

Contents

Series Foreword xv

Preface xvii

I FOUNDATIONS 1

1 Why Do We Need Something Different? 3

2 Questioning the Foundations of Traditional Safety Engineering 7

- 2.1 Confusing Safety with Reliability 7
- 2.2 Modeling Accident Causation as Event Chains 15
 - 2.2.1 Direct Causality 19
 - 2.2.2 Subjectivity in Selecting Events 20
 - 2.2.3 Subjectivity in Selecting the Chaining Conditions 22
 - 2.2.4 Discounting Systemic Factors 24
 - 2.2.5 Including Systems Factors in Accident Models 28
- 2.3 Limitations of Probabilistic Risk Assessment 33
- 2.4 The Role of Operators in Accidents 36
 - 2.4.1 Do Operators Cause Most Accidents? 37
 - 2.4.2 Hindsight Bias 38
 - 2.4.3 The Impact of System Design on Human Error 39
 - 2.4.4 The Role of Mental Models 41
 - 2.4.5 An Alternative View of Human Error 45
- 2.5 The Role of Software in Accidents 47
- 2.6 Static versus Dynamic Views of Systems 51
- 2.7 The Focus on Determining Blame 53
- 2.8 Goals for a New Accident Model 57

3 Systems Theory and Its Relationship to Safety 61

- 3.1 An Introduction to Systems Theory 61
- 3.2 Emergence and Hierarchy 63
- 3.3 Communication and Control 64
- 3.4 Using Systems Theory to Understand Accidents 67
- 3.5 Systems Engineering and Safety 69
- 3.6 Building Safety into the System Design 70

II	STAMP: AN ACCIDENT MODEL BASED ON SYSTEMS THEORY	73
4	A Systems-Theoretic View of Causality	75
4.1	Safety Constraints	76
4.2	The Hierarchical Safety Control Structure	80
4.3	Process Models	87
4.4	STAMP	89
4.5	A General Classification of Accident Causes	92
4.5.1	Controller Operation	92
4.5.2	Actuators and Controlled Processes	97
4.5.3	Coordination and Communication among Controllers and Decision Makers	98
4.5.4	Context and Environment	100
4.6	Applying the New Model	100
5	A Friendly Fire Accident	103
5.1	Background	103
5.2	The Hierarchical Safety Control Structure to Prevent Friendly Fire Accidents	105
5.3	The Accident Analysis Using STAMP	119
5.3.1	Proximate Events	119
5.3.2	Physical Process Failures and Dysfunctional Interactions	123
5.3.3	The Controllers of the Aircraft and Weapons	126
5.3.4	The ACE and Mission Director	140
5.3.5	The AWACS Operators	144
5.3.6	The Higher Levels of Control	155
5.4	Conclusions from the Friendly Fire Example	166
III	USING STAMP	169
6	Engineering and Operating Safer Systems Using STAMP	171
6.1	Why Are Safety Efforts Sometimes Not Cost-Effective?	171
6.2	The Role of System Engineering in Safety	176
6.3	A System Safety Engineering Process	177
6.3.1	Management	177
6.3.2	Engineering Development	177
6.3.3	Operations	179
7	Fundamentals	181
7.1	Defining Accidents and Unacceptable Losses	181
7.2	System Hazards	184
7.2.1	Drawing the System Boundaries	185
7.2.2	Identifying the High-Level System Hazards	187
7.3	System Safety Requirements and Constraints	191
7.4	The Safety Control Structure	195
7.4.1	The Safety Control Structure for a Technical System	195
7.4.2	Safety Control Structures in Social Systems	198

