Preface **1**
Chapter 1 — Risk Management **1**
Introduction 1
Technical, Process and Occupational Safety 3
Historical Development 4
1. Safety as a Value 5
2. Codes and Standards 6
3. Workers' Compensation 6
4. Occupational Safety 6
5. Systems Analysis 6
6. Regulations 7
7. Management Systems 7
8. Behavior-Based Safety 10
9. Safety Culture 10
Major Events 10
Health, Safety & Environmental Programs 11
Environmental / Sustainability 12
Health 12
Safety 13
Prescriptive / Non-Prescriptive 13
Safety Management Programs 14
Regulations 15
The Regulator's Dilemma 16
Process Safety Management 16
Definition of Process Safety Management 18
Safe Limits 19
Set Point Values 22
Operating, Safe and Emergency Limits 24
Measurement Strategies 28
Involvement 31
Thoroughness 31
Holistic 31
Environment 32
Quality Management 32
Statistical Process Control 32
ISO 9000 / 14001 32
Six Sigma 33
Risk 33
Components of Risk 34
Hazards 35
Consequence 35
Predicted Frequency 36
Safeguards 37
Presence of Persons 37
Single Contingency Events 38
Economies of Scale 39
Common Cause Events 39
Fukushima-Daiichi 39
Examples 40

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Utility Failure 40
Instruments on Manual 40
Instrument Pluggage 40
Vibration 40
External Events 40
Maintenance Availability 41
Human Error / Untrained Personnel 41
Subjective Nature of Risk 41
Degree of Control 42
Familiarity with the Hazard 42
Direct Benefit 42
Personal Impact 43
Natural vs. Man-Made Risks 43
Recency of Events 43
Perception of the Consequence Term 43
Comprehension Time 44
Randomness 45
Regression to the Mean 45
Bias toward Positive Evidence / Prior Beliefs 45
Availability 45
Quantification of Risk 46
Mathematical Terms 46
Frequency 46
Predicted Frequency 46
Probability 47
Likelihood and Failure Rate 47
Error / Statistical Significance Confidence 47
Failure / Fault 47
Independence and Randomness 48
FN Curves 48
Limitations 50
Acceptable Risk 50
The Third Law 51
Perfection as a Slogan 52
As Low as Reasonably Practical — ALARP 52
De Minimis Risk 54
Citations / 'Case Law' 54
RAGAGEP 54
Indexing Methods 55
Risk Matrices 55
Consequence Matrix 55
Worker Safety 56
Public Safety and Health 56
Environmental Impact 57
Economic Loss 57
Frequency Matrix 58
Risk Matrix 58
A — (Red) Very High 59
B — (Orange) High 59
C — (Yellow) Moderate 59
D — (Green) Low 59

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Other Categories 60
Limitations of Risk Matrices 60
Low-Hanging Fruit 61
Prepare for the Worst Case 61
Expensive Good Ideas 61
Black Swan Events 62
Different Industries 62
Oil Refineries 63
Offshore Oil and Gas 64
Lack of Escape Routes 65
Persons on Board (POB) 65
Cyclones / Hurricanes 66
Downers and Leaners 66
Blowouts 67
Hydrogen Sulfide 67
Dropped Objects 68
Helicopters 68
Ship Collision / Mooring Failure 68
Spill Response 68
Pipelines 69
Examples 69
Example 1 — Facility Design 70
Example 2 — Process Flow 70
Example 3 — Heat Exchanger 71
Example 4 — Risk Management Workflow 72
External Standard 72
Guidance 73
Risk Analysis Plan and Implement 73
Audit / Deltas 73
Success / Continuous Improvement 73
Example 5: Significant Potential Incident 73
Chapter 2 — Compliance and Standards 75
Introduction 75
Regulations 76
Rule-Based Approach 77
Goal-Driven Approach 78
Process Safety Regulations 78
Codes and Standards 80
Development of a Standard 81
Standards Organizations 82
American Chemistry Council / Responsible Care® 83
American National Standards Institute (ANSI) 85
American Petroleum Institute (API) 85
American Society of Mechanical Engineers (ASME) 86
International Organization for Standardization (ISO) 86
National Fire Protection Association (NFPA) 88
Other Industry Sources 88
Center for Chemical Process Safety 88
Center for Offshore Safety 88
Chemical Safety and Hazard Investigation Board 89
Company Standards 89

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Industry Information 90
Regulatory Guidance 90
Open Literature 90
Commercial Information 91
Analysis 91
United States Federal Regulations 91
The Regulatory Process 91
Code of Federal Regulations 92
General Duty Clauses 93
The Tenth Amendment to the United States Constitution 93
The Environmental Protection Agency (EPA) 93
The Occupational Safety & Health Administration (OSHA) 94
OSHA Inspections 95
Variances 96
Enforcement 97
The Entry Process 97
Fatality / Catastrophe 98
Programmed Inspections 98
Complaints 98
Citations 98
Willful 99
Serious 100
Other-than-Serious 100
Repeat and Failure-to-Abate 101
OSHA Standards 101
Part 29 101
Subparts of Part 29 103
Sections of Subparts 103
Interpretations and Guidance 104
The OSHA PSM Standard 105
Covered Processes 105
Other Standards 106
Audit Guidelines 107
National Emphasis Programs 109
Proposed Update 109
1. Atmospheric Storage Tanks 110
2. Oil- and Gas-Well Drilling and Servicing 110
3. Oil- and Gas-Production Facilities 111
4. Reactivity Hazards 111
5. Highly Hazardous Chemicals 112
6. Management System Elements 112
7. RAGAGEP 112
8. Definition of RAGAGEP 112
9. Safety-Critical Equipment 113
10. Organizational Changes 113
11. Emergency Planning 113
12. Third-Party Compliance Audits 113
13. Explosives, Blasting Agents and Pyrotechnics 113
14. Flammable Liquids and Spray Finishing 113
15. Ammonium Nitrate 114
16. Retail Facilities 114

Copyright © Ian Sutton. 1995-2014. All rights reserved.

