Hazard Analysis Techniques for System Safety

Hazard Analysis Techniques for System Safety

Clifton A. Ericson, II
Fredericksburg, Virginia

WILEY-INTERSCIENCE
A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print, however, may not be available in electronic format.

Library of Congress Cataloging-in-Publication Data:

Ericson, Clifton A.
Hazard analysis techniques for system safety / Clifton A. Ericson.
p. cm.
Includes index.
ISBN 0-471-72019-4 (cloth)
1. Industrial safety--Data processing. 2. System safety. I. Title.
T55.E72 2005
620.8′6--dc22
2005001260

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

PREFACE **xvii**

ACKNOWLEDGMENTS **xix**

1. System Safety **1**

1.1 Introduction / 1
1.2 System Safety Background / 2
1.3 System Safety Characterization / 3
1.4 System Safety Process / 4
1.5 System Concept / 5
1.5.1 General System Model / 5
1.5.2 System Attributes / 7
1.5.3 System Types / 8
1.5.4 System Life Cycle / 9
1.5.5 System Development / 10
1.6 Summary / 12

2. Hazards, Mishap, and Risk **13**

2.1 Introduction / 13
2.2 Hazard-Related Definitions / 14
2.3 Hazard Theory / 15
2.4 Hazard Actuation / 19
2.5 Hazard Causal Factors / 21
2.6 Hazard–Mishap Probability / 23
2.7 Recognizing Hazards / 23

2.8 Hazard Description / 27
2.9 Summary / 27

3. Hazard Analysis Types and Techniques 31

3.1 Types and Techniques / 31
3.2 Description of Hazard Analysis Types / 34
3.2.1 Conceptual Design Hazard Analysis Type (CD-HAT) / 34
3.2.2 Preliminary Design Hazard Analysis Type (PD-HAT) / 35
3.2.3 Detailed Design Hazard Analysis Type (DD-HAT) / 37
3.2.4 System Design Hazard Analysis Type (SD-HAT) / 38
3.2.5 Operations Design Hazard Analysis Type (OD-HAT) / 40
3.2.6 Human Design Hazard Analysis Type (HD-HAT) / 41
3.2.7 Requirements Design Hazard Analysis Type (RD-HAT) / 42
3.3 Timing of Hazard Analysis Types / 44
3.4 Interrelationship of Hazard Analysis Types / 44
3.5 Hazard Analysis Techniques / 45
3.5.1 Technique Attributes / 45
3.5.2 Primary Hazard Analysis Techniques / 46
3.6 Inductive and Deductive Techniques / 48
3.7 Qualitative and Quantitative Techniques / 51
3.8 Summary / 53

4. Preliminary Hazard List 55

4.1 Introduction / 55
4.2 Background / 55
4.3 History / 56
4.4 Theory / 56
4.5 Methodology / 57
4.6 Worksheet / 60
4.7 Hazard Checklists / 62
4.8 Guidelines / 64
4.9 Example: Ace Missile System / 65

4.10 Advantages and Disadvantages / 70
4.11 Common Mistakes to Avoid / 71
4.12 Summary / 71

5. Preliminary Hazard Analysis **73**

5.1 Introduction / 73
5.2 Background / 73
5.3 History / 74
5.4 Theory / 75
5.5 Methodology / 76
5.6 Worksheet / 78
5.7 Guidelines / 81
5.8 Example: Ace Missile System / 82
5.9 Advantages and Disadvantages / 85
5.10 Common Mistakes to Avoid / 85
5.11 Summary / 93

6. Subsystem Hazard Analysis **95**

6.1 Introduction / 95
6.2 Background / 95
6.3 History / 96
6.4 Theory / 96
6.5 Methodology / 97
6.6 Worksheet / 98
6.7 Guidelines / 102
6.8 Example: Ace Missile System / 103
6.9 Advantages and Disadvantages / 107
6.10 Common Mistakes to Avoid / 107
6.11 Summary / 113

7. System Hazard Analysis **115**

7.1 Introduction / 115
7.2 Background / 116
7.3 History / 117
7.4 Theory / 117
7.5 Methodology / 118
7.6 Worksheet / 120
7.7 Guidelines / 122

7.8 Example / 123
7.9 Advantages and Disadvantages / 128
7.10 Common Mistakes to Avoid / 129
7.11 Summary / 129

8. Operating and Support Hazard Analysis 131

8.1 Introduction / 131
8.2 Background / 131
8.3 History / 133
8.4 Definitions / 133
8.5 Theory / 134
8.6 Methodology / 135
8.7 Worksheet / 138
8.8 Hazard Checklists / 140
8.9 Support Tools / 140
8.10 Guidelines / 142
8.11 Examples / 143
8.11.1 Example 1 / 143
8.11.2 Example 2 / 143
8.12 Advantages and Disadvantages / 152
8.13 Common Mistakes to Avoid / 152
8.14 Summary / 152

9. Health Hazard Assessment 155

9.1 Introduction / 155
9.2 Background / 155
9.3 History / 156
9.4 Theory / 156
9.5 Methodology / 157
9.6 Worksheet / 160
9.7 Checklist / 162
9.8 Example / 164
9.9 Advantages and Disadvantages / 164
9.10 Common Mistakes to Avoid / 168
9.11 Summary / 168

10. Safety Requirements/Criteria Analysis 169

10.1 Introduction / 169
10.2 Background / 169

10.3 History / 170
10.4 Theory / 170
10.5 Methodology / 171
10.6 Worksheets / 172
10.7 Example / 175
10.8 Advantages and Disadvantages / 175
10.9 Common Mistakes to Avoid / 180
10.10 Summary / 180

11. Fault Tree Analysis 183

11.1 Introduction / 183
11.2 Background / 185
11.3 History / 186
11.4 Theory / 187
11.5 Methodology / 188
11.5.1 Building Blocks / 188
11.5.2 Definitions / 191
11.5.3 Construction—Basics / 193
11.5.4 Construction—Advanced / 195
11.5.5 Construction Rules / 196
11.6 Functional Block Diagrams / 197
11.7 Cut Sets / 198
11.8 MOCUS Algorithm / 199
11.9 Bottom-Up Algorithm / 199
11.10 Mathematics / 201
11.11 Probability / 202
11.12 Importance Measures / 204
11.13 Example 1 / 206
11.14 Example 2 / 207
11.15 Example 3 / 210
11.16 Phase- and Time-Dependent FTA / 215
11.17 Dynamic FTA / 218
11.18 Advantages and Disadvantages / 219
11.19 Common Mistakes to Avoid / 220
11.20 Summary / 220

12. Event Tree Analysis 223

12.1 Introduction / 223
12.2 Background / 223

12.3 History / 224
12.4 Definitions / 225
12.5 Theory / 225
12.6 Methodology / 228
12.7 Worksheet / 230
12.8 Example 1 / 231
12.9 Example 2 / 231
12.10 Example 3 / 231
12.11 Example 4 / 231
12.12 Advantages and Disadvantages / 233
12.13 Common Mistakes to Avoid / 233
12.14 Summary / 233

13. Failure Mode and Effects Analysis 235

13.1 Introduction / 235
13.2 Background / 236
13.3 History / 237
13.4 Definitions / 237
13.5 Theory / 238
13.5.1 Structural and Functional Models / 241
13.5.2 Product and Process FMEA / 242
13.5.3 Functional Failure Modes / 242
13.5.4 Hardware Failure Modes / 242
13.5.5 Software Failure Modes / 243
13.5.6 Quantitative Data Sources / 244
13.6 Methodology / 244
13.7 Worksheet / 247
13.8 Example 1: Hardware Product FMEA / 251
13.9 Example 2: Functional FMEA / 252
13.10 Level of Detail / 252
13.11 Advantages and Disadvantages / 255
13.12 Common Mistakes to Avoid / 258
13.13 Summary / 258

14. Fault Hazard Analysis 261

14.1 Introduction / 261
14.2 Background / 261
14.3 History / 262

14.4 Theory / 262
14.5 Methodology / 263
14.6 Worksheet / 265
14.7 Example / 266
14.8 Advantages and Disadvantages / 267
14.9 Common Mistakes to Avoid / 269
14.10 Summary / 269

15. Functional Hazard Analysis **271**

15.1 Introduction / 271
15.2 Background / 271
15.3 History / 272
15.4 Theory / 272
15.5 Methodology / 273
15.6 Worksheets / 275
15.7 Example 1: Aircraft Flight Functions / 277
15.8 Example 2: Aircraft Landing Gear Software / 278
15.9 Example 3: Ace Missile System / 278
15.10 Advantages and Disadvantages / 278
15.11 Common Mistakes to Avoid / 281
15.12 Summary / 284

16. Sneak Circuit Analysis **291**

16.1 Introduction / 291
16.2 Background / 292
16.3 History / 293
16.4 Definitions / 293
16.5 Theory / 294
16.6 Methodology / 295
16.6.1 Step 1: Acquire Data / 296
16.6.2 Step 2: Code Data / 296
16.6.3 Step 3: Process Data / 297
16.6.4 Step 4: Produce Network Trees / 297
16.6.5 Step 5: Identify Topographs / 298
16.6.6 Step 6: Perform Analysis / 298
16.6.7 Step 7: Generate Report / 299
16.7 Example 1: Sneak Path / 300
16.8 Example 2: Sneak Label / 301

16.9 Example 3: Sneak Indicator / 301
16.10 Example Sneak Clues / 301
16.11 Software Sneak Circuit Analysis / 303
16.12 Advantages and Disadvantages / 304
16.13 Common Mistakes to Avoid / 305
16.14 Summary / 305

17. Petri Net Analysis (PNA) 307

17.1 Introduction / 307
17.2 Background / 307
17.3 History / 308
17.4 Definitions / 308
17.5 Theory / 309
17.6 Methodology / 309
17.7 Examples / 313
17.8 Advantages and Disadvantages / 315
17.9 Common Mistakes to Avoid / 315
17.10 Summary / 315

18. Markov Analysis 317

18.1 Introduction / 317
18.2 Background / 318
18.3 History / 318
18.4 Definitions / 319
18.5 Theory / 320
18.6 Methodology / 320
18.6.1 State Transition Diagram Construction / 320
18.6.2 State Equation Construction / 323
18.7 Examples / 325
18.7.1 Markov Chain / 325
18.7.2 Markov Model of Two-Component Series System with No Repair / 325
18.7.3 Markov Model of Two-Component Parallel System with No Repair / 326
18.7.4 Markov Model of Two-Component Parallel System with Component Repair / 326
18.7.5 Markov Model of Two-Component Parallel System with Component/System Repair / 327

18.7.6 Markov Model of Two-Component Parallel System with Sequencing / 328
18.8 Markov Analysis and FTA Comparisons / 328
18.9 Advantages and Disadvantages / 331
18.10 Common Mistakes to Avoid / 332
18.11 Summary / 332

19. Barrier Analysis 335

19.1 Introduction / 335
19.2 Background / 335
19.3 History / 336
19.4 Definitions / 337
19.5 Theory / 337
19.6 Methodology / 338
19.6.1 Example Checklist of Energy Sources / 338
19.6.2 Considerations / 338
19.7 Worksheet / 344
19.8 Example / 347
19.9 Advantages and Disadvantages / 347
19.10 Common Mistakes to Avoid / 349
19.11 Summary / 350

20. Bent Pin Analysis 353

20.1 Introduction / 353
20.2 Background / 353
20.3 History / 354
20.4 Theory / 354
20.5 Methodology / 356
20.6 Worksheet / 356
20.7 Example / 358
20.8 Advantages and Disadvantages / 360
20.9 Common Mistakes to Avoid / 364
20.10 Summary / 364

21. Hazard and Operability Analysis 365

21.1 Introduction / 365
21.2 Background / 366
21.3 History / 366

21.4 Theory / 367
21.5 Methodology / 368
21.5.1 Design Representations / 370
21.5.2 System Parameters / 371
21.5.3 Guide Words / 372
21.5.4 Deviation from Design Intent / 372
21.6 Worksheet / 373
21.7 Example 1 / 375
21.8 Example 2 / 376
21.9 Advantages and Disadvantages / 376
21.10 Common Mistakes to Avoid / 379
21.11 Summary / 379

22. Cause–Consequence Analysis **383**

22.1 Introduction / 383
22.2 Background / 383
22.3 History / 384
22.4 Definitions / 385
22.5 Theory / 385
22.6 Methodology / 386
22.7 Symbols / 388
22.8 Worksheet / 388
22.9 Example 1: Three-Component Parallel System / 389
22.10 Example 2: Gas Pipeline System / 389
22.10.1 Reducing Repeated Events / 390
22.11 Advantages and Disadvantages / 394
22.12 Common Mistakes to Avoid / 395
22.13 Summary / 395

23. Common Cause Failure Analysis **397**

23.1 Introduction / 397
23.2 Background / 398
23.3 History / 399
23.4 Definitions / 399
23.5 Theory / 401
23.6 Methodology / 404
23.7 Defense Mechanisms / 413
23.8 Example / 414

23.9 Models / 419
23.10 Advantages and Disadvantages / 420
23.11 Common Mistakes to Avoid / 420
23.12 Summary / 420

24. Management Oversight Risk Tree Analysis 423

24.1 Introduction / 423
24.2 Background / 423
24.3 History / 424
24.4 Theory / 424
24.5 Methodology / 425
24.6 Worksheet / 425
24.7 Advantages and Disadvantages / 427
24.8 Common Mistakes to Avoid / 429
24.9 Summary / 430

25. Software Safety Assessment 431

25.1 Introduction / 431
25.2 Background / 431
25.3 History / 432
25.4 Theory / 432
25.5 Methodology / 433
25.6 Worksheet / 434
25.7 Software Risk Level / 436
25.8 Example / 437
25.9 Advantages and Disadvantages / 448
25.10 Common Mistakes to Avoid / 448
25.11 Summary / 448

26. Summary 451

26.1 Principle 1: Hazards, Mishaps, and Risk are Not Chance Events / 451
26.2 Principle 2: Hazards are Created During Design / 452
26.3 Principle 3: Hazards are Comprised of Three Components / 453
26.4 Principle 4: Hazard and Mishap Risk Management Is the Core Safety Process / 454
26.5 Principle 5: Hazard Analysis Is a Key Element of Hazard and Mishap Risk Management / 455

26.6 Principle 6: Hazard Management Involves Seven Key Hazard Analysis Types / 455
26.7 Principle 7: Hazard Analysis Primarily Encompasses Seven Hazard Analysis Techniques / 456
26.8 Finis / 457

Appendix A List of Acronyms **461**

Appendix B Glossary **467**

Appendix C Hazard Checklists **483**

Index **497**

Preface

During my 40-year career in system safety there have been two things about hazard analysis that have always bothered me. First, there has never been a formal description of hazard theory that defines the components of a hazard and the hazard–mishap actuation process. Second, there is a lack of good reference material describing in detail how to perform the most relevant hazard analysis techniques or methodologies. I wrote this book to resolve these issues for system safety engineers and practitioners. The material in this book is applicable to both experienced professionals and those analysts just starting out in the field.

One of the main features of this book is that it describes hazard theory in detail. The hazard–risk–mishap connection is explained, with illustrations and examples provided. In addition, the three required components of a hazard are presented, along with the hazard triangle model.

Another primary feature of this book is that it describes 22 of the most commonly used hazard analysis methodologies in the system safety discipline. Each of the 22 hazard analysis methodologies covered in this book is given an entire chapter devoted to just that technique. In addition, each methodology chapter is organized in a similar pattern that is intended to provide consistency in answering the most common questions that an analyst might have. Detailed examples are provided to help analysts learn and understand the methodologies.

System safety is a proven engineering discipline that is applied during system development to identify and mitigate hazards, and in so doing eliminate or reduce the risk of potential mishaps and accidents. System safety is ultimately about savings lives. It is my greatest hope that the readers of this book can use the material contained herein to better understand hazard identification and analysis. This, in turn, will help in designing and constructing systems that are safe, thereby saving many lives.

Acknowledgments

In a book of this undertaking there are naturally many people to acknowledge. This book reflects my life's journey through 40 years of engineering in the system safety discipline. My life has been touched (and influenced) by many people, far too many people to list and credit. For those that I have left out I apologize. But it seems that there are a few people that always remain in the forefront of one's memory.

The first and most important person that I would like to acknowledge is my wife Debbie. She has given me constant support and encouragement to excel in system safety in order to help make the world a safer place. She has also let me take time away from her to give to the System Safety Society and to the writing of this book.

I would like to acknowledge and dedicate this book to the Boeing System Safety organization on the Minuteman Weapon System development program. This was the crucible where the experiment of system safety really started, and this is where I started my career in system safety engineering. This group has provided my most profound work-related memories and probably had the greatest influence on my life. It was led by Niel Classon, who was an early visionary and leader in the system safety field. Other people in this organization that helped in my development include Dave Haasl, Gordon Willard, Dwight Leffingwell, Brad Wolfe, Joe Muldoon, Kaz Kanda, Harvey Moon, and Bob Schroder. Another Boeing manager that provided system safety guidance early in my career was Hal Trettin.

Later in my career Perry D'Antonio of Sandia National Laboratories pushed me to excel in the System Safety Society and to eventually become president of this international organization. Paige Ripani of Applied Ordnance Technology, Inc. helped turn my career in a new direction consulting for the Navy. And, last but not least, Ed Kratovil of the Naval Ordnance Safety and Security Activity (NOSSA) provided me with the opportunity to work on special Navy system and software safety projects.

In addition, I would like to acknowledge and thank the following individuals for reviewing early drafts of this manuscript: Jim Gerber, Sidney Andrews, Dave Shampine, Mary Ellen Caro, Tony Dunay, Chuck Dorney, John Leipper, Kurt Erthner, Ed Nicholson, William Hammer, and Jerry Barnette. Many of their comments and suggestions proved invaluable.

Chapter 1

System Safety

1.1 INTRODUCTION

We live in a world comprised of systems and risk. When viewed from an engineering perspective, most aspects of life involve systems. For example, houses are a type of system, automobiles are a type of system, and electrical power grids are another type of system. Commercial aircraft are systems that operate within an economical transportation system and a worldwide airspace control system. Systems have become a necessity for modern living.

With systems and technology also comes exposure to mishaps because systems can fail or work improperly resulting in damage, injury, and deaths. The possibility that a system fails and results in death, injury, damage, and the like is referred to as mishap risk. For example, there is the danger that a traffic light will fail, resulting in the mishap of another auto colliding with your auto. Automobiles, traffic, and traffic lights form a unique system that we use daily, and we accept the mishap risk potential because the risk is small. There is the danger that the gas furnace in our house will fail and explode, thereby resulting in the mishap of a burned house, or worse. This is another unique system, with known adverse side effects that we choose to live with because the mishap risk is small and the benefits are great.

Our lives are intertwined within a web of different systems, each of which can affect our safety. Each of these systems has a unique design and a unique set of components. In addition, each of these systems contains inherent hazards that present unique mishap risks. We are always making a trade-off between accepting the benefits of a system versus the mishap risk it presents. As we develop and build systems, we should be concerned about eliminating and reducing mishap risk. Some risks are so small that they can easily be accepted, while other risks are so large

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

they must be dealt with immediately. Mishap risk is usually small and acceptable when system design control (i.e., system safety) is applied during the development of the system.

Risks are akin to the invisible radio signals that fill the air around us, in that some are loud and clear, some very faint, and some are distorted and unclear. Life, as well as safety, is a matter of knowing, understanding, and choosing the risk to accept. System safety is the formal process of identifying and controlling mishap risk. As systems become more complex and more hazardous, more effort is required to understand and manage system mishap risk.

The key to system safety and effective risk management is the identification and mitigation of hazards. To successfully control hazards, it is necessary to understand hazards and know how to identify them. The purpose of this book is to better understand hazards and the tools and techniques for identifying them, in order that they can be effectively controlled during the development of a system.

1.2 SYSTEM SAFETY BACKGROUND

The ideal objective of system safety is to develop a system free of hazards. However, absolute safety is not possible because complete freedom from all hazardous conditions is not always possible, particularly when dealing with complex inherently hazardous systems, such as weapons systems, nuclear power plants, and commercial aircraft.

Since it is generally not possible to eliminate all hazards, the realistic objective becomes that of developing a system with acceptable mishap risk. This is accomplished by identifying potential hazards, assessing their risks, and implementing corrective actions to eliminate or mitigate the identified hazards. This involves a systematic approach to the management of mishap risk. Safety is a basic part of the risk management process.

Hazards will always exist, but their risk must and can be made acceptable. Therefore, safety is a relative term that implies a level of risk that is measurable and acceptable. System safety is not an absolute quantity, but rather an optimized level of mishap risk management that is constrained by cost, time, and operational effectiveness (performance). System safety requires that risk be evaluated, and the level of risk accepted or rejected by an appropriate decision authority. Mishap risk management is the basic process of system safety engineering and management functions. System safety is a process of disciplines and controls employed from the initial system design concepts, through detailed design and testing, to system disposal at the completion of its useful life (i.e., “cradle to grave” or “womb to tomb”).

The fundamental objective of system safety is to identify, eliminate or control, and document system hazards. System safety encompasses all the ideals of mishap risk management and design for safety; it is a discipline for hazard identification and control to an acceptable level of risk. Safety is a system attribute that must be intentionally designed into a product. From an historical perspective it has been learned that a proactive preventive approach to safety during system design and development is much more cost effective than trying to add safety into a system after the occurrence of an accident or mishap. System safety is an initial investment that saves future losses that could result from potential mishaps.

1.3 SYSTEM SAFETY CHARACTERIZATION

System safety is the process of managing the system, personnel, environmental, and health mishap risks encountered in the design development, test, production, use, and disposal of systems, subsystems, equipment, materials, and facilities.

A system safety program (SSP) is a formal approach to eliminate hazards through engineering, design, education, management policy, and supervisory control of conditions and practices. It ensures the accomplishment of the appropriate system safety management and engineering tasks. The formal system safety process has been primarily established by the U.S. Department of Defense (DoD) and its military branches and promulgated by MIL-STD-882. However, this same process is also followed in private industry for the development of commercial products, such as commercial aircraft, rail transportation, nuclear power, and automobiles, to mention just a few.

The goal of system safety is the protection of life, systems, equipment, and the environment. The basic objective is the elimination of hazards that can result in death, injury, system loss, and damage to the environment. When hazard elimination is not possible, the next objective is to reduce the risk of a mishap through design control measures. Reducing mishap risk is achieved by reducing the probability of the mishap and/or the severity of the mishap.

This objective can be attained at minimum cost when the SSP is implemented early in the conceptual phase and is continued throughout the system development and acquisition cycle. The overall complexity of today's systems, particularly weapons systems, is such that system safety is required in order to consciously prevent mishaps and accidents. Added to complexity is the inherent danger of energetic materials, the effects of environments, and the complexities of operational requirements. In addition, consideration must be given to hardware failures, human error, software interfaces, including programming errors, and vagaries of the environment.

System safety is defined in MIL-STD-882D as follows:

> The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

The intent of system safety is mishap risk management through hazard identification and mitigation techniques. System safety engineering is an element of systems engineering involving the application of scientific and engineering principles for the timely identification of hazards and initiation of those actions necessary to prevent or control hazards within the system. It draws upon professional knowledge and specialized skills in the mathematical and scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, evaluate, and document the safety of the system.

System safety management is an element of program management that ensures accomplishment of the correct mix of system safety tasks. This includes identification of system safety requirements; planning, organizing, and controlling those efforts that are directed toward achieving the safety goals; coordinating with other program elements; and analyzing, reviewing, and evaluating the program to ensure effective and timely realization of the system safety objectives.

The basic concept of system safety is that it is a formal process of intentionally designing in safety by designing out hazards or reducing the mishap risk of hazards. It is a proactive process performed throughout the system life cycle to save lives and resources by intentionally reducing the likelihood of mishaps to an insignificant level. The system life cycle is typically defined as the stages of concept, preliminary design, detailed design, test, manufacture, operation, and disposal (demilitarization). In order to be proactive, safety must begin when system development first begins at the conceptual stage.

The goal of system safety is to ensure the detection of hazards to the fullest extent possible and provide for the introduction of protective measures early enough in system development to avoid design changes late in the program. A safe design is a prerequisite for safe operations. Things that can go wrong with systems are predictable, and something that is predictable is also preventable. As Murphy's law states "whatever can go wrong, will go wrong." The goal of system safety is to find out what can go wrong (before it does) and establish controls to prevent it or reduce the probability of occurrence. This is accomplished through hazard identification and mitigation.

1.4 SYSTEM SAFETY PROCESS

MIL-STD-882D establishes the core system safety process in eight principal steps, which are shown in Figure 1.1. The core system safety process involves establishing an SSP to implement the mishap risk management process. The SSP is formally documented in the system safety program plan (SSPP), which specifies all of the safety tasks that will be performed, including the specific hazard analyses, reports, and so forth. As hazards are identified, their risk will be assessed, and hazard mitigation methods will be established to mitigate the risk as determined necessary. Hazard mitigation methods are implemented into system design via system safety requirements (SSRs). All identified hazards are converted into hazard action records

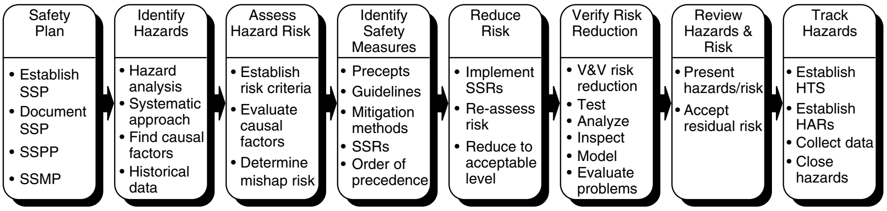


Figure 1.1 *Core system safety process.*

(HARs) and placed into a hazard tracking system (HTS). Hazards are continually tracked in the HTS until they can be closed.

It can be seen from the core system safety process that safety revolves around hazards. Hazard identification and elimination/mitigation is the key to this process. Therefore, it is critical that the system safety analyst understand hazards, hazard identification, and hazard mitigation.

The core system safety process can be reduced to the process shown in Figure 1.2. This is a mishap risk management process whereby safety is achieved through the identification of hazards, the assessment of hazard mishap risk, and the control of hazards presenting unacceptable risk. This is a closed-loop process whereby hazards are identified and tracked until acceptable closure action is implemented and verified. It should be performed in conjunction with actual system development, in order that the design can be influenced during the design process, rather than trying to enforce design changes after the system is developed.

System safety involves a life-cycle approach based on the idea that mishap and accident prevention measures must be initiated as early as possible in the life of a system and carried through to the end of its useful life. It is usually much cheaper and more effective to design safety features into an item of equipment than it is to add the safety features when the item is in production or in the field. Also, experience indicates that that some of the hazards in a newly designed system will escape detection, no matter how aggressive the safety program. Therefore, the safety program for a system must remain active throughout the life of the system to ensure that safety problems are recognized whenever they arise and that appropriate corrective action is taken.

The key to system safety is the management of hazards. To effectively manage hazards, one must understand hazard theory and the identification of hazards. The purpose of this book is to better understand hazards and the tools and techniques for identifying them. When hazards are identified and understood, they can then be properly eliminated or mitigated.

1.5 SYSTEM CONCEPT

1.5.1 General System Model

As implied in the name, system safety is involved with "systems" and with the many different characteristics and attributes associated with systems. Therefore, in order

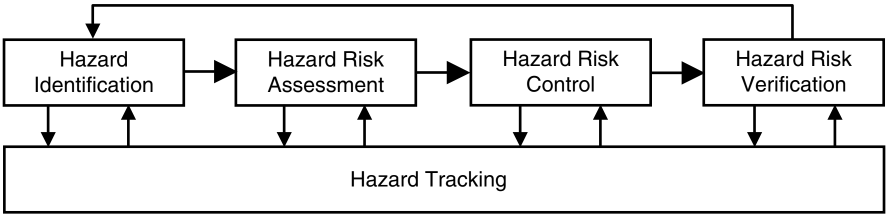


Figure 1.2 *Closed-loop hazard control process.*

to effectively apply the system safety process, it is necessary to completely understand the term *system* and all of its ramifications. This includes understanding what comprises a system, how a system operates, system analysis tools, the life cycle of a system, and the system development process. A proactive and preventive safety process can only be effectively implemented if the proper system-oriented safety tasks are performed during the appropriate system life-cycle phases, in conjunction with utilizing the appropriate system engineering tools. The timing and content of safety tasks must coincide with certain system development domains to ensure safety success.

The standard definition of a system from MIL-STD-882 is:

> A system is a composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.

Essentially a system is a combination of subsystems interconnected to accomplish the system objective.

A subsystem is a subset of the system that could include equipment, components, personnel, facilities, processes, documentation, procedures, and software interconnected in the system to perform a specific function that contributes to accomplishing the system objective.

The system objective is a desired result to be accomplished by the system. The system objective defines the purpose for the system. System functions are the operations the system must perform in order to accomplish its objective. System functions are generally performed by subsystems and define how the system operates.

Figure 1.3 depicts the generic concept of a system. This diagram shows a system comprised of many subsystems, with an interface between each subsystem. The

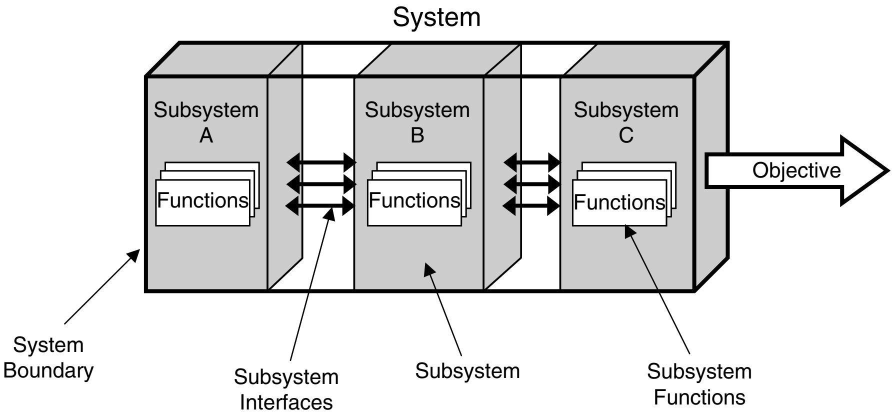


Figure 1.3 *System model.*

system has an objective and is surrounded by a boundary and an environment. System safety analysis involves evaluation of all system aspects, including functions, subsystems, interfaces, boundaries, and environments and the overall system itself.

1.5.2 System Attributes

Systems have many different attributes of interest to system safety. Defining and understanding a system's key attributes is necessary because they provide the framework for designing, building, operating, and analyzing systems. Key system attributes are shown in Table 1.1, where the major attribute categories are listed on the top row, with subelements identified below. Each of these attributes is usually addressed in system safety hazard analyses at some point in the system development program.

Each of the system attributes must be understood in order to perform a complete and thorough hazard analysis. Examples of safety considerations for the elements attribute are as follows:

- *Hardware* Failure modes, hazardous energy sources
- *Software* Design errors, design incompatibilities
- *Personnel* Human error, human injury, human control interface
- *Environment* Weather, external equipment
- *Procedures* Instructions, tasks, warning notes
- *Interfaces* Erroneous input/output, unexpected complexities
- *Functions* Fail to perform, performs erroneously
- *Facilities* Building faults, storage compatibility, transportation faults

An SSP must adequately address each of these system attributes in order to ensure that an optimum degree of safety is achieved in the system. All of the system elements and their interrelationships must be considered in the safety analyses, assessments, and evaluations to ensure it truly is a *system* safety analysis. For example, it is possible for each operational phase or mode to have a different and/or significant impact upon system safety. Different functions are performed

TABLE 1.1 Key System Attributes

Hierarchy	Elements	Domains	Operations	Types
Systems	Hardware	Boundaries	Functions	Static
Subsystems	Software	Complexity	Tasks	Dynamic
Units	Humans	Criticality	Modes	Robotic
Assemblies	Procedures		Phases	Process
Components	Interfaces			Weapon
Piece part	Environments			Aircraft
	Facilities			Spacecraft
	Documentation			⋮

during each phase that could have a direct impact on subsequent phases. During certain phases safety barriers or interlocks are often removed, making the system more susceptible to the occurrence of a hazard, for example, at one point in the operational mission of a missile, the missile is powered and armed. This means that fewer potential failures are now necessary in order for a mishap to occur, and there are fewer safeguards activated in place to prevent hazards from occurring.

1.5.3 System Types

The types of systems dealt with in system safety are typically physical, human-made objects comprised of hardware, software, user interfaces, and procedures. These types of systems include ships, weapons, electrical power, railroads, aircraft, and the like that are used for some specific purpose or objective. Table 1.2 provides some example systems, showing their intended purpose and some of the subsystems comprising these systems. It is interesting to note that many of the systems are comprised of similar types of subsystems, which means that they may have similar types of hazards.

Understanding system type and scope is very important in system safety and hazard analysis. The system type can be an indication of the safety criticality involved. The scope of the system boundaries establishes the size and depth of the system. The system limitations describe basically what the system can and cannot safely do. Certain limitations may require the system to include special design safety features. Every system operates within one or more different environments. The specific environment establishes what the potential hazardous impact will be on the system. System criticality establishes the overall safety rating for the system. A nuclear power plant system has a high consequence safety rating, whereas a TV set as a system has a much lower safety criticality rating.

TABLE 1.2 Example System Types

System	Objective	Subsystems
Ship	Transport people/deliver weapons	Engines, hull, radar, communications, navigation, software, fuel, humans
Aircraft	Transport people/deliver weapons	Engines, airframe, radar, fuel, communications, navigation, software, humans
Missile	Deliver ordnance	Engines, structure, radar, communications, navigation, software
Automobile	Transportation	Engine, frame, computers, software, fuel, humans
Nuclear power plant	Deliver electrical power	Structure, reactor, computers, software, humans, transmission lines, radioactive material
Television	View video media	Structure, receiver, display, electrical power
Toaster	Browning of bread	Structure, timer, electrical elements, electrical power
Telephone	Communication	Structure, receiver, transmitter, electrical power, analog converter

1.5.4 System Life Cycle

The system life cycle involves the actual phases a system goes through from concept through disposal. This system life cycle is analogous to the human life cycle of conception, birth, childhood, adulthood, death, and burial. The life cycle of a system is very generic and generally a universal standard. The system life-cycle stages are generally condensed and summarized into the five major phases shown in Figure 1.4. All aspects of the system life cycle will fit into one of these major categories.

The life-cycle stages of a system are important divisions in the evolution of a product and are therefore very relevant to the system safety process. Safety tasks are planned and referenced around these five phases. In order to proactively design safety into a product, it is essential that the safety process start at the concept definition phase and continue throughout the life cycle.

Phase 1: Concept Definition This phase involves defining and evaluating a potential system concept in terms of feasibility, cost, and risk. The overall project goals and objectives are identified during this basic concept evaluation phase. Design requirements, functions, and end results are formulated. The basic system is roughly designed, along with a thumbnail sketch of the subsystems required and how they will interact. During this phase, safety is concerned with hazardous components and functions that must be used in the system. The system safety program plan (SSPP) is generally started during this phase to outline the overall system risk and safety tasks, including hazard analyses that must be performed.

Phase 2: Development and Test This phase involves designing, developing, and testing the actual system. Development proceeds from preliminary through detailed tasks. The development phase is generally broken into the following stages:

- *Preliminary Design* Initial basic design
- *Detailed Design* Final detailed design
- *Test* System testing to ensure all requirements are met

The preliminary design translates the initial concept into a workable design. During this phase subsystems, components, and functions are identified and established. Design requirements are then written to define the systems, subsystems, and software. Some testing of design alternatives may be performed. During this phase, safety is concerned with hazardous system designs, hazardous components/materials, and hazardous functions that can ultimately lead to mishaps and actions to eliminate/mitigate the hazards.

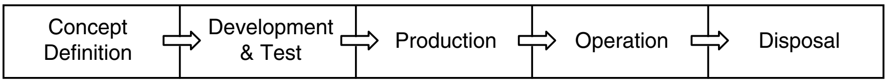


Figure 1.4 *Major system life-cycle phases.*

The preliminary design evolves into the final detailed design. The final design of the system involves completing development of the design specifications, sketches, drawings, and system processes and all subsystem designs. During the final design phase, safety is concerned with hazardous designs, failure modes, and human errors that can ultimately lead to mishaps during the life cycle of the system.

The system test phase involves verification and validation testing of the design to ensure that all design requirements are met and are effective. In addition, safety is concerned with potential hazards associated with the conduct of the test and additional system hazards identified during testing.

Phase 3: Production The final approved design is transformed into the operational end product during the production phase. During this phase, safety is concerned with safe production procedures, human error, tools, methods, and hazardous materials.

Phase 4: Operation The end product is put into actual operation by the user(s) during the operation phase. This phase includes use and support functions such as transportation/handling, storage/stowage, modification, and maintenance. The operational phase can last for many years, and during this phase performance and technology upgrades are likely. Safe system operation and support are the prime safety concerns during this phase. Safety concerns during this phase include operator actions, hardware failures, hazardous system designs, and safe design changes and system upgrades.

