

Learning from Failures

Decision Analysis of Major Disasters

Ashraf Labib



AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Butterworth-Heinemann is an imprint of Elsevier



Contents

Acknowledgments	xi
-----------------------	----

PART 1 BACKGROUND OF ANALYTICAL METHODS USED IN INVESTIGATION OF DISASTERS

CHAPTER 1 Introduction to the Concept of Learning from Failures	3
1.1 Introduction	3
1.2 Why Learning from Failures?	5
1.3 The Background of This Book	6
1.4 Who Should Use This Book	6
1.5 Introduction to the Concept of Learning from Failures	7
1.6 Taxonomy of Theories	10
1.6.1 Learning from Case Studies Versus the Narrative Fallacy Concept	11
1.6.2 Learning from Hindsight Rewards Versus Risk Aversion	11
1.6.3 Specific Versus Generic Lessons	12
1.6.4 High Reliability Theory Versus Normal Accidents Theory	13
1.6.5 Reliability Versus Safety	13
1.6.6 Concluding Remarks on Theories Related to Learning from Failures	14
1.7 Case Studies	15
1.7.1 Choice of Case Studies and Research Methodology	15
1.7.2 Types of Recommendations	17
1.8 Critical Commentary Section	17
CHAPTER 2 Introduction to Failure Analysis Techniques in Reliability Modeling	19
2.1 Introduction	19
2.2 FTA and RBD	20
2.3 Example: A Storage Tank	26
2.4 A Simple Illustrative Application Case (A Car Accident)	30
CHAPTER 3 Introduction to the Analytic Hierarchy Process	33
3.1 Introduction	33
3.2 An Overview of the Analytical Hierarchy Process	34
3.2.1 Problem Modeling	36
3.2.2 Pair-wise Comparisons	37
3.2.3 Judgment Scales	38
3.2.4 Priorities Derivation	38

	3.2.5 Consistency	42
	3.2.6 Sensitivity Analysis	42
	3.3 Conclusion and Future Developments	43
PART 2	A—Z OF DISASTROUS CASE STUDIES	
CHAPTER 4	Bhopal Disaster—Learning from Failures and Evaluating Risk	47
	4.1 Introduction	47
	4.2 Bhopal Narrative and the Incorporation of FTA and RBD	47
	4.2.1 Introduction	48
	4.2.2 Direct Causes of the Accident	50
	4.3 Theory/Calculation	52
	4.4 Discussion	60
	4.5 Concluding Remarks	60
	4.6 Critical Commentary Section	61
CHAPTER 5	BP Deepwater Horizon	63
	5.1 Case Study Deepwater Horizon	63
	5.1.1 Background to the Disaster	63
	5.1.2 Technical Cause of the Failure	65
	5.1.3 Consequences and Severity	66
	5.2 Analysis of First Group of Students	67
	5.2.1 The Technical Reasons	67
	5.2.2 The Design and Safety Reasons	68
	5.2.3 Financial and Organizational Factors	68
	5.2.4 Fault Tree Analysis	69
	5.2.5 Reliability Block Diagram	69
	5.2.6 Recommendations and Reliability Improvement	69
	5.3 Analysis of Second Group of Students	71
	5.3.1 Summary of the Technical Cause of the Disaster	71
	5.3.2 Lessons Learned	72
	5.4 Analysis of Third Group of Students	75
	5.4.1 Technical Cause of the Disaster	75
	5.4.2 Lessons Learned	77
	5.5 Feedback and Generic Lessons	78
	5.6 Critical Commentary Section	80
CHAPTER 6	BP Texas City Disaster	83
	6.1 What Happened	83
	6.2 The Process	83
	6.3 Sequence of Events and Incident	84

6.4	Investigation	89
6.5	Fault Tree Analysis and Reliability Block Diagram for the Texas City Disaster	90
6.6	Generic Lessons	93
6.7	Critical Commentary Section.....	94
CHAPTER 7	Chernobyl Disaster	97
7.1	Introduction	97
7.2	What Happened.....	99
7.3	The Technical and Logic of the Failure	99
7.4	Causes of the Incident.....	100
7.5	Fault Tree Analysis and Reliability Block Diagram for the Disaster.....	102
7.6	Generic Lessons and Proposed Improvements.....	103
7.7	Critical Commentary Section.....	106
CHAPTER 8	The Concorde Crash	107
8.1	Introduction	107
8.2	The Accident.....	108
8.2.1	A History of Problems.....	109
8.2.2	Options for Improvement	109
8.3	Theory and Use of γ Analysis (Modified FMEA).....	110
8.4	Application of the AHP to the Concorde Accident.....	114
8.4.1	Step 1: γ Analysis.....	114
8.4.2	Step 2: Construction of the Hierarchy	115
8.4.3	Step 3: Making Judgments	116
8.4.4	Step 4: Synthesis of Results with Respect to the Goal.....	116
8.5	Analysis of Results.....	116
8.6	Conclusion.....	120
8.7	Critical Commentary Section.....	121
CHAPTER 9	Fukushima Nuclear Disaster	123
9.1	Brief Introduction.....	123
9.1.1	The Evolutionary of the Disaster	123
9.1.2	The Consequences of the Failure	124
9.1.3	The Japanese Nuclear Industry.....	125
9.1.4	Some Basic Information About Risk Assessment in Nuclear Industry	125
9.2	Analysis of First Group of Delegates	127
9.2.1	Technical Background	127
9.2.2	The Cooling Water System	128