17. Concentrations of Highly Hazardous Chemicals 114
The Environmental Protection Agency (EPA) 114
The EPA Risk Management Program — 40 CFR 68 115
Tiering / Program Levels 115
Covered Chemicals 115
Formal Management System 115
Worst Case Release 116
Emergency Plan 116
Five-Year Accident History 116
BSEE 116
State Regulations 118
New Jersey Toxic Catastrophe Prevention Act 118
Delaware/Nevada 118
The Safety Case Regime 118
Elements of a Safety Case 119
Duty-Holder Responsibility 119
Responsibility of the Auditor / Assessor 119
Risk Management System 120
Management Systems 120
Living Document 120
Structure of a Safety Case 120
1. Facility Description 120
2. Safety Management System 121
3. Formal Safety Assessment 122
Preparation and Implementation 122
Assessment 123
Performance Measurement 124
International Agencies 124
Elements of PSM 124
1. Employee Participation 125
Written Plan of Action 126
Consultation 126
Access to Information 127
2. Process Safety Information 127
3. Process Hazards Analysis 130
Initial Hazard Analysis 133
Methodology 133
Issues to Address 133
Team 133
Revalidation 134
4. Operating Procedures 134
Written Down 136
Initial Start-Up 136
Temporary and Emergency Operations 137
Certification 137
5. Training 137
6. Contractors 140
Application 142
Employer Responsibilities 143
7. Prestartup Safety Review (PSSR) 143
Process Safety Information 144

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Construction and Equipment 144
Procedures 145
New / Modified Facilities 145
8. Mechanical Integrity 145
Application 148
Written Procedures 148
Training 148
Inspection and Testing 148
Deficiencies 148
Quality Assurance 149
9. Hot Work 149
10. Management of Change 150
Employer Responsibility 151
Written Down 152
Replacement In-Kind 152
Factors that Affect Change 152
Training and Participation / Accountability 152
Information Base 153
Operating Procedures 153
Making the Change 153
Training / PSI / Operating Procedures 153
11. Incident Investigation 153
Investigation 155
Timing 155
Team 155
Report 155
Follow Up 155
Participation 156
12. Emergency Planning and Response 156
13. Compliance Audits 158
Certification 160
Technical Qualifications 161
Report 161
Response 161
Retention of Reports 161
Chapter 3 — Culture and Participation 162
Introduction 162
Regulations and Standards 163
BSEE Standard for Culture 163
HSE and Culture 165
National Energy Board 166
Survey 166
Warning Flags over Your Organization 166
Flag One — Unrealistic Stretch Goals 167
Production Creep 167
Production Records 168
Initiative Overload 168
Flag Two — Excessive Cost Reduction 169
Reduction of "Non-Essentials" 171
Reductions in Work Force 171
The "Big Crew Change" 172

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Flattened Organizations 172
Aging Infrastructure 173
Out-Sourcing 173
Not Enough Time for Detailed Work 173
Project Cutbacks 174
Organizational Spread 174
Flag Three — Belief That "It Cannot Happen Here" 174
Lack of Direct Experience 174
Good Occupational Safety Performance 175
Failure to Learn from Near-Misses 175
Failure to Draw on Experience Elsewhere 175
Flag Four — Over-Confidence in Rule Compliance 176
Flag Five — Departmentalized Information Flow 176
Critical Safety Information Is Buried, Lost or Diluted 176
Team Player Culture 177
Fear of Litigation 177
Mergers, Acquisitions and Divestitures 178
Flag Six — Ineffective Audit Process 178
Softened News to Senior Managers 178
Failure to Identify Root Causes 179
Inadequate Follow Up 179
Thinking Backwards 179
Imagination 180
Culture Matrices 180
Elements of Culture 181
On-Going and Consistent 182
Actions and Words 182
External Evaluation 182
Learning from Incidents 183
Attention to Basics / Housekeeping 183
Mergers and Acquisitions 183
Generational Differences 184
Measurement 185
Key Performance Indicators 186
Lagging and Leading Indicators 186
Lagging Indicators 186
OSHA Recordable Rate 188
Process Safety 188
Leading Indicators 189
Near Misses 190
Unplanned Maintenance 190
Process Safety Incident 190
KPI Limitations 191
Activity and Quality 191
Quality of Reporting 191
Management Elements 192
API RP 754 192
Tiers 194
Tier 1 — Process Safety Event 195
Tier 2 — Process Safety Event 195
Tier 3 — Challenge to Safety Systems 195

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Tier 4 — Operating Discipline and Management System Performance 196
Data Submission 196
Selection of KPIs 196
Surveys 197
Creating a Strong Culture 197
Mission Statement 198
Guiding Tenets 199
Detailed Program 199
Behavior Based Safety 199
Observed Hazard Card 200
Five by Five Policy 202
Off-the-Job Safety 202
Pointless Activities 202
Employee Participation 203
Developing Employee Participation 204
Safety Committees 204
Involvement in PSM Elements 204
Difficulties with Workforce Involvement 204
Inefficiencies 205
Unwillingness to Accept Change 205
Labor / Management Relations 205
Stakeholder Outreach 205
Chapter 4 — Technical Information 207
Introduction 207
Table of Contents 208
Process Description 210
Flowsheets 211
Block Flow Diagrams 211
Process Flow Diagrams 212
Piping & Instrument Diagrams 213
Design Phases 214
Equipment and Line Designations 214
Instrument Designations 215
Updating P&IDs 215
Editing Engineering Information 215
Materials of Construction Table 216
Material Safety Data Sheet or Safety Data Sheet 216
Global Harmonization System 219
The Safety Diamond 220
Chapter 5 — Hazard Identification 222
Introduction 222
Hazards Management Process 224
Step 1. Identify the Hazards 226
Creative / Imaginative Techniques 227
Experience-Based 228
Logical / Rational 228
Step 2. Risk Rank 229
Step 3. Eliminate or Substitute the Hazard 229
Step 4. Remove the People 229
Step 5. Reduce the Consequence 229
Step 6. Reduce the Likelihood 229