Phase 5: Disposal This phase completes the useful life of the product. It involves disposing of the system in its entirety or individual elements, following completion of its useful life. This stage involves phase-out, deconfiguration, or decommissioning where the product is torn down, dismantled, or disassembled. Safe disassembly procedures and safe disposal of hazardous materials are safety concerns during this phase.

Normally each of these life-cycle phases occurs sequentially, but occasionally development tasks are performed concurrently, spirally, or incrementally to shorten the development process. Regardless of the development process used, sequential, concurrent, spiral, or incremental, the system life-cycle phases basically remain the same.

1.5.5 System Development

System development is the process of designing, developing, and testing a system design until the final product meets all requirements and fulfills all objectives. System development consists primarily of phases 1 and 2 of the system life cycle. It is during the development stages that system safety is “designed into” the product for safe operational usage. Figure 3.13 shows the five system life-cycle phases, with phase 2 expanded into preliminary design, final design, and test. These are the most significant phases for applying system safety.

There are several different models by which a system can be developed. Each of these models has advantages and disadvantages, but they all achieve the same end—development of a system. These development models include:

Engineering Development Model This is the standard traditional approach that has been in use for many years. This method performs the system life-cycle phases sequentially. The development and test phase is subdivided into preliminary design, final design, and test for more refinement. Under this model, each phase must be complete and successful before the next phase is entered. This method normally takes the longest length of time because the system is developed in sequential stages. Three major design reviews are conducted for exit from one phase and entry into the next. These are the system design review (SDR), preliminary design review (PDR), and critical design review (CDR). These design reviews are an important aspect of the hazard analysis types discussed in Chapter 3. Figure 1.5 depicts the traditional engineering development model.

Concurrent Engineering This method performs several of the development tasks concurrently in an attempt to save development time. This method has a higher probability for technical risk problems since some items are in preproduction before full development and testing.

Spiral Development In the spiral development process, a desired capability is identified, but the end-state requirements are not known at program initiation. Requirements are refined through demonstration, risk management, and continuous user feedback. Each increment provides the best possible capability, but the requirements for future increments depend on user feedback and technology maturation.

Incremental Development In the incremental development process, a desired capability is identified, an end-state requirement is known, and that requirement is met over time by developing several increments, each dependent on available mature technology. This method breaks the development process into incremental stages in order to reduce development risk. Basic designs, technologies, and methods are developed and proven before more detailed designs are developed.

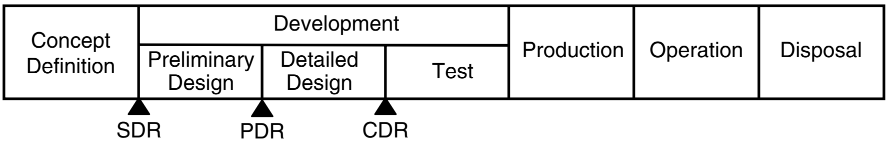


Figure 1.5 *Engineering development model.*

1.6 SUMMARY

This chapter discussed the basic concept of system safety. The following are basic principles that help summarize the discussion in this chapter:

1. The goal of system safety is to save lives and preserve resources by preventing mishaps.
2. Mishaps can be predicted and controlled through the system safety process.
3. The focus of system safety is on hazards, mishaps, and mishap risk.
4. Hazard analysis is essential because hazards are the key to preventing or mitigating mishaps.
5. System safety should be consistent with mission requirements, cost, and schedule.
6. System safety covers all system life-cycle phases, from “cradle to grave.”
7. System safety must be planned, proactive, integrated, comprehensive, and system oriented.

Chapter 2

Hazards, Mishap, and Risk

2.1 INTRODUCTION

In order to design in safety, hazards must be designed out (eliminated) or mitigated (reduced in risk). Hazard identification is a critical system safety function, and thus the correct understanding and appreciation of hazard theory is critical. This chapter focuses on what constitutes a hazard in order that hazards can be recognized and understood during the hazard identification, evaluation, and mitigation processes.

Hazard analysis provides the basic foundation for system safety. Hazard analysis is performed to identify hazards, hazard effects, and hazard causal factors. Hazard analysis is used to determine system risk, to determine the significance of hazards, and to establish design measures that will eliminate or mitigate the identified hazards. Hazard analysis is used to systematically examine systems, subsystems, facilities, components, software, personnel, and their interrelationships, with consideration given to logistics, training, maintenance, test, modification, and operational environments. To effectively perform hazard analyses, it is necessary to understand what comprises a hazard, how to recognize a hazard, and how to define a hazard. To develop the skills needed to identify hazards and hazard causal factors, it is necessary to understand the nature of hazards, their relationship to mishaps, and their effect upon system design.

Many important hazard-related concepts will be presented in this chapter, which will serve as building blocks for hazard analysis and risk evaluation. In sum and substance, humans inherently create the potential for mishaps. Potential mishaps exist as hazards, and hazards exist in system designs. Hazards are actually designed in to the systems we design, build, and operate. In order to perform hazard analysis, the analyst must first understand the nature of hazards. Hazards are predictable, and what can be predicted can also be eliminated or controlled.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

2.2 HAZARD-RELATED DEFINITIONS

The overall system safety process is one of mishap risk management, whereby safety is achieved through the identification of hazards, the assessment of hazard mishap risk, and the control of hazards presenting unacceptable risk. This is a closed-loop process, where hazards are identified, mitigated, and tracked until acceptable closure action is implemented and verified. System safety should be performed in conjunction with actual system development in order that the design can be influenced by safety during the design development process, rather than trying to enforce more costly design changes after the system is developed.

In theory this sounds simple, but in actual practice a common stumbling block is the basic concept of what comprises a hazard, a hazard causal factor (HCF), and a mishap. It is important to clearly understand the relationship between a hazard and an HCF when identifying, describing, and evaluating hazards. To better understand hazard theory, let us start by looking at some common safety-related definitions.

Accident

1. An undesirable and unexpected event; a mishap; an unfortunate chance or event (dictionary).
2. Any unplanned act or event that results in damage to property, material, equipment, or cargo, or personnel injury or death when not the result of enemy action (Navy OP4 & OP5).

Mishap

1. An unfortunate accident (dictionary).
2. An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (MIL-STD-882D).
3. An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. Accident. (MIL-STD-882C). [Note the last word “accident” in the definition.]

Hazard

1. To risk; to put in danger of loss or injury (dictionary).
2. Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment (MIL-STD-882D).
3. A condition that is a prerequisite for an accident (Army AR 385-16).

Risk

1. Hazard; peril; jeopardy (dictionary).
2. An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence (MIL-STD-882D).

Note both the differences and similarities between the above definitions. It should be apparent from these definitions that there is no significant differentiation between a mishap and an accident, and these terms can be used interchangeably. To be consistent with MIL-STD-882D terminology, the term *mishap* will be preferred over the term *accident.*

The dictionary definition states that an accident or mishap is a random chance event, which gives a sense of futility by implying that hazards are unpredictable and unavoidable. System safety, on the other hand, is built upon the premise that mishaps are not random events; instead they are deterministic and controllable events. Mishaps and accidents do not just happen; they are the result of a unique set of conditions (i.e., hazards), which are predictable when properly analyzed. A hazard is a potential condition that can result in a mishap or accident, given that the hazard occurs. This means that mishaps can be predicted via hazard identification. And, mishaps can be prevented or controlled via hazard elimination, control, or mitigation measures. This viewpoint provides a sense of control over the systems we develop and utilize.

2.3 HAZARD THEORY

Per the system safety definitions, a mishap is an actual event that has occurred and resulted in death, injury, and/or loss; and a hazard is a potential condition that can potentially result in death, injury, and/or loss. These definitions lead to the principle that a hazard is the precursor to a mishap; a hazard defines a potential event (i.e., mishap), while a mishap is the occurred event. This means that there is a direct relationship between a hazard and a mishap, as depicted in Figure 2.1.

The concept conveyed by Figure 2.1 is that a hazard and a mishap are two separate states of the same phenomenon, linked by a state transition that must occur.

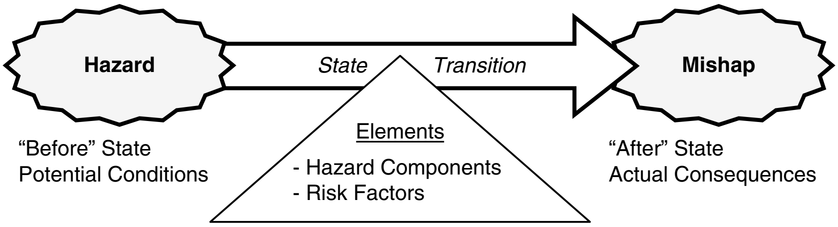


Figure 2.1 *Hazard–mishap relationship.*

You can think of these states as the *before* and *after* states. A hazard is a "potential event" at one end of the spectrum that may be transformed into an "actual event" (the mishap) at the other end of the spectrum based upon the state transition. An analogy might be water, where water is one entity, but it can be in a liquid state or a frozen state, and temperature is the transitional factor.

Figure 2.2 illustrates the hazard–mishap relationship from a different perspective. In this viewpoint, a hazard and a mishap are at opposite ends of the same entity. Again, some transitional event causes the change from the conditional hazard state to the actualized mishap state. Note that both states look almost the same, the difference being that the verb tense has changed from referring to a future potential event to referring to the present actualized event, where some loss or injury has been experienced. A hazard and a mishap are the same entity, only the state has changed, from a hypothesis to a reality.

Mishaps are the immediate result of actualized hazards. The state transition from a hazard to a mishap is based on two factors: (1) the unique set of hazard components involved and (2) the mishap risk presented by the hazard components. The hazard components are the items comprising a hazard, and the mishap risk is the probability of the mishap occurring and the severity of the resulting mishap loss.

Mishap risk is a fairly straightforward concept, where risk is defined as:

$$\text{Risk} = \text{probability} \times \text{severity}$$

The mishap probability factor is the probability of the hazard components occurring and transforming into the mishap. The mishap severity factor is the overall

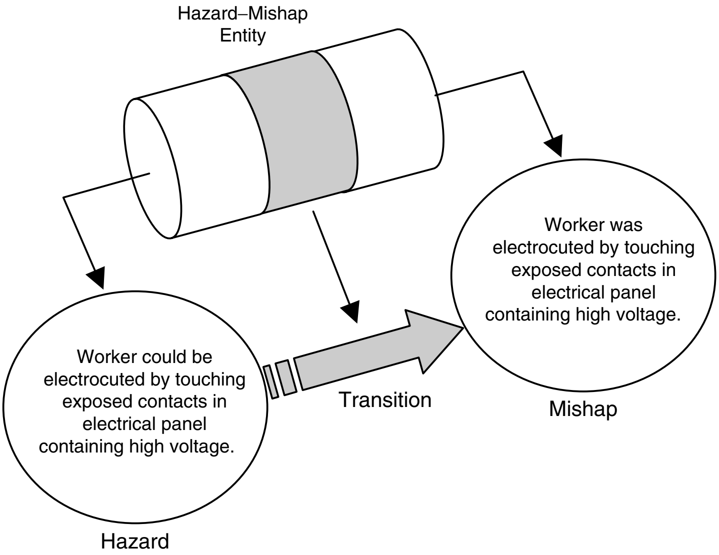

Hazard–Mishap Entity
Worker was electrocuted by touching exposed contacts in electrical panel containing high voltage.
Mishap
Transition
Worker could be electrocuted by touching exposed contacts in electrical panel containing high voltage.
Hazard

Figure 2.2 *Same entity—different states.*

consequence of the mishap, usually in terms of loss resulting from the mishap (i.e., the undesired outcome). Both probability and severity can be defined and assessed in either qualitative terms or quantitative terms. Time is factored into the risk concept through the probability calculation of a fault event, for example, $P_{\text{FAILURE}} = 1.0 - e^{-\lambda T}$, where $T =$ exposure time and $\lambda =$ failure rate.

The hazard component concept is a little more complex in definition. A hazard is an entity that contains only the elements necessary and sufficient to result in a mishap. The components of a hazard define the necessary conditions for a mishap and the end outcome or effect of the mishap.

A hazard is comprised of the following three basic components:

1. *Hazardous Element (HE)* This is the basic hazardous resource creating the impetus for the hazard, such as a hazardous energy source such as explosives being used in the system.
2. *Initiating Mechanism (IM)* This is the trigger or initiator event(s) causing the hazard to occur. The IM causes actualization or transformation of the hazard from a dormant state to an active mishap state.
3. *Target and Threat (T/T)* This is the person or thing that is vulnerable to injury and/or damage, and it describes the severity of the mishap event. This is the mishap outcome and the expected consequential damage and loss.

The three components of a hazard form what is known in system safety as the hazard triangle, as illustrated in Figure 2.3.

The hazard triangle illustrates that a hazard consists of three necessary and coupled components, each of which forms the side of a triangle. All three sides of the triangle are essential and required in order for a hazard to exist. Remove any one of the triangle sides and the hazard is eliminated because it is no longer able to produce a mishap (i.e., the triangle is incomplete). Reduce the probability of the IM triangle side and the mishap probability is reduced. Reduce an element in the HE or the T/T side of the triangle and the mishap severity is reduced. This aspect of a hazard is useful when determining where to mitigate a hazard.

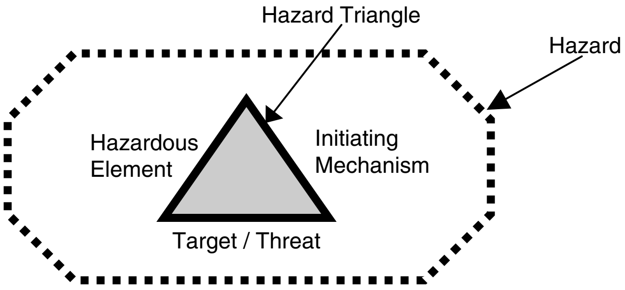


Figure 2.3 *Hazard triangle.*

TABLE 2.1 Example Hazard Components

Hazardous Element	Initiating Mechanism	Target/Threat
• Ordnance	• Inadvertent signal; radio frequency (RF) energy	• Explosion; death/injury
• High-pressure tank	• Tank rupture	• Explosion; death/injury
• Fuel	• Fuel leak and ignition source	• Fire; loss of system; death/injury
• High voltage	• Touching an exposed contact	• Electrocution; death/injury

Table 2.1 provides some example items and conditions for each of the three hazard components. To demonstrate the hazard component concept, consider a detailed breakdown of the following example hazard: "Worker is electrocuted by touching exposed contacts in electrical panel containing high voltage." Figure 2.4 shows how this hazard is divided into the three necessary hazard components.

Note in this example that all three hazard components are present and can be clearly identified. In this particular example there are actually two IMs involved. The T/T defines the mishap outcome, while the combined HE and T/T define the mishap severity. The HE and IM are the HCFs and define the mishap probability. If the high-voltage component can be removed from the system, the hazard is eliminated. If the voltage can be reduced to a lower less harmful level, then the mishap severity is reduced.

Key hazard theory concepts to remember are:

- Hazards result in (i.e., cause) mishaps.
- Hazards are (inadvertently) built into a system.
- Hazards are recognizable by their components.
- A design flaw can be a mishap waiting to happen.
- A hazard will occur according to the hazard components involved.
- A hazard is a deterministic entity and not a random event.
- Hazards (and mishaps) are predictable and, therefore, are preventable or controllable.

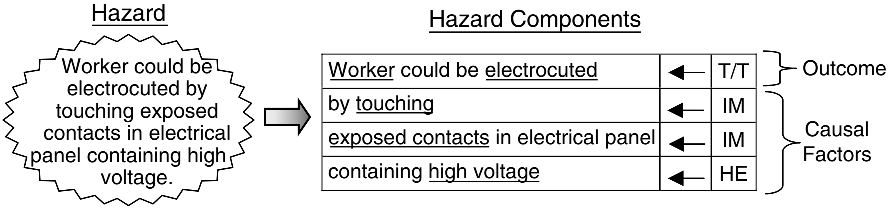

Hazard
Worker could be electrocuted by touching exposed contacts in electrical panel containing high voltage.
Hazard Components
Worker could be electrocuted
T/T
by touching
IM
exposed contacts in electrical panel
IM
containing high voltage
HE
Outcome
Causal Factors

Figure 2.4 Example of hazard components.

2.4 HAZARD ACTUATION

Mishaps are the immediate result of actualized hazards. The state transition from a hazard to a mishap is based on two factors: (1) the unique set of hazard components involved and (2) the mishap risk presented by the hazard components. The hazard components are the items comprising a hazard, and the mishap risk is the probability of the mishap occurring and the severity of the resulting mishap loss.

Figure 2.5 depicts a hazard using the analogy of a molecule, which is comprised of one or more atoms. The molecule represents a hazard, while the atoms represent the three types of components that make up the molecule. The concept is that a hazard is a unique entity, comprised of a unique set of components, similar to a molecule. This set of components consists of three specific required elements: an HE, IM, and T/T. All three specific elements are required, but each element can be one, or more, in quantity. The molecule model indicates that there is no particular order between the hazard components; they all merely exist within the hazard.

When the components within the hazard are in a specific alignment, the hazard transitions from a conditional state to a mishap state. This viewpoint shows that all of the randomly oriented hazard components must line up (or occur) in the correct sequence before the mishap actually occurs. This cause for this sequence of events determines the mishap probability, while the T/T determines the mishap severity. The HE is always present, and the mishap occurs only when the IMs force the transition.

Figure 2.6 presents another way of viewing the hazard–mishap relationship. The spinning wheels represent all of the components forming a particular hazard. Only when the timing is right, and all of the holes in the wheels line up perfectly, does the hazard move from a potential to an actual mishap.

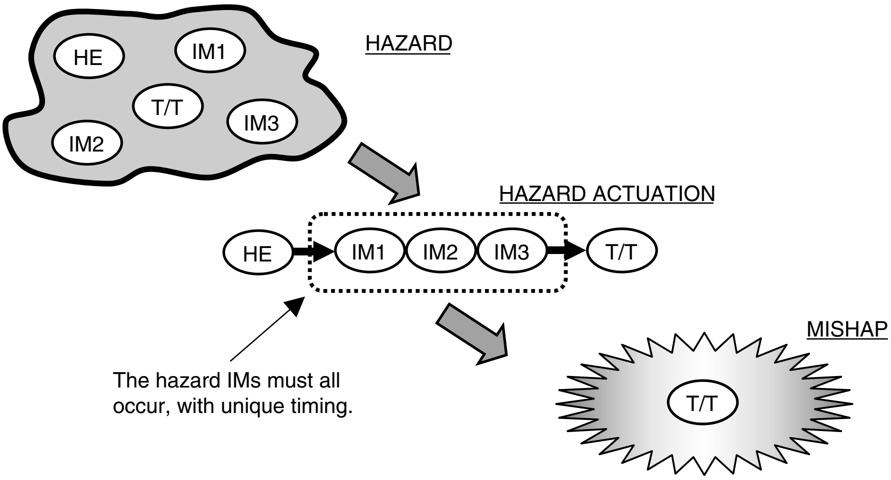


Figure 2.5 *Hazard–mishap actuation (view 1).*

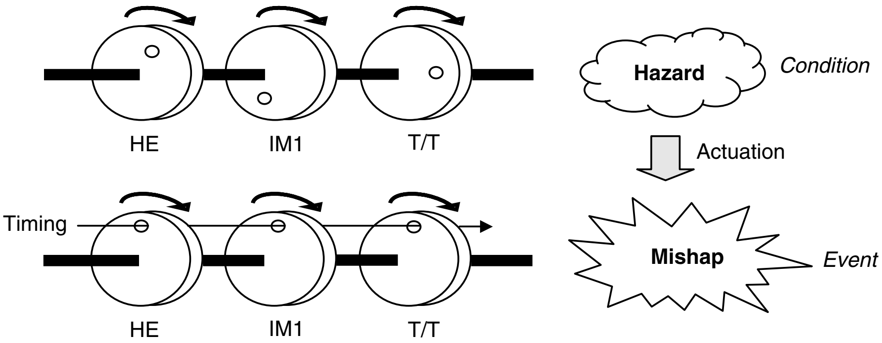


Figure 2.6 Hazard–mishap actuation (view 2).

There are two key points to remember about the hazard–mishap transition process. One, there is generally some sort of energy buildup in the transition phase, which ultimately causes the mishap damage. Two, there is usually a point of no return for the mishap, where there is no possibility of it being reversed. Each individual hazard is unique, and therefore this time period is unique to every hazard.

Figure 2.7 illustrates the hazard–mishap state transition. During the transition phase, the energy buildup occurs as the IMs are occurring. This could also be viewed as the elements of a function being completed, or a functional buildup occurring in a rapid or slow process. It is during this time period that the levels of safety are degrading and the transition process reaches a point of no return, where the hazard becomes irreversible.

A system is designed and built to a specification for the purpose of performing an intended function or functions. But, a system can also contain an inherent design flaw that is capable of performing an unintended and undesirable function. It is this design flaw that provides the necessary events and conditions that comprise a hazard. Quite often this design flaw (hazard) is hidden from the designers because it is not always obvious. These hazards can only be discovered and identified through hazard analysis.

Mishaps do not just happen, they are the result of design flaws inadvertently built into the system design. Thus, in a sense mishaps are predictable events. If a hazard is

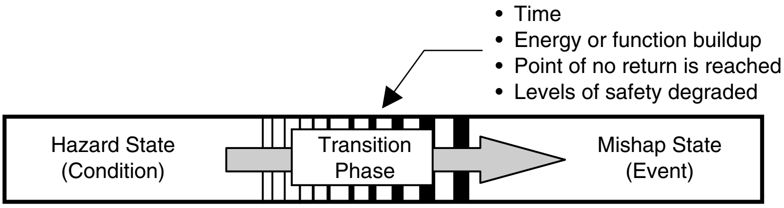

• Time
• Energy or function buildup
• Point of no return is reached
• Levels of safety degraded
Hazard State
(Condition)
Transition
Phase
Mishap State
(Event)

Figure 2.7 Hazard–mishap actuation transition.

eliminated or mitigated, the corresponding mishap is also eliminated or controlled. Therefore, hazard identification and control, via hazard analysis, is the key to mishap prevention.

2.5 HAZARD CAUSAL FACTORS

There is a difference between why hazards exist and how they exist. The basic reason why hazards exist are: (1) They are unavoidable because hazardous elements must be used in the system, and/or (2) they are the result of inadequate design safety consideration. Inadequate design safety consideration results from poor or insufficient design or the incorrect implementation of a good design. This includes inadequate consideration given to the potential effect of hardware failures, sneak paths, software glitches, human error, and the like. HCFs are the specific items responsible for how a unique hazard exists in a system.

Figure 2.8 depicts the overall HCF model. This model correlates all of the factors involved in hazard–mishap theory. The model illustrates that hazards create the potential for mishaps, and mishaps occur based on the level of risk involved (i.e., hazards and mishaps are linked by risk). The three basic hazard components

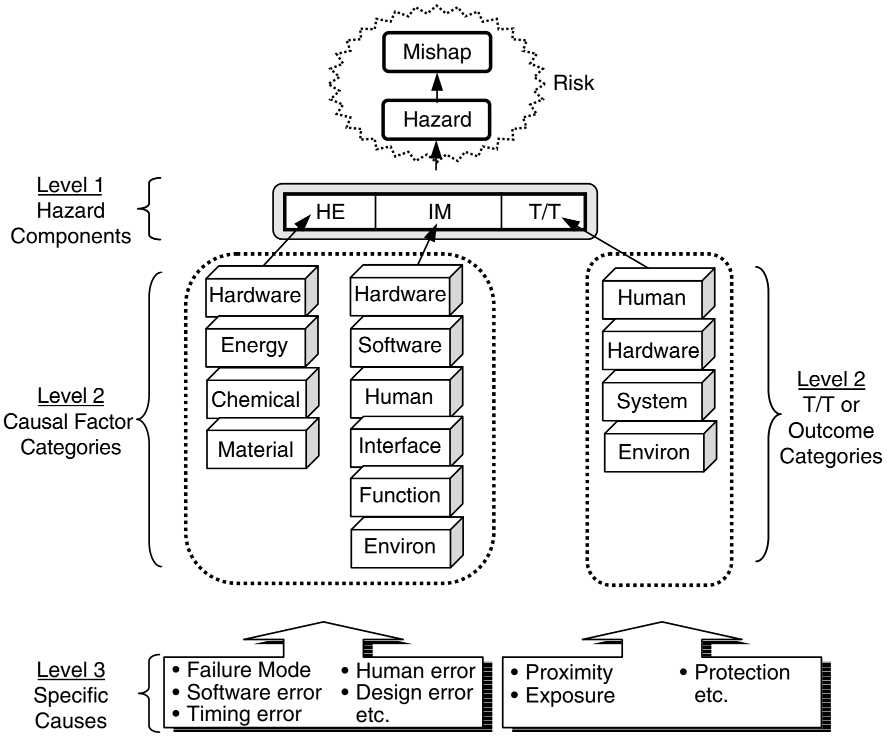


Figure 2.8 Hazard causal factor model.

define both the hazard and the mishap. The three basic hazard components can be further broken into major hazard causal factor categories, which are: (1) hardware, (2) software, (3) humans, (4) interfaces, (5) functions, and (6) the environment. Finally, the causal factor categories are refined even further into the actual specific detailed causes, such as a hardware component failure mode.

Figure 2.8 illustrates how hazard HCFs can be viewed at three different levels:

Level 1: Top Layer The three hazard components (HE, IM, T/T)

Level 2: Midlevel The HCF categories [hardware, software, human system integration (HSI), environment, functions, interfaces]

Level 3: Bottom Level The detailed specific causes (failure modes, errors, etc.)

The top-level hazard HCF categories define the basic root cause sources for all hazards. The first step in HCF identification is to identify the category and then identify the detailed specifics in each category, such as specific hardware component failures, operator errors, software error, and the like. High-level hazards in a preliminary hazard analysis (PHA) might identify root causes at the HCF category level, while a more detailed analysis, such as the subsystem hazard analysis (SSHA), would identify the specific detailed causes at the component level, such as specific component failure modes. A hazard can be initially identified from the causal sources without knowing the specific detailed root causes. However, in order to determine the mishap risk and the hazard mitigation measures required, the specific detailed root causes must eventually be known.

In summary, the basic principles of hazard–mishap theory are as follows:

1. Hazards cause mishaps; a hazard is a condition that defines a possible future event (i.e., mishap).
2. A hazard and a mishap are two different states of the same phenomenon (before and after).
3. Each hazard/mishap has its own inherent and unique risk (probability and severity).
4. A hazard is an entity comprised of three components (HE, IM, T/T).
5. The HE and IM are the HCFs and they establish the mishap probability risk factor.
6. The T/T along with parts of the HE and IM establish the mishap severity risk factor.
7. HCFs can be characterized on three different levels.
8. The probability of a hazard existing is either 1 or 0; however, the probability of a mishap is a function of the specific HCFs.

A hazard is like a minisystem; it is a unique and discrete entity comprised of a unique set of HCFs and outcomes. A hazard defines the terms and conditions of a potential mishap; it is the wrapper containing the entire potential mishap description. The mishap that results is the product of the hazard components.

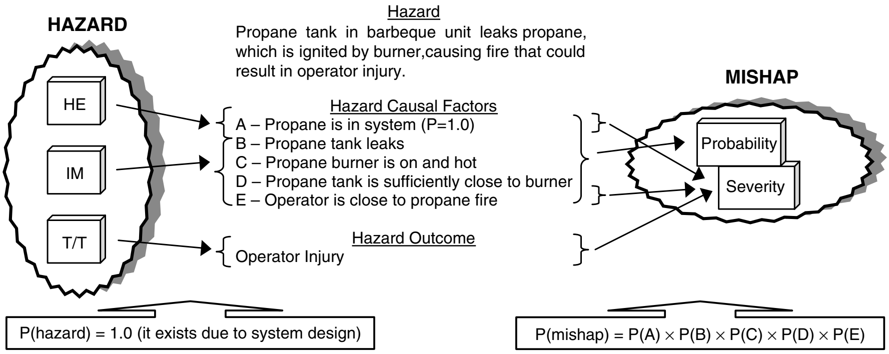

HAZARD
HE
IM
T/T
Hazard
Propane tank in barbeque unit leaks propane, which is ignited by burner,causing fire that could result in operator injury.
Hazard Causal Factors
A – Propane is in system (P=1.0)
B – Propane tank leaks
C – Propane burner is on and hot
D – Propane tank is sufficiently close to burner
E – Operator is close to propane fire
Hazard Outcome
Operator Injury
MISHAP
Probability
Severity
P(hazard) = 1.0 (it exists due to system design)
P(mishap) = P(A) × P(B) × P(C) × P(D) × P(E)

Figure 2.9 *Hazard component and probability example.*

2.6 HAZARD–MISHAP PROBABILITY

A hazard has a probability of either 1 or 0 of existing (either it exists or it does not; the three components are present or they are not present). A mishap, on the other hand, has a probability somewhere between 1 and 0 of occurring, based on the HCFs. The HE component has a probability of 1.0 of occurring, since it must be present in order for the hazard to exist. It is therefore the IM component that drives the mishap probability, that is, when the IMs occur, the mishap occurs. The IMs are factors such as human err, component failures, timing errors, and the like. This concept is illustrated in Figure 2.9.

The HCFs are the root cause of the hazard. The HCFs are in fact the hazard components that provide a threat and a mechanism for transitioning from a hazard to a mishap. The HE and the IM components of a hazard are the HCFs. These two HCFs establish the probability of the hazard becoming a mishap. The combined effect of the T/T and parts of the HE and IM components determine the severity of the hazard. For mishap severity the HE amount is usually of concern, and the IM factor that places the target in proximity of the HE.

2.7 RECOGNIZING HAZARDS

Hazard identification is one of the major tasks of system safety, and hazard identification involves hazard recognition. Hazard recognition is the cognitive process of visualizing a hazard from an assorted package of design information. In order to recognize or identify hazards four things are necessary:

1. An understanding of hazard theory
2. A hazard analyses technique to provide a consistent and methodical process
3. An understanding of hazard recognition methods
4. An understanding of the system design and operation

This chapter has discussed hazard theory in order that the safety analyst better understands the various aspects of a hazard, such as the hazard–mishap relationship, the three components of a hazard, and the types of hazard causal factors. Chapter 3 discusses the system safety hazard analysis types that are necessary to provide complete coverage for identifying various types of hazards. The rest of this book describes a number of different hazard analysis techniques that provide different levels of hazard analysis structure, rigor, and detail. This section concentrates on how to cognitively recognize a hazard.

One of the annoying truisms of system safety is that it is usually easier to mitigate a hazard than it is to recognize or find the hazard in the first place. An analyst can fully understand hazard theory and have a hazard analysis tool available, yet there is still the vexing reality of actually recognizing a hazard. Hazard recognition is a key aspect of the hazard identification process, and therefore a key element of all hazard analyses. Hazards sometimes seem like ubiquitous and elusive little creatures that must be hunted and captured, where the hunt is akin to the recognition process.

Another truism of system safety is that hazard recognition is somewhat more of an art than a science (this may be one reason why skilled system safety analysts are invaluable). However, there are some key recognition factors that can help the safety analyst visualize hazards, such as:

1. Utilizing the hazard triangle components
   a. HE Use hazardous element/component checklists
   b. IM Evaluate trigger events and causal factors
   c. T/T Evaluate possible threats and mishaps
2. Utilizing past knowledge from experience and lessons learned
3. Analyzing good design practices
4. Review of general design safety criteria, precepts, and principles
5. Review and analysis of generic level 2 hazard causal factors
6. Key failure state questions
7. Evaluation of top-level mishaps and safety critical functions

The hazard triangle concept provides the best hazard recognition resource, by evaluating individually each of the three hazard component categories (HE, IM, and T/T) from a systems context. This means, for example, identifying and evaluating all of the HE components in the unique system design as the first step. Subsequently, all system IM sources are evaluated for hazards, then all T/T sources.

When considering the HE component of the hazard triangle, focus on hazardous element checklists. The HE component involves items known to be a hazardous source, such as explosives, fuel, batteries, electricity, acceleration, chemicals, and the like. This means that generic hazard source checklists can be utilized to help recognize hazards within the unique system design. If a component in the system being analyzed is on one of the hazard source checklists, then this is a direct pointer to potential hazards that may be in the system. Speculate all of the possible ways that the hazardous element can be hazardous within the system design. There are many different types of hazard source checklists, such as those for energy sources, hazardous operations, chemicals, and so forth. Refer to Appendix C for some example checklists.

Hazards can be recognized by focusing on known consequential hazard triggering mechanisms (the IM hazard component). For example, in the design of aircraft it is common knowledge that fuel ignition sources and fuel leakage sources are initiating mechanisms for fire/explosion hazards. Therefore, hazard recognition would benefit from detailed review of the design for ignition sources and leakage sources when fuel is involved. Component failure modes and human error are common triggering modes for hazards.

Hazards can be recognized by focusing on known or preestablished undesired outcomes or mishaps (the target/threat hazard component). This means considering and evaluating known undesired outcomes within the system. For example, a missile system has certain undesired outcomes that are known right from the conceptual stage of system development. By following these undesired outcomes backward, certain hazards can be more readily recognized. In the design of missile systems, it is well accepted that inadvertent missile launch is an undesired mishap, and therefore any conditions contributing to this event would formulate a hazard, such as autoignition, switch failures, and human error.

Another method for recognizing hazards is through the use of past knowledge from experience and lessons learned. Mishap and hazard information from a previously developed system that is similar in nature or design to the system currently under analysis will aid in the hazard recognition process. For example, by reviewing the mishaps of an earlier spacecraft system, it might be discovered that the use of a particular seal design on a specific part of the spacecraft resulted in several mishaps. Seal design on this part of the spacecraft should then be recognized as a potential hazardous area requiring special focus in current new spacecraft design.

Another method for recognizing hazards is through the review and analysis of good design practices. By reverse engineering good design practices found in various design documents and standards, hazardous design situations can be identified. For example, a good design practice for interrupting direct current (DC) circuits is to place the switch or circuit breaker on the power branch, rather than the ground branch of the circuit. This prevents inadvertent operation should a fault to ground occur. A hazard analysis should look for this and similar hazards in a new design.

Another method for recognizing hazards is through the review of general design safety criteria, precepts, and principles. By considering the reasoning and logic behind specific safety criteria, precepts, and principles, some types of hazards can be more easily recognized. For example, there is a good safety reason for the following safety criteria: “Do not supply primary and redundant system circuits with power from the same bus or circuit.” This safety criterion is a clue that aids in recognizing hazards in systems involving redundancy. A hazard analysis should look for such hazards in a new design.

Another method for recognizing hazards is through the review and analysis of generic level 2 hazard causal factors. Considering the various causal factor

TABLE 2.2 Failure State Checklist

1	Fails to operate.
2	Operates incorrectly/erroneously.
3	Operates inadvertently.
4	Operates at wrong time (early, late).
5	Unable to stop operation.
6	Receives erroneous data.
7	Sends erroneous data.
8	Conflicting data or information.
9	The component is subjected to fluid from external source.
10	The component is subjected to heat from external source.

categories at a broad level can aid in recognizing hazards. The broad causal factor categories include, hardware, software, human, interfaces, and the environment. For example, by evaluating all of the potential environments the system will operate in, or to which the system will be exposed, can assist in recognizing system hazards caused by environmental factors.

TABLE 2.3 Example of Hazard Recognition

Hazard	Hazard Recognition Keys
Missile battery fluid leaks onto electronics installed below battery; electronics have hot surface that could cause ignition of fluid and a fire/explosion, resulting in equipment damage and/or personnel injury.	1. A battery is an HE checklist item, so the battery should be looked at from all possible hazard aspects, such as leakage, fire, toxicity, etc. 2. Battery fluid is an HE checklist item, so the battery fluid should be looked at from all possible hazard aspects, such as chemical damage, fire, etc. 3. High temperature is an HE checklist item, so components with high surface temperature should be evaluated as potential ignition sources. 4. Experience and lessons learned from other missile programs would show that battery leakage is a safety concern, and therefore should be considered as a hazard source. 5. Since a fluid is involved, key state question 9 (from Table 2.2) should be considered.
Premature in-bore explosion of artillery round inside gun barrel could occur due to excessive heat, resulting in operator death or injury.	1. Explosives are an HE checklist item, so the explosives should be looked at from all possible hazard aspects, such as excessive barrel heat, jamming, etc. 2. The potential mishap consequence of personnel injury from premature explosion of artillery round is a known mishap to be prevented; therefore, all possible causes should be considered. 3. Experience and lessons learned from other gun programs would show that in-bore explosion is a safety concern and, therefore, should be considered as a hazard source. 4. Since heat is always a concern with explosives, key state question 10 (from Table 2.2) should be considered.