9.2.3	Overview of the Disaster	129
9.2.4	Analysis of Contributory Factors	130
9.2.5	Fault Tree	132
9.2.6	Discussion of First Group of Delegates	132
9.2.7	Conclusion of First Group of Delegates	134
9.3	Analysis of Second Group of Delegates.....	134
9.3.1	The Analytic Hierarchy Process.....	134
9.3.2	Design Evaluation of the Fukushima Nuclear Plant.....	134
9.3.3	BWR Design for Mitigation of Abnormal Conditions	135
9.3.4	The Cooling System Design.....	135
9.3.5	Design Against Earthquakes and Tsunamis.....	137
9.3.6	Exploring the Incident.....	137
9.3.7	The Nuclear Safety Debate	139
9.3.8	The Nuclear Power Decision for Japan	140
9.3.9	Application of MCDM	141
9.3.10	AHP Results.....	141
9.3.11	Conclusion of the Second Group of Delegates.....	142
9.4	Feedback and Generic Lessons.....	144
9.4.1	Overall Criticism of the Two Groups	144
9.4.2	Wider Generic Lessons for the Nuclear Power Industry.....	144
9.5	Critical Commentary Section.....	151
CHAPTER 10	Hurricane Katrina Disaster	153
10.1	Introduction	153
10.2	Background to the Disaster.....	156
10.2.1	A Sinking Region	157
10.2.2	Hurricane Protection System.....	157
10.2.3	Hurricane Katrina	158
10.2.4	Consequences of Failure.....	159
10.3	Technical Causes of Failure	159
10.3.1	Direct Causes	160
10.3.2	Contributing Factors	161
10.4	Hybrid Modeling Approach.....	161
10.5	Fault Tree Analysis.....	161
10.6	Reliability Block Diagram.....	165
10.7	Failure Modes, Effects, and Criticality Analysis	166
10.8	An AHP Model for the Hurricane Katrina Disaster	172
10.9	Results of Sensitivity Analysis	177
10.10	Discussion and Lessons Learned.....	179
10.11	Concluding Remarks.....	180

CHAPTER 11	NASA's Space Shuttle Columbia Accident	183
11.1	What Happened?	183
11.2	Logic of the Technical Causes of the Failure	184
11.3	Consequences and Severity	184
11.4	Proposed Improvements and Generic Lessons	185
11.5	FTA and RBD	186
11.6	Generic Lessons	187
11.6.1	Generic Lessons That Are Mainly Related to Setting Priorities	193
11.6.2	Generic Lessons That Are Mainly Related to Responsibility and Skills	194
11.6.3	Generic Lessons That Are Mainly Related to Communication	195
11.7	Concluding Remarks	195
11.8	Critical Commentary Section	196
CHAPTER 12	Titanic, the Unsinkable Ship That Sank	197
12.1	Cruising	197
12.2	What Happened	197
12.3	Logic of the Technical Cause of the Disaster	198
12.4	Consequences and Severity	198
12.5	FTA and RBD for the Disaster	198
12.6	Proposed Improvements and Generic Lessons	200
PART 3	GENERIC LESSONS, OTHER MODELS OF LEARNING FROM FAILURES AND RESEARCH DIRECTIONS	
CHAPTER 13	Introduction to the Concept of the Generic Lesson as an Outcome of Learning from Failures	207
13.1	Why Failure Can Be the Best Thing to Happen	207
13.1.1	Lesson 1: Too Much Belief in Previous Successes	208
13.1.2	Lesson 2: Coping with Growth	208
13.1.3	Lesson 3: Misunderstanding Fashionable Paradigms	209
13.1.4	Lesson 4: Legislation	210
13.1.5	Lesson 5: The "I Operate, You Fix" Attitude	210
13.1.6	Lesson 6: No News Is Good News	211
13.1.7	Lesson 7: Bad News, Bad Person	211
13.1.8	Lesson 8: Everyone's Highest Priority Is Their Own Machine	212

13.1.9 Lesson 9: Solving a Crisis Is a Forgotten Experience	212
13.1.10 Lesson 10: Skill Levels Dilemma	213
13.2 Attributes of the Generic Lessons	213
13.3 Best Practice of Learning from Failures from Different Industries	215
13.4 Best Practice Can Be Learned from Worst Practice	216
CHAPTER 14 A Model of Learning and Unlearning from Failures	217
14.1 Introduction	217
14.2 Research Methodology	219
14.3 Routine Dynamics in Learning and Unlearning from Failures	220
14.3.1 Literature on Organizational Dynamic Routines	220
14.3.2 Literature Related to Learning from Disasters	223
14.3.3 Learning and Unlearning from Disasters—The Case of NASA	224
14.3.4 The Case of BP	226
14.4 A New Theory of Routines for Adaptive Organizational Learning from Failures	227
14.4.1 Lessons Learnt from the Maintenance and Reliability Field	227
14.4.2 The DMG	230
14.5 Case Study of Applying the Proposed Model to a Disaster Analysis	235
14.6 Theoretical Framework and Discussion	237
14.6.1 Near-Misses and Failures	237
14.6.2 High Severity with Low Frequency Versus High Severity with High Frequency	237
14.6.3 Holonic Theory	238
14.6.4 Adaptive Ostensive and Performative Routines	239
14.7 Conclusion	240
Not Just Rearranging the Deckchairs on the Titanic: Learning from Failures Through Risk and Reliability Analysis	243
References	291
Glossary of Terms	309
Index	311