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Step 7. Install Safeguards 230
Organization of a Hazards Analysis 230
Charge / Scope Letter 231
Objective 231
Physical Scope 232
Method(s) to be Used 232
Assigned Personnel 232
Risk Management Guidance 232
Schedule and Reporting 232
Abandoned Equipment 232
Preparations 232
Logistics 233
Meeting Protocol 233
Location of the Meeting 233
Projection of Notes 234
Documentation Requirements 234
Security of the Information 235
Time Required 235
Kick-Off and Close-Out Meetings 236
HAZID / Major Hazards Screening 236
The Team 237
Leader / Facilitator 238
Process Knowledge 239
Stimulate Thinking 239
Creative Thinking 240
Casual Remarks 240
"If we had unlimited money" 241
Generalizations 241
Team Management 241
Knowledge of Actual Incidents 242
Lawyer-Like Behavior 243
Persona 243
Personal Preparation 243
Engineering Standards 243
The Scribe 244
Operations / Maintenance Expert 244
Process and Instrument Experts 244
Specialists 245
Use of Sophisticated Language 245
The One-Minute Engineering Department 245
Results of the Analysis 246
Findings 246
Recommendations 246
Action Items 247
Risk Register 248
Finding Number and Date 249
Hazard 249
Source 249
Consequence(s) / Likelihood / Risk 249
Follow-Up 250
The Hazards Analysis Report 250

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Completeness of the Notes 251
Cross-Reference 252
Anonymity 252
Findings Terminology 252
Completeness 253
'Non-Findings' 253
Appearance 253
Pictures 253
Report Distribution 254
Communication with the Public 254
Table of Contents 254
1. Disclaimer 254
2. Executive Summary 255
3. Objectives of the Analysis 255
4. Summary of Findings 256
5. Method Used 256
6. Risk Ranking 257
7. The Team 257
8. Regulations and Standards 257
9. Attachments 258
10. Meeting Notes 258
Development of the Report 258
Step 1. Notes Clean-Up 258
Step 2. Team Review 259
Step 3. Draft Report 260
Step 4. Client Review 261
Step 5. Final Report 262
Step 6. Risk Register 263
Legal Issues 263
Need to Act on Findings 265
Informal Notes 265
Internal Communication 265
PHA Leadership 266
Special Types of Hazards Analysis 267
Temporary and Transient Operations 267
Non-Process Applications 267
Decommissioning / Demolition 268
Revalidation Hazards Analyses 268
Benefits and Limitations of Hazard Analyses 270
Strengths 270
Providing Time to Think 270
Challenging Conventional Thinking 270
Cross-Discipline Communication 270
Education 271
Development of Technical Information 271
Economic Payoff 271
Limitations and Concerns 271
Imprecision in Defining Terms 272
Multiple Contingencies 272
Complexities and Subtle Interactions 273
Dynamic Conditions 274

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Knowledge of Safe Operating Limits 274
Lack of Quantification 274
Team Quality 274
Personal Experience 275
Boredom 275
TRIZ 275
Confusion with Design Reviews 276
False Confidence 276
Equipment Orientation 277
Interfaces 277
Human Error 278
The Hazard and Operability Method (HAZOP) 279
Step 1. Node Selection and Purpose 280
Selection of Nodes 281
Pressure/Spec Breaks 282
Step 2. Process Guideword / Safe Limits 283
Step 3. Identification of Hazards and their Causes 283
Step 4. 'Announcement' of the Hazard 287
Step 5. Consequences 287
Step 6. Identification of Safeguards 288
Step 7. Predicted Frequency of Occurrence of the Hazard 288
Step 8. Risk Rank 289
Step 9. Findings 290
Step 10. Next Process Guideword / Node 290
Effectiveness of HAZOPs 290
Checklists 291
Checklist Categories and Guidewords 291
Structure of a Checklist 294
The What-If Method 296
Node / Functional Area Review 297
Equipment and Function Review 298
Ignition Source Controls 298
Instrumentation and Control Systems 299
Human Factors 299
Process Upsets 299
Siting 299
Structured What-If 299
Utility Systems 300
Batch Processes 300
Operating Procedures 301
Layout Reviews 301
What-If / Checklist Method 302
Failure Modes & Effects Analysis 302
Bow Tie Analysis 308
Indexing Methods 310
Interface Hazards Analysis 310
Chapter 6 — Operating Procedures 313
Introduction 313
Definition of Operating Procedures 317
Operations 317
Written Instructions 318

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Design or Operating Intent 318
Definition of Maintenance Procedures 319
Terminology 319
Engineering the Solution 322
Quick Assessment of Operating Procedures 324
The Users 327
Experienced Technicians 327
Less Experienced Technicians 327
Engineering / Management 327
DCS / SCADA Programmers 327
Auditors, Regulators and Inspectors 328
Translators 328
Elements of Operational Integrity Management 328
Workforce Involvement 328
Knowledge Management 329
Hazard Identification and Risk Management 330
Management of Change 331
Operational Readiness 331
Emergency Management 331
Technical Information 331
Types of Operating Procedure 331
Steady-State Operating Procedures 331
Types of Steady-State Procedure 332
Shift Change 332
Start-Up Procedures 334
Shutdown Procedures 334
Levels of Shutdown 335
Stand-By 335
Unit Shutdown 335
Facility Shutdown 336
Emergency Shutdown 336
Turnaround 336
Trouble Shooting Procedures 336
Elements of Troubleshooting Procedures 338
Structure of Troubleshooting Procedures 338
Temporary Operating Procedures 338
Batch Procedures 340
Standard Operating Procedures 340
Maintenance Procedures 344
Job Safe Practices 345
Software Analogy 347
Modular Design 347
Connecting the Modules 348
If / Then / Else Instructions 349
Modular Operating Manual 350
Data Base Structure 353
Top-Down Development 354
Prototyping 356
Limitations of Modularity 357
Design of an Operating Manual 357
Adding and Removing Modules 361