Another method for recognizing hazards is through the use of key state questions. This is a method involving a set of clue questions that must be answered, each of which can trigger the recognition of a hazard. The key states are potential states or ways the subsystem could fail or operate incorrectly and thereby result in creating a hazard. For example, when evaluating each subsystem, answering the question "What happens when the subsystem *fails to operate*?" may lead to the recognition of a hazard. Table 2.2 contains a partial failure state checklist that provides some example key questions that should be asked when identifying hazards. Each system development SSP should develop its specialized and unique list of key failure state questions.

Table 2.3 demonstrates the hazard recognition process by listing the key considerations involved in the recognition of a hazard. The left-hand column of Table 2.3 states the identified hazard, while the right-hand column lists the key factors used to help recognize the hazard. It should be noted that it is very likely that additional hazards could probably be identified by using the listed hazard recognition keys, other than the single hazard shown in each of the above examples.

Another method for recognizing hazards is through the evaluation of top-level mishaps (TLMs) and safety critical functions (SCFs). Looking for potential causal factors of already established TLMs is a way of identifying hazards. Also, a technique for identifying hazards is by carefully examining what might cause the inadvertent or premature occurrence of each of the elements in an SCF.

2.8 HAZARD DESCRIPTION

Correctly describing the hazard is a very important aspect of hazard theory and analysis. The hazard description must contain all three components of the HCM (hazardous element, initiating mechanism, and target/threat). The hazard description should also be clear, concise, descriptive and to the point.

If the hazard description is not properly worded, it will be difficult for anyone other than the original analyst to completely understand the hazard. If the hazard is not clearly understood, the concomitant risk of the hazard may not be correctly determined. This can lead to other undesirable consequences, such as spending too much time mitigating a low-risk hazard, when it was incorrectly thought to be high-risk hazard.

Table 2.4 shows some good and poor example hazard descriptions. Note that the good examples contain all three elements of hazard: hazardous element, initiating mechanism, and target/threat.

2.9 SUMMARY

This chapter discussed the basic hazard–mishap–risk concept. The following are basic principles that help summarize the discussion in this chapter:

1. A hazard is potential condition built into the system design, which if it occurs, will result in an undesired event (i.e., mishap or accident).

TABLE 2.4 Example Hazard Descriptions

Poor Examples	Good Examples
Repair technician slips on oil.	Overhead valve V21 leaks oil on walkway below; spill is not cleaned; repair technician walking in area slips on oil and falls on concrete floor, causing serious injury.
Signal MG71 occurs.	Missile launch signal MG71 is inadvertently generated during standby alert, causing inadvertent launch of missile and death/injury to personnel in the area of impacting missile.
Round fired prematurely.	Artillery round fired from gun explodes or detonates prior to safe separation distance, resulting in death or injury to personnel within safe distance area.
Ship causes oil spill.	Ship operator allows ship to run aground, causing catastrophic hull damage, causing massive oil leakage, resulting in major environmental damage.

2. Hazards are essentially the cause, or the precursor, for accidents and mishaps.
3. A hazard describes the special circumstances, conditions, and components that can result in accidents and mishaps. A hazard defines and predicts a potential future mishap.
4. A hazard consists of three required components, referred to as the hazard triangle:
   - Hazardous element (source)
   - Initiating mechanism (mechanism)
   - Threat/target of damage, injury or loss (outcome).
5. A hazard is a deterministic entity that has its own unique design, components, characteristics, and properties.
6. If any side of the hazard triangle is eliminated through design techniques, the hazard and its associated risk are also eliminated.
7. If a hazard cannot be eliminated, then its risk can be reduced (mitigated or controlled) by reducing the hazard's probability of occurrence and/or the mishap severity through design techniques.
8. When a hazard is created, its outcome is almost always fixed and unchangeable. For this reason it is very difficult to reduce hazard severity, it is much easier to reduce the hazard probability (mishap risk probability). The risk severity of a hazard almost always remains the same after mitigation.
9. It is important that a hazard description is clear, concise, and complete; it must contain all three components of the hazard triangle (HE, IM, and T/T).
10. Hazards occur in a somewhat predictable manner, based on the necessary and sufficient conditions of their design. What is predictable (hazard) is also preventable or controllable (mishap). By focusing on hazards and hazard analysis, mishap risk can be eliminated or reduced.

11. When identifying hazards, the following factors help trigger the recognition of a hazard:
    - Evaluation of the hazard triangle components
    - Utilizing past knowledge from experience and lessons learned
    - Analyzing good design practices
    - Review of general design safety criteria, precepts, and principles
    - Review and analysis of generic level 2 hazard causal factors
    - Key state questions
12. Just as a picture is worth a thousand words, a good hazard description creates a picture that is invaluable in preventing a potential mishap.

Chapter 3

Hazard Analysis Types and Techniques

3.1 TYPES AND TECHNIQUES

Hazard analyses are performed to identify hazards, hazard effects, and hazard causal factors. Hazard analyses are used to determine system risk and thereby ascertain the significance of hazards so that safety design measures can be established to eliminate or mitigate the hazard. Analyses are performed to systematically examine the system, subsystem, facility, components, software, personnel, and their interrelationships.

There are two categories of hazard analyses: *types* and *techniques.* Hazard analysis type defines an analysis category (e.g., detailed design analysis), and technique defines a unique analysis methodology (e.g., fault tree analysis). The type establishes analysis timing, depth of detail, and system coverage. The technique refers to a specific and unique analysis methodology that provides specific results. System safety is built upon seven basic types, while there are well over 100 different techniques available.[1] In general, there are several different techniques available for achieving each of the various types. The overarching distinctions between type and technique are summarized in Table 3.1.

Hazard analysis type describes the scope, coverage, detail, and life-cycle phase timing of the particular hazard analysis. Each type of analysis is intended to provide a time- or phase-dependent analysis that readily identifies hazards for a particular design phase in the system development life cycle. Since more detailed design

[1] Refer to the *System Safety Analysis Handbook* published by the System Safety Society.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

TABLE 3.1 Hazard Analysis Type vs. Technique

Type	Technique
• Establishes where, when, and what to analyze. • Establishes a specific analysis task at specific time in program life cycle. • Establishes what is desired from the analysis. • Provides a specific design focus.	• Establishes how to perform the analysis. • Establishes a specific and unique analysis methodology. • Provides the information to satisfy the intent of the analysis type.

and operation information is available as the development program progresses, so in turn more detailed information is available for a particular type of hazard analysis. The depth of detail for the analysis type increases as the level of design detail progresses.

Each of these analysis types define a point in time when the analysis should begin, the level of detail of the analysis, the type of information available, and the analysis output. The goals of each analysis type can be achieved by various analysis techniques. The analyst needs to carefully select the appropriate techniques to achieve the goals of each of the analysis types.

There are seven hazard analysis types in the system safety discipline:

1. Conceptual design hazard analysis type (CD-HAT)
2. Preliminary design hazard analysis type (PD-HAT)
3. Detailed design hazard analysis type (DD-HAT)
4. System design hazard analysis type (SD-HAT)
5. Operations design hazard analysis type (OD-HAT)
6. Health design hazard analysis type (HD-HAT)
7. Requirements design hazard analysis type (RD-HAT)

An important principle about hazard analysis is that one particular hazard analysis type does not necessarily identify all the hazards within a system; identification of hazards may take more than one analysis type (hence the seven types). A corollary to this principle is that one particular hazard analysis type does not necessarily identify all of the hazard causal factors; more than one analysis type may be required. After performing all seven of the hazard analysis types, all hazards and causal factors should have been identified; however, additional hazards may be discovered during the test program.

Figure 3.1 conveys the filter concept behind the seven hazard analysis types. In this concept, each hazard analysis type acts like a filter that identifies certain types of hazards. Each successive filter serves to identify hazards missed by the previous filter. The thick dark arrows at the top of the filter signify hazards existing in the system design. When all of the hazard analysis types have been applied, the only

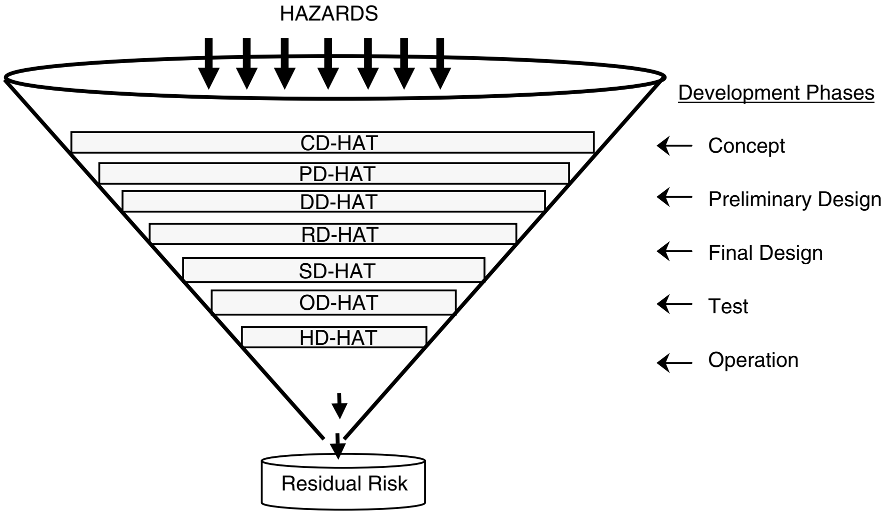


Figure 3.1 *Hazard filters.*

known hazards remaining have been reduced to an acceptable level of risk, denoted by the smaller thin arrows. Use of all seven hazards analysis types is critical in identifying and mitigating all hazards and reducing system residual risk.

Each hazard analysis type serves a unique function or purpose. For a best practice system safety program (SSP), it is recommended that all seven of these hazard analysis types be applied; however, tailoring is permissible. If tailoring is utilized, the specifics should be spelled out in the system safety management plan (SSMP) and/or the system safety program plan (SSPP).

Figure 3.2 depicts the relationship between hazard types and techniques. In this relationship, the seven hazard analysis types form the central focus for SSP hazard analysis. There are many different analysis techniques to select from when performing the analysis types, and there are many different factors that must go into the hazard analysis, such as the system life-cycle stages of concept, design, test, manufacture, operation, and disposal. The system modes, phases, and functions must be considered. The system hardware, software, firmware, human interfaces, and environmental aspects must also be considered.

Some textbooks refer to the seven types as preliminary hazard list (PHL), preliminary hazard analysis (PHA), subsystem hazard analysis (SSHA), system hazard analysis (SHA), operating and support hazard analysis (O&SHA), health hazard analysis (HHA), and safety requirement/criteria analysis (SRCA). These names are, however, the same names as the basic hazard analysis techniques established by MIL-STD-882, versions A, B, and C. The concept of analysis types is a good concept, but having types and techniques with the same name is somewhat confusing. The approach recommended in this book ensures there are no common names between types and techniques, thus avoiding much confusion.

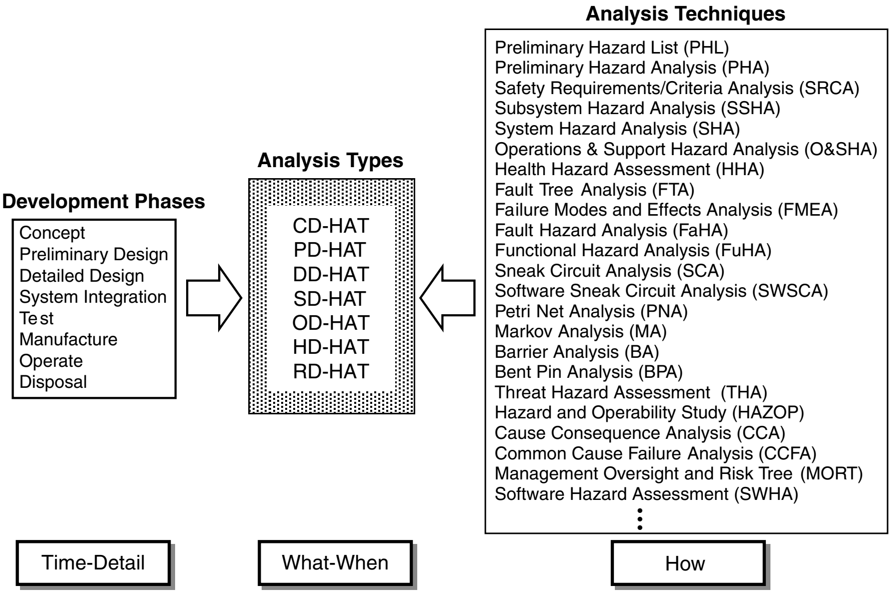

Development Phases
Concept
Preliminary Design
Detailed Design
System Integration
Test
Manufacture
Operate
Disposal
Analysis Types
CD-HAT
PD-HAT
DD-HAT
SD-HAT
OD-HAT
HD-HAT
RD-HAT
Analysis Techniques
Preliminary Hazard List (PHL)
Preliminary Hazard Analysis (PHA)
Safety Requirements/Criteria Analysis (SRCA)
Subsystem Hazard Analysis (SSHA)
System Hazard Analysis (SHA)
Operations & Support Hazard Analysis (O&SHA)
Health Hazard Assessment (HHA)
Fault Tree Analysis (FTA)
Failure Modes and Effects Analysis (FMEA)
Fault Hazard Analysis (FaHA)
Functional Hazard Analysis (FuHA)
Sneak Circuit Analysis (SCA)
Software Sneak Circuit Analysis (SWSCA)
Petri Net Analysis (PNA)
Markov Analysis (MA)
Barrier Analysis (BA)
Bent Pin Analysis (BPA)
Threat Hazard Assessment (THA)
Hazard and Operability Study (HAZOP)
Cause Consequence Analysis (CCA)
Common Cause Failure Analysis (CCFA)
Management Oversight and Risk Tree (MORT)
Software Hazard Assessment (SWHA)
Time-Detail
What-When
How

Figure 3.2 *Type—technique relationship.*

3.2 DESCRIPTION OF HAZARD ANALYSIS TYPES

3.2.1 Conceptual Design Hazard Analysis Type (CD-HAT)

The CD-HAT is a high-level (low level of detail) form of hazard analysis that identifies top-level hazards that can be recognized during the conceptual design phase. The CD-HAT is the first analysis type performed and is the starting point for all subsequent hazard analyses. The CD-HAT provides a basis for initially estimating the overall SSP effort.

The purpose of the CD-HAT is to compile a list of hazards very early in the product or system development life cycle to identify potentially hazardous areas. These hazardous areas identify where management should place design safety emphasis. The CD-HAT searches for hazards that may be inherent in the design or operational concept. It is a brainstorming, “what-if” analysis. A hazard list is generated from the brainstorming session, or sessions, where everything conceivable is considered and documented. The topics include review of safety experience on similar systems, hazard checklists, mishap/incident hazard tracking logs, safety lessons learned, and so forth to identify possible hazards.

The key to a successful SSP is involvement early in the development program, beginning during conceptual design. The CD-HAT is started when the concept definition for a product or system begins and carries into the preliminary design phase. It is performed early in the program life cycle in order to influence design concepts and decisions for safety as early as possible. The CD-HAT is the first analysis type performed and precedes the PD-HAT since it provides input for the PD-HAT.

If the CD-HAT is not performed during concept definition, it should be performed prior to, and as part of, any PD-HAT effort since it is an essential precursor to the PD-HAT. Once the initial CD-HAT is completed and documented, it is rarely updated as additional hazard identification analysis is achieved via the PD-HAT. In general, the CD-HAT supports the system design review (SDR), and CD-HAT effort ends at the start of the PD-HAT.

The following are the basic requirements of a comprehensive CD-HAT:

1. Will be applied during the design concept phase of system development.
2. Will be a high-level analysis (low level of detail) based on conceptual design information.
3. Will identify system hazards and potential mishaps.
4. Will consider hazards during system test, manufacture, operation, maintenance, and disposal.
5. Will consider system hardware, software, firmware, human interfaces, and environmental aspects.

Input information for the CD-HAT analysis type includes everything that is available during conceptual design. Experience has shown that generally the CD-HAT can be performed utilizing the following types of information:

1. Design concept
2. Statement of work (SOW), specification, drawings (if available)
3. Preliminary (conceptual) indentured equipment list
4. Preliminary (conceptual) functions list
5. Energy sources in the system
6. Hazard checklists (generic)
7. Lessons learned (similar systems)

The primary purpose of the CD-HAT is to generate a list of system-level hazards, which can be used as an initial risk assessment and as the starting point for the subsequent hazard analysis types. As such, the following information is typically output from the CD-HAT analysis:

1. System hazards
2. Top-level mishaps (TLMs)
3. Information to support the PD-HAT analysis

3.2.2 Preliminary Design Hazard Analysis Type (PD-HAT)

The PD-HAT is a preliminary level form of analysis that does not go into extensive detail; it is preliminary in nature. The PD-HAT is performed to identify system-level hazards and to obtain an initial risk assessment of a system design. It is performed early, during the preliminary design phase, in order to affect design decisions as early as possible to avoid future costly design changes.

The PD-HAT is the basic hazard analysis that establishes the framework for all of the follow-on hazard analyses. It provides a preliminary safety engineering evaluation of the design in terms of potential hazards, causal factors, and mishap risk. The intent of the PD-HAT is to recognize the hazardous system states and to begin the process of controlling hazards identified by the CD-HAT. As the design progresses in detail, more detailed analyses are performed to facilitate the elimination or mitigation of all hazards.

Identification of safety critical functions (SCFs) and TLMs is a key element of the PD-HAT. The specific definition of what constitutes classification as safety critical (SC) is generally program specific, as different types of systems may warrant different definitions based on the hazardous nature of the system.

The PD-HAT should be started during the design conceptual stage (after the CD-HAT) and continued through preliminary design. If the PD-HAT is not initiated during conceptual design, it should be initiated with the start of preliminary design. It is important that safety considerations identified in the PD-HAT are included in trade studies and design alternatives as early as possible in the design process.

Work on the PD-HAT usually concludes when the DD-HAT is initiated. In general, the PD-HAT supports all preliminary design reviews. The PD-HAT may also be used on an existing operational system for the initial examination of proposed design changes to the system.

The following are the basic requirements of a comprehensive PD-HAT:

1. Will be applied during the design concept and preliminary design phases of system development.
2. Will focus on all system hazards resulting from the preliminary design concept and component selection.
3. Will be a high- to medium-level analysis (low to medium level of detail) that is based on preliminary design information.
4. Will identify hazards, potential mishaps, causal factors, risk, and SCFs. It will identify applicable safety guidelines, requirements, principles, and precepts to mitigate hazards. It will also provide recommendations to mitigate hazards.
5. Will consider hazards during system test, manufacture, operation, maintenance, and disposal.
6. Will consider system hardware, software, firmware, human interfaces, and environmental aspects.

Input information for the PD-HAT consists of the preliminary design information that is available during the preliminary design development phase. Typically the following types of information are available and utilized in the PD-HAT:

1. Results of the CD-HAT analysis
2. SOW

3. System specification
4. Design drawings and sketches
5. Preliminary indentured equipment list
6. Functional flow diagrams of activities, functions, and operations
7. Concepts for operation, test, manufacturing, storage, repair, and transportation
8. Energy sources
9. Hazard checklists (generic)
10. Lessons learned from experiences of similar previous programs or activities
11. Failure modes review
12. Safety guidelines and requirements from standards and manuals

The primary purpose of the PD-HAT is to perform a formal analysis for identifying system-level hazards and evaluating the associated risk levels. As such, the following information is typically output from the PD-HAT:

1. System-level hazards
2. Hazard effects and mishaps
3. Hazard causal factors (to subsystem identification)
4. SCFs
5. TLMs
6. Safety design criteria, principles, and precepts for design guidance in hazard mitigation
7. Risk assessment (before and after design safety features for hazard mitigation)
8. Safety recommendations for eliminating or mitigating the hazards
9. Information to support DD-HAT, SD-HAT, and OD-HAT analyses

3.2.3 Detailed Design Hazard Analysis Type (DD-HAT)

The DD-HAT is a detailed form of analysis, performed to further evaluate hazards from the PHA with new detailed design information. The DD-HAT also evaluates the functional relationships of components and equipment comprising each subsystem. The analysis will help identify all components and equipment whose performance degradation or functional failure could result in hazardous conditions. Of particular concern is the identification of single-point failures (SPFs). The DD-HAT is also used to identify new hazards that can be recognized from the detailed design information that is available and to identify the hazard causal factors of specific subsystems and their associated risk levels.

The DD-HAT is an analysis of the detailed design and can therefore run from the start of detailed design through completion of final manufacturing drawings. Once the initial DD-HAT is completed and documented, it is not generally updated and enhanced, except for the evaluation of design changes.

The following are the basic requirements of a comprehensive DD-HAT analysis:

1. Will be a detailed analysis at the subsystem and component level.
2. Will be applied during the detailed design of the system.
3. Will identify hazards, resulting mishaps, causal factors, risk, and SCFs. It will also identify applicable safety recommendations for hazard mitigation.
4. Will consider hazards during system test, manufacture, operation, maintenance, and disposal.
5. Will consider system hardware, software, firmware, human interfaces, and environmental aspects.

Input information for the DD-HAT analysis consists of all detailed design data. Typically the following types of information are available and utilized in the DD-HAT:

1. PD-HAT analysis results
2. System description (design and functions)
3. Detailed design information (drawings, schematics, etc.)
4. Indentured equipment list
5. Functional block diagrams
6. Hazard checklists

The primary purpose of the DD-HAT is to evaluate the detailed design for hazards and hazard causal factors and the associated subsystem risk levels. As such, the following information is typical output from the DD-HAT:

1. Subsystem hazards
2. Detailed causal factors
3. Risk assessment
4. Safety critical subsystem interfaces
5. Safety design recommendations to mitigate hazards
6. Special detailed analyses of specific hazards using special analysis techniques such as fault tree analysis (FTA)
7. Information to support the RD-HAT and SD-HAT analyses

3.2.4 System Design Hazard Analysis Type (SD-HAT)

The SD-HAT assesses the total system design safety by evaluating the integrated system design. The primary emphasis of the SD-HAT, inclusive of both hardware and software, is to verify that the product is in compliance with the specified safety requirements at the system level. This includes compliance with acceptable mishap risk levels. The SD-HAT examines the entire system as a whole by integrating the essential outputs from the DD-HAT analyses. Emphasis is placed on the interactions and the interfaces of all the subsystems as they operate together.

The SD-HAT provides determination of system risks in terms of hazard severity and hazard probability. System hazards are evaluated to identify all causal factors, including hardware, software, firmware, and human interaction. The causal factors may involve many interrelated fault events from many different subsystems. Thus, the SD-HAT evaluates all the subsystem interfaces and interrelationships for each system hazard.

The SD-HAT is system oriented, and therefore it usually begins during preliminary design and is complete by the end of final design, except for closure of all hazards. The SD-HAT is finalized at completion of the test program when all hazards have been tested for closure. SD-HAT documentation generally supports safety decisions for commencement of operational evaluations. The SD-HAT should be updated as a result of any system design changes, including software and firmware design changes to ensure that the design change does not adversely affect system mishap risk.

The following are the basic requirements of a comprehensive SD-HAT analysis:

1. Will be applied primarily during the detailed design phase of system development; it can be initiated during preliminary design.
2. Is a detailed level of analysis that provides focus from an integrated system viewpoint.
3. Will be based on detailed and final design information.
4. Will identify new hazards associated with the subsystem interfaces.
5. Will consider hazards during system test, manufacture, operation, maintenance, and disposal.
6. Will consider system hardware, software, firmware, human interfaces, and environmental aspects.

Typically the following types of information are available and utilized in the SD-HAT analysis:

1. PD-HAT, DD-HAT, RD-HAT, OD-HAT, and other detailed hazard analyses
2. System design requirements
3. System description (design and functions)
4. Equipment and function indenture lists
5. System interface specifications
6. Test data

The primary purpose of the SD-HAT analysis is to perform a formal analysis for identifying system-level hazards and evaluating the associated risk levels. As such, the following information is typically output from the SD-HAT:

1. System interface hazards
2. System hazard causal factors (hardware, software, firmware, human interaction, and environmental)

3. Assessment of system risk
4. Special detailed analyses of specific hazards using special analysis techniques such as FTA
5. Information to support the safety assessment report (SAR)

3.2.5 Operations Design Hazard Analysis Type (OD-HAT)

The OD-HAT analysis evaluates the operations and support functions involved with the system. These functions include use, test, maintenance, training, storage, handling, transportation, and demilitarization or disposal. The OD-HAT analysis identifies operational hazards that can be eliminated or mitigated through design features and through modified operational procedures when necessary. The OD-HAT analysis considers human limitations and potential human errors (human factors). The human is considered an element of the total system, receiving inputs and initiating outputs.

The OD-HAT analysis is performed when operations information becomes available and should start early enough to provide inputs to the design. The OD-HAT should be completed prior to the conduct of any operating and support functions.

The following are the basic requirements of a comprehensive OD-HAT analysis:

1. Will be performed during the detailed design phases of system development when the operating and support procedures are being written.
2. Will focus on hazards occurring during operations and support.
3. Will provide an integrated assessment of the system design, related equipment, facilities, operational tasks, and human factors.
4. Will be a detailed analysis based on final design information.
5. Will identify hazards, potential mishaps, causal factors, risk and safety critical factors, applicable safety requirements, and hazard mitigation recommendations.
6. Will consider hazards during system use, test, maintenance, training, storage, handling, transportation, and demilitarization or disposal.

The following types of information are utilized in the OD-HAT:

1. PD-HAT, DD-HAT, SD-HAT, and any other applicable hazard analyses
2. Engineering descriptions/drawings of the system, support equipment, and facilities
3. Available procedures and operating manuals
4. Operational requirements, constraints, and required personnel capabilities
5. Human factors engineering data and reports
6. Lessons learned, including human factors
7. Operational sequence diagrams

The OD-HAT focus is on operating and support tasks and procedures. The following information is typically available from the OD-HAT:

1. Task-oriented hazards (caused by design, software, human, timing, etc.)
2. Hazard mishap effect
3. Hazard causal factors (including human factors)
4. Risk assessment
5. Hazard mitigation recommendations and derived design safety requirements
6. Derived procedural safety requirements
7. Cautions and warnings for procedures and manuals
8. Input information to support the SD-HAT analysis

3.2.6 Human Design Hazard Analysis Type (HD-HAT)

The HD-HAT analysis is intended to systematically identify and evaluate human health hazards, evaluate proposed hazardous materials, and propose measures to eliminate or control these hazards through engineering design changes or protective measures to reduce the risk to an acceptable level.

The HD-HAT assesses design safety by evaluating the human health aspects involved with the system. These aspects include manufacture, use, test, maintenance, training, storage, handling, transportation, and demilitarization or disposal.

The HD-HAT concentrates on human health hazards. The HD-HAT is started during preliminary design and continues to be performed as more information becomes available. The HD-HAT should be completed and system risk known prior to the conduct of any of the manufacturing, test, or operational phases.

The following are the basic requirements of a comprehensive HD-HAT analysis:

1. Will be applied during the preliminary and detailed design phases of system development.
2. Will focus on the human environment within the system.
3. Will be a detailed analysis based on system design and operational tasks affecting the human environment.
4. Will identify hazards, potential mishaps, causal factors, risk and safety critical factors, and applicable safety requirements.
5. Will consider human health hazards during system test, manufacture, operation, maintenance, and demilitarization or disposal. Consideration should include, but is not limited to, the following:
   a. Materials hazardous to human health (e.g., material safety data sheets)
   b. Chemical hazards
   c. Radiological hazards
   d. Biological hazards

e. Ergonomic hazards
f. Physical hazards

Typically the following types of information are available and utilized in the HD-HAT analysis:

1. CD-HAT, PD-HAT, DD-HAT, SD-HAT, OD-HAT, and any other applicable detailed hazard analyses
2. Materials and compounds used in the system production and operation
3. Material safety data sheets
4. System operational tasks and procedures, including maintenance procedures
5. System design

The following information is typically available from the HD-HAT analysis:

1. Human health hazards
2. Hazard mishap effects
3. Hazard causal factors
4. Risk assessment
5. Derived design safety requirements
6. Derived procedural safety requirements (including cautions, warnings, and personal protective equipment)
7. Input information for the Occupational Safety and Health Administration (OSHA) and environmental evaluations
8. Information to support the OD-HAT and SD-HAT analyses

3.2.7 Requirements Design Hazard Analysis Type (RD-HAT)

The RD-HAT is a form of analysis that verifies and validates the design safety requirements and ensures that no safety gaps exist in the requirements. The RD-HAT applies to hardware, software, firmware, and test requirements. Since the RD-HAT is an evaluation of design and test safety requirements, it is performed during the design and test stages of the development program. The RD-HAT can run from mid-preliminary design through the end of testing.

Safety design requirements are generated from three sources: (1) the system specification, (2) generic requirements from similar systems, subsystems, and processes, and (3) requirements derived from recommendations to mitigate identified system-unique hazards. The intent of the RD-HAT is to ensure that all of the appropriate safety requirements are included within the design requirements and that they are verified and validated through testing, analysis, or inspection. Applicable generic system safety design requirements are obtained from such sources as federal, military, national, and industry regulations, codes, standards, specifications, guidelines, and other related documents for the system under development.

The RD-HAT supports closure of identified hazards. Safety requirements levied against the design to mitigate identified hazards must be verified and validated before a hazard in the hazard tracking system can be closed. The RD-HAT provides a means of traceability for all safety requirements, verifying their implementation and validating their success.

The RD-HAT is an evolving analysis that is performed over a period of time, where it is continually updated and enhanced as more design and test information becomes available. The RD-HAT is typically performed in conjunction with the PD-HAT, DD-HAT, SD-HAT, and OD-HAT analyses. The RD-HAT should be complete at the end of testing.

The following are the basic requirements of a comprehensive RD-HAT analysis:

1. Will be applied from the preliminary design phases through testing of the system.
2. Will focus on safety requirements intended to eliminate and/or mitigate identified hazards.
3. Will be a detailed analysis based on detailed design requirements and design information.
4. Will ensure that all identified hazards have suitable safety requirements to eliminate and/or mitigate the hazards.
5. Will ensure that all safety requirements are verified and validated through analysis, testing, or inspection.

Typically the following types of information are available and utilized in the RD-HAT:

1. Hazards without mitigating safety requirements
2. Design safety requirements (hardware, software, firmware)
3. Test requirements
4. Test results
5. Unverified safety requirements

The primary purposes of the RD-HAT are to establish traceability of safety requirements and to assist in the closure of mitigated hazards. The following information is typically output from the RD-HAT:

1. Traceability matrix of all safety design requirements to identified hazards
2. Traceability matrix of all safety design requirements to test requirements and test results
3. Identification of new safety design requirements and tests necessary to cover gaps discovered by items 1 and 2 above
4. Data supporting closure of hazards

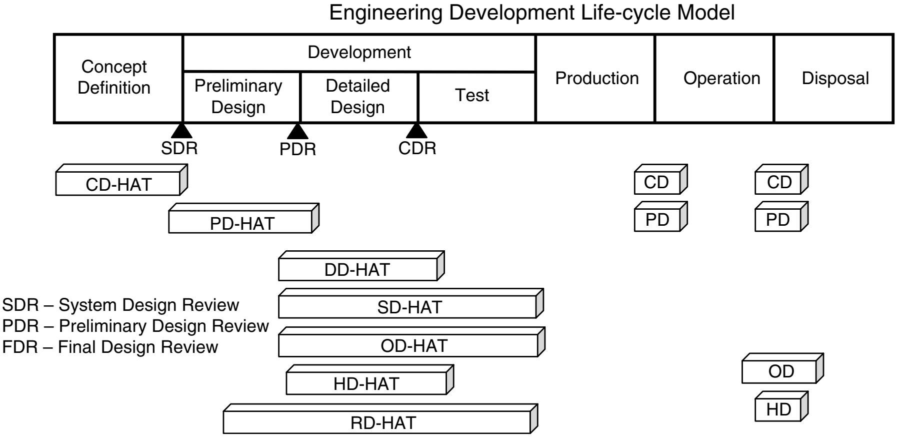


Figure 3.3 *Overall timing of hazard analysis types.*

3.3 TIMING OF HAZARD ANALYSIS TYPES

Figure 3.3 contains a consolidated view of the time period over which the hazard analysis types are typically performed. This schedule shows the most typical timing that has been found practical through many years of trial and error. The system development phases shown are from the standard engineering development life-cycle model.

The time period for performing the hazard analysis is not rigidly fixed but is dependent on many variables, such as size of the system and project, safety criticality of the system, personal experience, common sense, and so forth. The time period is shown as a bar because the analysis can be performed at any time during the period shown. Specifying the time period for a hazard analysis is part of the safety program tailoring process and should be documented in the SSPP. Each of the hazard analysis types has a functional time period when it is most effectively applied to achieve the desired intent and goals.

Note how each of the hazard analysis types correlates very closely to its associated development phase. Also, note that some of the analysis types should be performed in a later development phase if that phase was not specifically covered by the original analysis.

3.4 INTERRELATIONSHIP OF HAZARD ANALYSIS TYPES

Figure 3.4 shows the relative relationship of each of the hazard analysis types and their interdependencies. This figure shows how the output of one analysis type can provide input data for another analysis type.

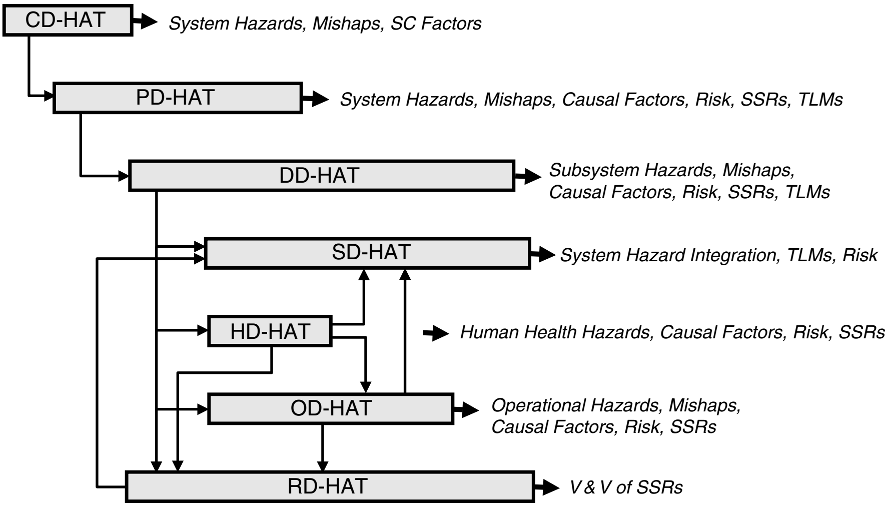

CD-HAT
System Hazards, Mishaps, SC Factors
PD-HAT
System Hazards, Mishaps, Causal Factors, Risk, SSRs, TLMs
DD-HAT
Subsystem Hazards, Mishaps, Causal Factors, Risk, SSRs, TLMs
SD-HAT
System Hazard Integration, TLMs, Risk
HD-HAT
Human Health Hazards, Causal Factors, Risk, SSRs
OD-HAT
Operational Hazards, Mishaps, Causal Factors, Risk, SSRs
RD-HAT
V & V of SSRs

Figure 3.4 *Interrelationships between analysis types.*

3.5 HAZARD ANALYSIS TECHNIQUES

Hazard analysis technique defines a unique analysis methodology (e.g., fault tree analysis). The technique refers to a specific and unique analysis methodology that is performed following a specific set of rules and provides specific results.

As previously mentioned, there are over 100 different hazard analysis techniques in existence, and the number continues to slowly grow. Many of the techniques are minor variations of other techniques. And, many of the techniques are not widely practiced. This book presents 22 of the most commonly used techniques by system safety practitioners. Table 3.2 lists the hazard analysis techniques covered in this book, along with the corresponding chapter number describing the technique.

Each of these hazard analysis techniques is important enough to warrant an individual chapter devoted to describing just that technique. The system safety engineer/analyst should be thoroughly familiar with each of the analysis techniques presented in this book. They form the basic building blocks for performing hazard and safety analysis on any type of system.

3.5.1 Technique Attributes

Hazard analysis techniques can have many different inherent attributes, which makes their utility different. The appropriate technique to use can often be determined from the inherent attributes of the technique. Table 3.3 contains a list of the most significant attributes for a hazard analysis methodology.

TABLE 3.2 Hazard Analysis Techniques Presented in This Book

No.	Title	Chapter
1	Preliminary hazard list (PHL) analysis	4
2	Preliminary hazard analysis (PHA)	5
3	Subsystem hazard analysis (SSHA)	6
4	System hazard analysis (SHA)	7
5	Operating and support hazard analysis (O&SHA)	8
6	Health hazard assessment (HHA)	9
7	Safety requirements/criteria analysis (SRCA)	10
8	Fault tree analysis (FTA)	11
9	Event tree analysis (ETA)	12
10	Failure mode and effects analysis (FMEA)	13
11	Fault hazard analysis	14
12	Functional hazard analysis	15
13	Sneak circuit analysis (SCA)	16
14	Petri net analysis (PNA)	17
15	Markov analysis (MA)	18
16	Barrier analysis	19
17	Bent pin analysis (BPA)	20
18	HAZOP analysis	21
19	Cause consequence analysis (CCA)	22
20	Common cause failure analysis (CCFA)	23
21	MORT analysis	24
22	Software safety assessment (SWSA)	25

Table 3.4 summarizes some of the select attributes for the analysis techniques presented in this book. These attributes will be covered in greater detail in each chapter covering a particular technique.

