B. S. Dhillon

Series on Industrial & Systems Engineering – Vol. 1

# Engineering Safety

- Fundamentals
- Techniques
- Applications

# Contents

*Preface* vii
*Author Biography* xi

**Chapter 1 Introduction** **1**

1.1 Background 1
1.2 Need for Safety and Engineering Safety Goals 2
1.3 Safety Facts and Figures 2
1.4 Major Disasters 4
1.5 Safety Terms and Definitions 4
1.6 Useful Information on Safety 5
1.6.1 Books, Standards, and Reports 6
1.6.2 Journals 8
1.6.3 Organizations 8
1.6.4 Data Information Sources 9
Problems 10
References 10

**Chapter 2 Safety Mathematics and Reliability Basics** **13**

2.1 Introduction 13
2.2 Mean, Median, Mode, Range, Mean Deviation, and Standard Deviation 14
2.2.1 Mean 14
2.2.2 Median 14

2.2.3 Mode 15
2.2.4 Range 15
2.2.5 Mean Deviation 16
2.2.6 Standard Deviation 16
2.3 Sets, Boolean Algebra Laws, Probability Definition, and Probability Properties 17
2.3.1 Sets 18
2.3.2 Boolean Algebra Laws 18
2.3.3 Probability Definition 19
2.3.4 Probability Properties 19
2.4 Statistical Distributions 21
2.4.1 Poisson Distribution 21
2.4.2 Binomial Distribution 21
2.4.3 Exponential Distribution 22
2.4.4 Rayleigh Distribution 23
2.4.5 Weibull Distribution 24
2.4.6 Normal Distribution 24
2.5 Laplace Transform Definition and Final Value Theorem 25
2.6 First Order Differential Equation Solution Through Laplace Transforms 26
2.7 Bathtub Hazard Rate Curve 27
2.8 Reliability Measures 29
2.8.1 Reliability 29
2.8.2 Hazard Rate 30
2.8.3 Mean Time to Failure 31
2.9 Reliability Networks 31
2.9.1 Series Network 31
2.9.2 Parallel Network 33
2.9.3 Parallel-Series Network 34
2.9.4 Series-Parallel Network 35
2.9.5 Standby System 37
Problems 38
References 39

**Chapter 3 Workplace Accidents and Safety** 41

3.1 Introduction 41
3.2 Workplace Accident Facts and Figures 42

3.3 Work Accident Death Comparisons with other Accident Types, Work Accident Cost in Relation to Total Cost, Accident Death Rates by Industry, and Common Causes of Work Injuries 43
3.4 Accident Causation Theories 44
3.4.1 The Domino Accident Causation Theory 45
3.4.2 The Human Factors Accident Causation Theory 46
3.5 The Occupational Safety and Health Act (OSHA) 48
3.5.1 Occupational Safety and Health Administration Objectives and Employer and Employee Rights and Responsibilities 48
3.5.2 Record Keeping and Reporting Requirements and Safety and Health Standards 51
3.5.3 Occupational Safety and Health Administration Achievements, Shortcomings, and Strategic Plan for 1997–2002 52
3.6 Workers' Compensation 54
Problems 54
References 55

**Chapter 4 Safety Management and Control 57**

4.1 Introduction 57
4.2 Safety Management Principles 58
4.3 Safety Department Functions, Safety Manager Qualifications and Functions, and Safety Engineer Qualifications and Functions 59
4.4 Developing a Safety Program Plan, Plant Safety Checklist for Managers, Safety Responsibilities of Non-Safety Managers, and Managerial Deficiencies Leading to Accidents 61
4.5 Safety Committees, Motivating Employees to Work Safely, and Safety-Related Strategies for Safety Professionals 66
4.5.1 Motivating Employees to Work Safely 67
4.5.2 Safety-Related Strategies for Safety Professionals 68
4.6 Product Safety Management Program, Organization Tasks, and Functions of Non-Safety Organizations 69
4.7 Safety Performance Measures 72
4.7.1 Index I: Disabling Injury Frequency Rate 73
4.7.2 Index II: Disabling Injury Severity Rate 73

4.7.3 Drawbacks of the Standard Indexes 74
Problems 74
References 75

**Chapter 5 Safety Analysis Methods and Techniques 77**

5.1 Introduction 77
5.2 Failure Modes and Effect Analysis (FMEA) 78
5.2.1 Failure Mode Effects and Criticality Analysis (FMECA) 79
5.3 Fault Tree Analysis (FTA) 80
5.3.1 Probability Evaluation of Fault Trees 81
5.3.2 Advantages and Disadvantages of Fault Tree Analysis (FTA) 83
5.4 Markov Method 84
5.5 Technic of Operations Review (TOR) 86
5.6 Preliminary Hazard Analysis (PHA) 87
5.7 Hazards and Operability Analysis (HAZOP) 88
5.8 Interface Safety Analysis 89
5.9 Job Safety Analysis (JSA) 90
5.10 Control Charts 90
Problems 93
References 93

**Chapter 6 Risk Management 95**

6.1 Introduction 95
6.2 Risk Management Related Terms and Definitions 96
6.3 Risk Components and Types, Risk Management Objectives, and Risk Analysis Objectives in Hazardous System Life Cycle 97
6.4 Risk Management Process, Interested Parties in the Risk Management Process, Functions and Qualifications of a Risk Manager 99
6.5 Risk Management Rules and Audits 100
6.6 Risk Analysis Process and Methods 101
6.6.1 Hazard and Operability Study (HAZOP) 103
6.6.2 Event Tree Analysis (ETA) 103
6.6.3 Consequence Analysis 104

6.6.4 Frequency Analysis 104
6.7 Common Errors in Risk Management, Risk Estimates for Selective Events, and Risk Analysis Advantages 105
Problems 106
References 107