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Numbering the Modules 361
Module Design 362
The Title Block 363
Procedure Name 364
Module Number 365
Purpose of the Procedure 365
Revision Number 365
Date of Revision 365
Covered Persons 366
Company / Facility 366
Safe Upper and Lower Limits 366
Special Safety Items 366
Equipment Information 366
Training 367
The Operating Task Instructions 367
Step Number Column 368
Person 368
Action 368
Discussion / Illustration 368
The Authorization Block 369
Written By 370
Approval — Superintendent 370
Approval — Manager 370
Authorization Sheet 370
Overall Module 371
Links to Other Procedures and Manuals 374
Links to Technical Information 374
Training 374
Two-Page Modules 374
Content Development 376
Level of Detail 376
Level 1 — Overview / Checklists 376
Level 2 — Equipment Description 377
Level 3 — Valve Detail 377
Sources of Information 378
Existing Procedures 378
Technician Interviews 378
Engineering Information 379
Vendor Manuals 379
Process Hazards Analyses 379
The Procedures-Writing Team 379
Writing and Publishing 379
Project Organization 380
1. Define the Scope of Work 380
Physical Area / Equipment Covered 381
Users 381
Types of Procedure 381
Job Task Analysis 381
Design of the Manual 382
Regulations / Standards 382
Writer's Guide 382

Copyright © Ian Sutton. 1995-2014. All rights reserved.

2. Create the Team 382
Steering Committee 382
Project Manager 383
Project Lead 383
Technicians 383
Technology Expert 384
Interviewer-Writers 384
Publisher / Webmaster 384
3. Develop a Detailed Plan 384
Schedule and Progress Metric 385
Budget 386
Prepare the SOPs 387
4. Collect Information 387
Operator Interviews 387
Existing Procedures / Vendor Manuals 387
Logbooks 388
5. Write the Procedures 388
Draft Releases 388
Plan to Throw One Away — You Will Anyway 389
6. Review and Sign 389
7. Publish 389
Potential Difficulties 390
Poorly Defined Goals 390
Too Many People 390
Extended Review Cycle 391
Lack of Signatures 391
Maintaining the Procedures 392
Procedures Modification Process 393
Organization 394
Writing Guidelines 394
Vigorous Writing 395
Minimalist Writing 396
Short, Pithy Instructions 396
Avoid Repetition of Instructions 397
Omit Needless Words 397
Omit Adverbs 397
Short and Old Words 398
Avoid Wordy Phrases and Padded Syllables 398
Writing Style 399
Imperative Tense 399
Active Voice 400
Reading Grade Level 400
List Instructions Singly 401
Implied Instructions 402
Bulleted Lists 402
Conditional Instructions 402
Positive / Negative Instructions 403
Vocabulary 404
Identification of Equipment 404
Consistency 404
Should / Would / Could 404

Copyright © Ian Sutton. 1995-2014. All rights reserved.

The Word 'You' 405
The Word 'This' 405
Arabic Numerals 406
Adverbs and Adjectives 406
Articles 406
Humor 406
Spelling 407
Latinate Abbreviations 408
Apostrophes 409
Ambiguous Words 409
Repetition of Messages 409
Danger, Warning, Caution, Note 410
Proofreader Marks 410
Illustrations 411
Photographs 412
P&IDs 412
Iconic Flow Diagrams / Schematics 412
Maps / Plot Plans 414
Publishing 414
Color 414
White Space 415
Fonts 415
Paragraph Formatting 416
Emphasis Techniques 416
Heading 417
Page Numbering 417
Single-Sided versus Double-Sided Printing 417
Indexing 417
Glossary 417
The Binder 418
Multiple Languages 418
Chapter 7 — Training and Competence 419
Introduction 419
Levels of Competence 419
Level 1 — Basic Skills 419
Level 2 — Certification 420
Level 3 — Master Technician 420
Elements of a Training Program 420
Orientation 420
Initial / Basic Training 421
Site Training 422
Abnormal Situation Management 422
Refresher Training 423
SEMS (BSEE) 423
PSM (OSHA) 430
Procedures and Training 431
Management of a Training Program 433
Training Matrix 433
Budget Allocation 436
Measuring Progress 436
Economics of Training 437

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Process Simulators and Emulators 438
Features 438
Benefits 438
Simulator Design 438
Testing and Certification 440
Safe Gulf 441
Pipeline Operator Training 442
Chapter 8 — Prestartup Reviews 444
Introduction 444
What the Review Is Not 445
Regulations 445
OSHA's PSM 445
(i) Construction and Equipment 447
(ii) Procedures 447
(iii) New / Modified Facilities 447
SEMS 447
Types of Review 448
Review Not Required 448
Small Projects / Engineering Changes 448
Medium Size 449
Large Projects 449
Restart Reviews 449
Organizational Responsibility 450
Time Required 450
Team Structure 450
Using the Elements of Process Safety Management 451
Knowledge Management 452
Operating Procedures 452
Asset Integrity / Reliability 452
Training / Performance 452
Chapter 9 — Asset Integrity 453
Introduction 453
Engineering Standards 453
Inherent Safety 453
Eliminate 454
Remove Equipment 454
Remove People 455
Minimize 456
Substitute 456
Moderate 456
Equipment Modification 457
Spacing 457
Underground Location 457
Simplify 457
Applying Inherent Safety 458
Law of Unintended Consequences 460
Serendipity 460
Undesirable Outcome 460
Original Situation Worse 461
Passive Safety Systems 461
Active Safety Systems 462

