

CONTENTS

| | |
|--|------|
| Foreword | xiii |
| Preface | xv |
| Introduction | xix |
| Acknowledgements | xx |
| | |
| 1. An Incomplete History of Risk Management | 1 |
| <i>Concern Over Technological Risks</i> | 3 |
| <i>Responses to Risks</i> | 4 |
| <i>Conclusion</i> | 7 |
| | |
| 2. Hazards and Risks: Concepts and Definitions of Important Terms | 9 |
| <i>Hazard</i> | 9 |
| <i>Risk</i> | 12 |
| <i>Accidents, Failures, and Other Undesired Events</i> | 15 |
| <i>Risk Management</i> | 16 |
| <i>Conclusion</i> | 18 |
| | |
| 3. How We Think About Risk | 19 |
| <i>Risk Perception</i> | 20 |
| <i>Risk Judgment</i> | 22 |

| | |
|--|-----------|
| Rules That Shape Our Decisions About Risk | 24 |
| <i>Representativeness</i> | 26 |
| <i>Options and Decision Making</i> | 27 |
| <i>The Role of Trust in Communicating Risk</i> | 27 |
| What All This Means As We Assess and Manage Risks | 28 |
| | |
| 4. Accident Theory | 31 |
| <i>Single-Event Model</i> | 32 |
| <i>Chain-of-Events Models</i> | 33 |
| <i>Hierarchical Models</i> | 34 |
| <i>Factorial Model</i> | 36 |
| <i>Systems Accident</i> | 37 |
| <i>Individual and Human Factors</i> | 39 |
| <i>Conclusion</i> | 40 |
| | |
| 5. An Overview of the Risk Management Process | 43 |
| <i>System Definition</i> | 45 |
| <i>Hazard Identification</i> | 46 |
| <i>Risk Estimation</i> | 46 |
| <i>Risk Evaluation</i> | 47 |
| <i>Risk Control</i> | 48 |
| <i>Risk Monitoring and Re-evaluation</i> | 49 |
| <i>Risk Communication</i> | 50 |
| <i>Conclusion</i> | 50 |
| | |
| 6. Risk Communication | 51 |
| <i>Elements of a Risk Communication Process</i> | 53 |
| <i>Problems in Risk Communication</i> | 54 |
| <i>Effectively Communicating Risks</i> | 57 |
| <i>Conclusion</i> | 61 |

| | |
|---|-----------|
| 7. An Overview of Risk Assessment Tools | 63 |
| <i>Inductive and Deductive Tools</i> | 64 |
| <i>Tabular or Graphic Tools</i> | 65 |
| <i>Qualitative, Semi-quantitative, or Quantitative Tools</i> | 65 |
| <i>Where Do They End?</i> | 66 |
| <i>Tasks Common to All Tools</i> | 66 |
| <i>Preliminary Risk Analysis (PRA) and Preliminary Hazard Analysis (PHA)</i> | 69 |
| Description | 69 |
| Background | 69 |
| Features and Benefits | 70 |
| Limitations | 70 |
| When Used | 70 |
| Conducting a Preliminary Risk Analysis | 70 |
| <i>Failure Mode and Effects Analysis (FMEA) or Failure Mode, Effects, and Criticality Analysis (FMECA)</i> | 72 |
| Description | 72 |
| Background | 73 |
| Features and Benefits | 74 |
| Limitations | 74 |
| When Used | 74 |
| Conducting an FMECA | 74 |
| <i>Fault Tree Analysis (FTA)</i> | 76 |
| Description | 76 |
| Background | 76 |
| Features and Benefits | 77 |
| Limitations | 77 |
| When Used | 78 |
| Conducting a Fault Tree Analysis | 78 |

| | |
|---|------------|
| Event Tree Analysis (ETA) | 80 |
| Description | 80 |
| Background | 80 |
| Features and Benefits | 80 |
| Limitations | 81 |
| When Used | 81 |
| How to Perform an Event Tree Analysis | 81 |
| Hazard and Operability Studies (HAZOPS) | 83 |
| Description | 83 |
| Background | 83 |
| Features and Benefits | 83 |
| Limitations | 84 |
| When Used | 84 |
| How to Perform a HAZOPS | 84 |
| Conclusion | 85 |
| 8. Risk Evaluation | 87 |
| Three Possible Outcomes of a Risk Evaluation | 90 |
| Evaluating Risks | 92 |
| Safety Factor | 94 |
| Conclusion | 94 |
| 9. Risk Control | 95 |
| Prevent or Protect | 96 |
| Control Measures | 96 |
| Layers of Control | 102 |
| Problems with Automated Controls | 103 |
| Problems with Procedural Controls | 104 |
| Selecting Controls | 106 |
| Conclusion | 107 |