3.5.2 Primary Hazard Analysis Techniques

Of the 22 most commonly used techniques described in this book, there are seven techniques that are considered the primary techniques used by system safety

TABLE 3.3 Major Attributes of Analysis Techniques

	Attribute	Description
1	Qualitative/quantitative	Analysis assessment is performed qualitatively or quantitatively
2	Level of detail	Level of design detail that can be evaluated by the technique
3	Data required	Type and level of design data required for the technique
4	Program timing	Effective time during system development for the technique
5	Time required	Relative amount of time required for the analysis
6	Inductive/deductive	Technique uses inductive or deductive reasoning
7	Complexity	Relative complexity of the technique
8	Difficulty	Relative difficulty of the technique
9	Technical expertise	Relative technical expertise and experience required
10	Tools required	Technique is standalone or additional tools are necessary
11	Cost	Relative cost of the technique
12	Primary safety tool	Technique is a primary or secondary safety tool

TABLE 3.4 Summary of Select Attributes for Analysis Techniques[a]

Technique	Type	Identify Hazards	Identify Root Causes	Life-Cycle Phase	Qualitative/ Quantitative	Skill	Level of Detail	I/D
PHL	CD-HAT	Y	N	CD-PD	Qual.	SS	Minimal	I
PHA	PD-HAT	Y	P	CD-PD	Qual.	SS	Moderate to in-depth	I-D
SSHA	DD-HAT	Y	Y	DD	Qual.	SS, Engr., M&S	In-depth	I-D
SHA	SD-HAT	Y	Y	PD-DD-T	Qual.	SS, Engr., M&S	In-depth	I-D
O&SHA	OD-HAT	Y	Y	PD-DD-T	Qual.	SS, Engr., M&S	In-depth	I-D
HHA	HD-HAT	Y	Y	PD-DD-T	Qual.	SS, Engr., M&S	In-depth	I-D
SRCA	RD-HAT	P	N	PD-DD	Qual.	SS	In-depth	N/A
FTA	SD-HAT, DD-HAT	P	Y	PD-DD	Qual./Quant.	SS, Engr., M&S	Moderate to in-depth	D
ETA	SD-HAT	P	P	PD-DD	Qual./Quant.	SS, Engr., M&S	Moderate to in-depth	D
FMECA	DD-HAT	P	P	PD-DD	Qual./Quant.	SS, Engr., M&S	In-depth	I
FaHA	DD-HAT	Y	P	PD-DD	Qual.	SS, Engr., M&S	In-depth	I
FuHA	SD-HAT, DD-HAT	Y	P	CD-PD-DD	Qual.	SS, Engr., M&S	Moderate to in-depth	I
SCA	SD-HAT, DD-HAT	P	Y	DD	Qual.	SS, Engr., M&S	Moderate to in-depth	D
PNA	SD-HAT, DD-HAT	P	N	PD-DD	Qual./Quant.	SS, Engr., M&S	In-depth	D
MA	SD-HAT, DD-HAT	P	N	PD-DD	Qual./Quant.	SS, Engr., M&S	Moderate to in-depth	D
BA	SD-HAT	Y	P	PD-DD	Qual.	SS, Eg	Moderate to in-depth	I
BPA	DD-HAT	Y	P	PD-DD	Qual.	SS, Engr., M&S	In-depth	D
HAZOP	SD-HAT, DD-HAT	Y	P	PD-DD	Qual.	SS, Engr., M&S	Moderate to in-depth	I
CCA	SD-HAT, DD-HAT	Y	P	PD-DD	Qual./Quant.	SS, Engr., M&S	Moderate to in-depth	D
CCFA	SD-HAT, DD-HAT	Y	P	PD-DD	Qual.	SS, Engr., M&S	Moderate to in-depth	D
MORT	SD-HAT, DD-HAT	Y	P	PD-DD	Qual./Quant.	SS, M&S	Moderate to in-depth	D
SWSA	SD-HAT, DD-HAT	Y	P	CD-PD	Qual.	SS, Engr., M&S	Moderate to in-depth	N/A

[a] Abbreviations: Y = yes, N = no, P = partially; Skill required: SS = system safety; Engr. = engineering electrical/mechanical/software; M&S = math & statistics; life-cycle phase: CD = conceptual design, PD = preliminary design, DD = detailed design, T = testing; I-inductive, D = deductive.

TABLE 3.5 Primary Hazard Analysis Techniques

Primary Analysis Technique	Analysis Type
PHL	CD-HAT
PHA	PD-HAT
SSHA	DD-HAT
SHA	SD-HAT
O&SHA	OD-HAT
HHA	HD-HAT
SRCA	RD-HAT

practitioners. Table 3.5 lists these primary analysis techniques, along with the analysis type that each technique best fits.

The primary analysis techniques were established and promulgated by MIL-STD-882 and have proven effective over many years of usage. These seven hazard analysis techniques provide the majority of hazard analysis on an SSP. It is recommended that the system safety engineer/analyst be especially familiar with these techniques.

3.6 INDUCTIVE AND DEDUCTIVE TECHNIQUES

System safety hazard analysis techniques are quite often labeled as being either an inductive or deductive methodology. For example, a failure mode and effects analysis (FMEA) is usually referred to as an inductive approach, while an FTA is referred to as a deductive approach. Understanding how to correctly use the terms inductive and deductive is often confusing and even sometimes incorrectly applied. The question is: What do these terms really mean, how should they be used, and does their use provide any value to the safety analyst?

The terms deductive and inductive refer to forms of logic. Deductive comes from deductive reasoning and inductive comes from inductive reasoning. The great detective Sherlock Holmes was a master of both deductive and inductive reasoning in solving criminal cases from clues, premises, and information.

Deductive reasoning is a logical process in which a conclusion is drawn from a set of premises and contains no more information than the premises taken collectively. For example, all dogs are animals; this is a dog; therefore, this is an animal. The truth of the conclusion is dependent upon the premises; the conclusion cannot be false if the premises on which it is based are true. For example, all men are apes; this is a man; therefore, this is an ape. The conclusion seems logically true, however, it is false because the premise is false. In deductive reasoning the conclusion does not exceed or imply more than the premises upon which it is based.

Inductive reasoning is a logical process in which a conclusion is proposed that contains more information than the observation or experience on which it is based. For example, every crow ever seen was black; therefore, all crows are black. The truth of the conclusion is verifiable only in terms of future experience, and certainty is attainable only if all possible instances have been examined.

In the example, there is no certainty that a white crow will not be found tomorrow, although past experience would make such an occurrence seem unlikely. In inductive reasoning the conclusion is broader and may imply more than the known premises can guarantee with the data available.

Given these definitions, an inductive hazard analysis might conclude more than the given data intends to yield. This is useful for general hazard identification. It means a safety analyst might try to identify (or conclude) a hazard from limited design knowledge or information. For example, when analyzing the preliminary design of a high-speed subway system, a safety analyst might conclude that the structural failure of a train car axle is a potential hazard that could result in car derailment and passenger injury. The analyst does not know this for sure; there is no conclusive evidence available, but the conclusion appears reasonable from past knowledge and experience. In this case the conclusion seems realistic but is beyond any factual knowledge or proof available at the time of the analysis; however, a credible hazard has been identified.

A deductive hazard analysis would conclude no more than the data provides. In the above example, the analysis must go in the opposite direction. The specific causal factors supporting the conclusion must be identified and established, and then the conclusion will be true. It seems like reverse logic, however, the hazard can be validly deduced only from the specific detailed causal factors.

Deductive and inductive qualities have become intangible attributes of hazard analysis techniques. An inductive analysis would be used to broadly identify hazards without proven assurance of the causal factors, while a deductive analysis would attempt to find the specific causal factors for identified hazards. An inductive analysis can be thought of as a “what-if” analysis. The analyst asks: What if this part failed, what are the consequences? A deductive analysis can be thought of as a “how-can” analysis. The analyst asks, if this event were to occur, how can it happen or what are the causal factors?

In system safety, inductive analysis tends to be for hazard identification (when the specific root causes are not known or proven), and deductive analysis for root cause identification (when the hazard is known). Obviously there is a fine line between these definitions because sometime the root causes are known from the start of an inductive hazard analysis. This is why some analysis techniques can actually move in both directions. The preliminary hazard analysis (PHA) is a good example of this. Using the standard PHA worksheet, hazards are identified inductively by asking what if this component fails, and hazards are also identified by asking how can this undesired event happen.

Two additional terms that are confusing to system safety analysts are top-down analysis and bottom-up analysis. In general, top-down analysis means starting the analysis from a high-level system viewpoint, for example, a missile navigation system, and continually burrowing into deeper levels of detail until the discrete component level is reached, such as a resistor or diode. A bottom-up analysis moves in the opposite direction. It begins at a low system level, such as the resistor or diode component, and moves upward until the system top level is reached. These definitions are illustrated in Figure 3.5.

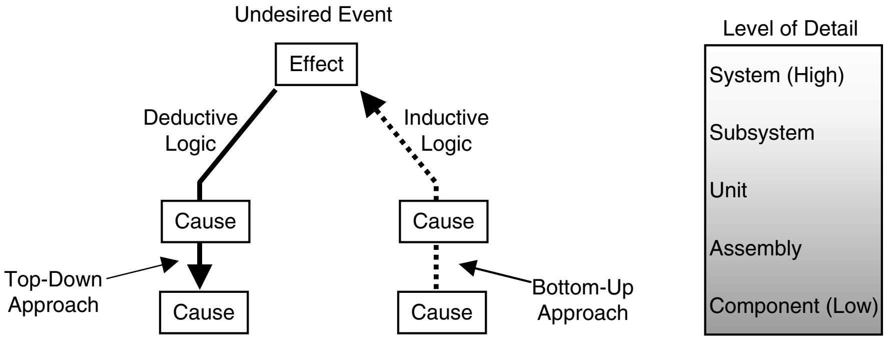


Figure 3.5 *Inductive and deductive analysis relationship.*

Some system safety practitioners advocate that a deductive analysis is always a top-down approach and that an inductive analysis is always a bottom-up approach. This may be a good generalization but is likely not always the case. Table 3.6 summarizes some of the characteristics of inductive and deductive analysis techniques.

TABLE 3.6 Inductive and Deductive Analysis Characteristics

	Inductive	Deductive
Methodology	• What-if • Going from the specific to the general	• How-Can • Going from the general to the specific
General characteristics	• System is broken down into individual components • Potential failures for each component are considered (what can go wrong?) • Effects of each failure are defined (what happens if it goes wrong?)	• General nature of the hazard has already been identified (fire, inadvertent launch, etc.) • System is reviewed to define the cause of each hazard (how can it happen?)
Applicability	• Systems with few components • Systems where single-point failures (SPFs) are predominant • Preliminary or overview analysis	• All sizes of systems • Developed for complex systems • Designed to identify hazards caused by multiple failures
Potential pitfalls	• Difficult to apply to complex systems • Large number of components to consider • Consideration of failure combinations becomes difficult	• Detailed system documentation required • Large amount of data involved • Time consuming
Examples	• Failure mode and effects analysis (FMEA) • Hazard and operability analysis (HAZOP)	• Fault tree analysis (FTA) • Event tree analysis (ETA) • Common cause failure analysis (CCFA)

The bottom line is that in the long run it does not really matter to the safety analyst if a hazard analysis technique is inductive or deductive. An analyst does not select an analysis technique based on whether its methodology is inductive, deductive, top-down, or bottom-up. What is important is that there are various techniques available for identifying hazards and hazard causal factors and that the safety analyst knows how to correctly use and apply the appropriate techniques. An analyst is more concerned with the actual task of identifying and mitigating hazards.

3.7 QUALITATIVE AND QUANTITATIVE TECHNIQUES

System safety analysts are often in a quandary as whether to use a qualitative analysis technique or a quantitative analysis technique. Understanding which analysis type to use, and when, often seems more of an art than a science. The qualitative–quantitative factor is one of the basic attributes of a hazard analysis technique.

Most hazard analysis techniques are performed to identify hazards and then determine the mishap risk of the hazard, where mishap risk is defined as risk = probability × severity. The probability risk factor means the probability of the mishap actually occurring, given the latent hazard conditions and the severity factor means the damage/and/or loss resulting from the mishap after it occurs. To determine the risk of an identified hazard, a risk characterization methodology must be utilized for the probability and severity parameters. Both quantitative and qualitative risk characterization methods have been developed for use in the system safety discipline. Both approaches are useful, but each approach contains inherent unique advantages and disadvantages.

Qualitative analysis involves the use of qualitative criterion in the analysis. Typically this approach uses categories to separate different parameters, with qualitative definitions that establish the ranges for each category. Qualitative judgments are made as to which category something might fit into. This approach has the characteristic of being subjective, but it allows more generalization and is therefore less restricting. For example, arbitrary categories have been established in MIL-STD-882 that provide a qualitative measure of the most reasonable likelihood of occurrence of a mishap. For example, if the safety analyst assesses that an event will occur frequently, it is assigned an index level A; if it occurs occasionally, it is given an index level C. This qualitative index value is then used in qualitative risk calculations and assessments.

Quantitative analysis involves the use of numerical or quantitative data in the analysis and provides a quantitative result. This approach has the characteristic of being more objective and possibly more accurate. It should be noted, however, that quantitative results can be biased by the validity and accuracy of the input numbers. For this reason, quantitative results should not be viewed as an exact number but as an estimate with a range of variability depending upon the goodness quality of the data.

Table 3.7 identifies some of the attributes that can be used to judge the strengths and weaknesses of qualitative and quantitative approaches. The system safety discipline primarily uses the qualitative risk characterization approach for a majority of

TABLE 3.7 Differences Between Quantitative and Qualitative Techniques

	Attribute	Qualitative	Quantitative
1	Numerical results	No	Yes
2	Cost	Lower	Higher
3	Subjective/objective	Subjective	Objective
4	Difficulty	Lower	Higher
5	Complexity	Lower	Higher
6	Data	Less detailed	More detailed
7	Technical expertise	Lower	Higher
8	Time required	Lower	Higher
9	Tools required	Seldom	Usually
10	Accuracy	Lower	Higher

safety work, based on the advantages provided. This approach has been recommended in MIL-STD-882 since the original version in 1969.

System safety prefers the qualitative risk characterization method because for a large system with many hazards it can become cost prohibitive to quantitatively analyze and predict the risk of each and every hazard. In addition, low-risk hazards do not require the refinement provided by quantitative analysis. It may be necessary to conduct a quantitative analysis only on a select few high-consequence hazards. Experience over the years has proven that qualitative methods are very effective and in most cases provide decision-making capability comparable to quantitative analysis.

Qualitative risk characterization provides a very practical and effective approach when cost and time are concerns and/or when the availability of supporting data is low. The key to developing a qualitative risk characterization approach is by carefully defining severity and mishap probability categories.

Quantitative risk characterization provides a useful approach when accuracy is required. Occasionally a numerical design requirement must be met, and the only way to provide evidence that it is met is through quantitative analysis. Probabilistic risk assessment (PRA) is a quantitative analysis that estimates the probability factor of mishap risk. For high-consequence systems it is often necessary to conduct a PRA to determine all of the causal factors for a given mishap and their total probability of causing the mishap to occur.

Scientific theory teaches that when something can be measured (quantitatively) more is known about it, and therefore numerical results provide more value. This is generally true; however, the strict use of quantitative methods must be tempered by utility. Sometimes qualitative judgments provide useful results at less time and expense. In a risk assessment, precise numerical accuracy is not always necessary. Mishap risks are not easily estimated using probability and statistics when the hazard causal factors are not yet well understood. Qualitative measures provide a useful and valid judgment at much less expense than quantitative measures, and they can be obtained much earlier in the system development life cycle. It makes sense to first evaluate all identified hazards qualitatively, and then, for high-risk hazards conduct a quantitative analysis for more precise knowledge.

TABLE 3.8 Hazard Analysis Type/Technique Summary

Type	Coverage	Hazard Focus	Primary Technique
CD-HAT	Conceptual design	System hazards	PHL
PD-HAT	Preliminary design	Systems hazards	PHA
DD-HAT	Detailed subsystem design	Subsystem hazards	SSHA
SD-HAT	Integrated system design	Integrated system hazards	SHA
OD-HAT	Operational design	Operational hazards	O&SHA
HD-HAT	Human health design	Human health hazards	HHA
RD-HAT	Design, test, and safety requirements	Requirements/testing	SRCA

In any evaluation of mishap risk assessment, the question of measure and acceptability parameters arises. There is always the danger that system safety analysts and managers will become so enamored with probability and statistics that simpler and more meaningful engineering processes will be ignored. Before embarking in a particular direction, be sure that the limitations and principles of both approaches are well understood, as well as the actual analysis needs. Quantitative models are useful, but do not ever equate mathematical model results with reality.

3.8 SUMMARY

This chapter discussed the basic concept of hazard analysis types and techniques. The following are basic principles that help summarize the discussion in this chapter:

1. A hazard analysis type defines the analysis purpose, timing, scope, level of detail, and system coverage; it does not specify how to perform the analysis.
2. A hazard analysis technique defines a specific and unique analysis methodology that provides a specific methodology and results.
3. The seven hazard analysis types, their coverage, and intended focus are summarized in Table 3.8. In addition, the primary technique for satisfying the type requirements is listed.
4. There are seven hazard analysis types in the system safety discipline that, together, help ensure identification and resolution of system hazards. There are over 100 different analysis techniques that can be used to satisfy the analysis type requirements.
5. One particular hazard analysis type does not necessarily identify all the hazards within a system; it may take more than one type, and usually all seven types.
6. A best practice SSP includes all seven hazard analysis types to ensure complete hazard coverage and provide optimum safety assurance.
7. The seven primary hazard analysis techniques are generally the best option for satisfying the corresponding analysis type requirement in an SSP.

Chapter 4

Preliminary Hazard List

4.1 INTRODUCTION

The preliminary hazard list (PHL) is an analysis technique for identifying and listing potential hazards and mishaps that may exist in a system. The PHL is performed during conceptual or preliminary design and is the starting point for all subsequent hazard analyses. Once a hazard is identified in the PHL, the hazard will be used to launch in-depth hazard analyses and evaluations, as more system design details become available. The PHL is a means for management to focus on hazardous areas that may require more resources to eliminate the hazard or control risk to an acceptable level. Every hazard identified on the PHL will be analyzed with more detailed analysis techniques.

This analysis technique falls under the conceptual design hazard analysis type (CD-HAT). The PHL evaluates design at the conceptual level, without detailed information, and it provides a preliminary list of hazards. There are no alternate names for this technique.

4.2 BACKGROUND

The primary purpose of the PHL is to identify and list potential system hazards. A secondary purpose of the PHL is to identify safety critical parameters and mishap categories. The PHL analysis is usually performed very early in the design development process and prior to performing any other hazard analysis. The PHL is used as a management tool to allocate resources to particularly hazardous areas within the design, and it becomes the foundation for all other subsequent hazard analyses

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

performed on the program. Follow-on hazard analyses will evaluate these hazards in greater detail as the design detail progresses. The intent of the PHL is to affect the design for safety as early as possible in the development program.

The PHL is applicable to any type of system at a conceptual or preliminary stage of development. The PHL can be performed on a subsystem, a single system, or an integrated set of systems. The PHL is generally based on preliminary design concepts and is usually performed early in the development process, sometimes during the proposal phase or immediately after contract award in order to influence design and mishap risk decisions as the design is formulated and developed.

The technique, when applied to a given system by experienced system safety personnel, is thorough at identifying high-level system hazards and generic hazards that may exist in a system. A basic understanding of hazard theory is essential as well as knowledge of system safety concepts. Experience with the particular type of system under investigation, and its basic components, is necessary in order to identify system hazards. The technique is uncomplicated and easily learned. Typical PHL forms and instructions are provided in this chapter.

The PHL technique is similar to a brainstorming session, whereby hazards are postulated and collated in a list. This list is then the starting point for subsequent hazard analyses, which will validate the hazard and begin the process of identifying causal factors, risk, and mitigation methods. Generating a PHL is a prerequisite to performing any other type of hazard analysis. Use of this technique is highly recommended. It is the starting point for more detailed hazard analysis and safety tasks, and it is easily performed.

4.3 HISTORY

The technique was established very early in the history of the system safety discipline. It was formally instituted and promulgated by the developers of MIL-STD-882.

4.4 THEORY

The PHL is a simple and straightforward analysis technique that provides a list of known and suspected hazards. A PHL analysis can be as simple as conducting a hazard brainstorming session on a system, or it can be a slightly more structured process that helps ensure that all hazards are identified. The PHL method described here is a process with some structure and rigor, with the application of a few basic guidelines.

The PHL analysis should involve a group of engineers/analysts with expertise in a variety of specialized areas. The methodology described herein can be used by an individual analyst or a brainstorming group to help focus the analysis. The recommended methodology also provides a vehicle for documenting the analysis results on a worksheet.

Figure 4.1 shows an overview of the basic PHL process and summarizes the important relationships involved in the PHL process. This process consists of combining design information with known hazard information to identify hazards.

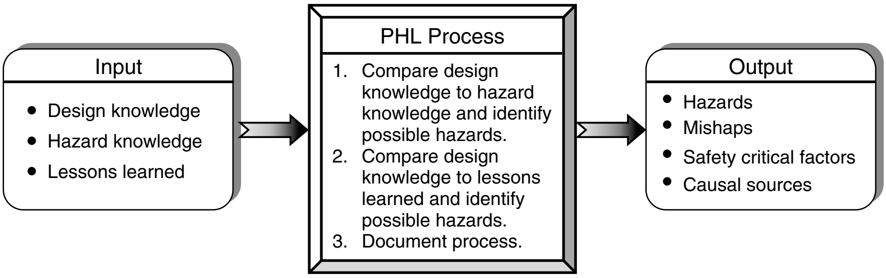

Input
• Design knowledge
• Hazard knowledge
• Lessons learned
PHL Process
1. Compare design knowledge to hazard knowledge and identify possible hazards.
2. Compare design knowledge to lessons learned and identify possible hazards.
3. Document process.
Output
• Hazards
• Mishaps
• Safety critical factors
• Causal sources

Figure 4.1 *Preliminary hazard list overview.*

Known hazardous elements and mishap lessons learned are compared to the system design to determine if the design concept utilizes any of these potential hazard elements.

To perform the PHL analysis, the system safety analyst must have two things—design knowledge and hazard knowledge. Design knowledge means the analyst must posses a basic understanding of the system design, including a list of major components. Hazard knowledge means the analyst needs a basic understanding about hazards, hazard sources, hazard components, and hazards in similar systems. Hazard knowledge is primarily derived from hazard checklists and from lessons learned on the same or similar systems and equipment.

In performing the PHL analysis, the analyst compares the design knowledge and information to hazard checklists. This allows the analyst to visualize or postulate possible hazards. For example, if the analyst discovers that the system design will be using jet fuel, he then compares jet fuel to a hazard checklist. From the hazard checklist it will be obvious that jet fuel is a hazardous element and that a jet fuel fire/explosion is a potential mishap with many different ignition sources presenting many different hazards.

The primary output from the PHL is a list of hazards. It is also necessary and beneficial to collect and record additional information, such as the prime hazard causal factors (e.g., hardware failure, software error, human error, etc.), the major mishap category for the hazard (e.g., fire, inadvertent launch, physical injury, etc.), and any safety critical (SC) factors that will be useful for subsequent analysis (e.g., SC function, SC hardware item, etc.).

4.5 METHODOLOGY

Table 4.1 lists and describes the basic steps of the PHL process and summarizes the important relationships involved. A worksheet is utilized during this analysis process.

The PHL process begins by acquiring design information in the form of the design concept, the operational concept, major components planned for use in the system, major system functions, and software functions. Sources for this information could include: statement of work (SOW), design specifications, sketches, drawings, or schematics. Additional design integration data can be utilized to better

TABLE 4.1 PHL Analysis Process

Step	Task	Description
1	Define system	Define, scope, and bound the system. Define the mission, mission phases, and mission environments. Understand the system design, operational concepts, and major system components.
2	Plan PHL	Establish PHL goals, definitions, worksheets, schedule, and process. Identify system elements and functions to be analyzed.
3	Select team	Select all team members to participate in PHL and establish responsibilities. Utilize team member expertise from several different disciplines (e.g., design, test, manufacturing, etc.).
4	Acquire data	Acquire all of the necessary design, operational, and process data needed for the analysis (e.g., equipment lists, functional diagrams, operational concepts, etc.). Acquire hazard checklists, lessons learned, and other hazard data applicable to the system.
5	Conduct PHL	a. Construct list of hardware components and system functions. b. Evaluate conceptual system hardware; compare with hazard checklists. c. Evaluate system operational functions; compare with hazard checklists. d. Identify and evaluate system energy sources to be used; compare with energy hazard checklists. e. Evaluate system software functions; compare with hazard checklists. f. Evaluate possible failure states.
6	Build hazard list	Develop list of identified and suspected system hazards and potential system mishaps. Identify SCFs and TLMs if possible from information available.
7	Recommend corrective action	Recommend safety guidelines and design safety methods that will eliminate or mitigate hazards.
8	Document PHL	Document the entire PHL process and PHL worksheets in a PHL report. Include conclusions and recommendations.

understand, analyze, and model the system. Typical design integration data includes functional block diagrams, equipment indenture lists [e.g., work breakdown structure (WBS), reliability block diagrams, and concept of operations]. If the design integration data is not available, the safety analyst may have to make assumptions in order to perform the PHL analysis. All assumptions should be documented.

The next step in the PHL analysis is to acquire the appropriate *hazard checklists.* Hazard checklists are generic lists of items known to be hazardous or that might create potentially hazardous designs or situations. The hazard checklist should not be considered complete or all-inclusive. Hazard checklists help trigger the analyst's recognition of potential hazardous sources from past lessons learned. Typical hazard checklists include:

1. Energy sources
2. Hazardous functions

3. Hazardous operations
4. Hazardous components
5. Hazardous materials
6. Lessons learned from similar type systems
7. Undesired mishaps
8. Failure mode and failure state considerations

When all of the data is available, the analysis can begin. PHL analysis involves comparing the design and integration information to the hazard checklists. If the system design uses a known hazard component, hazardous function, hazardous operation, and the like, then a potential hazard exists. This potential hazard is recorded on the analysis form and then further evaluated with the level of design information that is available. Checklists also aid in the brainstorming process for new hazard possibilities brought about by the unique system design. PHL output includes: identified hazards, hazard causal factor areas (if possible), resulting mishap effect, and safety critical factors (if any).

The overall PHL methodology is illustrated in Figure 4.2*a*. In this methodology a system list is constructed that identifies planned items in the hardware, energy

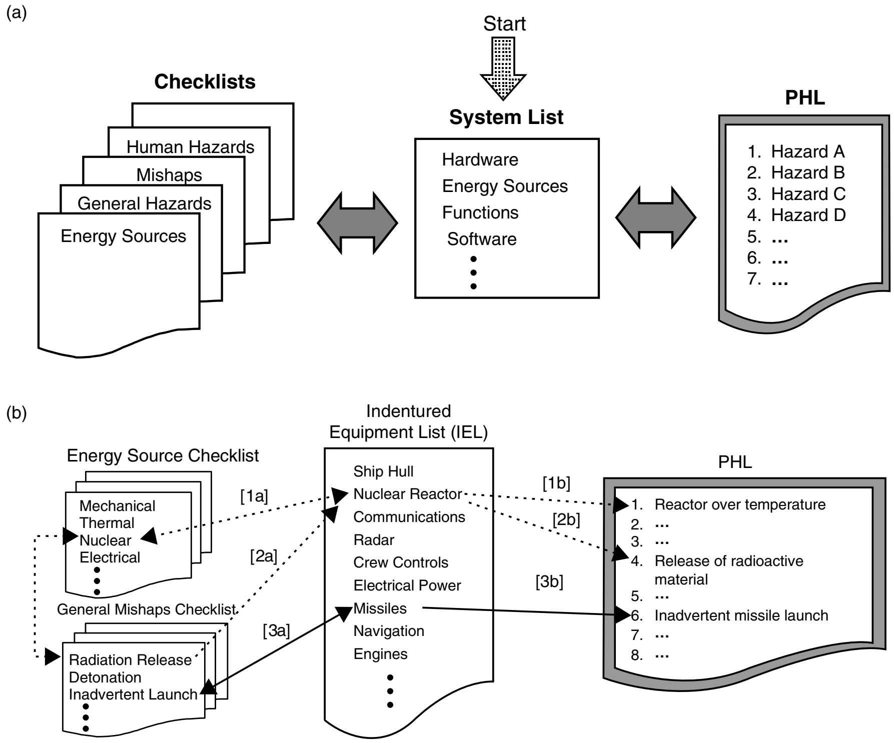


Figure 4.2 *(a) PHL methodology. (b) PHL methodology example.*

sources, functions, and software categories. Items on the system list are then compared to items on the various safety checklists. Matches between the two lists triggers ideas for potential hazards, which are then compiled in the PHL. The overall PHL methodology is demonstrated by the brief example in Figure 4.2*b*. The system in this example involves the conceptual design for a new nuclear-powered aircraft carrier system.

From the design and operational concept information (Fig. 4.2) an indentured equipment list (IEL) is constructed for the PHL. The equipment on the IEL is then compared with the hazard checklists to stimulate hazard identification. For example, "Nuclear reactor" appears on the IEL and it also appears on the hazardous energy source checklist. This match (1a) triggers the identification of one or more possible hazards, such as "Reactor over temperature." This hazard is then added to the PHL (1b) as hazard 1.

"Nuclear reactor" appears on the IEL and it also appears on the general mishaps checklist. This match (2a) triggers the identification of one or more possible hazards, "Accidental release of radioactive material." This hazard is then added to the PHL (2b) as hazard 4.

"Missiles" appear on the IEL and "Inadvertent weapon launch" appears on the general mishaps checklist. This match (3a) triggers the identification of "inadvertent missile launch" as a possible hazard, which is added to the PHL (3b) as hazard 6.

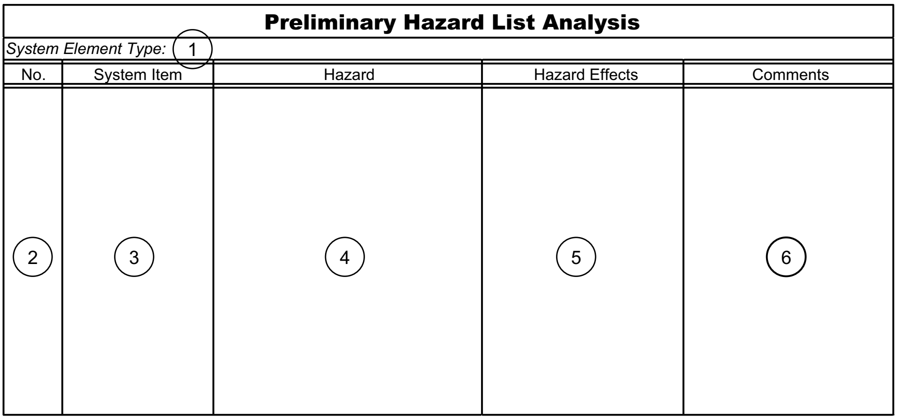
4.6 WORKSHEET

It is desirable to perform the PHL analysis using a worksheet. The worksheet will help to add rigor to the analysis, record the process and data, and help support justification for the identified hazards. The format of the analysis worksheet is not critical, and typically columnar-type worksheets are utilized.

The following basic information should be obtained from the PHL analysis worksheet:

1. Actual and suspected hazards
2. Top-level mishap
3. Recommendations (such as safety requirements/guidelines that can be applied)

The primary purpose of a worksheet is to provide structure and documentation to the analysis process. The recommended PHL worksheet for system safety usage is shown in Figure 4.3. In the PHL worksheet in the Figure 4.3 second column contains a list of system items from which hazards can easily be recognized. For example, by listing all of the system functions, hazards can be postulated by answering the questions: What if the function fails to occur? or What if the function occurs inadvertently?



Preliminary Hazard List Analysis

System Element Type: 1

No.	System Item	Hazard	Hazard Effects	Comments
2	3	4	5	6

Figure 4.3 *PHL worksheet.*

The PHL worksheet columns are defined as follows:

1. *System Element Type* This column identifies the type of system items under analysis, such as system hardware, system functions, system software, energy sources, and the like.
2. *Hazard Number* This column identifies the hazard number for reference purposes.
3. *System Item* This column is a subelement of data item 1 and identifies the major system items of interest in the identified category. In the example to follow, the items are first broken into categories of hardware, software, energy sources, and functions. Hazards are postulated through close examination of each listed item under each category. For example, if explosives is an intended hardware element, then explosives would be listed under hardware and again under energy sources. There may be some duplication, but this allows for the identification of all explosives-related hazards.
4. *Hazard* This column identifies the specific hazard that is created as a result of the indicated system item. (Remember: Document all potential hazards, even if they are later proven by other analyses to be nonhazardous in this application.)
5. *Hazard Effects* This column identifies the effect of the identified hazard. The effect would be described in terms of resulting system operation, misoperation, death, injury, damage, and so forth. Generally the effect is the resulting mishap.
6. *Comments* This column records any significant information, assumptions, recommendations, and the like resulting from the analysis. For example, safety critical functions (SCFs), top-level mishaps (TLMs), or system safety design guidelines might be identified here.

4.7 HAZARD CHECKLISTS

Hazard checklists provide a common source for readily recognizing hazards. Since no single checklist is ever really adequate in itself, it becomes necessary to develop and utilize several different checklists. Utilizing several checklists may generate some repetition, but will also result in improved coverage of hazardous elements.

Remember that a checklist should never be considered a complete and final list but merely a mechanism or catalyst for stimulating hazard recognition. Refer to Appendix C of this book for a more complete set of hazard checklists. To illustrate the hazard checklist concept, some example checklists are provided in Figures 4.4 through 4.8. These example checklists are not intended to represent ultimate checklist sources, but are some typical example checklists used in recognizing hazards.

Figure 4.4 is a checklist of energy sources that are considered to be hazardous elements when used within a system. The hazard is generally from the various modes of energy release that are possible from hazardous energy sources. For example, electricity/voltage is a hazardous energy source. The various hazards that can result from undesired energy release include personnel electrocution, ignition source for fuels and/or materials, sneak path power for an unintended circuit, and so forth.

Figure 4.5 contains a checklist of general sources that have been found to produce hazardous conditions and potential accidents, when the proper system conditions are present.

Figure 4.6 is a checklist of functions that are hazardous due to the critical nature of the mission. This checklist is an example particularly intended for space programs.

Figure 4.7 is a checklist of operations that are considered hazardous due to the materials used or due to the critical nature of the operation.

Figure 4.8 is a checklist of possible failure modes or failure states that are considered hazardous, depending on the critical nature of the operation or function involved. This checklist is a set of key questions to ask regarding the state of the component, subsystem, or system functions. These are potential ways the subsystem

1. Fuels
2. Propellants
3. Initiators
4. Explosive charges
5. Charged electrical capacitors
6. Storage batteries
7. Static electrical charges
8. Pressure containers
9. Spring-loaded devices
10. Suspension systems
11. Gas generators
12. Electrical generators
13. RF energy sources
14. Radioactive energy sources
15. Falling objects
16. Catapulted objects
17. Heating devices
18. Pumps, blowers, fans
19. Rotating machinery
20. Actuating devices
21. Nuclear
22. Cryogenics

Figure 4.4 *Example of hazard checklist for energy sources.*

1. Acceleration
2. Contamination
3. Corrosion
4. Chemical dissociation
5. Electrical
   - Shock
   - Thermal
   - Inadvertent activation
   - Power source failure
6. Explosion
7. Fire
8. Heat and temperature
   - High temperature
   - Low temperature
   - Temperature variations
9. Leakage
10. Moisture
    - High humidity
    - Low humidity
11. Oxidation
12. Pressure
    - High
    - Low
    - Rapid change
13. Radiation
    - Thermal
    - Electromagnetic
    - Ionizing
    - Ultraviolet
14. Chemical replacement
15. Shock (mechanical)
16. Stress concentrations
17. Stress reversals
18. Structural damage or failure
19. Toxicity
20. Vibration and noise
21. Weather and environment
22. Gravity

Figure 4.5 *Example of hazard checklist for general sources.*

could fail and thereby result in creating a hazard. For example, when evaluating each subsystem, answering the question "Does *fail to operate* cause a hazard?" may lead to the recognition of a hazard. Note that when new hardware elements and functions are invented and used, new hazardous elements will be introduced requiring expanded and updated checklists.