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Administrative Safety Systems 462
Safety Critical Items 462
Priority 1 462
Priority 2 462
Priority 3 463
RAGAGEP 463
Chapter 10 — Management of Change 464
Introduction 464
Benefits of Management of Change 464
Increased Production, Productivity and Quality 464
Maintenance Expense and Safety 465
Environmental Performance 465
Personal Reputation 465
Definition of MOC 465
Deviation beyond Limits 466
Impact on other Process Safety Elements 467
Critical Changes 467
In-Kind / Not-In-Kind Change 467
Same Specification 468
Same Service and Materials of Construction 468
Same Storage and Handling Process 468
Procedural Replacement 469
Process Chemistry 469
Instrumentation and Control Systems 469
Types of Change 469
Initiated Equipment Change 469
Large and Small Changes 470
Turnarounds 470
Field Change 470
Non-Initiated Equipment Change 471
Overt Change 471
Covert Change 471
Temporary Changes 472
Emergency Changes 474
Administrative and Organizational Change 475
Reorganization 476
Management by Contractors 476
Informal Aspects of MOC 476
The Management of Change Process 477
Section A — Initiator Request 478
Initiator 478
Personal Recognition 479
Company Loyalty 479
Safety 479
Sponsor 480
Request Process 480
Step 1 — Problem / Opportunity Identified 481
Step 2 — Need For Change 481
Step 3 — Corrective Action 481
Step 4 — System Change 482
Management of Change Form — Section A 482

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Name of the Sponsor / Initiator(s) / Date 483
Description of Problem and Its Consequences 483
Proposed Change 484
Justification 484
Emergency Change/ Temporary Change 484
Previous Actions Taken 484
Section B — First Review 485
In-Kind / Not-In-Kind Change 486
Selecting the First Reviewers 486
Management of Change Form — Section B 487
Name / Date 488
Discussion 488
Suggested Modifications 488
Section C — Detailed Evaluation 488
Review Process 489
MOC Coordinator 490
Review Team 491
Process Manager 491
Engineering Manager 491
Operations Manager 491
Builders 492
Project Team 492
Software 492
Reviewers 493
1. Confirm the Problem 493
2. Problem Analysis 493
3. Identify Possible Solutions 493
Qualifications 493
Experience 493
Technical Knowledge 494
Feasibility 494
"Out-of-the-Box" Thinking 495
Recommendations 495
Management of Change Form — Section C 495
Section D — Formal Approval 496
Management of Change Committee 497
Operations 497
Maintenance 497
Technical 498
Engineering/Construction 498
Process Hazards Analysis 498
Variance Procedures 498
Section E — New Limits / Process Safety Update 499
Section F — Notification 499
Section G — Implementation 500
Section H — Follow-Up 501
Chapter 11 — Incident Investigation and Root Cause Analysis 503
Introduction 503
Management Level 504
Line Supervision 504
Facility Management 504

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Executive Management 505
Industry Regulations and Standards 505
Incident Investigation and Analysis Philosophy 505
Trust and Candor 506
Listen to the Facts 507
Technical Expertise 507
Root Cause Analysis 508
Difficulties with "Root Cause" 508
Ockham's Razor 510
Project Management 510
Attorney-Client Privilege 510
Blame and Fault-Finding 510
Management Trust 511
Early Reporting of Bad News 512
Management Pressure 512
Safety as a Cause of Incidents 512
Communications 512
Technicians 513
Mid-Level Managers 513
Senior Managers 513
Definitions 513
Incident 514
Accident 514
Near Miss / Hit 514
Potential Incident 515
High Potential Incident 515
Incident Investigation Steps 515
Step 1 — Initial Investigation 516
Step 2 — Evaluation and Team Formation 516
Step 3 — Information Gathering 518
Step 4 — Timeline Development 518
Step 5 — Root Cause Analysis 518
Step 6 — Report and Recommendations 518
Step 1. Initial Investigation 519
The 'Go Team' 519
Immediate Actions 519
Team Preparation 520
Drug and Alcohol Testing 521
Incident Report Form 521
Incident Number 522
Title 522
Location, Date and Time of Event 522
Duration of Event 523
Date and Time of Report 523
How Observed 523
Person(s) Reporting 523
Preliminary Ranking 523
Incident Type 523
Incident Flags 523
First Description of Event 523
Immediate Corrective Actions Taken 524

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Witnesses 524
Contractor Involvement 524
Detailed Location 524
Consequences 524
Emergency Response 525
Security Issues 525
System Alert 525
Incident Owner / Department 525
Notes and Attachments 525
First Management Report 525
Step 2. Evaluation and Team Formation 526
Evaluation 526
Team Formation 527
Outside Investigators 527
Corporate Support 528
Team Members 528
Sponsor 528
Incident Owner 528
Facility Manager 529
Lead Investigator 529
Administrator 530
Area Supervisor 530
HSE Representative 530
Process Safety Management Coordinator 530
Employee Representative 530
Process / Facilities Engineer 530
Maintenance Technicians 530
Subject Matter Experts 531
Contractors / Vendors 531
Emergency Response Specialists 531
Attorneys 531
Charter / Terms of Reference 531
Team Member Qualifications 532
Objectivity 532
Common Sense 532
Jumping to Conclusions 533
Haughtiness and Empathy 533
Understand Incident Investigation Methodology 534
You Do Know What You Don't Know 534
Understand Process Systems 534
Logical Thinking / Painstaking 534
Step 3. Information Gathering 535
Interviews 536
Interview Guidelines 537
Regulatory / Legal Interviews 539
Witness Interviews 540
Interviewer Attributes 541
Rapport and Trust 541
Technical Skills 542
Critical Factors Recognition 542
Objective 542