**Chapter 7 Human Factors in Safety 109**

7.1 Introduction 109
7.2 Terms and Definitions 110
7.3 Job Stress 110
7.3.1 Classification of Occupational Stressors and Workplace Stress Effects 111
7.3.2 Physical Stress Influencing Factors 112
7.3.3 Human Operator's Stress Characteristics and Stressors' Checklist 113
7.4 Worksite Analysis Program for Human Factors 114
7.5 Symptoms of Human Factor-Related Problems in Organizations, Identification of Specific Human Factors Problems, and Strategies for Solving Human Factors Problems 116
7.6 Typical Human Behaviors, Occupational Safety and Health Administration Ergonomics Guidelines, and Human Factors/Safety Issues 119
7.7 Employee Training and Education 121
7.8 Human Error and Human Reliability Prediction Models 122
7.8.1 Human Reliability Prediction Models 123
Problems 127
References 127

**Chapter 8 Safety Costing 129**

8.1 Introduction 129
8.2 Safety Cost Facts, Figures, and Examples 130
8.3 Resource Losses Related to Safety and Health and a Company's Losses Due to an Accident Involving its Product 131
8.4 Safety Cost Estimation Methods 133
8.4.1 The Heinrich Method 133

8.4.2 The Simonds Method 133
8.4.3 The Wallach Method 134
8.5 Safety Cost Estimation Models 135
8.5.1 Accident Hidden Cost Estimation Model 135
8.5.2 Accident Prevention Program Cost Estimation Model 136
8.5.3 Product Life Cycle Safety cost Estimation Model I 136
8.5.4 Product Life Cycle Safety Cost Estimation Model II 136
8.5.5 Total Safety Cost Estimation Model 137
8.6 Safety Cost Performance Measurement Indexes 138
8.6.1 Average Injury Cost Per Unit Turnover Index 138
8.6.2 Average Cost Per Injury Index 138
8.6.3 Average Injury Cost Per Profit Dollar Index 139
8.7 Accident Data Shortcomings and Cost-Benefit Analysis Related Facts with Respect to Safety and Health Regulations 139
Problems 141
References 141

**Chapter 9 Maintenance Safety 143**

9.1 Introduction 143
9.2 Facts, Figures, and Examples 144
9.3 Reasons for Safety Problems in Maintenance and Factors Responsible for Dubious Safety Reputation in Maintenance Work 145
9.4 Maintenance Personnel Safety and Typical Human Behaviors 146
9.5 Maintenance Safety-Related Questions for Equipment Manufacturers and Useful Guidelines for Equipment Designers to Improve Safety in Maintenance 147
9.6 Maintenance Safety Models 149
9.6.1 Model I 149
9.6.2 Model II 152
Problems 156
References 156

**Chapter 10 Software Safety 159**

10.1 Introduction 159

10.2 Terms and Definitions 160
10.3 Facts, Figures and Examples of Software Error 160
10.4 Software Reliability versus Software Safety and Security versus Safety 161
10.5 Computer Related Myths, Software Risk Increasing Ways and Categories, and Software Hazard Causing Ways 162
10.6 Basic Software System Safety Tasks, Software Quality Assurance Organization's Role with Respect to Safety, and Software Safety Assurance Program* 164
10.7 Software Hazard Analysis Methods 167
10.7.1 Software Sneak Circuit Analysis 168
10.7.2 Code Walk-Through 168
10.7.3 Nuclear Safety Cross-Check Analysis (NSCCA) 168
10.7.4 Proof of Correctness 169
10.7.5 Event-Tree Analysis 170
10.7.6 Failure Modes and Effects Analysis (FMEA) 170
10.7.7 Software Fault Tree Analysis 170
10.8 Software Standards 171
10.9 Practical Software Safety Design-Related Guidelines 173
Problems 173
References 174

**Chapter 11 Robot Safety 177**

11.1 Introduction 177
11.2 Terms and Definitions 178
11.3 Robot Accident Facts, Figures, and Fatality-Related Examples 179
11.4 Unique Robot Safety Problems, Robot Accident Types, and Robot Hazard Causes 180
11.5 Safety Considerations in Robot Life Cycle 182
11.5.1 Design Phase 182
11.5.2 Installation Phase 183
11.5.3 Programming Phase 183
11.5.4 Operation and Maintenance Phase 183
11.6 Common Robot Safety Features and Robot Safeguard Approaches 184
11.7 Robot Safety Analysis Methods 186
11.7.1 Failure Modes and Effect Analysis (FMEA) 186

11.7.2 Fault Tree Analysis (FTA) 187
11.7.3 The Markov Method 188
11.8 A Methodology for Safer Robot Design and General Guidelines for Minimizing the Safety Problems of Robots 193
Problems 196
References 196

**Chapter 12 Safety in Health Care Systems 199**

12.1 Introduction 199
12.2 Facts and Figures 200
12.3 Medical Device/Equipment Safety versus Reliability 200
12.4 Medical Device Safety Types, and Medical Device Hardware and Software Safety 201
12.5 Patient Injury and Medical Device Accident Causes 202
12.6 Human Error in Health Care Systems 203
12.6.1 Medical Device/Equipment Associated Operator Errors 205
12.6.2 Medical Devices/Equipment with a High Occurrence of Human Error 205
12.7 Medical Device Safety Requirements and Legal Aspects 205
12.8 Models for Predicting Accident Occurrence Probability of a Medical Device/Equipment 208
12.8.1 Model I 208
12.8.2 Model II 209
12.9 Organizations, Standards, and Data Sources 211
12.9.1 Organizations 211
12.9.2 Standards 211
12.9.3 Data Sources 212
Problems 212
References 213

***Index*** 215