1. Crew egress/ingress
2. Ground to stage power transfer
3. Launch escape
4. Stage firing and separation
5. Ground control communication
6. Rendezvous and docking
7. Ground control of crew
8. Ground data communication to crew
9. Extra vehicular activity
10. In-flight tests by crew
11. In-flight emergencies
    - Loss of communications
    - Loss of power/control
    - Fire toxicity
    - Explosion
12. Life support
13. Parachute deployment and descent
14. Crew recovery
15. Vehicle safing and recovery
16. Vehicle inerting and decontamination
17. Payload mating
18. Fairing separation
19. Orbital injection
20. Solar panel deployment
21. Orbit positioning
22. Orbit correction
23. Data acquisition
24. Midcourse correction
25. Star acquisition (navigation)
26. On-orbit performance
27. Retrothrust
28. Reentry

Figure 4.6 *Example of hazard checklist for space functions.*

1. Welding
2. Cleaning
3. Extreme temperature operations
4. Extreme weight operations
5. Hoisting, handling, and assembly operations
6. Test chamber operations
7. Proof test of major components/subsystems/systems
8. Propellant loading/transfer/handling
9. High-energy pressurization/hydrostatic-pneumostatic testing
10. Nuclear component handling/checkout
11. Ordnance installation/checkout/test
12. Tank entry/confined space entry
13. Transport and handling of end item
14. Manned vehicle tests
15. Static firing

Figure 4.7 *Example of hazard checklist for general operations.*

4.8 GUIDELINES

The following are some basic guidelines that should be followed when completing the PHL worksheet:

1. Remember that the objective of the PHL is to identify system hazards and/or mishaps.
2. The best approach is to start by investigating system hardware items, system functions, and system energy sources.
3. Utilize hazard checklists and lessons learned for hazard recognition.

1. Fails to operate
2. Operates incorrectly/erroneously
3. Operates inadvertently
4. Operates at incorrect time (early, late)
5. Unable to stop operation
6. Receives erroneous data
7. Sends erroneous data

Figure 4.8 *Example of hazard checklist for failure states.*

4. A hazard write-up should be understandable but does not have to be detailed in description (i.e., the PHL hazard does not have to include all three elements of a hazard: hazardous element, initiating mechanisms, and outcome).

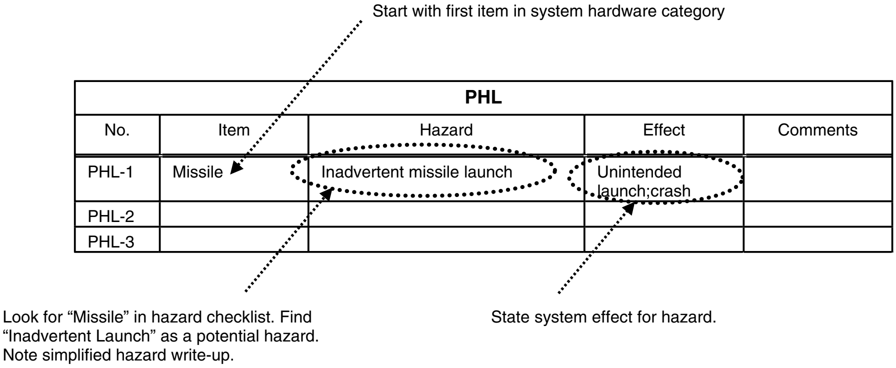
Chapter 2 described the three components of a hazard: (1) hazardous element, (2) initiating mechanism, and (3) Threat and target (outcome). Typically when a hazard is identified and described, the hazard write-up description will identify and include all three components. However, in the PHL, a complete and full hazard description is not always provided. This is primarily because of the preliminary nature of the analysis and that all identified hazards are more fully investigated and described in the preliminary hazard analysis (PHA) and subsystem hazard analysis (SSHA).

Figure 4.9 shows how to apply the PHL guidelines when using the PHL worksheet.

4.9 EXAMPLE: ACE MISSILE SYSTEM

In order to demonstrate the PHL methodology, a hypothetical small missile system will be analyzed. The basic system design is shown in Figure 4.10 for the Ace Missile System. The major segments of the system are the missile segment and the weapon control system (WCS) segment. The missile segment includes only those components specifically comprising the missile. The WCS segment includes those components involved in command and control over the missile, such as the operator's console, system computer, radar, system power, and so forth.

The basic equipment and functions for this system are identified in Figure 4.11. During the conceptual design stage, this is the typical level of information that is available. Some basic design decisions may be necessary, such as the type of engine



Start with first item in system hardware category

PHL				
No.	Item	Hazard	Effect	Comments
PHL-1	Missile	Inadvertent missile launch	Unintended launch;crash	
PHL-2				
PHL-3				

Look for "Missile" in hazard checklist. Find "Inadvertent Launch" as a potential hazard. Note simplified hazard write-up.

State system effect for hazard.

Figure 4.9 *PHL guidelines.*

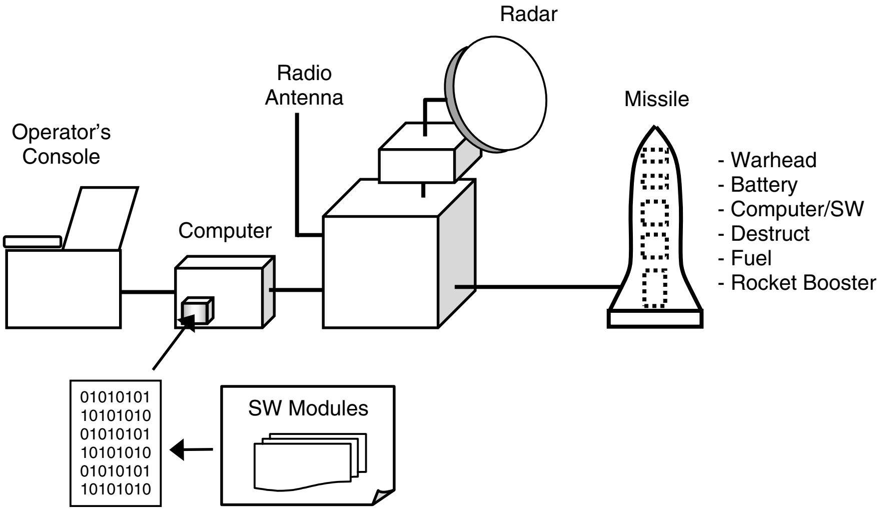
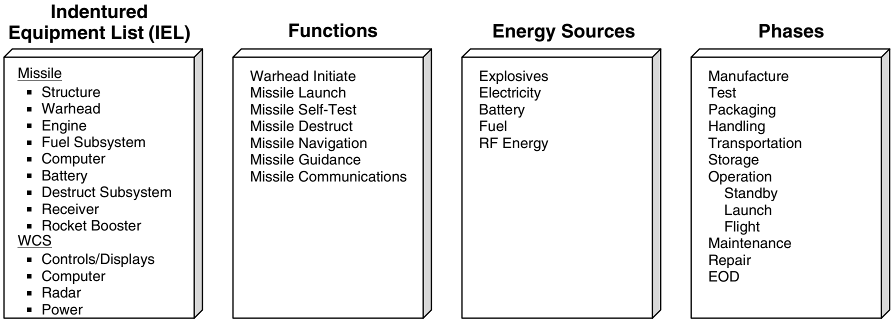


Figure 4.10 Ace Missile System.

to be utilized, jet or solid rocket. A design safety trade study might be performed to evaluate the hazards of a jet system versus a rocket system. From this basic design information a very credible list of hazards can easily be generated.

Figure 4.12 shows the basic planned operational phases for the missile system. As design development progresses, each of these phases will be expanded in greater detail. The lists of components, functions, and phases are generated by the missile project designers or the safety analyst. The PHL begins by comparing each system component and function to hazard checklists, to stimulate ideas on potential hazards involved with this system design.

Tables 4.2, 4.3, and 4.4 contain a PHL analysis of the system hardware, functions, and energy sources, respectively. For example, Table 4.2 evaluates system hardware



Indentured Equipment List (IEL)

Missile
- Structure
- Warhead
- Engine
- Fuel Subsystem
- Computer
- Battery
- Destruct Subsystem
- Receiver
- Rocket Booster

WCS
- Controls/Displays
- Computer
- Radar
- Power

Functions

Warhead Initiate
Missile Launch
Missile Self-Test
Missile Destruct
Missile Navigation
Missile Guidance
Missile Communications

Energy Sources

Explosives
Electricity
Battery
Fuel
RF Energy

Phases

Manufacture
Test
Packaging
Handling
Transportation
Storage
Operation
  Standby
  Launch
  Flight
Maintenance
Repair
EOD

Figure 4.11 Ace Missile System conceptual information.

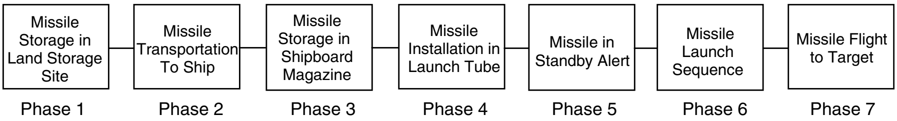

Missile Storage in Land Storage Site
Phase 1
Missile Transportation To Ship
Phase 2
Missile Storage in Shipboard Magazine
Phase 3
Missile Installation in Launch Tube
Phase 4
Missile in Standby Alert
Phase 5
Missile Launch Sequence
Phase 6
Missile Flight to Target
Phase 7

Figure 4.12 *Missile functional flow diagram of operational phases.*

TABLE 4.2 PHL Analysis of Ace Missile System—System Hardware Evaluation

Preliminary Hazard List Analysis				
System Element Type: **System Hardware**				
No.	System Item	Hazard	Hazard Effects	Comments
PHL-1	Missile structure	Missile body breaks up resulting in fuel leakage; and ignition source causing fire	Missile fire	Ground operations
PHL-2	Missile structure	Missile body breaks up causing missile crash	Missile crash	Flight
PHL-3	Missile warhead (W/H)	Detonation of W/H explosives from fire, bullet, shock, etc.	W/H explosives detonation	Use insensitive munitions (IM)
PHL-4	Missile W/H	Initiation of W/H from inadvertent initiation commands	Inadvertent W/H initiation	Initiation requires both arm and fire signals
PHL-5	Missile W/H	Missile W/H fails to initiate	Dud	Unexploded ordnance (UXO) concern
PHL-6	Missile engine	Engine fails to start (missile crash)	Incorrect target	Unsafe missile state, fuel release
PHL-7	Missile engine	Engine fails during flight resulting in crash	Incorrect target	
PHL-8	Missile fuel subsystem	Engine fuel tank leakage and ignition source present resulting in fire	Missile fire	
PHL-9	Missile computer	Computer inadvertently generates W/H Arm-1 and Arm-2 commands, causing W/H initiation	Inadvertent W/H initiation	
PHL-10	Missile computer	Computer fails to generate W/H Arm-1 or Arm-2 commands	Inability to initiate W/H	Dud; not a safety concern
PHL-11	Missile computer	Computer inadvertently generates missile destruct command	Inadvertent destruct	Safe separation issue

(*continued*)

TABLE 4.2 ***Continued***

Preliminary Hazard List Analysis				
System Element Type: **System Hardware**				
No.	System Item	Hazard	Hazard Effects	Comments
PHL-12	Missile computer	Computer fails to generate missile destruct command	Inability to destruct missile	
PHL-13	Missile battery	Battery is inadvertently activated, providing power for W/H Arm and Fire commands	Inadvertent W/H Initiation	Mishap also requires Arm and Fire signals
PHL-14	Missile battery	Battery electrolyte leakage occurs and ignition source present resulting in fire	Missile fire	
PHL-15	Missile destruct subsystem	Destruct system fails	Unable to destruct missile	Also requires fault necessitating destruct
PHL-16	Receiver	Receiver fails—no communication with missile	Unable to destruct missile	
PHL-17	Receiver	Receiver fails—creates erroneous destruct command	Inadvertent missile destruct	
PHL-18	Rocket booster	Inadvertent ignition of rocket	Inadvertent launch	Uncontrolled flight
PHL-19	WCS computer	Computer inadvertently generates missile launch commands	Inadvertent missile launch	
PHL-20	WCS radar	Electromagnetic radiation (EMR) injures exposed personnel	Personnel RF energy injury	
PHL-21	WCS radar	EMR causes ignition of explosives	Explosives detonation	
PHL-22	WCS radar	EMR causes ignition of fuel	Missile fuel fire	
PHL-23	WCS power	High-voltage electronics causes fire	Cabinet fire	System damage or personnel injury

starting with the first component in the IEL, missile body, then the warhead, then the engine, and so forth. In this example, the PHL worksheet was developed as a single long table extending over several pages, but the worksheet could have been broken into many single pages.

TABLE 4.3 PHL Analysis of Ace Missile System—System Functions Evaluation

Preliminary Hazard List Analysis				
System Element Type: **System Functions**				
No.	System Item	Hazard	Hazard Effects	Comments
PHL-24	Warhead initiate	Warhead initiate function occurs inadvertently	Inadvertent W/H initiation	Initiation requires Arm-1 and Arm-2 functions
PHL-25	Warhead initiate	Warhead initiate function fails to occur	Dud warhead	Not a safety concern
PHL-26	Missile launch	Missile launch function occurs inadvertently	Inadvertent missile launch	
PHL-27	Missile self-test	Self-test function fails, resulting in unknown missile status	Unsafe missile state	
PHL-28	Missile destruct	Missile destruct function occurs inadvertently	Inadvertent missile destruct	
PHL-29	Missile navigation	Errors occur in missile navigation function	Incorrect target	
PHL-30	Missile guidance	Errors occur in missile guidance function	Incorrect target	
PHL-31	Communications with missile	Communication is lost, causing inability to initiate missile destruct system	Inability to destruct missile	

The following results should be noted from the PHL analysis of the Ace Missile System:

1. A total of 40 hazards have been identified by the PHL analysis.
2. No recommended action resulted from the PHL analysis, only the identification of hazards. These hazards provide design guidance to the system areas that will present mishap risk and require further design attention for safety.
3. Each of the 40 hazards identified in the PHL will be carried into the PHA for further analysis and investigation.
4. Although this PHL did not focus on SCFs and TLMs, it is possible to start generating this information, as shown in Table 4.5. The TLMs shown in Table 4.5 have been established from the entire list of PHL hazards. All of the identified hazards have been consolidated into these TLM categories. After establishing the TLMs, it was then possible to identify SCFs that are associated with certain TLMs, as shown in Table 4.5.

TABLE 4.4 PHL Analysis of Ace Missile System—System Energy Sources Evaluation

Preliminary Hazard List Analysis				
System Element Type: **System Energy Sources**				
No.	System Item	Hazard	Hazard Effects	Comments
PHL-32	Explosives	Inadvertent detonation of W/H explosives	Inadvertent W/H initiation	
PHL-33	Explosives	Inadvertent detonation of missile destruct explosives	Inadvertent missile destruct	
PHL-34	Electricity	Personnel injury during maintenance of high-voltage electrical equipment	Personnel electrical injury	
PHL-35	Battery	Missile battery inadvertently activated	Premature battery power	Power to missile subsystems and W/H
PHL-36	Fuel	Missile fuel ignition causing fire	Missile fuel fire	
PHL-37	RF energy	Radar RF energy injures personnel	Personnel injury from RF energy	
PHL-38	RF energy	Radar RF energy detonates W/H explosives	Explosives detonation	
PHL-39	RF energy	Radar RF energy detonates missile destruct explosives	Explosives detonation	
PHL-40	RF energy	Radar RF energy ignites fuel	Missile fuel fire	

4.10 ADVANTAGES AND DISADVANTAGES

The following are advantages of the PHL technique:

1. The PHL is easily and quickly performed.
2. The PHL does not require considerable expertise for technique application.

TABLE 4.5 Missile System TLMs and SCFs from PHL Analysis

TLM No.	Top-Level Mishap	SCF
1	Inadvertent W/H initiation	Warhead initiation sequence
2	Inadvertent missile launch	Missile launch sequence
3	Inadvertent missile destruct	Destruct initiation sequence
4	Incorrect target	
5	Missile fire	
6	Missile destruct fails	Destruct initiation sequence
7	Personnel injury	
8	Unknown missile state	
9	Inadvertent explosives detonation	

3. The PHL is comparatively inexpensive, yet provides meaningful results.
4. The PHL process provides rigor for focusing on hazards.
5. The PHL provides an indication of where major system hazards and mishap risk will exist.

There are no disadvantages of the PHL technique.

4.11 COMMON MISTAKES TO AVOID

When first learning how to perform a PHL, it is commonplace to commit some typical errors. The following is a list of errors often made during the conduct of a PHL:

1. Not listing all concerns or credible hazards. It is important to list all possible suspected or credible hazards and not leave any potential concerns out of the analysis.
2. Failure to document hazards identified but found to be not credible. The PHL is a historical document encompassing all hazard identification areas that were considered.
3. Not utilizing a structured approach of some type. Always use a worksheet and include all equipment, energy sources, functions, and the like.
4. Not collecting and utilizing common hazard source checklists.
5. Not researching similar systems or equipment for mishaps and lessons learned that can be applied.
6. Not establishing a correct list of hardware, functions, and mission phases.
7. Assuming the reader will understand the hazard description from a brief abbreviated statement filled with project-unique terms and acronyms.

4.12 SUMMARY

This chapter discussed the PHL analysis technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of PHL analysis is to identify potential hazards and mishaps existing in a system conceptual design.
2. The PHL provides hazard information that serves as a starting point for the PHA.
3. The PHL is an aid for safety and design decision making early in the development program and provides information on where to apply safety and design resources during the development program.
4. The use of a functional flow diagram and an indentured equipment list greatly aids and simplifies the PHL process.

5. In performing the PHL, hazard checklists are utilized. However, a hazard checklist should never be considered a complete and final list but merely a catalog for stimulating hazard ideas.
6. Do not exclude any thoughts, ideas, or concerns when postulating hazards. In addition to identifying real hazards, it is also important to show that certain hazards were suspected and considered, even though they were later found to not be possible for various design reasons. This provides evidence that all possibilities were considered.
7. Write a full, credible, and meaningful hazard description that is understandable to the reader and not just to the analyst. Do not assume the reader understands the hazard from a brief abbreviated statement filled with project-unique terms and acronyms.
8. When possible, identify the three elements comprising a hazard:
   - Hazardous element (source)
   - Initiating mechanism (mechanism)
   - Target/threat (outcome)
9. Typically when a hazard is identified and described, the hazard write-up description will identify and include all three elements of a hazard. However, in the PHL a complete and full hazard description is not always provided. This is primarily because of the preliminary nature of the analysis, and that all identified hazards are more fully investigated and described in the PHA.

BIBLIOGRAPHY

Layton, D., *System Safety: Including DOD Standards*, Weber Systems, Inc., 1989.

Roland, H. E. and B. Moriarty, *System Safety Engineering and Management*, 2nd ed., Wiley, New York, 1990.

Stephans, R. A., *System Safety for the 21st Century*, Wiley, Hoboken, NJ, 2004.

Stephenson, J., *System Safety 2000*, Wiley, New York, 1991.

System Safety Society, *System Safety Analysis Handbook*, System Safety Society.

Vincoli, J. W., *A Basic Guide to System Safety*, Van Nostrand Reinhold, New York, 1993.

Chapter 5

Preliminary Hazard Analysis

5.1 INTRODUCTION

The preliminary hazard analysis (PHA) technique is a safety analysis tool for identifying hazards, their associated causal factors, effects, level of risk, and mitigating design measures when detailed design information is not available. The PHA provides a methodology for identifying and collating hazards in the system and establishing the initial system safety requirements (SSRs) for design from preliminary and limited design information. The intent of the PHA is to affect the design for safety as early as possible in the development program. The PHA normally does not continue beyond the subsystem hazard analysis (SSHA).

5.2 BACKGROUND

This analysis technique falls under the preliminary design hazard analysis type (PD-HAT) because it evaluates design at the preliminary level without detailed information. The analysis types are described in Chapter 3. Gross hazard analysis and potential hazard analysis are alternate names for this analysis technique.

The purpose of the PHA is to analyze identified hazards, usually provided by the preliminary hazard list (PHL), and to identify previously unrecognized hazards early in the system development. The PHA is performed at the preliminary design level, as its name implies. In addition, the PHA identifies hazard causal factors, consequences, and relative risk associated with the initial design concept. The PHA

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

provides a mechanism for identifying initial design SSRs that assist in designing in safety early in the design process. The PHA also identifies safety critical functions (SCFs) and top-level mishaps (TLMs) that provide a safety focus during the design process.

The PHA is applicable to the analysis of all types of systems, facilities, operations, and functions; the PHA can be performed on a unit, subsystem, system, or an integrated set of systems. The PHA is generally based on preliminary or baseline design concepts and is usually generated early in the system development process in order to influence design and mishap risk decisions as the design is developed into detail. The PHA technique, when methodically applied to a given system by experienced safety personnel, is thorough in identifying system hazards based on the limited design data available.

A basic understanding of hazard analysis theory is essential as well as knowledge of system safety concepts. Experience with, or a good working knowledge of, the particular type of system and subsystem is necessary in order to identify and analyze all hazards. The PHA methodology is uncomplicated and easily learned. Standard PHA forms and instructions are provided in this chapter, and standard hazard checklists are readily available.

The PHA is probably the most commonly performed hazard analysis technique. In most cases, the PHA identifies the majority of the system hazards. The remaining hazards are usually uncovered when subsequent hazard analyses are generated and more design details are available. Subsequent hazard analyses refine the hazard cause–effect relationship and uncover previously unidentified hazards and refine the design safety requirements.

There are no alternatives to a PHA. A PHL might be done in place of the PHA, but this is *not* recommended since the PHL is only a list of hazards and not as detailed as a PHA and does not provide all of the required information. A subsystem hazard analysis (SSHA) might be done in place of the PHA, but this is *not* recommended since the SSHA is a more detailed analysis primarily of faults and failures that can create safety hazards. A modified failure mode and effects analysis (FMEA) could be used as a PHA, but this is *not* recommended since the FMEA primarily looks at failure modes only, while the PHA considers many more system aspects.

Use of the PHA technique is highly recommended for every program, regardless of size or cost, to support the goal of identifying and mitigating all system hazards early in the program. The PHA is the starting point for further hazard analysis and safety tasks, is easily performed, and identifies a majority of the system hazards. The PHA is a primary system safety hazard analysis technique for a system safety program.

5.3 HISTORY

The PHA technique was established very early in the history of the system safety discipline. It was formally instituted and promulgated by the developers of MIL-STD-882. It was originally called a gross hazard analysis (GHA) because it was performed at a gross (preliminary) level of detail (see MIL-S-38130).

5.4 THEORY

Figure 5.1 shows an overview of the basic PHA process and summarizes the important relationships involved in the PHA process. The PHA process consists of utilizing both design information and known hazard information to identify and evaluate hazards and to identify SC factors that are relevant to design safety. The PHA evaluates hazards identified by the PHL analysis in further detail.

The purpose of the PHA is to identify hazards, hazard causal factors, hazard mishap risk, and SSRs to mitigate hazards with unacceptable risk during the preliminary design phase of system development. To perform the PHA analysis, the system safety analyst must have three things—design knowledge, hazard knowledge, and the PHL. Design knowledge means the analyst must possess a basic understanding of the system design, including a list of major components. Hazard knowledge means the analyst needs a basic understanding about hazards, hazard sources, hazard components (hazard element, initiating mechanism, and target/threat) and hazards in similar systems. Hazard knowledge is primarily derived from hazard checklists and from lessons learned on the same or similar systems.

The starting point for the PHA is the PHL collection of identified hazards. The PHA evaluates these hazards in more detail. In addition, the analyst compares the design knowledge and information to hazard checklists in order to identify previously unforeseen hazards. This allows the analyst to visualize or postulate possible hazards. For example, if the analyst discovers that the system design will be using jet fuel, he then compares jet fuel to a hazard checklist. From the hazard checklist it will be obvious that jet fuel is a hazardous element, and that a jet fuel fire/explosion is a potential mishap with many different ignition sources presenting many different hazards.

Output from the PHA includes identified and suspected hazards, hazard causal factors, the resulting mishap effect, mishap risk, SCFs, and TLMs. PHA output also includes design methods and SSRs established to eliminate and/or mitigate identified hazards. It is important to identify SCFs because these are the areas that generally affect design safety and that are usually involved in major system hazards.

Since the PHA is initiated very early in the design phase, the data available to the analyst may be incomplete and informal (i.e., preliminary). Therefore, the analysis process should be structured to permit continual revision and updating as the conceptual approach is modified and refined. When the subsystem design details are complete enough to allow the analyst to begin the SSHA in detail, the PHA is generally terminated.

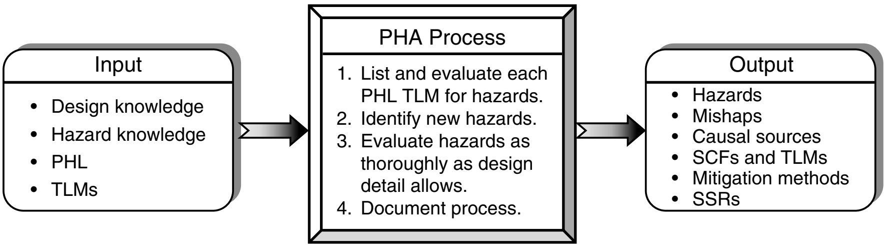


Figure 5.1 *PHA overview.*

5.5 METHODOLOGY

The PHA methodology is shown in Figure 5.2. This process uses design and hazard information to stimulate hazard and causal factor identification. The PHA analysis begins with hazards identified from the PHL. The next step is to once again employ the use of hazard checklists (as done in the PHL analysis) and undesired mishap checklists. The basic inputs for the PHA include the functional flow diagram, the reliability block diagram, indentured equipment list, system design, PHL hazards, hazard checklists, and mishap checklists—the first three of these are derived from the system design by the various system design organizations.

Hazard checklists are generic lists of known hazardous items and potentially hazardous designs, functions, or situations and are fully defined and discussed in Chapter 4. Hazard checklists should not be considered complete or all-inclusive but merely a list of items to help trigger the analyst's recognition of potential hazard sources from past lessons learned. Typical hazard checklists include:

1. Energy sources
2. Hazardous functions
3. Hazardous operations
4. Hazardous components
5. Hazardous materials
6. Lessons learned from similar type systems
7. Undesired mishaps
8. Failure mode and failure state considerations

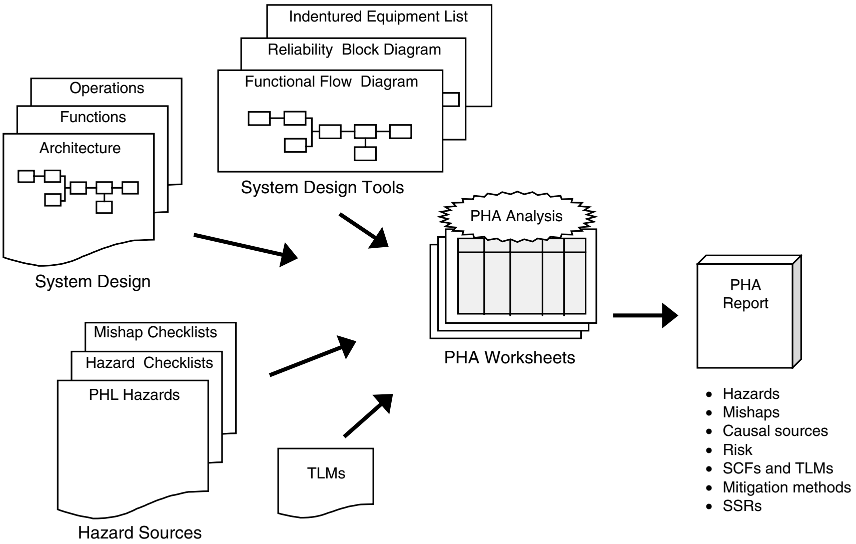


Figure 5.2 *Preliminary hazard analysis methodology.*

Refer to Chapter 4, on PHL analysis, for examples of each of these hazard checklists. Appendix C of this book contains a more complete set of hazard checklists that can be used in a PHA.

Table 5.1 lists and describes the basic steps of the PHA process. This process involves analyzing PHL-identified hazards in more detail and performing a detailed analysis of the system against hazard checklists.

TABLE 5.1 PHA Process

Step	Task	Description
1	Define system.	Define, scope, and bound the system. Define the mission, mission phases, and mission environments. Understand the system design, operation, and major system components.
2	Plan PHA.	Establish PHA definitions, worksheets, schedule, and process. Identify system elements and functions to be analyzed.
3	Establish safety criteria.	Identify applicable design safety criteria, safety precepts/principles, safety guidelines, and safety critical factors.
4	Acquire data.	Acquire all of the necessary design, operational, and process data needed for the analysis (e.g., functional diagrams, drawings, operational concepts, etc.). Acquire hazard checklists, lessons learned, and other hazard data applicable to the system. Acquire all regulatory data and information that are applicable.
5	Conduct PHA.	a. Construct list of equipment, functions, and energy sources for analysis. b. Prepare a worksheet for each identified equipment item, function, and energy source. c. Compare system hardware items with hazard checklists and TLMs. d. Compare system operational functions with hazard checklists and TLMs. e. Compare system energy sources with energy hazard checklists and TLMs. f. Compare system software functions with hazard checklists and TLMs. g. Expand the list of SCFs and TLMs and utilize in the analysis. h. Be cognizant of functional relationships, timing, and concurrent functions when identifying hazards. i. Utilize hazard/mishap lessons learned from other systems.
6	Evaluate risk.	Identify the level of mishap risk presented for each identified hazard, both with and without hazard mitigations in the system design.
7	Recommend corrective action.	Recommend corrective action necessary to eliminate or mitigate identified hazards. Work with the design organization to translate the recommendations into SSRs. Also, identify safety features already in the design or procedures that are present for hazard mitigation.
8	Monitor corrective action.	Review test results to ensure that safety recommendations and SSRs are effective in mitigating hazards as anticipated.
9	Track hazards.	Transfer newly identified hazards into the HTS. Update the HTS as hazards, hazard causal factors, and risk are identified in the PHA.
10	Document PHA.	Document the entire PHA process and PHA worksheets in a PHA report. Include conclusions and recommendations.

When performing a PHA, the following factors should be considered, as a minimum:

1. Hazardous components (e.g., energy sources, fuels, propellants, explosives, pressure systems, etc.)
2. Subsystem interfaces (e.g., signals, voltages, timing, human interaction, hardware, etc.)
3. System compatibility constraints (e.g., material compatibility, electromagnetic interference, transient current, ionizing radiation, etc.)
4. Environmental constraints (e.g., drop, shock, extreme temperatures, noise and health hazards, fire, electrostatic discharge, lightning, X-ray, electromagnetic radiation, laser radiation, etc.)
5. Undesired states (e.g., inadvertent activation, fire/explosive initiation and propagation, failure to safe, etc.)
6. Malfunctions to the system, subsystems, or computing system
7. Software errors (e.g., programming errors, programming omissions, logic errors, etc.)
8. Operating, test, maintenance, and emergency procedures
9. Human error (e.g., operator functions, tasks, requirements, etc.)
10. Crash and survival safety (e.g., egress, rescue, salvage, etc.)
11. Life-cycle support (e.g., demilitarization/disposal, EOD, surveillance, handling, transportation, storage, etc.)
12. Facilities, support equipment, and training
13. Safety equipment and safeguards (e.g., interlocks, system redundancy, fail-safe design considerations, subsystem protection, fire suppression systems, personal protective equipment, warning labels, etc.)
14. Protective clothing, equipment, or devices
15. Training and certification pertaining to safe operation and maintenance of the system
16. System phases (test, manufacture, operations, maintenance, transportation, storage, disposal, etc.)

5.6 WORKSHEET

The PHA is a detailed hazard analysis utilizing structure and rigor. It is desirable to perform the PHA using a specialized worksheet. Although the format of the PHA analysis worksheet is not critical, it is important that, as a minimum, the PHA generate the following information:

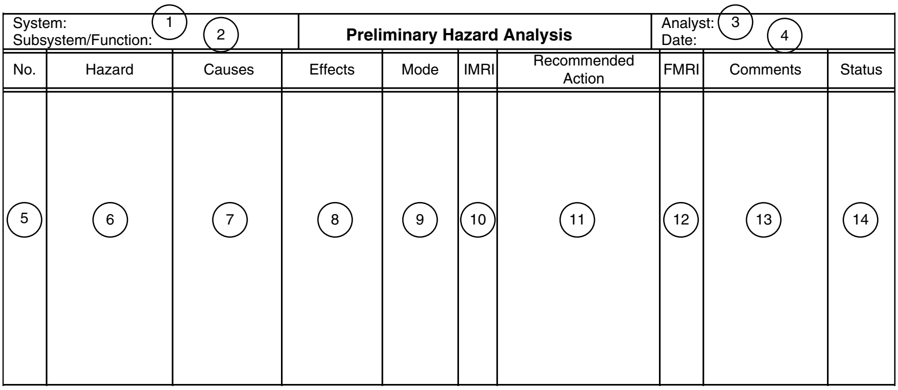
1. System hazards
2. Hazard effects (e.g., actions, outcomes, mishaps)
3. Hazard causal factors (or potential causal factor areas)

4. Mishap risk assessment (before and after design safety features are implemented)
5. SCFs and TLMs
6. Recommendations for eliminating or mitigating the hazards

Figure 5.3 shows the columnar format PHA worksheet recommended for SSP usage. This particular worksheet format has proven to be useful and effective in many applications and it provides all of the information necessary from a PHA.

The following instructions describe the information required under each column entry of the PHA worksheet:

1. *System* This entry identifies the system under analysis.
2. *Subsystem/Function* This entry identifies the subsystem or function under analysis.
3. *Analyst* This entry identifies the name of the PHA analyst.
4. *Date* This entry identifies the date of the analysis.
5. *Hazard Number* This column identifies the number assigned to the identified hazard in the PHA (e.g., PHA-1, PHA-2, etc.). This is for future reference to the particular hazard source and may be used, for example, in the hazard action record (HAR) and the hazard tracking system (HTS).
6. *Hazard* This column identifies the specific hazard being postulated and evaluated. (Remember: Document all hazard considerations, even if they are later proven to be nonhazardous.)
7. *Causes* This column identifies conditions, events, or faults that could cause the hazard to exist and the events that can trigger the hazardous elements to become a mishap or accident.
8. *Effects* This column identifies the effects and consequences of the hazard, should it occur. Generally, the worst-case result is the stated effect. The effect ultimately identifies and describes the potential mishap involved.



System: ① Subsystem/Function: ②			Preliminary Hazard Analysis				Analyst: ③ Date: ④		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭

Figure 5.3 *Recommended PHA worksheet.*

9. *Mode* This entry identifies the system mode(s) of operation, or operational phases, where the identified hazard is of concern.
10. *Initial Mishap Risk Index (IMRI)* This column provides a qualitative measure of mishap risk significance for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values from MIL-STD-882 are shown below.

Severity	Probability
I. Catastrophic	A. Frequent
II. Critical	B. Probable
III. Marginal	C. Occasional
IV. Negligible	D. Remote
	E. Improbable

11. *Recommended Action* This column establishes recommended preventive measures to eliminate or mitigate the identified hazards. Recommendations generally take the form of guideline safety requirements from existing sources or a proposed mitigation method that is eventually translated into a new derived SSR intended to mitigate the hazard. SSRs are generated after coordination with the design and requirements organizations. Hazard mitigation methods should follow the preferred order of precedence established in MIL-STD-882 for invoking or developing safety requirements, which is shown below.

Order of Precedence
1. Eliminate hazard through design selection.
2. Incorporate safety devices.
3. Provide warning devices.
4. Develop procedures and training.

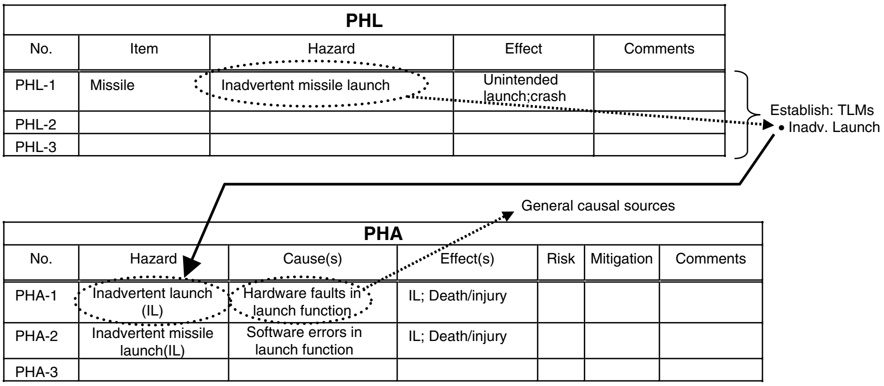
12. *Final Mishap Risk Index (FMRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, given that mitigation techniques and safety requirements are applied to the hazard. The same risk matrix table used to evaluate column 10 is also used here.
13. *Comments* This column provides a place to record useful information regarding the hazard or the analysis process that are not noted elsewhere. This column can be used to record the final SSR number for the developed SSR, which will later be used for traceability.
14. *Status* This column states the current status of the hazard, as being either open or closed.