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Effective Note Taking 543
Management Interviews 543
Documentation 543
Engineering Information 543
Operating Information 543
Instrument Records 544
Log Books, Maintenance Records and JSAs 544
Hazards Analysis Reports 544
Management of Change Records 544
Operating Manuals / Procedures 544
Incident Investigations and Audits 544
Vendor Data 544
Field Information 544
Damage Assessment 545
Photographs and DVDs 545
Closed Circuit Television 546
Instrument Records 546
Testing / Lab Analysis 546
Step 4. Timeline Development 546
Timeline Steps 547
Section 1 — Events Prior to the Incident 547
Section 2 — The Incident 547
Section 3 — Post-Incident Response 547
Timeline Construction 548
Conditions 549
Multiple Timelines 549
Timeline Table 552
Background Information 553
Step 5. Root Cause Analysis 554
Levels of Root Cause 555
Single Incidents 555
Multiple Incidents 555
Types of Root Cause Analysis 556
Argument by Analogy: Story Telling 557
False Extrapolation 557
Linearity 558
World Views 558
Safeguards 558
Management Action 559
Categorization 559
Equipment Failure 560
Human Error as a Root Cause 561
Process Systems Failure 561
System Analysis 561
Why Trees 562
Single Chain of Events 562
Wrong Chain 562
Fault Tree Analysis 563
Linkage of Fault Trees to the Timeline 567
Common Cause Events 568
6. Report and Recommendations 568

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Levels of Recommendation 569
Short Term Recommendations 570
Intermediate Recommendations 570
Long Term Recommendations 570
Industry Guidance 570
Report Structure 571
Executive Summary 571
What Happened? 572
What Could Have Happened? 572
What Was the Cause? 572
What Actions Should Be Taken? 572
Recognition 572
Terms of Reference 573
Reason for Selection 573
Sequence of Events 573
Consequences 573
Root Causes 573
Other Hazards 573
Recommendations 574
Attachments 574
Attachment A — Regulations and Standards 574
Attachment B — Root Cause Analysis 574
Attachment C — Organization Chart 574
Attachment D — Review of Similar Events 574
Attachment E — Investigation Team 574
Attachment F — Review of Modern Designs 575
Attachment G — Index to Pictures and Documents 575
Attachment H — Detailed Timeline 575
Issuing the Report 575
Writing the Report 575
Presenting the Report 575
Follow Up and Recommendations Tracking 576
Legal Issues 576
Information Security and Chain of Custody 577
Record Retention 579
Removing Evidence 579
File Systems 580
Incident / Risk Register 580
Feedback 582
Incident Data Bases 584
National Response Center (NRC) 584
Accidental Release Information Program (ARIP) Database 584
CFOI (Census of Fatal Occupational Injuries) 585
Major Accident Reporting System (MARS) 585
Marsh & McLennan Reviews 585
Annual Loss Prevention Symposia 586
Process Safety Beacon 586
Government Agencies 586
Chapter 12 ─ Emergency Management 587
Introduction 587
Abnormal Situation Management 589

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Human Response 589
Human Error Rate 589
Fixation 590
Heroism and Buddy Loyalty 590
Trouble Shooting 591
Levels of Emergency 591
Cause of Emergency 593
Emergency Operations 594
Local Emergency Response 595
General Emergency Response 595
Recovery Operations 595
Investigation and Follow Up 596
Emergency Planning 596
Organization and Personnel 596
Emergency Response Manual 596
Emergency Procedures 598
Emergency Response Training 599
Communications 600
Emergency Shutdown 600
ESD Hierarchy 600
Shutdown Zones 602
System Reset 602
Fire and Gas Detection 602
Fire Detection 603
Fire Eyes / Flame Detectors 604
Smoke Detectors 605
Heat Detectors 605
Fusible Links 605
Low Oxygen Detectors 606
Combustible Gas Detectors 606
Manual Call Points 606
Toxic Gas Releases 606
Escape Routes 607
Fire Fighting 607
Single Fire Concept 607
Deluge Systems 607
Fire Zones 608
Chapter 13 — Audits and Assessments 610
Introduction 610
Formal Audits 611
Reasons for Audits 612
Accident Follow-Up 613
Regulatory / Standards Compliance 613
Stakeholder Outreach 613
Voluntary Check 613
Insurance and Business Security 614
Audit Standards 614
Regulations 614
Reporting Requirements 614
Industry Standards 614
Internal Standards 615

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Audit Frequency 615
Audit Personnel 615
Outside Auditors 615
Internal Auditors 616
Team Composition 617
Auditor Attributes 617
Audit Service Providers 617
Interview Skills 618
Technical Knowledge 618
Writing Skills 619
Demeanor 619
The Host Company 619
First Impressions 620
Employees 620
Planning the Audit 620
Goals 621
Determine the Audit Standard 621
Scope 621
Budget 622
Schedule 623
One-Point Contact 623
Pre-Audit Activities 624
Audit Forms 624
Conducting the Audit 626
Auditor Preparation 626
Kick Off Meeting 627
Plant Tour 627
Information Collection 627
Role of Personnel 628
Interviews 628
On-Site Inspection 629
Close-Out Meeting 629
Report 629
Draft Report 630
Generalities 630
Report Distribution 631
Letter of Certification 631
Audit Verification 632
Positive Findings 632
Report Retention 632
Findings 633
Follow Up 633
Unannounced Audits 633
The SEMS Audit Rule 634
SEMS II 647
Audit Requirements 648
Independent Third Party Auditors (I3Ps) 651
I3P Qualifications 651
National Emphasis Program (NEP) 652
Reviews and Expert Assessments 652
Review Issues 653