| | |
|--|------------|
| 10. Risk Monitoring | 109 |
| <i>Conclusion</i> | 111 |
| 11. Risk-Related Documentation and Records | 113 |
| <i>Types of Documents and Records</i> | 114 |
| <i>Purpose of Risk-related Documents and Records</i> | 115 |
| <i>“Risk Management File”</i> | 116 |
| <i>“Risk Management Plan”</i> | 116 |
| <i>“Risk Management Report”</i> | 116 |
| <i>Documents and Records Required by HACCP</i> | 117 |
| <i>“Risk Information Library”</i> | 117 |
| <i>Conclusion</i> | 118 |
| 12. Hazard Analysis and Critical Control Points (HACCP) | 119 |
| <i>Information Needed for HACCP</i> | 122 |
| <i>Definitions Used in HACCP</i> | 123 |
| <i>Conducting a HACCP</i> | 124 |
| <i>Preliminary Tasks</i> | 124 |
| <i>HACCP Principles</i> | 126 |
| <i>Functional Documents</i> | 138 |
| <i>Records</i> | 139 |
| <i>Conclusion</i> | 141 |
| 13. Preliminary Risk Analysis (PRA) | 147 |
| <i>Types of PRAs</i> | 148 |
| <i>Information Needed</i> | 154 |
| <i>Performing a PRA</i> | 154 |
| <i>Conclusion</i> | 158 |

| | |
|--|------------|
| 14. Failure Mode, Effects, and Criticality Analysis (FMECA) | 163 |
| <i>Types of FMECAs</i> | 166 |
| <i>Information Needed</i> | 169 |
| <i>Terminology Used in FMECAs</i> | 169 |
| <i>Performing an FMECA</i> | 172 |
| <i>Conclusion</i> | 181 |
| | |
| 15. Hazard and Operability Studies (HAZOPS) | 185 |
| <i>Types of HAZOPS</i> | 186 |
| <i>Information Required</i> | 187 |
| <i>Terminology Used in HAZOPS</i> | 189 |
| <i>Performing a HAZOPS</i> | 190 |
| <i>A HAZOPS Variation</i> | 195 |
| <i>CHAZOPS: HAZOPS for Computerized Systems</i> | 195 |
| <i>Procedural HAZOPS</i> | 196 |
| <i>Conclusion</i> | 197 |
| | |
| 16. Fault Tree Analysis (FTA) | 201 |
| <i>Definitions</i> | 204 |
| <i>Structure of a Fault Tree</i> | 205 |
| <i>Events</i> | 206 |
| <i>Gates</i> | 209 |
| <i>AND Gates</i> | 210 |
| <i>OR Gates</i> | 211 |
| <i>Specialized Gates</i> | 211 |
| <i>Conducting an FTA</i> | 212 |
| <i>Documentation</i> | 221 |
| <i>Conclusion</i> | 222 |

| | |
|--|------------|
| 17. Event Tree Analysis (ETA) | 223 |
| <i>Definitions</i> | 225 |
| <i>Performing an ETA</i> | 226 |
| <i>Documentation</i> | 232 |
| <i>Conclusion</i> | 232 |
| | |
| 18. Auditing a Risk Management Program | 233 |
| <i>Items to Consider When Auditing a Risk Management Program</i> | 238 |
| <i>Items to Consider When Auditing a Risk Assessment</i> | 238 |
| <i>Conclusion</i> | 239 |
| | |
| 19. The Organization and Risk Management | 241 |
| <i>Enterprise Risk Management</i> | 242 |
| <i>Integrating Risk Management and Quality System Elements</i> | 243 |
| <i>Problem Investigations</i> | 244 |
| <i>The Risks of Being Risk Adverse</i> | 246 |
| <i>Supporting Risk Management</i> | 246 |
| <i>Managing Risk in the Future</i> | 249 |
| | |
| References | 251 |
| | |
| Index | 267 |