5.7 GUIDELINES

The following are some basic guidelines that should be followed when completing the PHA worksheet:

1. Remember that the objective of the PHA is to identify system hazards, effects, causal factor areas, and risk. Another by-product of the PHA is the identification of TLMs and SCFs.
2. Start by listing and systematically evaluating system hardware subsystems, system functions, and system energy sources on separate worksheet pages. For each of these categories identify hazards that may cause the TLMs identified from the PHL. Also, utilize hazard checklists to identify new TLMs and hazards.
3. PHL hazards must be converted to TLMs for the PHA. Utilize TLMs along with hazard checklists and lessons learned for hazard recognition to identify hazards.
4. Do not worry about reidentifying the same hazard when evaluating system hardware, system functions, and system energy sources. The idea is to provide thorough coverage in order to identify all hazards.
5. Expand each identified hazard in more detail to identify causal factors, effects, and risk.
6. As causal factors and effects are identified, hazard risk can be determined or estimated.
7. Continue to establish TLMs and SCFs as the PHA progresses and utilize in the analysis.
8. A hazard write-up in the PHA worksheet should be clear and understandable with as much information necessary to understand the hazard.
9. The PHL hazard column does not have to contain all three elements of a hazard: hazardous element (HE), initiating mechanisms (IMs) and outcome (O). The combined columns of the PHA worksheet can contain all three components of a hazard. For example, it is acceptable to place the HE in the hazard section, the IMs in the cause section, and the O in the effect section. The hazard, causes, and effects columns should together completely describe the hazard.
10. Use analysis aids to help recognize and identify new hazards, such as hazard checklists, lesson learned from hazard databases and libraries, mishap investigations, and the like. Also, use applicable hazards from the PHA of other similar systems.
11. After performing the PHA, review the PHL hazards to ensure all have been covered via the TLM process. This is because the PHL hazards were not incorporated one for one.

Figure 5.4 shows how to apply the PHA guidelines when using the PHA worksheet.



PHL				
No.	Item	Hazard	Effect	Comments
PHL-1	Missile	Inadvertent missile launch	Unintended launch;crash	
PHL-2				
PHL-3				

PHA						
No.	Hazard	Cause(s)	Effect(s)	Risk	Mitigation	Comments
PHA-1	Inadvertent launch (IL)	Hardware faults in launch function	IL; Death/injury			
PHA-2	Inadvertent missile launch(IL)	Software errors in launch function	IL; Death/injury			
PHA-3						

Figure 5.4 *PHA guidelines.*

5.8 EXAMPLE: ACE MISSILE SYSTEM

To demonstrate the PHA methodology, the same hypothetical Ace Missile System from Chapter 4 will be used. The basic preliminary design is shown in Figure 5.5, however, note that the conceptual design changed slightly from the concept phase to the preliminary design phase (as happens in many development programs). The design concept has now expanded from a single missile system to multiple missiles in launch tubes. These changes will be reflected in the PHA. The major segments of the system are the missile segment and the weapon control system (WCS) segment.

During preliminary design development, the system design has been modified and improved to include the following:

1. Multiple missiles instead of a single missile.
2. The missiles are now contained in launch tubes.
3. A radio transmitter was added to WCS design for missile destruct subsystem.

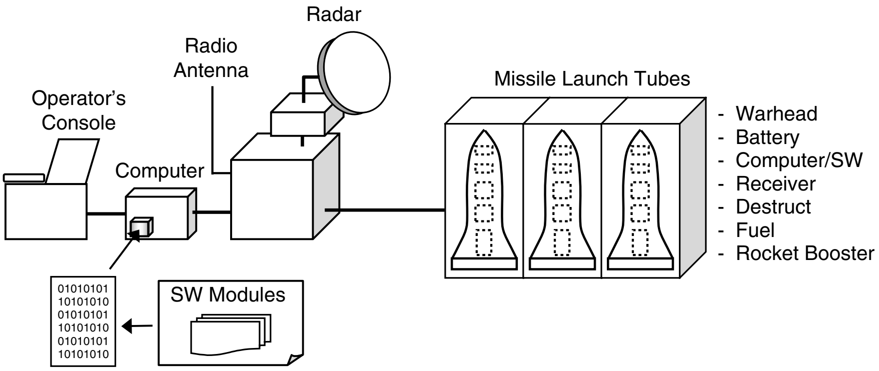


Figure 5.5 *Ace Missile System.*

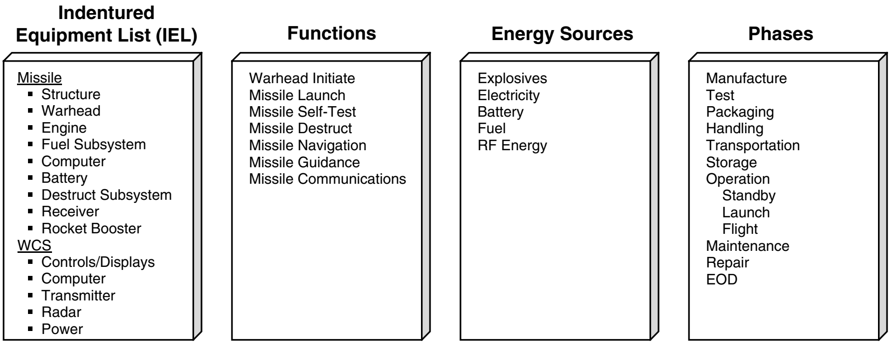


Figure 5.6 *Ace Missile System information.*

Figure 5.6 lists the major system components, functions, phases, and energy sources that should be considered for the PHA. This is the typical level of information available for the PHA.

Figure 5.6 contains a preliminary indentured equipment list (IEL) for this system that will be used for the conduct of the PHA. This is the level of information typically available during preliminary design. As the design development progresses, the IEL will be expanded in breadth and depth for the subsystem hazard analysis (SSHA). The IEL is basically a hierarchy of equipment that establishes relationships, interfaces, and equipment types. A new PHA worksheet page will be started for each IEL item.

Sometimes a more detailed hierarchy is available at the time of the PHA, but usually it is not. The basic ground rule is that the higher level of detail goes into the PHA, and the more detailed breakdown goes into the SSHA. Sometimes the decision is quite obvious, while at other times the decision is somewhat arbitrary. In this example, the computer software would be included in the PHA only as a general category, and it would also be included in the SSHA when the indenture list is continued to a lower level of detail for the software (e.g., module level).

The PHA will analyze the system at the subsystem level because that is the level of design detail available. The SSHA will utilize the PHA hazards and carry the analysis a level lower as more design detail becomes available.

It is also helpful when performing the PHA to utilize functional flow diagrams (FFDs) of the system if they are available. The FFD shows the steps that must take place in order to perform a particular system function. The FFD helps identify

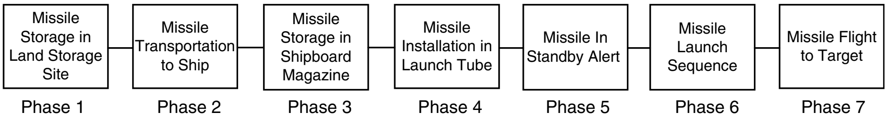

Missile Storage in Land Storage Site
Phase 1
Missile Transportation to Ship
Phase 2
Missile Storage in Shipboard Magazine
Phase 3
Missile Installation in Launch Tube
Phase 4
Missile In Standby Alert
Phase 5
Missile Launch Sequence
Phase 6
Missile Flight to Target
Phase 7

Figure 5.7 *Ace Missile functional flow diagram of operational phases.*

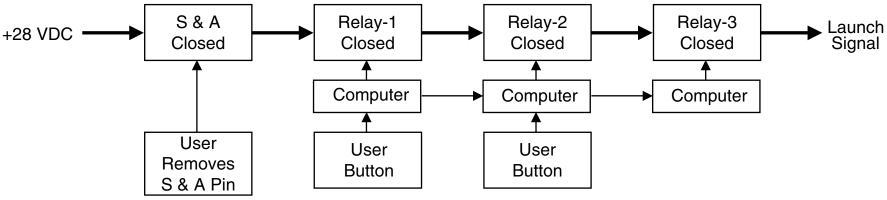


Figure 5.8 *Ace Missile launch signal functional flow diagram.*

subsystem interfaces and relationships that can be used in the analysis. Sometimes it is necessary for the system safety analyst to develop both IELs and FFDs if the project design team has not developed them.

Figure 5.7 is an FFD showing the basic planned operational phases for the missile system. As design development progresses, each of these phases will be expanded in greater detail.

Figure 5.8 is an FFD showing the elements and sequence of events required to generate the missile launch signal.

Figure 5.9 is an FFD showing the elements and sequence of events required to generate the missile launch signal.

The hazards identified by the PHL analysis form the initial set of hazards for the PHA. Since the PHL hazards are generalized, brief, and mixed, it is better to condense the PHL hazards to TLMs and then use the TLMs for the hazard categories that the PHA should be considering for all aspects of the system design and operation. Table 5.2 contains the list of TLMs resulting from the PHL analysis in Chapter 4.

If a new PHA worksheet were started for every IEL item, system function, and system energy source, there would be a minimum of 26 worksheets (14 IEL items + 7 functions + 5 energy sources). In order to not overwhelm the reader, only 6 worksheets are provided (5 IEL items and 1 function). These samples should provide sufficient information on how to perform the PHA. These same examples will be carried into the SSHA. Tables 5.3 through 5.8 contain five example worksheets from the example missile system PHA.

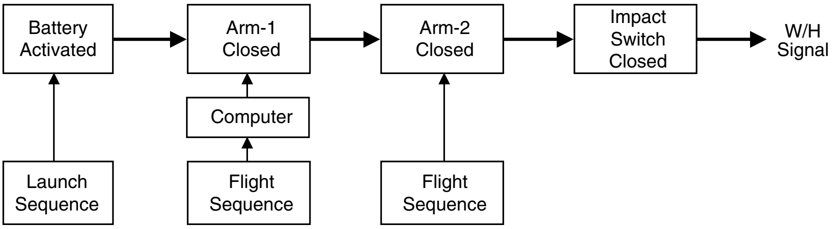


Figure 5.9 *Ace Missile warhead initiate signal functional flow diagram.*

TABLE 5.2 Missile System TLMs from PHL Analysis

TLM No.	Top-Level Mishap
1	Inadvertent W/H explosives initiation
2	Inadvertent launch
3	Inadvertent missile destruct
4	Incorrect target
5	Missile fire
6	Missile destruct fails
7	Personnel injury
8	Unknown missile state
9	Inadvertent explosives detonation

The following should be noted from the PHA of the Ace Missile System:

1. The recommended action is not always in the form of a direct SSR. Additional research may be necessary to convert the recommendation into a meaningful design requirement.
2. As a result of the PHA, TLM 10 was added to the list of TLMs. The new TLM list is shown in Table 5.9.

5.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the PHA technique. The PHA:

1. Is easily and quickly performed.
2. Is comparatively inexpensive yet provides meaningful results.
3. Provides rigor for focusing for the identification and evaluation of hazards.
4. Is a methodical analysis technique.
5. Identifies the majority of system hazards and provides an indication of system risk.
6. Commercial software is available to assist in the PHA process.

While there are no disadvantages in the PHA technique, it is sometimes improperly depended upon as the only hazard analysis technique that is applied.

5.10 COMMON MISTAKES TO AVOID

When first learning how to perform a PHA, it is commonplace to commit some typical errors. The following is a list of common errors made during the conduct of a PHA.

1. Not listing all concerns or credible hazards. It is important to list all possible suspected or credible hazards and not leave any potential concerns out of the analysis.

TABLE 5.3 Ace Missile System PHA—Worksheet 1

System: Ace Missile System Subsystem: ***Missile Structure Subsystem***			**Preliminary Hazard Analysis**				Analyst: Date:		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
PHA-1	Missile structure fails, resulting in unstable missile flight and missile crash	Manufacturing defect; design error	Unstable flight, resulting in crash causing death/injury; incorrect target	Flight	1D	Use 5× safety factor on structure design	1E		Open
PHA-2	Missile body breaks up, resulting in fuel leakage; and ignition source, causing fire	Manufacturing defect; design error	Missile fire, causing death/injury	Ground operations	1D	Use 5× safety factor on structure design	1E		Open
PHA-3	Missile structure fails during handling, resulting in personnel injury	Manufacturing defect; design error; handling equipment failure	Personnel injury	PHS&T[a]	2D	Use 5× safety factor on structure design Establish SSRs for handling equipment	2E		Open
							Page: 1 of 6		

Teaching Notes:

- Focus of this PHA worksheet is on the missile structure subsystem.
- PHA-1 was identified from missile structure contributions to TLM-4 (incorrect target).
- PHA-2 was identified from missile structure contributions to TLM-5 (missile fire).
- PHA-3 was identified from missile structure contributions to TLM-7 (personnel injury).

[a] PHS&T = packaging, handling, storage, and transportation.

TABLE 5.4 Ace Missile System PHA—Worksheet 2

System: Ace Missile System Subsystem: ***Missile Warhead Subsystem***			**Preliminary Hazard Analysis**				Analyst: Date:		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
PHA-4	Inadvertent W/H explosives initiation due to erroneous initiate commands	Erroneous commands from hardware faults; software faults; human error	Personnel death/ injury		1D	Use multiple independent switches in fuze design Conduct FTA of fuze design	1E		Open
PHA-5	Inadvertent W/H explosives initiation due to external environment	Bullet strike, shrapnel, heat	Personnel death/ injury		1D	Use insensitive munitions Provide protective covering when possible	1E		Open
PHA-6	Failure of W/H explosives to initiate when commanded	Hardware faults; software faults	Dud missile; not a safety concern		—		—	Not a safety concern	Closed
							Page: 2 of 6		

Teaching Notes:

- Focus of this PHA worksheet is on the missile warhead subsystem.
- PHA-4 was identified by considering W/H contributions to TLM-1 and failure state hazard checklist.
- PHA-5 was identified by considering W/H contributions to TLM-1 and explosives insensitive munitions considerations.
- PHA-6 was identified by considering failure state hazard checklist as applied to the W/H.

TABLE 5.5 Ace Missile System PHA—Worksheet 3

System: Ace Missile System Subsystem: ***Missile Destruct Subsystem***			**Preliminary Hazard Analysis**				Analyst: Date:		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
PHA-7	Inadvertent missile destruct occurs during flight	Erroneous commands from hardware faults; software faults; human error	Missile debris lands on occupied area resulting in death/injury; incorrect target	Flight	1D	Provide safety interlock inhibiting signal until required	1E		Open
PHA-8	Inadvertent missile destruct occurs during ground operations	Wire short; explosives detonation	Explosion and debris cause personnel death/injury	Standby PHS&T	1D	Ensure high reliability of S&A Isolate critical pins in connector designs	1E		Open
PHA-9	Missile destruct fails to occur when commanded	Command error; radio transmission fault	Missile strikes undesired area resulting in death/injury; incorrect target	Flight	1D	Ensure high reliability of S&A Provide redundant design	1E		Open
							Page: 3 of 6		

Teaching Notes:

- Focus of this PHA worksheet is on the missile destruct subsystem.
- PHA-7 was identified by considering destruct subsystem contributions to TLM-3.
- PHA-8 was identified by considering destruct subsystem contributions to TLM-3.
- PHA-9 was identified by considering failure state hazard checklist as applied to the destruct subsystem.

TABLE 5.6 Ace Missile System PHA—Worksheet 4

System: Ace Missile System Subsystem: ***Missile Rocket Booster Subsystem***			**Preliminary Hazard Analysis**				Analyst: Date:		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
PHA-10	Inadvertent ignition	Erroneous commands from hardware faults; software faults; human error; igniter failure	Inadvertent missile launch resulting in death/injury when missile hits ground	Flight	1D	Provide safety interlock inhibiting signal until required Verify software design	1E		Open
PHA-11	Explosion of rocket propellant	Manufacturing defect; bullet strike; fire	Explosives ignition resulting in personnel death/injury	PHS&T	1D	Provide protective covering Use safe propellant	1E		Open
PHA-12	Failure of rocket booster to start	Failure of commands; igniter failure	Unable to launch missile; not a safety concern	Launch	—		—	Not a safety concern	Closed
PHA-13	Failure of booster in flight	Manufacturing defect; installation error	Unstable flight resulting in crash causing death/injury; incorrect target	Flight	1D	QA of manufacturing and installation	1E		Open
								Page: 4 of 6	

Teaching Notes:

- Focus of this PHA worksheet is on the missile rocket booster subsystem.
- PHA-10 was identified by considering rocket booster contributions to TLM-2.
- PHA-11 was identified by considering rocket booster contributions and energy sources and TLM-9.
- PHA-12 was identified by considering the failure state hazard checklist as applied to the rocket booster.
- PHA-13 was identified by considering the failure state hazard checklist as applied to the rocket booster.

TABLE 5.7 Ace Missile System PHA—Worksheet 5

System: Ace Missile System Subsystem: ***WCS Radar Subsystem***			**Preliminary Hazard Analysis**				Analyst: Date:		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
PHA-14	Electromagnetic radiation (EMR) injures exposed personnel	Personnel in excessive RF energy zone	Personnel injury from RF energy	Ground operations	1D	Establish safe personnel distances and place warning in all procedures	1E		Open
PHA-15	EMR causes ignition of explosives	Fuel in excessive RF energy zone	Explosives ignition resulting in personnel death/injury	Ground operations	1D	Establish safe explosives distances and place warning in all procedures	1E		Open
PHA-16	EMR causes ignition of fuel	Explosives in excessive RF energy zone	Fuel fire resulting in personnel death/injury	Ground operations	1D	Establish safe fuel distances and place warning in all procedures	1E		Open
PHA-17	High-voltage radar electronics causes fire	Overheating of high-voltage radar electronics causes fire	Fire causing system damage and/or death/injury	Ground operations	1D	Provide temperature warning	1E		Open
PHA-18	Personnel injury from high-voltage electronics during maintenance	Personnel touches exposed contacts with high-voltage present	Personnel injury from electrical hazard	Maintenance	2D	Design unit to prevent personnel contact with voltage	2E		Open
							Page: 5 of 6		

Teaching Notes:

- Focus of this PHA worksheet is on the WCS radar subsystem.
- PHA-14 was identified by considering radar contributions to TLM-7 and RF energy source.
- PHA-15 was identified by considering radar and RF energy sources and TLM-9.
- PHA-16 was identified by considering radar contributions to TLM-5 and RF energy source.
- PHA-17 was identified by considering radar contributions to TLM-7 and electrical energy source.
- PHA-18 was identified by considering radar contributions to TLM-7 and electrical energy source.

TABLE 5.8 Ace Missile System PHA—Worksheet 6

System: Ace Missile System Subsystem: ***Warhead Initiate Function***			**Preliminary Hazard Analysis**				Analyst: Date:		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
PHA-19	Warhead initiate function occurs inadvertently	Erroneous commands from hardware faults; software faults; human error	Premature warhead initiation resulting in death/injury	PHS&T Flight	1D	Provide safety interlock inhibiting signal until required	1E		Open
PHA-20	Warhead initiate function fails to occur	Hardware faults; software faults	Warhead fails to initiate when desire; dud warhead	Flight	—		—	Not a safety concern	Closed
PHA-21	Unable to safe warhead after initiate command	Hardware faults; software faults	Warhead explodes when missile strikes ground, resulting in death/injury	Flight	1D	Design for high reliability	1E	Although not in design data, safing function is needed New TLM	Open
								Page: 6 of 6	

Teaching Notes:

- Focus of this PHA worksheet is on the warhead initiate function.
- PHA-19 was identified by considering warhead initiate function to TLM-1.
- PHA-20 was identified by considering warhead initiate function to the failure state hazard checklist.
- PHA-21 was identified by considering warhead Initiate safing function to the failure state hazard checklist.

TABLE 5.9 Expanded List of TLMs from PHA

No.	TLM
1	Inadvertent W/H explosives initiation
2	Inadvertent launch
3	Inadvertent missile destruct
4	Incorrect target
5	Missile fire
6	Missile destruct fails
7	Personnel injury
8	Unknown missile state
9	Inadvertent explosives detonation
10	Unable to safe warhead

2. Failure to document hazards identified but found to be not credible. The PHA is a historical document encompassing all hazard identification areas that were considered.
3. Not utilizing a structured approach of some type. Always use a worksheet and include all equipment, energy sources, functions, and the like.
4. Not collecting and utilizing common hazard source checklists.
5. Not researching similar systems or equipment for mishaps and lessons learned that can be applied.
6. Not establishing a correct list of hardware, functions, and mission phases.
7. Assuming the reader will understand the hazard description from a brief abbreviated statement filled with project-unique terms and acronyms.
8. Inadequately describing the identified hazard (insufficient detail, too much detail, incorrect hazard effect, wrong equipment indenture level, not identifying all three elements of a hazard, etc.).
9. Inadequately describing the causal factors (the identified causal factor does not support the hazard, the causal factor is not detailed enough, not all of the causal factors are identified, etc.).
10. Inadequately describing the hazard mishap risk index (MRI). For example, the MRI is not stated or is incomplete, the hazard severity level does not support actual hazardous effects, the final MRI is a higher risk than the initial MRI, the final severity level in the risk is less than the initial severity level (sometimes possible, but not usually), or the hazard probability is not supported by the causal factors.
11. Providing recommended hazard mitigation methods that do not address the actual causal factor(s).
12. Incorrectly closing the hazard.
13. The PHA is initiated beyond the preliminary design stage or the PHA is continued beyond the preliminary design stage.
14. Not establishing and utilizing a list of TLMs and SCFs.

5.11 SUMMARY

This chapter discussed the PHA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The PHA is an analysis tool for identifying system hazards, causal factors, mishap risk, and safety recommendations for mitigating risk. It is based upon preliminary design information.
2. The primary purpose of the PHA is to identify and mitigate hazards early in the design development process in order to influence the design when the cost impact is minimal.
3. The use of a specialized worksheet provides structure and rigor to the PHA process.
4. The use of a functional flow diagram, reliability block diagram, and an indentured equipment list greatly aids and simplifies the PHA process.
5. Do not exclude any thoughts, ideas, or concerns when postulating hazards. In addition to identifying real hazards, it is also important to show that certain hazards were suspected and considered, even though they were later found to not be possible for various design reasons. This provides evidence that all possibilities were considered.
6. Write a full, credible, and meaningful hazard description that is understandable to the reader and not just to the analyst. Do not assume the reader understands the hazard from a brief abbreviated statement filled with project-unique terms and acronyms.
7. Identify the three elements comprising a hazard using the PHA worksheet columns:
   - *Hazard Column* Hazardous element (source)
   - *Causes Column* Initiating mechanism (mechanism)
   - *Effects Column* Target/threat (outcome)

BIBLIOGRAPHY

Ericson, C. A., Boeing Document D2-113072-1, *System Safety Analytical Technology: Preliminary Hazard Analysis*, 1969.

Layton, D., *System Safety: Including DOD Standards*, Weber Systems, 1989.

Roland, H. E. and B. Moriarty, *System Safety Engineering and Management*, 2nd ed., Wiley, New York, 1990.

Stephans, R. A., *System Safety for the 21st Century*, Wiley, Hoboken, NJ, 2004.

Stephenson, J., *System Safety 2000*, Wiley, New York, 1991.

System Safety Society, *System Safety Analysis Handbook*, System Safety Society.

Vincoli, J. W., *A Basic Guide to System Safety*, Van Nostrand Reinhold, New York, 1993.

Chapter 6

Subsystem Hazard Analysis

6.1 INTRODUCTION

The subsystem hazard analysis (SSHA) technique is a safety analysis tool for identifying hazards, their associated causal factors, effects, level of risk, and mitigating design measures. The SSHA is performed when detailed design information is available as it provides a methodology for analyzing in greater depth the causal factors for hazards previously identified by earlier analyses, such as the preliminary hazard analysis (PHA). The SSHA helps derive detailed system safety requirements (SSRs) for incorporating design safety methods into the system design.

6.2 BACKGROUND

This analysis technique falls under the detailed design hazard analysis type (DD-HAT) because it evaluates design at the detailed subsystem level of design information. The analysis types are described in Chapter 3.

The purpose of the SSHA is to expand upon the analysis of previously identified hazards and to identify new hazards from detailed design information. The SSHA provides for the identification of detailed causal factors of known and newly identified hazards and, in turn, provides for the identification of detailed SSRs for design. The SSHA provides a safety focus from a detailed subsystem viewpoint through analysis of the subsystem structure and components. The SSHA helps verify subsystem compliance with safety requirements contained in subsystem specifications.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

The SSHA is applicable to the analysis of all types of systems and subsystems and is typically performed at the detailed component level of a subsystem. The SSHA is usually performed during detailed design development and helps to guide the detailed design for safety.

The technique provides sufficient thoroughness to identify hazards and detailed hazard causal factors when applied to a given system/subsystem by experienced safety personnel. An understanding of hazard analysis theory, as well as knowledge of system safety concepts, is essential. Experience with and/or a good working knowledge of the particular type of system and subsystem is necessary in order to identify and analyze all hazards. The methodology is uncomplicated and easily learned. Standard SSHA forms and instructions have been developed and are included as part of this chapter.

The SSHA is an in-depth and detailed analysis of hazards previously identified by the PHA. The SSHA also identifies new hazards. It requires detailed design information and a good understanding of the system design and operation.

Use of the SSHA technique is recommended for identification of subsystem-level hazards and further investigation of detailed causal factors of previously identified hazards. A fault hazard analysis (FaHA) or failure mode and effects analysis (FMEA) may be done in place of the SSHA. Using these alternate techniques is *not* recommended. Both the FaHA and FMEA techniques focus on failure modes and can therefore miss or overlook certain hazards.

6.3 HISTORY

The technique was established very early in the history of the system safety discipline. It was formally instituted and promulgated by the developers of MIL-STD-882. It was developed to replace the fault hazard analysis technique, which was previously used for the hazard analysis of subsystems.

6.4 THEORY

The SSHA is performed to evaluate previously identified hazards at the subsystem level, identify new subsystem-level hazards, and determine mishap risk. The SSHA refines the hazard causal factors to the detailed root cause level. Through this refining process the SSHA ensures design SSRs adequately control hazards at the subsystem design level. The SSHA is a robust, rigorous, and structured methodology that consists of utilizing both detailed design information and known hazard information to identify hazards and their detailed causal factors.

Hazards from the PHA are imported into the SSHA, and the causal factors are identified from the detailed component design information. The SSHA can be structured to follow an indentured equipment list (IEL) that has been expanded in detail from the IEL used in the PHA.

Output from the SSHA includes identified and suspected hazards, hazard causal factors, the resulting mishap effect, and safety critical factors. SSHA output also includes

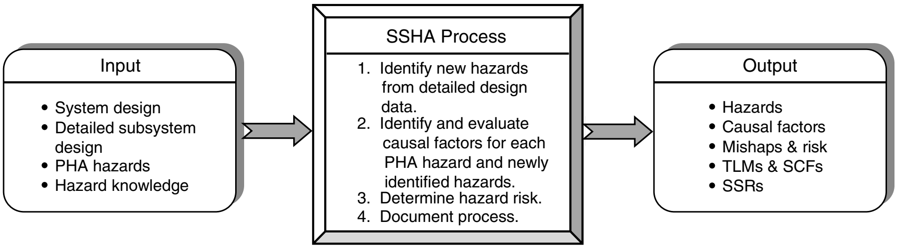

Input
• System design
• Detailed subsystem design
• PHA hazards
• Hazard knowledge
SSHA Process
1. Identify new hazards from detailed design data.
2. Identify and evaluate causal factors for each PHA hazard and newly identified hazards.
3. Determine hazard risk.
4. Document process.
Output
• Hazards
• Causal factors
• Mishaps & risk
• TLMs & SCFs
• SSRs

Figure 6.1 *Subsystem hazard analysis overview.*

design methods and SSRs established to eliminate and/or mitigate identified hazards with unacceptable risk. The SSHA also identifies safety critical functions (SCFs) and top-level mishaps (TLMs) that provide a safety focus during the design process.

Figure 6.1 shows an overview of the SSHA process and summarizes the important relationships involved.

6.5 METHODOLOGY

The SSHA methodology is shown in Figure 6.2. The SSHA process uses different kinds of design information to stimulate hazard identification. The analysis begins

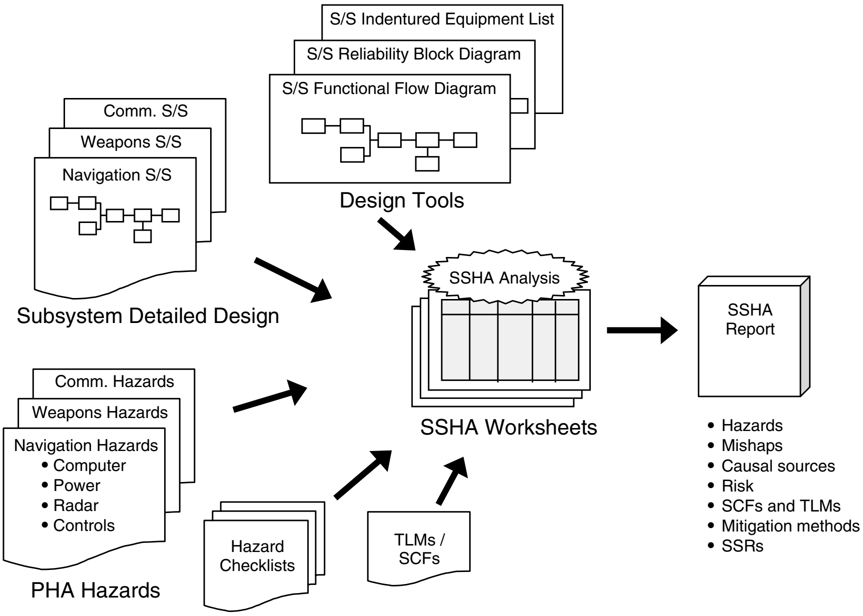


Figure 6.2 *SSHA methodology.*

with hazards identified from the PHA. Hazard checklists (or catalogs) and undesired mishap checklists are employed to help identify new hazards previously unseen. Three of the best tools for aiding the SSHA analyst are the functional flow diagram, the reliability block diagram, and an indentured equipment list, all of which are derived from the system design. Using the detailed design information that is available during the SSHA, hazard causal factors can be evaluated in greater detail.

The functional block diagram simplifies system design and operation for clarity and understanding. It shows the relationships and interfaces between subsystems. It also shows the functions that must be performed by the system. The indentured equipment list identifies all of the specific hardware and software in the system design. By comparing the detailed equipment to known hazard checklists, hazards are easily identified.

Table 6.1 lists and describes the basic steps of the SSHA process. The SSHA process involves performing a detailed analysis of each subsystem in the system under investigation.

As a minimum, when performing the SSHA consideration should be given to:

1. Performance of the subsystem hardware
2. Performance degradation of the subsystem hardware
3. Inadvertent functioning of the subsystem hardware
4. Functional failure of the subsystem hardware
5. Common mode failures
6. Timing errors
7. Design errors or defects
8. Human error and the human system interface design
9. Software errors and the software–machine interface
10. Functional relationships or interfaces between components and equipment comprising each subsystem

6.6 WORKSHEET

It is desirable to perform the SSHA analysis using a worksheet. The worksheet will help to add rigor to the analysis, record the process and data, and help support justification for the identified hazards and safety recommendations. The format of the analysis worksheet is not critical, and typically columnar type worksheets are utilized.

As a minimum, the following basic information should be obtained from the SSHA analysis worksheet:

1. Hazards
2. Hazard effects (mishaps)
3. Detailed hazard causal factors (materials, processes, excessive exposures, failures, etc.)

TABLE 6.1 SSHA Process

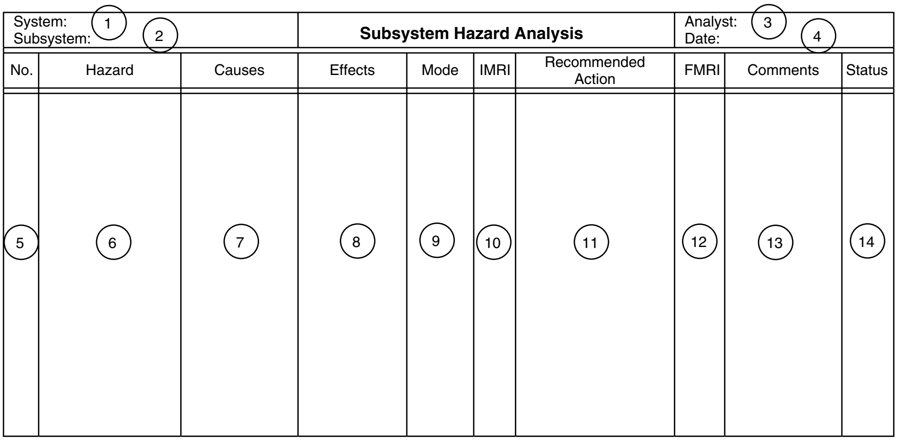
Step	Task	Description
1	Define system.	Define, scope, and bound the operation to be performed. Understand the system design and operation. Understand the detailed subsystem designs.
2	Plan SSHA.	Establish SSHA goals, definitions, worksheets, schedule, and process. Identify the subsystems to be analyzed.
3	Establish safety criteria.	Identify applicable design safety criteria, safety precepts/principles, safety guidelines, and safety critical factors.
4	Acquire data.	Acquire all of the necessary detailed design and operational data needed for the analysis. This includes both schematics, operation manuals, functional flow diagrams, reliability block diagrams, etc. Acquire hazard checklists, lessons learned, and other hazard data applicable to the system.
5	Conduct SSHA.	a. Construct list of discrete subsystem components for SSHA worksheets. b. Begin by populating the SSHA worksheet with the hazards identified in the PHA. c. Evaluate each discrete component in the list and identify hazard causal factors from the subsystem components. d. Utilize TLMs and SCFs to identify new hazards. e. Utilize hazard checklists to identify new hazards. f. Utilize hazard/mishap lessons learned to identify new hazards. g. Be cognizant of functional relationships, timing, and concurrent functions when identifying hazards.
6	Evaluate risk.	Identify the level of mishap risk presented to the system by each identified hazard, both before and after recommended hazard mitigations have been established for the system design.
7	Recommend corrective action.	Recommend corrective action necessary to eliminate or mitigate identified hazards. Work with the design organization to translate the recommendations into SSRs. Also, identify safety features already in the design or procedures that are present for hazard mitigation.
8	Monitor corrective action.	Review test results to ensure that safety recommendations and SSRs are effective in mitigating hazards as anticipated.
9	Track hazards.	Transfer newly identified hazards into the hazard tracking system (HTS). Update hazards in the HTS as causal factors and risk are identified in the SSHA.
10	Document SSHA.	Document the entire SSHA process on the worksheets. Update for new information and closure of assigned corrective actions.

4. Risk assessment (before and after design safety features are implemented)
5. Recommendations for eliminating or mitigating the hazards (which can be converted into derived SSRs).

The recommended SSHA worksheet for SSP usage is the columnar format shown in Figure 6.3. This particular worksheet format has proven to be useful and effective in many applied situations, and it provides all of the information required from an SSHA.

The following instructions describe the information required under each column entry of the SSHA worksheet:

1. *System* This entry identifies the system under analysis.
2. *Subsystem* This entry identifies the subsystem under analysis.
3. *Analyst* This entry identifies the name of the SSHA analyst.
4. *Date* This entry identifies the date of the analysis.
5. *Hazard Number* This column identifies the number assigned to the identified hazard in the SSHA (e.g., SSHA-1, SSHA-2). This is for future reference to the particular hazard source and may be used, for example, in the hazard action record (HAR).
6. *Hazard* This column identifies the specific hazard being postulated. (Remember, document all hazard considerations, even if they are proven to be nonhazardous.) The SSHA is started by transferring all hazards from the PHA into the SSHA for more thorough detailed analysis.
7. *Causes* This column identifies conditions, events, or faults that could cause the hazard to exist and the events that can trigger the hazardous elements to become a mishap or accident. The detailed design information that is



System: 1 Subsystem: 2			Subsystem Hazard Analysis				Analyst: 3 Date: 4		
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
5	6	7	8	9	10	11	12	13	14

Figure 6.3 *Recommended SSHA worksheet.*

available during the SSHA provides for the identification of the specific hazard causal factors.

8. *Effects* This column identifies the effect and consequences of the hazard, assuming it occurs. Generally the worst-case result is the stated effect.
9. *Mode* This entry identifies the system mode(s) of operation, or operational phases, where the identified hazard is of concern.
10. *Initial Mishap Risk Index (IMRI)* This column provides a qualitative measure of mishap risk significance for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values from MIL-STD-882 are shown below.