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Management Systems Effectiveness 653
Workforce Involvement 654
Real World Usefulness 654
"Learned to Live with It" Problems 654
Lessons Learned 654
Reviewer Attributes 654
Management Elements Assessment 655
Level 1 — Risk Management 656
Level 2 — Management Element Spreadsheet 658
Level 3 — Detailed Questions 659
Scoring Template 661
Guidance 661
Benefits of the Elements Assessment Approach 662
Independent of Events 662
Handling Abstraction 662
Smoothing of Results 663
Objectivity 663
Chapter 14 — Consequence Analysis 664
Introduction 664
Range of Consequences 664
Safety 666
Health 667
Environmental 667
Economic 667
Effect of a Release 667
Hole Size 668
Fires 668
Flammable Range 668
Ignition Temperature / Energy 669
Spontaneous Combustion 670
Ignition Sources 671
Vacuum Trucks 671
Radiant Heat 671
Static Electricity 672
Lightning 673
Pyrophorics / Iron Sulfide 673
Flammability Hazard Ranking 673
Passive Fire Protection / Fireproofing 674
Explosions 675
Physical Explosions 675
Vapor Cloud Explosions 675
Deflagrations and Detonations 676
Blast Effects 677
BLEVEs 677
Dust Explosions 677
Toxic Gas Releases 677
Gas Release Modeling 678
Effect of Toxic Gases 679
Probit Equations 681
Short-Term Exposure Limits 681
Emergency Response Planning Guidelines (ERPGs) 682

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Immediately Dangerous to Life and Health 683
Permissible Exposure Limits (PEL) 684
Threshold Limit Values (TLV) 684
Short Term Exposure Limit (STEL) 685
Levels of Concern (EPA) 685
Acutely Toxic Concentration / Levels (New Jersey / Delaware) 685
Substance Hazards Index 685
Location of Monitors 686
Chapter 15 — Frequency Analysis 687
Introduction 687
The Pareto Principle 687
Importance Ranking 688
Fault Tree Analysis 689
Gates 691
OR Gate 691
AND Gate 693
VOTING Gate 696
Events 698
Top Event 698
Intermediate Events 699
Base Events 699
House Event 700
Top-Down Development of a Fault Tree 700
1. Define the Top Event 701
2. Build the Tree 701
3. Identify the Cut Sets 708
4. Eliminate Repeat Sets 709
5. Eliminate Repeat Events in a Set 710
6. Eliminate Redundant Events 711
7. Quantify the Risk 713
Mathematics of an OR Gate 713
Mathematics of an AND Gate 714
Mathematics of a Voting Gate 715
Cut Set Quantification 715
8. Risk Rank 716
Event Contribution 716
Important Few 718
Unimportant Many 718
Power of the AND Gate 718
Importance Equalization 718
Cost-Benefit Analysis 718
Importance Ranking Using Cut Sets 719
Birnbaum Factor Method 719
Fussell-Vesely Method 719
Perturbation Method 719
Common Cause Events 720
Fukushima-Daiichi 723
Generic Fault Trees 724
Generic Safety Fault Tree 724
Generic Reliability Fault Tree 726
Discussion of the Fault Tree Method 727

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Qualitative Fault Tree Analysis 727
Event Tree Analysis 728
Quantification of an Event Tree 730
Scope of Event 732
Combining Event Trees and Fault Trees 732
Short Sequence of Events 734
Many Events 734
Partial Success 734
Discrete Event Analysis 734
Non-Linearities and Complexities 734
Conveying Statistical Uncertainty 735
Monte Carlo Simulation 735
Random Number Generators 735
Seed Numbers 736
Speeding the Simulation 736
Markov Models 737
Top-Down / Bottom-Up Approach 740
Top-Down 740
Bottom-Up 740
Qualitative Insights 740
Limitations to Quantification 741
Mathematical Understanding 741
Value-Laden Assumptions 741
Lack of Exhaustivity 742
Human Behavior 742
Data Quality 742
Safeguards 743
Safeguard Level 1: Normal Operations 744
Safeguard Level 2: Procedural Safeguards 745
Safeguard Level 3: Safety Instrumented Systems 745
Safeguard Level 4: Mechanical Safeguards 746
Safeguard Level 5: Passive Safeguards 746
Safeguard Level 6: Emergency Response 746
Layer of Protection Analysis 746
The LOPA Process 747
Single Scenarios 748
IPLs 748
Specific 749
Independent 749
Dependable 750
Auditable 750
Human Response 750
Implementing LOPA 750
Team Makeup 750
Timing 750
Tools 751
Procedures and Inspections 751
Risk Criteria 751
Failure Rate Data 751
Conditional Probability / Bayes' Theorem 752
Evaluation of Tests 752

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Sequential Observations 753
Combining Data Sources 753
Chapter 16 — Reliability, Availability and Maintainability 759
Introduction 759
Benefits of a RAM Program 761
Increased Production and Profitability 761
Increased Productivity 762
Reduced Investment 762
Lower Maintenance Costs 762
Lower Inventories 762
Enhanced Customer Satisfaction 762
Personal Recognition 762
Personal Life 763
Improved Public Perception 763
Reliability and Safety 763
Hazardous Operations 763
Unsafe Process Conditions 763
Safety Bypasses 763
Transient Stresses 763
Reduced Chance of Catastrophic Losses 764
Increased Safety May Reduce Reliability 764
Loss of Experience 764
Engineering Practices 764
Daily Operations 764
Definitions 764
Reliability 765
Availability 765
Effectiveness 767
Maintainability 767
Failure Modes 768
Equipment Description 768
Primary, Secondary and Command Failures 768
Catastrophic, Degraded and Incipient Failures 768
Real Failures / Necessary Replacements 768
Failure Rates 769
Constant / Exponential Distribution 770
Lognormal Distribution 771
Bathtub Curve 771
Early Failures 772
Constant Failure Rate 772
Wear-Out Failures 772
Reliability Block Diagrams 773
Active / Standby Redundancy 776
Quantification of Block Diagrams 777
Human Reliability 778
Types of Human Error 779
Errors of Intent 779
Mistakes 779
Slips 779
Fixation 780
Error in an Emergency 780