8	STPA: A New Hazard Analysis Technique	211
8.1	Goals for a New Hazard Analysis Technique	211
8.2	The STPA Process	212
8.3	Identifying Potentially Hazardous Control Actions (Step 1)	217
8.4	Determining How Unsafe Control Actions Could Occur (Step 2)	220
8.4.1	Identifying Causal Scenarios	221
8.4.2	Considering the Degradation of Controls over Time	226
8.5	Human Controllers	227
8.6	Using STPA on Organizational Components of the Safety Control Structure	231
8.6.1	Programmatic and Organizational Risk Analysis	231
8.6.2	Gap Analysis	232
8.6.3	Hazard Analysis to Identify Organizational and Programmatic Risks	235
8.6.4	Use of the Analysis and Potential Extensions	238
8.6.5	Comparisons with Traditional Programmatic Risk Analysis Techniques	239
8.7	Reengineering a Sociotechnical System: Pharmaceutical Safety and the Vioxx Tragedy	239
8.7.1	The Events Surrounding the Approval and Withdrawal of Vioxx	240
8.7.2	Analysis of the Vioxx Case	242
8.8	Comparison of STPA with Traditional Hazard Analysis Techniques	248
8.9	Summary	249
9	Safety-Guided Design	251
9.1	The Safety-Guided Design Process	251
9.2	An Example of Safety-Guided Design for an Industrial Robot	252
9.3	Designing for Safety	263
9.3.1	Controlled Process and Physical Component Design	263
9.3.2	Functional Design of the Control Algorithm	265
9.4	Special Considerations in Designing for Human Controllers	273
9.4.1	Easy but Ineffective Approaches	273
9.4.2	The Role of Humans in Control Systems	275
9.4.3	Human Error Fundamentals	278
9.4.4	Providing Control Options	281
9.4.5	Matching Tasks to Human Characteristics	283
9.4.6	Designing to Reduce Common Human Errors	284
9.4.7	Support in Creating and Maintaining Accurate Process Models	286
9.4.8	Providing Information and Feedback	295
9.5	Summary	306
10	Integrating Safety into System Engineering	307
10.1	The Role of Specifications and the Safety Information System	307
10.2	Intent Specifications	309
10.3	An Integrated System and Safety Engineering Process	314
10.3.1	Establishing the Goals for the System	315
10.3.2	Defining Accidents	317
10.3.3	Identifying the System Hazards	317
10.3.4	Integrating Safety into Architecture Selection and System Trade Studies	318

10.3.5	Documenting Environmental Assumptions	327
10.3.6	System-Level Requirements Generation	329
10.3.7	Identifying High-Level Design and Safety Constraints	331
10.3.8	System Design and Analysis	338
10.3.9	Documenting System Limitations	345
10.3.10	System Certification, Maintenance, and Evolution	347
11	Analyzing Accidents and Incidents (CAST)	349
11.1	The General Process of Applying STAMP to Accident Analysis	350
11.2	Creating the Proximal Event Chain	352
11.3	Defining the System(s) and Hazards Involved in the Loss	353
11.4	Documenting the Safety Control Structure	356
11.5	Analyzing the Physical Process	357
11.6	Analyzing the Higher Levels of the Safety Control Structure	360
11.7	A Few Words about Hindsight Bias and Examples	372
11.8	Coordination and Communication	378
11.9	Dynamics and Migration to a High-Risk State	382
11.10	Generating Recommendations from the CAST Analysis	383
11.11	Experimental Comparisons of CAST with Traditional Accident Analysis	388
11.12	Summary	390
12	Controlling Safety during Operations	391
12.1	Operations Based on STAMP	392
12.2	Detecting Development Process Flaws during Operations	394
12.3	Managing or Controlling Change	396
12.3.1	Planned Changes	397
12.3.2	Unplanned Changes	398
12.4	Feedback Channels	400
12.4.1	Audits and Performance Assessments	401
12.4.2	Anomaly, Incident, and Accident Investigation	403
12.4.3	Reporting Systems	404
12.5	Using the Feedback	409
12.6	Education and Training	410
12.7	Creating an Operations Safety Management Plan	412
12.8	Applying STAMP to Occupational Safety	414
13	Managing Safety and the Safety Culture	415
13.1	Why Should Managers Care about and Invest in Safety?	415
13.2	General Requirements for Achieving Safety Goals	420
13.2.1	Management Commitment and Leadership	421
13.2.2	Corporate Safety Policy	422
13.2.3	Communication and Risk Awareness	423
13.2.4	Controls on System Migration toward Higher Risk	425
13.2.5	Safety, Culture, and Blame	426
13.2.6	Creating an Effective Safety Control Structure	433
13.2.7	The Safety Information System	440

13.2.8	Continual Improvement and Learning	442
13.2.9	Education, Training, and Capability Development	442
13.3	Final Thoughts	443
14	SUBSAFE: An Example of a Successful Safety Program	445
14.1	History	445
14.2	SUBSAFE Goals and Requirements	448
14.3	SUBSAFE Risk Management Fundamentals	450
14.4	Separation of Powers	451
14.5	Certification	452
14.5.1	Initial Certification	453
14.5.2	Maintaining Certification	454
14.6	Audit Procedures and Approach	455
14.7	Problem Reporting and Critiques	458
14.8	Challenges	458
14.9	Continual Training and Education	459
14.10	Execution and Compliance over the Life of a Submarine	459
14.11	Lessons to Be Learned from SUBSAFE	460
	Epilogue	463
	APPENDIXES	465
A	Definitions	467
B	The Loss of a Satellite	469
C	A Bacterial Contamination of a Public Water Supply	495
D	A Brief Introduction to System Dynamics Modeling	517
	References	521
	Index	531