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

11. *Recommended Action* This column establishes recommended preventive measures to eliminate or mitigate the identified hazards. Recommendations generally take the form of guideline safety requirements from existing sources, or a proposed mitigation method that is eventually translated into a new derived SSR intended to mitigate the hazard. SSRs are generated after coordination with the design and requirements organizations. Hazard mitigation methods should follow the preferred order of precedence established in MIL-STD-882 for invoking or developing safety requirements, which is shown below.

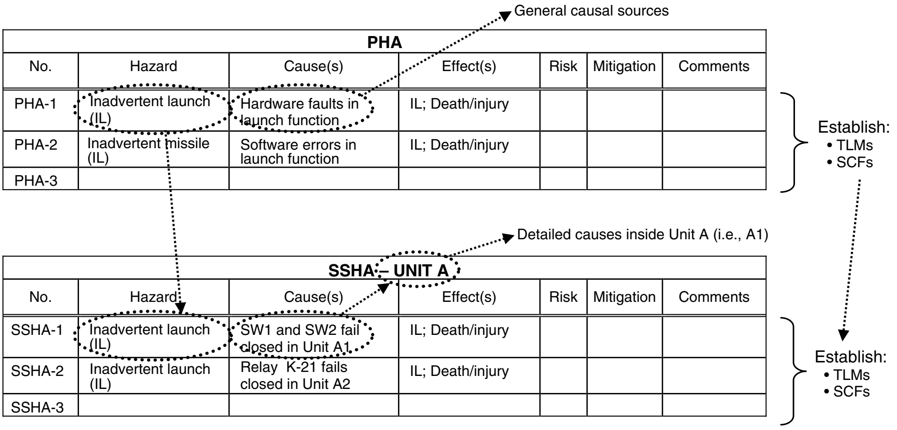
Order of Precedence
1. Eliminate hazard through design selection.
2. Control hazard through design methods.
3. Control hazard through safety devices.
4. Control hazard through warning devices.
5. Control hazard through procedures and training.

12. *Final Mishap Risk Index (FMRI)* This column provides a qualitative measure of mishap risk significance for the potential effect of the identified hazard, given that mitigation techniques and safety requirements are applied to the hazard. The same values used in column 10 are also used here.
13. *Comments* This column provides a place to record useful information regarding the hazard or the analysis process.
14. *Status* This column states the current status of the hazard, as being either open or closed.

6.7 GUIDELINES

The following are some basic guidelines that should be followed when completing the SSHA worksheet:

1. Remember that the objective of the SSHA is to identify detailed subsystem causes of identified hazards, plus previously undiscovered hazards. It refines risk estimates and mitigation methods.
2. Isolate the subsystem and only look within that subsystem for hazards. The effect of an SSHA hazard only goes to the subsystem boundary. The SHA identifies hazards at the SSHA interface and includes interface boundary causal factors.
3. Start the SSHA by populating the SSHA worksheet with hazards identified from the PHA. Evaluate the subsystem components to identify the specific causal factors to these hazards. In effect, the PHA functional hazards and energy source hazards are transferred to the SSHA subsystem responsible for those areas.
4. Identify new hazards and their causal factors by evaluating the subsystem hardware components and software modules. Use analysis aids to help recognize and identify new hazards, such as TLMs, hazard checklists, lesson learned, mishap investigations, and hazards from similar systems.
5. Most hazards will be inherent-type hazards (contact with high voltage, excessive weight, fire, etc.). Some hazards may contribute to system hazards (e.g., inadvertent missile launch), but generally several subsystems will be required for this type of system hazard (thus need for SHA).
6. Consider erroneous input to subsystem as the cause of a subsystem hazard (command fault).
7. The PHA and SSHA hazards establish the TLMs. The TLMs are used in the SHA for hazard identification. Continue to establish TLMs and SCFs as the SSHA progresses and utilize in the analysis.
8. A hazard write-up in the SSHA worksheet should be clear and understandable with as much information necessary to understand the hazard.
9. The SSHA hazard column does not have to contain all three elements of a hazard: hazardous element (HE), initiating mechanisms (IMs), and outcome (O). The combined columns of the SSHA worksheet can contain all three components of a hazard. For example, it is acceptable to place the HE in the hazard section, the IMs in the cause section and the O in the effect section. The hazard, causes, and effects columns should together completely describe the hazard. These columns should provide the three sides of the hazard triangle.
10. The SSHA does not evaluate functions unless the function resides entirely within the subsystem. Functions tend to cross subsystem boundaries and are therefore evaluated in the SHA.



PHA						
No.	Hazard	Cause(s)	Effect(s)	Risk	Mitigation	Comments
PHA-1	Inadvertent launch (IL)	Hardware faults in launch function	IL; Death/injury			
PHA-2	Inadvertent missile (IL)	Software errors in launch function	IL; Death/injury			
PHA-3						

SSHA – UNIT A						
No.	Hazard	Cause(s)	Effect(s)	Risk	Mitigation	Comments
SSHA-1	Inadvertent launch (IL)	SW1 and SW2 fail closed in Unit A1	IL; Death/injury			
SSHA-2	Inadvertent launch (IL)	Relay K-21 fails closed in Unit A2	IL; Death/injury			
SSHA-3						

Figure 6.4 *SSHA guidelines.*

Figure 6.4 shows how to apply the SSHA guidelines when using the SSHA worksheet.

6.8 EXAMPLE: ACE MISSILE SYSTEM

In order to demonstrate the SSHA methodology, the same hypothetical small missile system from Chapters 4 and 5 will be used. The basic system design information provided is shown in Figure 6.5.

Figure 6.6 lists the major system components, functions, phases, and energy sources that should be considered for the SSHA. The major segments of the system are the missile and the weapon control system (WCS).

Figure 6.7 shows the basic planned operational phases for the missile system.

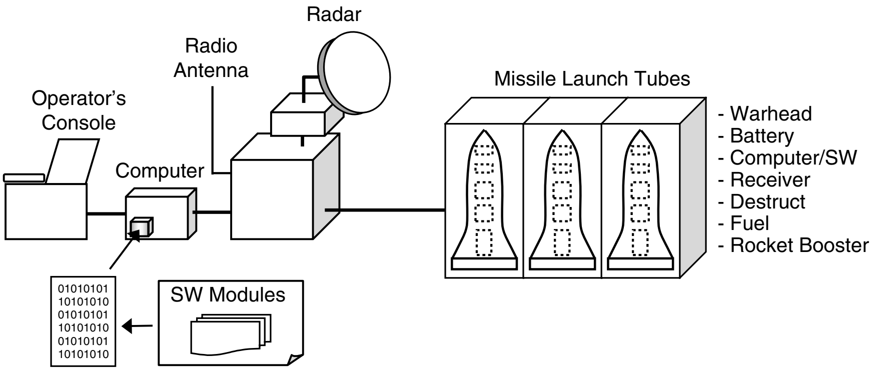


Figure 6.5 *Ace Missile System.*

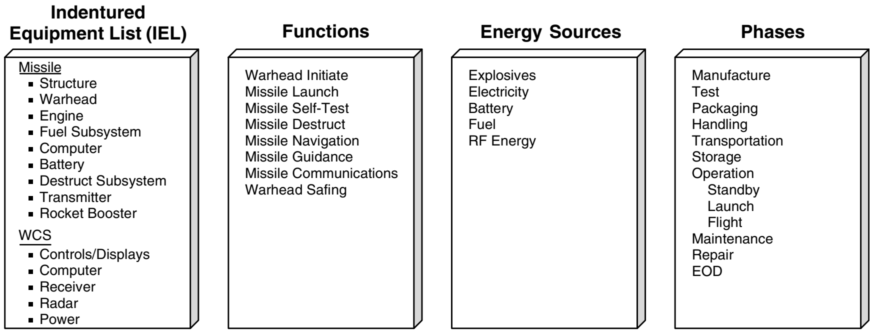


Figure 6.6 *Ace Missile System component list and function list.*

Table 6.2 shows the IEL for the Ace Missile System, which will be used for the SSHA. Note that this IEL has been expanded in detail from the PHA.

The SSHA is initiated when sufficient subsystem detailed design data becomes available. The IEL shown in Table 6.2 shows the information available for the PHA and for the SSHA. The IEL shows all of the system equipment as it is “indentured” by system, subsystem, assembly, unit, and component. It is a hierarchy of equipment that establishes relationships, interfaces, and equipment types.

When establishing which equipment level should go into the PHA and which should go into the SSHA, the basic ground rule is that the higher level of detail goes into the PHA, and the more detailed breakdown goes into the SSHA. Sometimes the decision is quite obvious, while at other times the decision is somewhat arbitrary. In this example, the computer software would be included in the PHA as a general category, and it would also be included in the SSHA when the indenture list is continued to a lower level of detail.

It is also helpful when performing the SSHA to utilize functional flow diagrams (FFDs) of the system if they are available. The FFD shows the steps that must take place in order to perform a particular system function. The FFD helps identify subsystem interfaces and relationships that can be used in the analysis. Sometimes it is necessary for the system safety analyst to develop both IELs and FFDs if none have been developed by the project.

Figure 6.8 is an FFD showing the elements and sequence of events required to generate the missile launch signal.

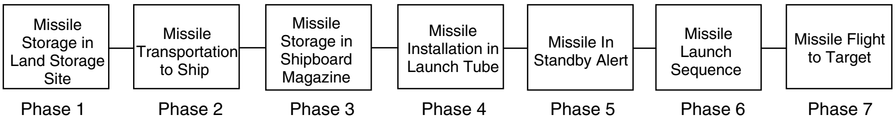

Missile Storage in Land Storage Site
Phase 1
Missile Transportation to Ship
Phase 2
Missile Storage in Shipboard Magazine
Phase 3
Missile Installation in Launch Tube
Phase 4
Missile In Standby Alert
Phase 5
Missile Launch Sequence
Phase 6
Missile Flight to Target
Phase 7

Figure 6.7 *Ace Missile functional flow diagram of operational phases.*

TABLE 6.2 Ace Missile System IEL

No.	Indentured Equipment List	PHA Level	SSHA Level
1.0	Missile Structure Subsystem	X	X
	1.1 Structural Frame		X
	1.2 Skin		X
	1.3 Deployable Fins		X
	1.4 Flight Controls		X
2.0	Missile Warhead Subsystem	X	X
	2.1 Electronics		X
	2.2 Fuze		X
	2.3 Safe and Arm (S&A) Device		X
	2.4 High Explosives		X
3.0	Missile Engine Subsystem	X	X
	3.1 Jet Engine		X
	3.2 Engine Controls		X
4.0	Missile Fuel Subsystem	X	X
	4.1 Fuel Tank		X
	4.2 Fuel		X
5.0	Missile Computer Subsystem	X	X
	5.1 Electronics		X
	5.2 Embedded Software		X
6.0	Missile Battery Subsystem	X	X
	6.1 Battery Structure		X
	6.2 Battery Electrolyte		X
	6.3 Battery Squib		X
7.0	Missile Destruct Subsystem	X	X
	7.1 Safe and Arm (S&A)		X
	7.2 Initiator		X
	7.3 Explosives		X
8.0	Missile Transmitter Subsystem	X	X
	8.1 Electronics Unit		X
	8.2 Power Supply		X
9.0	Missile Rocket Booster Subsystem	X	X
	9.1 Initiator		X
	9.2 Solid Propellant		X
10.0	WCS Controls & Displays Subsystem	X	X
	8.1 Displays		X
	8.2 Controls		X
11.0	WCS Computer Subsystem	X	X
	9.1 Electronics		X
	9.2 Embedded Software		X
12.0	WCS Receiver Subsystem	X	X
	10.1 Electronics Unit		X
	10.2 Power Supply		X
13.0	WCS Radar Subsystem	X	X
	11.1 Electronics		X
	11.2 Wave guides		X
14.0	WCS Power Subsystem	X	X
	12.1 Electrical Power		X
	12.2 Circuit Breakers		X

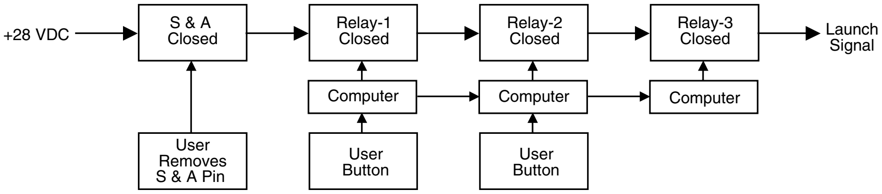


Figure 6.8 Missile launch signal functional flow diagram.

Figure 6.9 is an FFD showing the elements and sequence of events required to generate the missile launch signal.

During detailed design development, the system design has been modified and improved to include the following:

1. Spring-loaded wings have been added to the missile body.
2. The missile wings are normally closed within the missile the body and spring open after launch.
3. As a result of the PHA, a warhead safing function has been added to the system design and the list of functions.

The SSHA does not evaluate functions unless the function resides entirely within the subsystem. Functions tend to cross subsystem boundaries and are, therefore, evaluated in the SHA, which looks for system interface hazards.

The SSHA is started by transferring the PHA hazards to the hazard column of the SSHA. These hazards are then evaluated in detail for subsystem causal factors. Also, with the new detailed design information, additional hazards may be identified. Note that the PHA hazards are repeated for each unit with the subsystem for the SSHA. The causal factors for that unit are then evaluated and applied against the hazard. In some cases the unit cannot possibly contribute to the hazard, while in other cases the detailed unit causes are identified. Demonstration that the unit cannot contribute to a hazard is a beneficial by-product of the SSHA.

Note that the lower level items in the system hierarchy table (i.e., IEL) are addressed by the SSHA, and the higher level information was addressed by the

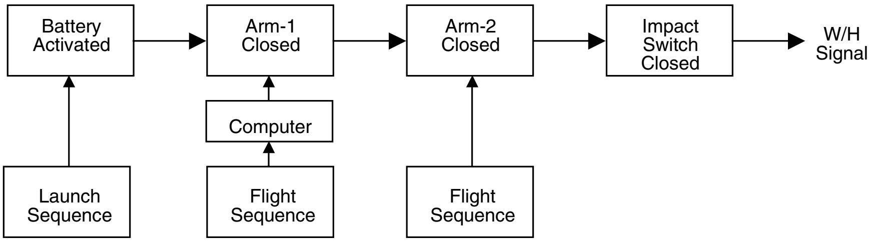


Figure 6.9 Ace Missile warhead initiate signal functional flow diagram.

PHA. If a new SSHA worksheet were started for every IEL item, there would be a minimum of 14 worksheets (14 IEL items). In order to not overwhelm the reader, only 5 worksheets are provided (5 IEL items). These samples should provide sufficient information on how to perform the SSHA. Tables 6.3 through 6.7 contain the SSHA worksheets for the example missile system.

The following should be noted from the SSHA of the Ace Missile System:

1. The recommended action is not always in the form of an SSR. Additional research may be necessary to convert the recommendation into a meaningful design requirement.
2. Each of the PHA hazards has been carried into the SSHA for further analysis and investigation.
3. Three new hazards were identified by the SSHA that were not in the PHA.
4. The original 10 TLMs from the PHA have not changed and still apply.

6.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the SSHA technique. The SSHA:

1. Provides rigor for focusing on hazards and detailed causal factors.
2. Focuses on hazards and not just failure modes as is done in an FMEA.
3. Is cost effective in providing meaningful results.

There are no disadvantages of the SSHA technique.

6.10 COMMON MISTAKES TO AVOID

When first learning how to perform an SSHA, it is commonplace to commit some typical errors. The following is a list of common errors made during the conduct of a SSHA.

1. Not listing all concerns or credible hazards. It is important to list all possible suspected or credible hazards and not leave any potential concerns out of the analysis.
2. Failure to document hazards identified but found to be not credible. The SSHA is a historical document encompassing all hazard identification areas that were considered.
3. Not utilizing a structured approach of some type. Always use a worksheet and include all equipment, energy sources, functions, and the like.
4. Not collecting and utilizing common hazard source checklists.

TABLE 6.3 Ace Missile System SSHA—Worksheet 1

System: Subsystem: ***Missile Structure Subsystem***			**Subsystem Hazard Analysis**			Analyst: Date:			
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
SSHA-1	Missile structure fails, resulting in unstable missile flight and missile crash	Frame collapses or skin tears open from flight stresses	Unstable flight resulting in crash causing death/injury; incorrect target	Flight	1D	Use 5× safety factor on structure design	1E	From PHA-1	Open
SSHA-2	Missile body breaks-up, resulting in fuel leakage; and ignition source causing fire	Missile is dropped; frame collapses from loading stresses	Missile fire causing death/injury	PHS&T	1D	Use 5× safety factor on structure design	1E	From PHA-2	Open
SSHA-3	Missile structure fails during handling resulting in personnel injury	Handling equipment fails; frame collapses from loading stresses	Personnel injury	PHS&T	2D	Use 5× safety factor on structure design	2E	From PHA-3	Open
SSHA-4	Flight controls fail, resulting in errant uncontrolled flight	Hydraulic failure; jam in mechanical flight controls	Unstable flight, resulting in crash causing death/injury; incorrect target	Flight	1D	Design flight controls to prevent jamming	1E	New hazard (not in PHA)	Open
SSHA-5	Fins accidentally deploy during handling	Deploy switch fails; release mechanism fails	Personnel injury	PHS&T	2D	Design fin deploy removal locking pin for PHS&T	2E	New hazard (not in PHA)	Open
							Page: 1 of 5		

Teaching Notes:

- In the SSHA for the missile structure subsystem, the structure components comprising the subsystem will be evaluated—frame, skin, deployable fins, and flight controls.
- The same PHA hazards are analyzed; however, the detailed causal factors are now visible from the component information. In addition, new hazards may become visible.

TABLE 6.4 Ace Missile System SSHA—Worksheet 2

System: Subsystem: ***Missile Warhead Subsystem***			**Subsystem Hazard Analysis**			Analyst: Date:			
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
SSHA-6	Inadvertent W/H explosives initiation due to erroneous initiate commands	Fuze failure; software errors	Personnel death/injury	Flight PHS&T	1D	Conduct FTA of fuze design Use 3 independent switches in fuze design	1E	From PHA-4 (human error in controls subsystem)	Open
SSHA-7	Inadvertent W/H explosives detonation due to external environment	Bullet strike, shrapnel, heat	Personnel death/injury	PHS&T	1D	Use insensitive munitions Provide protective covering when possible	1E	From PHA-5	Open
SSHA-8	Unable to safe warhead after initiate command	Failure in electronics; software error; fuze switches cannot be reversed	Warhead explodes when missile impacts ground, resulting in death/injury	Flight	1D	Use redundancy in design Verify software code Use reversible Fuze switches	1E	From PHA-21	Open
							Page: 2 of 5		

Teaching Notes:

- In the SSHA for the warhead subsystem, the warhead components comprising the subsystem will be evaluated—electronics, fuze, S&A, and high explosives.

TABLE 6.5 Ace Missile System SSHA—Worksheet 3

System: Subsystem: ***Missile Destruct Subsystem***			**Subsystem Hazard Analysis**			Analyst: Date:			
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
SSHA-9	Inadvertent missile destruct occurs during flight	Initiator fails; wire short providing voltage to initiator	Missile debris lands on occupied area resulting in death/injury; incorrect target	Flight	1D	Provide safety interlock inhibiting signal until required	1E	From PHA-7 (command faults from computer)	Open
SSHA-10	Inadvertent missile destruct occurs during ground operations	S&A armed fails and power present; initiator faults; wire short	Explosion and debris cause personnel death/injury	Standby PHS&T	1D	Ensure high reliability of S&A Isolate critical pins in connector designs	1E	From PHA-8	Open
SSHA-11	Missile destruct fails to occur when commanded	S&A pin not removed; S&A fails in safe mode	Missile strikes undesired area resulting in death/injury; incorrect target	Flight	1D	Ensure high reliability of S&A	1E	From PHA-9 (command error; radio transmission fault)	Open
SSHA-12	Inadvertent detonation of high explosives	Bullet strike; shrapnel; heat	Explosion and debris cause personnel death/injury	Ground operations	1D	Use IM explosives	1E	New hazard (not in PHA)	Open
							Page: 3 of 5		

Teaching Notes:

- In the SSHA for the missile destruct subsystem, the destruct components comprising the subsystem will be evaluated—S&A, initiator, and high explosives.
- The same PHA hazards are analyzed; however, the detailed causal factors are now visible from the component information. In addition, new hazards may become visible.

TABLE 6.6 Ace Missile System SSHA—Worksheet 4

System: Subsystem: ***Missile Rocket Booster Subsystem***			**Subsystem Hazard Analysis**			Analyst: Date:			
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
SSHA-13	Inadvertent ignition	Erroneous commands from hardware faults; software faults; human error; igniter failure	Inadvertent missile launch, resulting in death/injury when missile hits ground	Flight	1D	Provide safety interlock inhibiting signal until required Verify software design	1E	From PHA-10	Open
SSHA-14	Explosion of rocket propellant	Manufacturing defect; bullet strike; fire	Explosives ignition, resulting in personnel death/injury	PHS&T	1D	Provide protective covering Use safe propellant	1E	From PHA-11	Open
SSHA-15	Failure of booster in flight	Manufacturing defect; installation error	Unstable flight, resulting in crash causing death/injury; incorrect target	Flight	1D	QA of manufacturing and installation	1E	From PHA-13	Open
							Page: 4 of 5		

Teaching Notes:

- In the SSHA for the missile rocket booster subsystem, the rocket booster components comprising the subsystem will be evaluated—initiator and solid propellant.

TABLE 6.7 Ace Missile System SSHA—Worksheet 5

System: Subsystem: ***WCS Radar Subsystem***			**Subsystem Hazard Analysis**			Analyst: Date:			
No.	Hazard	Causes	Effects	Mode	IMRI	Recommended Action	FMRI	Comments	Status
SSHA-16	Electromagnetic radiation (EMR) injures exposed personnel	Personnel in excessive RF energy zone	Personnel injury from RF energy	Ground operations	1D	Establish safe personnel distances and place warning in all procedures	1E	From PHA-14	Open
SSHA-17	EMR causes ignition of explosives	Fuel in excessive RF energy zone	Explosives ignition resulting in personnel death/injury	Ground operations	1D	Establish safe explosives distances and place warning in all procedures	1E	From PHA-15	Open
SSHA-18	EMR causes ignition of fuel	Explosives in excessive RF energy zone	Fuel fire resulting in personnel death/injury	Ground operations	1D	Establish safe fuel distances and place warning in all procedures	1E	From PHA-16	Open
SSHA-19	High-voltage radar electronics causes fire	Overheating of high-voltage radar electronics causes fire	Fire causing system damage and/or death/injury	Ground operations	1D	Provide temperature warning	1E	From PHA-17	Open
SSHA-20	Personnel injury from high-voltage electronics during maintenance	Personnel touches exposed contacts with high-voltage present	Personnel injury from electrical hazard	Maintenance	2D	Design unit to prevent personnel contact with voltage	2E	From PHA-18	Open
							Page: 5 of 5		

Teaching Notes:

- In the SSHA for the WCS radar subsystem, the radar components comprising the subsystem will be evaluated—electronics, wave guide, electrical power, and mechanical controls.
- The same PHA hazards are analyzed; however, the detailed causal factors are now visible from the component information. In addition, new hazards may become visible.

5. Not researching similar systems or equipment for mishaps and lessons learned that can be applied.
6. Not establishing a correct list of hardware, functions, and mission phases.
7. Assuming the reader will understand the hazard description from a brief abbreviated statement filled with project-unique terms and acronyms.
8. Inadequately describing the identified hazard (insufficient detail, too much detail, incorrect hazard effect, wrong equipment indenture level, not identifying all three elements of a hazard, etc.).
9. Inadequately describing the causal factors (the identified causal factor does not support the hazard, the causal factor is not detailed enough, not all of the causal factors are identified, etc.).
10. Inadequately describing the hazard mishap risk index (MRI). For example, the MRI is not stated or is incomplete, the hazard severity level does not support actual hazardous effects, the final MRI is a higher risk than the initial MRI, the final severity level in the risk is less than the initial severity level (sometimes possible, but not usually), or the hazard probability is not supported by the causal factors.
11. Providing recommended hazard mitigation methods that do not address the actual causal factor(s).
12. Incorrectly closing the hazard.
13. Not establishing and utilizing a list of TLMs and SCFs.

6.11 SUMMARY

This chapter discussed the SSHA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The SSHA is an analysis tool for identifying system hazards, causal factors, mishap risk, and safety recommendations for mitigating risk. It is based upon detailed design information.
2. The primary purpose of the SSHA is to identify and mitigate hazards in the design development process in order to influence the design when the cost impact is minimal.
3. The use of a specialized worksheet provides structure and rigor to the SSHA process.
4. The use of a functional flow diagram, reliability block diagram, and an indentured equipment list greatly aids and simplifies the SSHA process.
5. Do not exclude any thoughts, ideas, or concerns when postulating hazards. In addition to identifying real hazards, it is also important to show that certain hazards were suspected and considered, even though they were later found to not be possible for various design reasons. This provides evidence that all possibilities were considered.

6. Write a full, credible, and meaningful hazard description that is understandable to the reader and not just to the analyst. Do not assume the reader understands the hazard from a brief abbreviated statement filled with project-unique terms and acronyms.
7. Identify the three elements comprising a hazard using the SSHA worksheet columns:
   - *Hazard Column* Hazardous element (source)
   - *Causes Column* Initiating mechanism (mechanism)
   - *Effects Column* Target/threat (outcome)

BIBLIOGRAPHY

Layton, D., *System Safety: Including DOD Standards*, Weber Systems, 1989.

Roland, H. E. and B. Moriarty, *System Safety Engineering and Management*, 2nd ed., Wiley, 1990.

Stephans, R. A., *System Safety for the 21st Century*, Wiley, Hoboken, NJ, 2004.

Stephenson, J., *System Safety 2000*, Wiley, New York, 1991.

System Safety Society, *System Safety Analysis Handbook*, System Safety Society.

Vincoli, J. W., *A Basic Guide to System Safety*, Van Nostrand Reinhold, New York, 1993.

Chapter 7

System Hazard Analysis

7.1 INTRODUCTION

The system hazard analysis (SHA) is an analysis methodology for evaluating risk and safety compliance at the system level, with a focus on interfaces and safety critical functions (SCFs). The SHA ensures that identified hazards are understood at the system level, that all causal factors are identified and mitigated, and that the overall system risk is known and accepted. SHA also provides a mechanism for identifying previously unforeseen interface hazards and evaluating causal factors in greater depth.

The SHA is a detailed study of hazards resulting from system integration. This means evaluating all identified hazards and hazard causal factors across subsystem interfaces. The SHA expands upon the subsystem hazard analysis (SSHA) and may use techniques, such as fault tree analysis (FTA), to assess the impact of certain hazards at the system level. The system-level evaluation should include analysis of all possible causal factors from sources such as design errors, hardware failures, human errors, software errors, and the like.

Overall the SHA:

1. Verifies system compliance with safety requirements contained in the system specifications and other applicable documents.
2. Identifies hazards associated with the subsystem interfaces and system functional faults.
3. Assesses the risk associated with the total system design including software and specifically of the subsystem interfaces.
4. Recommends actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

7.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (SD-HAT). The analysis types are described in Chapter 3. There are no alternate names for this technique, although there are other safety analysis techniques that are sometimes used in place of the SHA, such as FTA.

The SHA assesses the safety of the total system design by evaluating the integrated system. The primary emphasis of the SHA, inclusive of hardware, software, and human systems integration (HSI), is to verify that the product is in compliance with the specified and derived system safety requirements (SSRs) at the system level. This includes compliance with acceptable mishap risk levels. The SHA examines the entire system as a whole by integrating the essential outputs from the SSHAs. Emphasis is placed on the interactions and the interfaces of all the subsystems as they operate together.

The SHA evaluates subsystem interrelationships for the following:

1. Compliance with specified safety design criteria
2. Possible independent, dependent, and simultaneous hazardous events including system failures, failures of safety devices, and system interactions that could create a hazard or result in an increase in mishap risk
3. Degradation in the safety of a subsystem or the total system from normal operation of another subsystem
4. Design changes that affect subsystems
5. Effects of human errors
6. Degradation in the safety of the total system from commercial off-the-shelf (COTS) hardware or software
7. Assurance that SCFs are adequately safe from a total system viewpoint and that all interface and common cause failure (CCF) considerations have been evaluated.

The SHA can be applied to any system; it is applied during and after detailed design to identify and resolve subsystem interface problems. The SHA technique, when applied to a given system by experienced safety personnel, is thorough in evaluating system-level hazards and causal factors and ensuring safe system integration. Success of the SHA is highly dependent on completion of other system safety analyses, such as the preliminary hazard analysis (PHA), SSHA, safety requirements/criteria analysis (SRCA), and operations and support hazard analysis (O&SHA).

A basic understanding of hazard analysis theory is essential as well as knowledge of system safety concepts. Experience with and/or a good working knowledge of the particular type of system and subsystems is necessary in order to identify and analyze all hazards. The SHA methodology is uncomplicated and easily learned. Standard SHA forms and instructions have been developed and are included as part of this chapter.

The overall purpose of the SHA is to ensure safety at the integrated system level. The preferred approach utilizes the SHA worksheet presented in this chapter. Particular interface concerns and/or top-level mishaps (TLMs) may require a separate analysis, such as FTA, to identify all of the unique details and causal factors of the TLMs. High-consequence TLMs may require a common cause failure analysis (CCFA) to ensure that all design redundancy is truly independent and effective.

Use of this technique is recommended for identification of system-level interface hazards. There is no alternative hazard analysis technique for the SHA. Other hazard analysis techniques, such as the FTA or CCFA, may be used to supplement the SHA but are *not* recommended as a replacement for the SHA.

7.3 HISTORY

The SHA technique was established very early in the history of the system safety discipline. It was formally instituted and promulgated by the developers of MIL-STD-882. It was developed to ensure safety at the integrated system level.

7.4 THEORY

The intent of SHA is to ensure complete system-level hazard mitigation and demonstrate safety compliance with system-level safety requirements. Two key concepts involved with an SHA are safety critical function and safety critical function thread.

Figure 7.1 shows an overview of the basic SHA process and summarizes the important relationships involved. The SHA provides a mechanism to identify all hazard causal factors and their mitigation. It also provides the means to evaluate all subsystem interfaces for hazard causal factors.

System design, design criteria, and previously identified hazards are starting considerations in the SHA. Hazard action records (HARs), from the hazard tracking system (HTS), contain the previously identified hazards, causal factors, and actions resulting from the PHA, SSHA, O&SHA, and HHA. Through review of the hazards

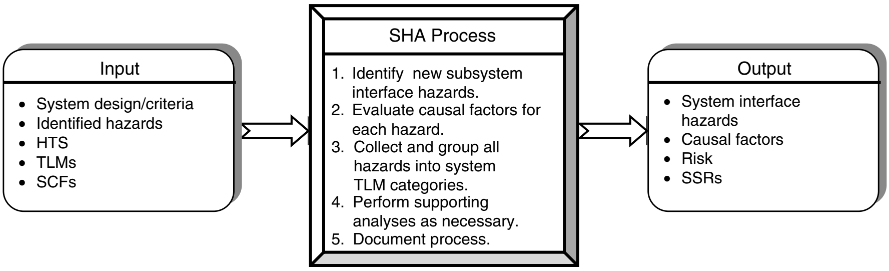

Input
• System design/criteria
• Identified hazards
• HTS
• TLMs
• SCFs
SHA Process
1. Identify new subsystem interface hazards.
2. Evaluate causal factors for each hazard.
3. Collect and group all hazards into system TLM categories.
4. Perform supporting analyses as necessary.
5. Document process.
Output
• System interface hazards
• Causal factors
• Risk
• SSRs

Figure 7.1 *SHA overview.*

with possible interface concerns, the SHA identifies interface-related hazards that were previously undiscovered or interface causal factors to existing hazards.

As part of the SHA, all identified hazards are combined under TLMs. The SHA then evaluates each TLM to determine if all causal factors are identified and adequately mitigated to an acceptable level of system risk. A review of the TLMs in the SHA will indicate if additional in-depth analysis of any sort is necessary, such as for a safety critical hazard or an interface concern.

7.5 METHODOLOGY

The SHA is initiated when detailed design data is available. The SHA is usually initiated when the SSHA is essentially complete and when the O&SHA has been initiated but not necessarily completed. O&SHA information is utilized as it is developed. An overview of the SHA methodology is shown in Figure 7.2.

The SHA process involves reviewing and utilizing the results of previously identified hazards. This review is primarily focused on the evaluation of subsystem interfaces for potential hazards not yet identified. System and subsystem design safety requirements are utilized by the SHA to evaluate system compliance. Subsystem interface information, primarily from the SSHA and interface specifications, is also utilized by the SHA to assist in the identification of interface-related hazards.

The TLMs must be established during the SHA, if not previously done during the PHA or SSHA. This is accomplished by reviewing all identified hazards and their resulting mishap consequences. Design requirement and guideline documents help

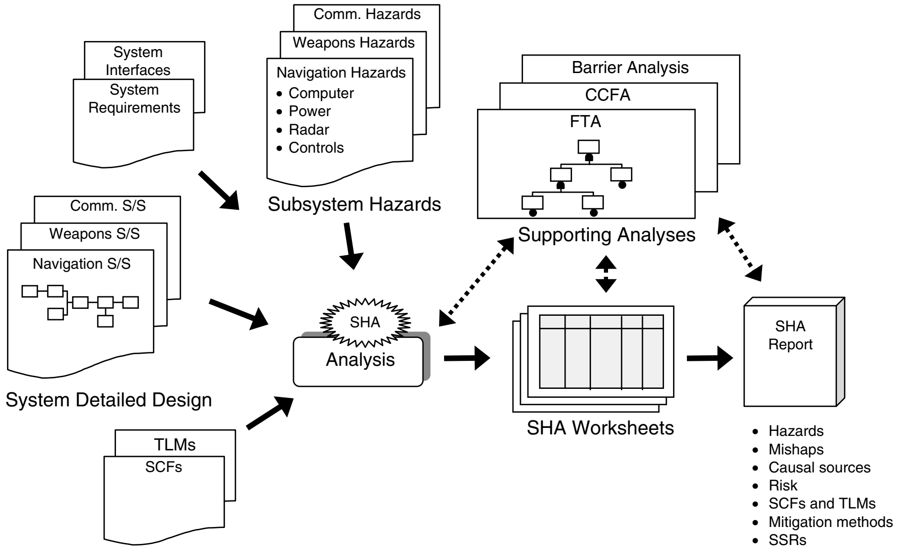


Figure 7.2 *SHA methodology.*

establish TLMs, such as the "inadvertent missile launch" TLM. Table 7.1 lists and describes the basic steps in the SHA process.

Most hazards will have most likely already been identified by the time the PHL, PHA, SSHA, and O&SHA are complete. Since the SHA focuses on interface hazards and causal factors, the SHA sometimes does not result in a large quantity of hazards.

TABLE 7.1 SHA Process

Step	Task	Description
1	Define system.	Define the system, scope, and system boundaries. Define the mission, mission phases, and mission environments. Understand the system design and operation.
2	Plan SHA.	Establish SHA goals, definitions, worksheets, schedule, and process. Identify the subsystems and interfaces to be analyzed. It is very likely that SCFs and TLMs will provide the interfaces of most interest.
3	Establish safety criteria.	Identify applicable design safety criteria, safety precepts/principles, safety guidelines, and safety critical factors.
4	Establish TLMs and SCFs.	If not previously done, establish the TLMs from the identified hazards and the system SCFs.
5	Identify system interface hazards.	a. Identify system SCFs. b. Build SCFs threads identifying the component/function within the thread. c. Evaluate each SCF thread and identify interface-type hazards from the thread component. d. Utilize hazard checklists and mishap lessons learned to identify hazards. e. Conduct supporting analyses, such as FTA, as found necessary during the SHA.
6	Perform supporting analyses.	Certain safety critical (SC) hazards may require a more detailed and/or quantitative analysis, such as an FTA or CCFA. Perform these analyses as found necessary during the SHA.
7	Evaluate risk.	Identify the level of mishap risk presented to the system by each identified hazard, both before and after recommended hazard mitigations have been established for the system design.
8	Recommend corrective action.	Recommend any corrective action as found necessary during the SHA.
9	Monitor corrective action.	Review test results to ensure that safety recommendations and SSRs are effective in mitigating hazards as anticipated.
10	Track hazards.	Transfer newly identified hazards into the HTS. Update the HTS as hazards, hazard causal factors, and risk are identified in the SHA.
11	Document SHA.	Document the entire SHA process on the worksheets. Update for new information and closure of assigned corrective actions.

7.6 WORKSHEET

It is desirable to perform the SHA analysis using a worksheet. The worksheet will help to add rigor to the analysis, record the process and data, and help support justification for the identified hazards and safety recommendations. The format of the analysis worksheet is not critical and typically columnar-type worksheets are utilized.