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Incorrect Response 780
Human Reliability Analysis 780
THERP 781
Chapter 17 — Managing a Risk Program 782
Introduction 782
Clients / Customers 782
Senior Management 782
Facility Managers 782
Project Managers and Design Engineers 782
Regulators / Auditors 783
Program Organization 783
Step 1 — Determine the Objectives 783
Step 2 — Set Up an Organization 783
Management 784
Steering Committee 784
Coordinator 785
Sub-Committees 785
Operating Binders 786
Step 3 — Create the Metrics and Baseline 787
Step 4 — Develop a Plan 789
Goals 790
Resources Needed 790
Develop a Schedule 790
Reviews and Signatures 791
Step 5 — Implement the Plan 792
Step 6 — Audit / Improve 792
Risk Management on Projects 792
Phase I — Concept Selection 795
Phase II — Preliminary Engineering 795
Philosophies 795
Hazards Analysis 796
Phase III — Detailed Engineering 797
Phase IV — Fabrication and Construction 797
Phase V — Commissioning and Start-Up 797
Chapter 18 — Project Management 798
Introduction 798
Phase / Gate System 798
Hazards Analysis on Projects 799
Phase I — Concept Selection 801
Documents 802
Hazards Analysis 802
Phase II — Preliminary Design (FEED) 803
Documents 803
Hazards Analysis 804
Phase III — Detailed Engineering 805
Documents 805
Hazards Analysis 805
Phase IV — Fabrication and Construction 805
Precommissioning 806
Punchlists 806
Transfer of Care, Custody and Control 807

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Documents 807
Turnover Packages 807
Procedures 810
Hazards Analysis 810
Phase V — Commissioning and Start-Up 811
Commissioning 811
Operational Readiness Review 811
Startup and Line Out 812
Documents 812
Start-Up Procedures 812
Acceptance Test 813
Warranty 813
Hazards Analysis 813
Project Organization 813
Chapter 19 — Contractors 815
Introduction 815
Regulations and Standards 817
OSHA PSM Standard 817
OSHA PSM Guidance 819
Application 819
Employer Responsibilities 819
BSEE SEMS 820
API RP 76 821
Types of Contractor 821
Contract Companies 823
Selecting a Contract Company 823
Contractor HSE Program 824
Design Companies 825
Subcontractors 825
Contract Workers 825
Maintenance Contractors 826
Visitor / Consultant 826
Bridging Documents 826
Operator/Contractor Bridging Document 827
Bridging through a Regulation 827
Contractor Management 828
Contractor Selection 828
Record Keeping 829
Contractor Training 829
Safety Meetings 829
Equipment 830
Infractions 830
Contractor Training 830
Safety Meetings 831
Contractor Evaluation 831
Chapter 20 — The Risk Management Professional 833
Introduction 833
Attributes 833
Education and Certification 833
Technical Knowledge 833
Holistic 833

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Numerate 834
Communication Skills 834
Industrial Experience 834
Knowledge of Past Events 834
Professional Involvement 835
Network 835
The Resumé / CV 835
Level of Detail 836
Publications 836
Gaps / Negative Facts 836
Multiple Resumés 836
Declining Experience 836
Professional Engineer 837
Consultants 837
True Expertise 837
The Consultant as Outsider 838
Consultants — Not Contractors 838
Cuts Gordian Knots 839
Quick Study 839
Role of the Client 840
Response to Criticism 840
Marketing 840
Communicating with Management/Clients 840
Presentations 841
Meetings 841
Report Writing 842
Draft Report 842
Language of the Report 843
Completeness / Thoroughness 843
Personal Information 843
Writing Style 844
Non-Emotional Language 844
Minimalist Writing — Make Every Word Tell 844
Omit Needless Words / Tautologies 845
Short, Simple Words 845
Minimize 'Soft' Materials 846
Eschew Obfuscation 846
Develop a Theme 847
Modifiers 847
No Typos 847
Date Format 847
Active/Passive Voice 848
He / She 848
You / I 848
Choice of Words 849
Use of Humor 849
Copyright 849
Responsible Document Creation 850
Anecdotes / Story-Telling 851
Stories 852
Elements of a Story 852

Copyright © Ian Sutton. 1995-2014. All rights reserved.

Characters 852
Setting 853
Plot 853
Conflict 853
Resolution 853
Sensitivity 853
Communicating with the Public 853
The Community 854
Other Businesses 855
The Media 855
Regulators / Non-Governmental Organizations (NGOs) 855
Types of Public Communication 856
Developing a Risk Communication Program 856
Communicating New Paradigms 856
Trade Secrets (OSHA) 857
Litigation Support 861
Use of Legal Services 862
Types of Litigation 862
The Participants 863
Timeline / Story Line 863
Documentation 863
The Discovery Process 864
Depositions 864
Witnesses to Fact 865
The Expert Witness 865
Acceptance by the Court 866
Daubert and Frye Rules 867
Prior Testimony 867
Timeline / Story Line 867
The Report 868
Attributes of an Expert Witness 868
To Thine Own Self Be True 868
Be Prepared 868
Be a True Expert 868
Be a Teacher 869
"Reasonable"Risk 869
Privilege 869
Citations 871

Copyright © Ian Sutton. 1995-2014. All rights reserved.