2.11 Hazard Mitigation is not Hazard Elimination / 545
   34.2.12 Hazard Risk is the Same as Mishap Risk / 546
34.2.13 There are Both Primary and Secondary Hazard Analysis Techniques / 546
34.2.14 There are Pseudo-Hazards and Real Hazards / 546
34.3 FINIS / 547

Appendix A List of Acronyms 549
Appendix B Glossary 552
Appendix C Hazard Checklists 567
Appendix D References 609
Index 613