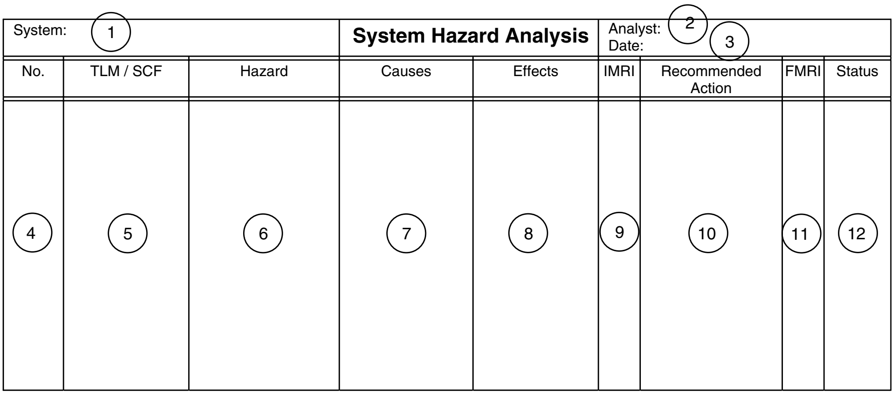
As a minimum, the following basic information should be obtained from the SHA analysis worksheet:

1. Interface or system hazards
2. Hazard causal factors
3. Hazard risk
4. Information to determine if further causal factor analysis is necessary for a particular hazard

The recommended SHA columnar-type worksheet is shown in Figure 7.3.

The following instructions describe the information required under each column entry of the SHA worksheet:

1. *System* This entry identifies the system under analysis.
2. *Analyst* This entry identifies the name of the SHA analyst.
3. *Date* This entry identifies the date of the SHA analysis.
4. *Hazard Number* This column identifies the number assigned to the identified hazard in the SHA (e.g., SHA-1, SHA-2, etc.). This is for future reference to the particular hazard source and may be used, for example, in the hazard action record (HAR) and the hazard tracking system (HTS).



System: 1			System Hazard Analysis		Analyst: 2 Date: 3			
No.	TLM / SCF	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Status
4	5	6	7	8	9	10	11	12

Figure 7.3 *Recommended SHA worksheet.*

5. *TLM/SCF* This column identifies the TLM or the SCF that is being investigated for possible interface hazards.
6. *Hazard* This column identifies the specific hazard being postulated. (Remember to document all hazard considerations even if they are proven to be nonhazardous.)
7. *Causes* This column identifies conditions, events, or faults that could cause the hazard to exist and the events that can trigger the hazardous elements to become a mishap or accident.
8. *Effects* This column identifies the effects and consequences of the hazard, should it occur. Generally the worst-case result is the stated effect.
9. *Initial Mishap Risk Index (IMRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values from MIL-STD-882 as shown below.

Severity	Probability
I. Catastrophic	A. Frequent
II. Critical	B. Probable
III. Marginal	C. Occasional
IV. Negligible	D. Remote
	E. Improbable

10. *Recommended Action* This column establishes recommended preventive measures to eliminate or mitigate the identified hazards. Recommendations generally take the form of guideline safety requirements from existing sources, or a proposed mitigation method that is eventually translated into a new derived SSR intended to mitigate the hazard. SSRs are generated after coordination with the design and requirements organizations. Hazard mitigation methods should follow the preferred order of precedence established in MIL-STD-882 for invoking or developing safety requirements, which are shown below.

Order of Precedence
1. Eliminate hazard through design selection
2. Incorporate safety devices
3. Provide warning devices
4. Develop procedures and training

11. *Recommended Action* This column may also include actions such as further and more detailed analysis using other techniques to determine if and where other mitigation is required.

12. *Final Mishap Risk Index (FMRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, given that mitigation techniques and safety requirements are applied to the hazard. The same risk matrix table used to evaluate column 9 are also used here. The implementation of recommended mitigation measures should be verified and validated prior to accepting final mishap residual risk.
13. *Status* This column states the current status of the hazard, as being either open or closed.

7.7 GUIDELINES

The following are some basic guidelines that should be followed when completing the SHA worksheet:

1. The SHA identifies hazards caused by subsystem interface factors, environmental factors, or common cause factors.
2. The SHA should not be a continuation of subsystem hazards (e.g., personnel contacts high voltage in unit B) because these types of hazards have been adequately treated by the SSHA. Do not place all SSHA hazards into the SHA.
3. Start the SHA by considering TLMs and SCFs for interface hazards. These are the significant safety areas that can provide the sources for identifying system interface hazards.
4. For each SCF determine the hazardous undesired event(s) for that function. For example, the SCF "missile launch function" creates an undesired event of "inadvertent launch," which may consist of several different interface hazards.
5. For each SC function create a SCF thread. This thread consists of the items necessary for safe operation of the SCF.
6. Evaluate and analyze the items in each SCF thread for interface causal factors contributing to the undesired event for the thread.
7. For TLMs that do not directly relate to a SCF, it may be necessary to establish a pseudo-SCF for them. The pseudo-SCF thread than can be evaluated in a similar manner.
8. The SSHA does not evaluate functions unless the function resides entirely within the subsystem. Functions tend to cross subsystem boundaries and are, therefore, evaluated in the SHA.
9. Perform supporting analyses as determined necessary (e.g., FTA, bent pin analysis, CCFA).

The SCFs and TLMs emphasize safety critical areas that should receive special analysis attention. In many instances there is a direct relationship between SCFs and TLMs, as some TLMs are the inverse of an SCF. This is the reason for the SCF/TLM column in the SHA worksheet.

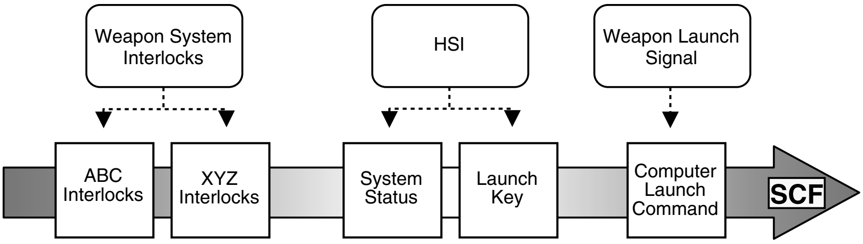


Figure 7.4 *SCF thread with intended results.*

Figure 7.4 depicts an SCF thread for missile launch processing under normal expected conditions.

Figure 7.5 shows how this thread can be used to understand the hazard causal factors within a thread when evaluating the undesired event for that thread.

Figure 7.6 depicts how a SCF thread can be utilized in the SHA.

7.8 EXAMPLE

In order to demonstrate the SHA methodology, the same hypothetical small missile system from Chapters 4 and 5 will be used. The basic system design information provided is shown in Figure 7.7.

Figure 7.8 lists the major system components, functions, phases, and energy sources that should be considered for the SSHA. The major segments of the system are the missile and the weapon control system (WCS).

Figure 7.9 shows the basic planned operational phases for the missile system.

Table 7.2 contains the list of TLMs resulting from previous hazard analyses. These are the TLMs that will be used in the SHA worksheets.

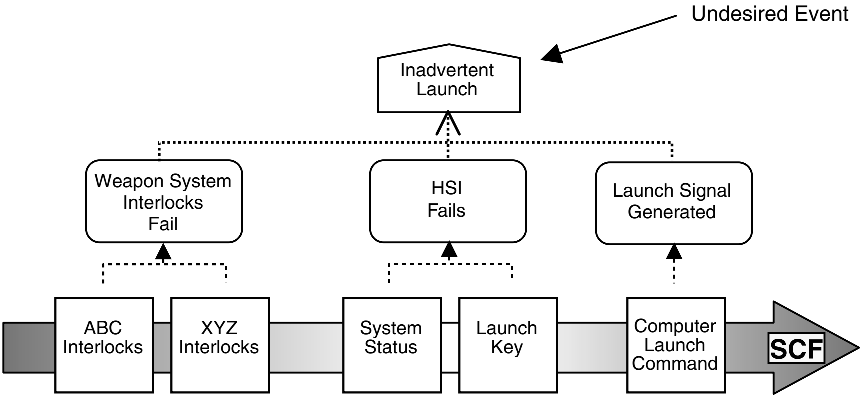
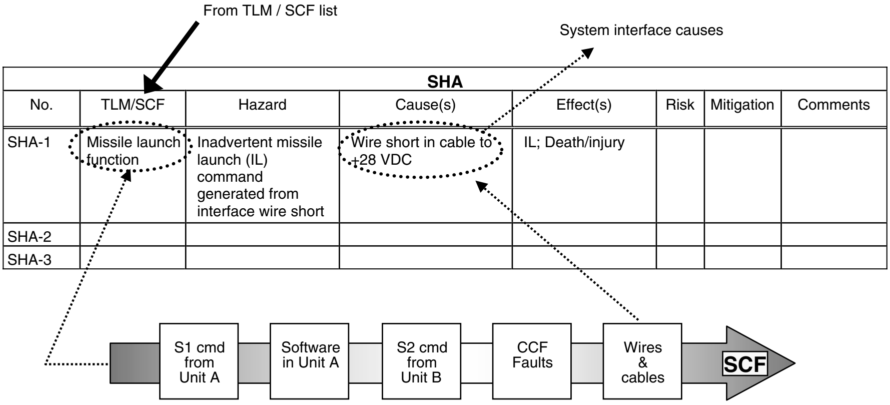


Figure 7.5 *SCF thread with unintended results.*



SHA							
No.	TLM/SCF	Hazard	Cause(s)	Effect(s)	Risk	Mitigation	Comments
SHA-1	Missile launch function	Inadvertent missile launch (IL) command generated from interface wire short	Wire short in cable to +28 VDC	IL; Death/injury			
SHA-2							
SHA-3							

Figure 7.6 *SCF thread used in SHA.*

Tables 7.3 and 7.4 contain the SHA worksheets for the entire Ace missile weapon system.

Since TLM 1 and TLM 2 are safety critical mishaps, it has been recommended in SHA-1 and SHA-2 that an FTA is performed on these TLMs to ensure all causal factors have been identified and that no interface problems or common cause faults have been overlooked.

Figure 7.10 is a functional block diagram (FBD) for the missile warhead initiation function. This FBD shows what tasks and functions must transpire in order for missile initiation to occur.

As part of the SHA, FTAs would be performed on TLM 1 and TLM 2 as recommended in the SHA worksheets. To continue this example, a top-level fault tree (FT) will be constructed for TLM 2, "inadvertent warhead initiation." In

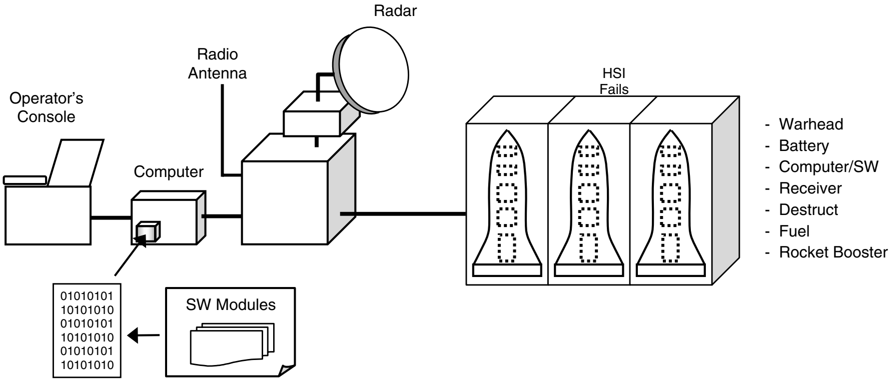


Figure 7.7 *Ace Missile System.*

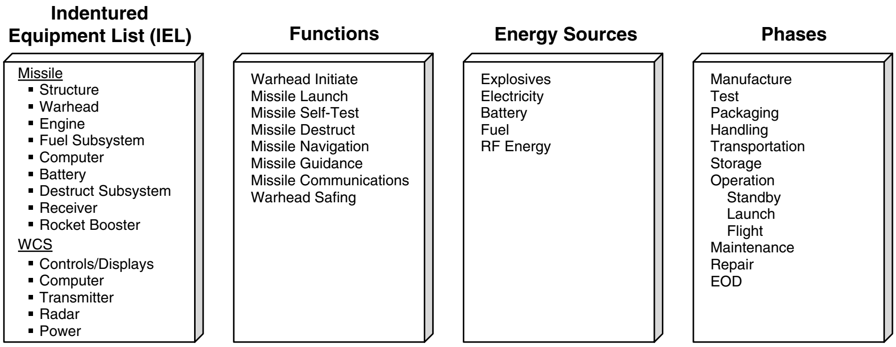


Figure 7.8 *Missile system component list and function list.*

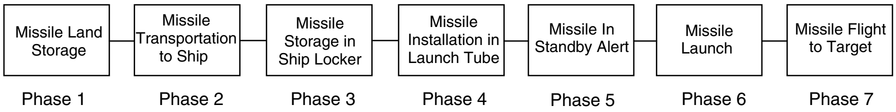


Figure 7.9 *Ace Missile functional flow diagram of operational phases.*

performing the FTA, the safety analyst will use the FBD, detailed schematics, software code, and the like.

Figure 7.11 contains the top-level FTA for TLM 2. The FTA cannot be completed in this example because not enough design information has been provided. The top-level FTA is shown here to demonstrate the SHA process. A completed FTA may uncover common cause failures that bypass the designed-in redundancy. Further, more detailed information on FTA can be found in Chapter 11.

TABLE 7.2 Ace Missile System TLMs

No.	TLM
1	Inadvertent W/H explosives initiation
2	Inadvertent launch
3	Inadvertent missile destruct
4	Incorrect target
5	Missile fire
6	Missile destruct fails
7	Personnel injury
8	Unknown missile state
9	Inadvertent explosives detonation
10	Unable to safe warhead

TABLE 7.3 Missile System SHA—Worksheet

System:			System Hazard Analysis		Analyst: Date:			
Hazard No.	TLM/SCF	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Status
SHA-1	Missile launch function	Inadvertent missile launch signal is generated by a short circuit in missile interface cable	After missile is installed in launch tube the S&A is armed. A short in missile interface cable between WCS and missile provides +28 V to missile launch initiator	Inadvertent launch of missile, resulting in death/injury	1D	Design connector such that missile launch signal pin is isolated from pins with voltage Perform FTA on IL to study in detail	1E	Open
SHA-2	Warhead initiation function	Premature warhead initiation signal is generated by damaged fuze and impact switch due to common cause shock environment	The impact switch and 3 fuze switches are failed closed from missile being dropped. After the missile is launched and warhead power is applied, the initiation signal goes immediately to warhead	Inadvertent warhead initiation, resulting in death/injury	1D	Design to prevent shock sensitivity Do not allow use of dropped missiles Perform FTA on W/H initiation to study in detail	1E	Open
						Page: 1 of 2		

TABLE 7.4 Missile System SHA—Worksheet 2

System:			System Hazard Analysis		Analyst: Date:			
Hazard No.	TLM/SCF	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Status
SHA-3	Missile destruct function	Inadvertent missile destruct signal is generated by erroneous radio link	Radio link with missile is faulty due to weather, and missile computer erroneously interprets radio transmission as requesting a missile destruct	Inadvertent initiation of missile destruct, resulting in death/injury	1D	Design destruct command to be a unique word that cannot easily be created Design such that two different destruct commands must be sent and interpreted by computer	1E	Open
SHA-4	Missile destruct function	Missile destruct fails when commanded by operator due to RF interference or jamming	RF interference or jamming in area prevents correct radio transmission to missile, resulting in loss of destruct command	Inability to destroy errant missile, resulting in death/injury upon impact	1D	Design such that multiple RF channels can be used	1E	Open
						Page: 2 of 2		

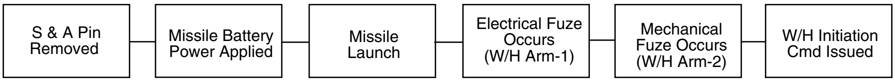

S & A Pin Removed
Missile Battery Power Applied
Missile Launch
Electrical Fuze Occurs (W/H Arm-1)
Mechanical Fuze Occurs (W/H Arm-2)
W/H Initiation Cmd Issued

Figure 7.10 *Functional block diagram (FBD) for missile warhead initiation.*

The following results should be noted from the SHA of the Ace Missile System:

1. All of the identified hazards fall under one of the 10 TLM categories.
2. The recommended action is not always in the form of a direct SSR. Additional research may be necessary to convert the recommendation into a meaningful design requirement.
3. The SHA often recommends further detailed analysis of a particular hazard, TLM, or safety concern. In this case the SHA recommended that FTAs be performed on TLM 1 and TLM 2. When complete, these FTAs should show that these undesired events are within acceptable levels of probability of occurrence and that no critical common cause faults exist. If the FTAs do not show acceptable risk, then new interface hazard causal factors may have been identified, which have not been mitigated.

7.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the SHA technique. The SHA:

1. Identifies system interface-type hazards.
2. Consolidates hazards to ensure that all causal factors are thoroughly investigated and mitigated.
3. Identifies critical system-level hazards that must be evaluated in more detail through the use of other analysis techniques.
4. Provides the basis for making an assessment of overall system risk.

There are no disadvantages of the SHA technique.

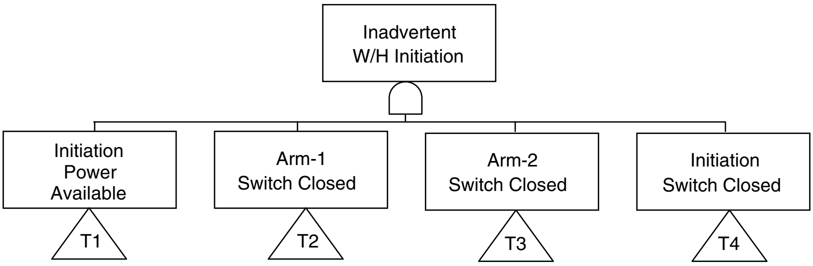


Figure 7.11 *Inadvertent warhead ignition FT.*

7.10 COMMON MISTAKES TO AVOID

When first learning how to perform an SHA, it is commonplace to commit some typical mistakes. The following is a list of errors often encountered during the conduct of an SHA:

1. The causal factors for a hazard are not thoroughly investigated.
2. The mishap risk index (MRI) risk severity level does not appropriately support the identified hazardous effects.
3. Hazards are closed prematurely without complete causal factor analysis and test verification.
4. Failure to consider common cause events and dependent events.
5. A series of FTAs are used in place of the SHA worksheets. The FTA should be a supporting analysis only.

7.11 SUMMARY

This chapter discussed the SHA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of the SHA is to ensure safety of the total system, which involves ensuring that system risk is acceptable. The SHA assesses system compliance with safety requirements and criteria, through traceability of hazards and verification of SSRs.
2. The SHA identifies system hazards overlooked by other analyses, particularly those types of hazards perpetuated through subsystem interface incompatibilities.
3. The SCFs and safety critical TLMs may require more detailed analysis by other techniques (e.g., FTA, CCFA, etc.) to ensure that all causal factors are identified and mitigated.
4. The use of worksheets provides structure and rigor to the SHA process.

BIBLIOGRAPHY

Layton, D., *System Safety: Including DOD Standards*, Weber Systems, 1989.

Roland, H. E. and B. Moriarty, *System Safety Engineering and Management*, 2nd ed., Wiley, 1990.

Stephans, R. A., *System Safety for the 21st Century*, Wiley, Hoboken, NJ, 2004.

Stephenson, J., *System Safety 2000*, Wiley, New York, 1991.

System Safety Society, *System Safety Analysis Handbook*, System Safety Society.

Vincoli, J. W., *A Basic Guide to System Safety*, Van Nostrand Reinhold, New York, 1993.

Chapter 8

Operating and Support Hazard Analysis

8.1 INTRODUCTION

The operating and support hazard analysis (O&SHA) is an analysis technique for identifying hazards in system operational tasks, along with the hazard causal factors, effects, risk, and mitigating methods. The O&SHA is an analysis technique for specifically assessing the safety of operations by integrally evaluating operational procedures, the system design, and the human system integration (HSI) interface.

The scope of the O&SHA includes normal operation, test, installation, maintenance, repair, training, storage, handling, transportation, and emergency/rescue operations. Consideration is given to system design, operational design, hardware failure modes, human error, and task design. Human factors and HSI design considerations are a large factor in system operation and therefore also in the O&SHA. The O&SHA is conducted during system development in order to affect the design for future safe operations.

8.2 BACKGROUND

This analysis technique falls under the operations design hazard analysis type (OD-HAT) because it evaluates procedures and tasks performed by humans. The basic analysis types are described in Chapter 3. An alternate name for this analysis technique is the operating hazard analysis (OHA).

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

The purpose of the O&SHA is to ensure the safety of the system and personnel in the performance of system operation. Operational hazards can be introduced by the system design, procedure design, human error, and/or the environment. The overall O&SHA goal is to:

1. Provide safety focus from an operations and operational task viewpoint.
2. Identify task or operationally oriented hazards caused by design, hardware failures, software errors, human error, timing, and the like.
3. Assess the operations mishap risk.
4. Identify design system safety requirements (SSRs) to mitigate operational task hazards.
5. Ensure all operational procedures are safe.

The O&SHA is conducted during system development and is directed toward developing safe design and procedures to enhance safety during operation and maintenance. The O&SHA identifies the functions and procedures that could be hazardous to personnel or, through personnel errors, could create hazards to equipment, personnel, or both. Corrective action resulting from this analysis is usually in the form of design requirements and procedural inputs to operating, maintenance, and training manuals. Many of the procedural inputs from system safety are in the form of caution and warning notes.

The O&SHA is applicable to the analysis of all types of operations, procedures, tasks, and functions. It can be performed on draft procedural instructions or detailed instruction manuals. The O&SHA is specifically oriented toward the hazard analysis of tasks for system operation, maintenance, repair, test, and troubleshooting.

The O&SHA technique provides sufficient thoroughness in identifying and mitigating operations and support-type hazards when applied to a given system/subsystem by experienced safety personnel. A basic understanding of hazard analysis theory is essential as well as knowledge of system safety concepts. Experience with, or a good working knowledge of, the particular type of system and subsystem is necessary in order to identify and analyze hazards that may exist within procedures and instructions. The methodology is uncomplicated and easily learned. Standard O&SHA forms and instructions have been developed that are included as part of this chapter.

The O&SHA evaluates the system design and operational procedures to identify hazards and to eliminate or mitigate operational task hazards. The O&SHA can also provide insight into design changes that might adversely affect operational tasks and procedures. The O&SHA effort should start early enough during system development to provide inputs to the design and prior to system test and operation. The O&SHA worksheet provides a format for entering the sequence of operations, procedures, tasks, and steps necessary for task accomplishment. The worksheet also provides a format for analyzing this sequence in a structured process that produces a consistent and logically reasoned evaluation of hazards and controls.

Although some system safety programs (SSPs) may attempt to replace the O&SHA with a preliminary hazard analysis (PHA), this is *not* recommended since the PHA is not oriented specifically for the analysis of operational tasks. Use of the O&SHA technique is recommended for identification and mitigation of operational and procedural hazards.

8.3 HISTORY

The O&SHA technique was established very early in the history of the system safety discipline. It was formally instituted and promulgated by the developers of MIL-STD-882. It was developed to ensure the safe operation of an integrated system. It was originally called operating hazard analysis (OHA) but was later expanded in scope and renamed O&SHA to more accurately reflect all operational support activities.

8.4 DEFINITIONS

To facilitate a better understanding of O&SHA, the following definitions of specific terms are provided:

Operation An operation is the performance of procedures to meet an overall objective. For example, a missile maintenance operation may be "replacing missile battery." The objective is to perform all the necessary procedures and tasks to replace the battery.

Procedure A procedure is a set of tasks that must be performed to accomplish an operation. Tasks within a procedure are designed to be followed sequentially to properly and safely accomplish the operation. For example, the above battery replacement operation may be comprised of two primary procedures: (1) battery removal and (2) battery replacement. Each of these procedures contains a specific set of tasks that must be performed.

Task A task is an element of work, which together with other elements of work comprises a procedure. For example, battery removal may consist of a series of sequential elements of work, such as power shutdown, compartment cover removal, removal of electrical terminals, unbolting of battery hold down bolts, and battery removal.

Figure 8.1 portrays these definitions and their interrelationships. It should be noted that tasks might be further broken down into subtasks, sub-subtasks, and so forth.

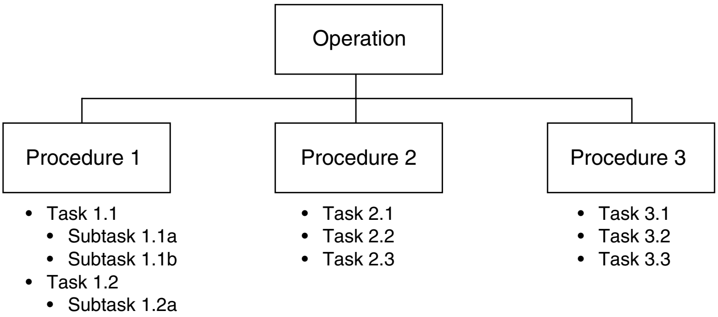


Figure 8.1 *Operation definitions.*

8.5 THEORY

Figure 8.2 shows an overview of the basic O&SHA process and summarizes the important relationships involved. The intent of the O&SHA is to identify and mitigate hazards associated with the operational phases of the system, such as deployment, maintenance, calibration, test, training, and the like. This process consists of utilizing both design information and known hazard information to verify complete safety coverage and control of hazards. Operational task hazards are identified through the meticulous analysis of each detailed procedure that is to be performed during system operation or support.

Input information for the O&SHA consists of all system design and operation information, operation and support manuals, as well as hazards identified by other program hazard analyses. Typically the following types of information are available and utilized in the O&SHA:

1. Hazards and top-level mishaps (TLMs) identified from the preliminary hazard list (PHL), PHA, subsystem hazard analysis (SSHA), system hazard analysis (SHA), and health hazard assessment (HHA)
2. Engineering descriptions of the system, support equipment, and facilities
3. Written procedures and manuals for operational tasks to be performed

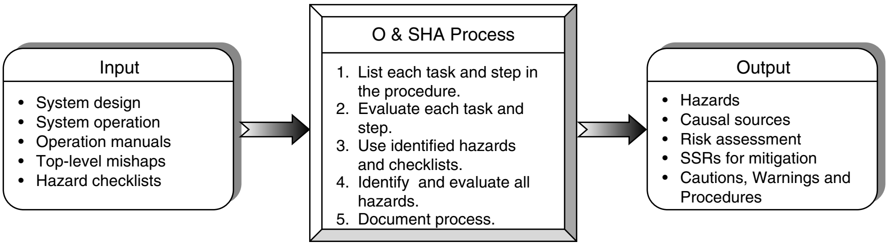


Figure 8.2 *O&SHA overview.*

4. Chemicals, materials, and compounds used in the system production, operation, and support
5. Human factors engineering data and reports
6. Lessons learned, including human error mishaps
7. Hazard checklists

The primary purpose of the O&SHA is to identify and mitigate hazards resulting from the system fabrication, operation, and maintenance. As such, the following information is typically output from the O&SHA:

1. Task hazards
2. Hazard causal factors (materials, processes, excessive exposures, errors, etc.)
3. Risk assessment
4. Safety design requirements to mitigate the hazard
5. The identification of caution and warning notes for procedures and manuals
6. The identification of special HSI design methods to counteract human-error-related hazards

Generally, the O&SHA evaluates manuals and procedural documentation that are in the draft stage. The output of the O&SHA will add cautions and warnings and possibly new procedures to the final documentation.

8.6 METHODOLOGY

The O&SHA process methodology is shown in Figure 8.3. The idea behind this process is that different types of information are used to stimulate hazard identification. The analyst employs hazard checklists, mishap checklists, and system tools. Typical system tools might include functional flow diagrams (FFDs), operational sequence diagrams (OSDs), and indentured task lists (ITLs).

Table 8.1 lists and describes the basic steps of the O&SHA process. The O&SHA process involves performing a detailed analysis of each step or task in the operational procedure under investigation.

The objective of the O&SHA is to identify and mitigate hazards that might occur during the operation and support of the system. The human should be considered an element of the total system, both receiving inputs and initiating outputs during the conduct of this analysis. Hazards may result due to system design, support equipment design, test equipment, human error, HSI, and/or procedure design. O&SHA consideration includes the environment, personnel, procedures, and equipment involved throughout the operation of a system. The O&SHA may be performed on such activities as testing, installation, modification, maintenance, support, transportation, ground servicing, storage, operations, emergency escape, egress, rescue, postaccident responses, and training. The O&SHA also ensures that operation and maintenance manuals properly address safety and health

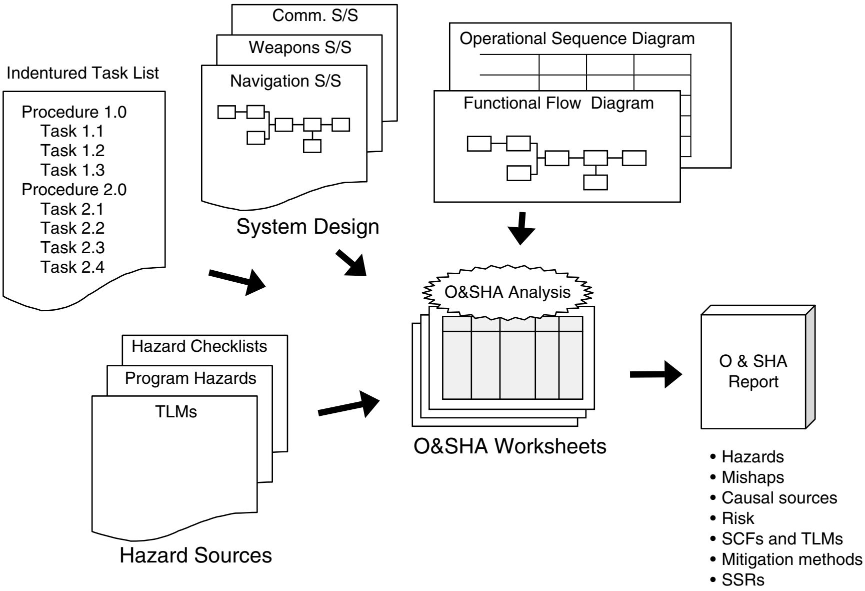


Figure 8.3 *O&SHA methodology.*

requirements. The O&SHA may also evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks.

The O&SHA effort should start early enough to provide inputs to the design and prior to system test and operation. The O&SHA is most effective as a continuing closed-loop iterative process, whereby proposed changes, additions, and formulation of functional activities are evaluated for safety considerations, prior to formal acceptance.

O&SHA considerations should include:

1. Potentially hazardous system states under operator control
2. Operator hazards resulting from system design (hardware aging and wear, distractions, confusion factors, worker overload, operational tempo, exposed hot surfaces, environmental stimuli, etc.)
3. Operator hazards resulting from potential human error
4. Errors in procedures and instructions
5. Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods
6. Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate or control hazards or reduce associated risks
7. Requirements for safety devices and equipment, including personnel safety and life support equipment

TABLE 8.1 O&SHA Process

Step	Task	Description
1	Define system operation.	Define, scope, and bound the operation to be performed. Understand the operation and its objective.
2	Acquire data.	Acquire all of the necessary design and operational data needed for the analysis. These data include both schematics and operation manuals.
3	List procedures and detailed tasks.	Make a detailed list of all procedures and tasks to be considered in the O&SHA. This list can be taken directly from manuals, procedures, or operational plans that are already written or in draft form.
4	Conduct O&SHA.	a. Input task list into the O&SHA worksheets. b. Evaluate each item in the task list and identify hazards for the task. c. Compare procedures and tasks with hazard checklists. d. Compare procedures and tasks with lessons learned. e. Be cognizant of task relationships, timing, and concurrent tasks when identifying hazards.
5	Evaluate risk.	Identify the level of mishap risk presented by the hazard with, and without, mitigations in the system design.
6	Recommend corrective action.	Recommend corrective action necessary to eliminate or mitigate identified hazards. Work with the design organization to translate the recommendations into SSRs. Also, identify safety features already in the design or procedures that are present for hazard mitigation.
7	Ensure caution and warnings are implemented.	Review documented procedures to ensure that corrective action is being implemented. Ensure that all caution and warning notes are inputted in manuals and/or posted on equipment appropriately, as recommended in the O&SHA.
8	Monitor corrective action.	Participate in verification and validation of procedures and review the results to ensure that SSRs effectively mitigate hazards.
9	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS). Update hazards in the HTS as causal factors and risk are identified in the O&SHA.
10	Document O&SHA.	Document the entire O&SHA process on the worksheets. Update for new information and closure of assigned corrective actions.

8. Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render safe, explosive ordnance disposal, back-out, etc.), including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication

9. Requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous materials
10. Requirements for safety training and personnel certification
11. The safety effect of nondevelopmental items (NDI) and commercial off-the-shelf (COTS) items, both in hardware and software, during system operation
12. The safety effect of concurrent tasks and/or procedures

8.7 WORKSHEET

The O&SHA is a detailed hazard analysis utilizing structure and rigor. It is desirable to perform the O&SHA using a specialized worksheet. Although the specific format of the analysis worksheet is not critical, as a minimum, the following basic information is required from the O&SHA:

1. Specific tasks under analysis
2. Identified hazard
3. Effect of hazard
4. Hazard causal factors (varying levels of detail)
5. Recommended mitigating action (design requirement, safety devices, warning devices, special procedures and training, caution and warning notes, etc.)
6. Risk assessment (initial and final)

Figure 8.4 shows the columnar format O&SHA worksheet recommended for SSP usage. This particular worksheet format has proven to be useful and effective in many applications, and it provides all of the information necessary from an O&SHA.

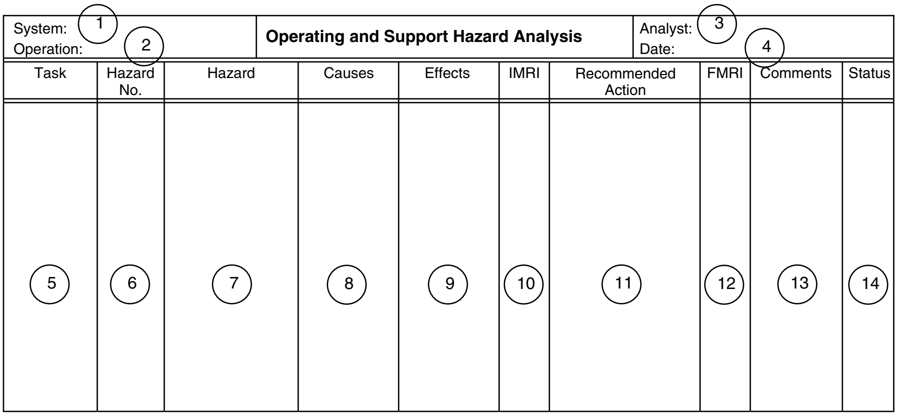


Figure 8.4 Recommended O&SHA worksheet.

The following instructions describe the information required under each column entry of the O&SHA worksheet:

1. *System* This entry identifies the system under analysis.
2. *Operation* This entry identifies the system operation under analysis.
3. *Analyst* This entry identifies the name of the O&SHA analyst.
4. *Date* This entry identifies the date of the O&SHA analysis.
5. *Task* This column identifies the operational task being analyzed. List and describe each of the steps or tasks to be performed. If possible, include the purpose and the mode or phase of operation being performed.
6. *Hazard Number* This is the number assigned to the identified hazard in the O&SHA (e.g., O&SHA-1, O&SHA-2). This is for future reference to the particular hazard source and may be used, for example, in the hazard action record (HAR). The hazard number is at the end of the worksheet because not all tasks listed will have hazards associated with them, and this column could be confusing at the front of the worksheet.
7. *Hazard* This column identifies the specific hazard, or hazards, that could possibly result from the task. (Remember: Document all hazard considerations, even if they are later proven to be nonhazardous.)
8. *Causes* This column identifies conditions, events, or faults that could cause the hazard to exist and the events that can trigger the hazardous elements to become a mishap or accident.
9. *Effects* This column identifies the effect and consequences of the hazard, should it occur. The worst-case result should be the stated effect.
10. *Initial Mishap Risk Index (IMRI)* This column provides a qualitative measure of mishap risk significance for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values from MIL-STD-882 are shown below.

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

11. *Recommended Action* This column establishes recommended preventive measures to eliminate or mitigate the identified hazards. Recommendations generally take the form of guideline safety requirements from existing sources or a proposed mitigation method that is eventually translated into a new derived SSR intended to mitigate the hazard. SSRs are generated after coordination with the design and requirements organizations. Hazard mitigation methods should follow the preferred order of precedence

established in MIL-STD-882 for invoking or developing safety requirements, which are shown below.

Order of Precedence
1. Eliminate hazard through design selection.
2. Control hazard through design methods.
3. Control hazard through safety devices.
4. Control hazard through warning devices.
5. Control hazard through procedures and training.

12. *Final Mishap Risk Index (FMRI)* This column provides a qualitative measure of mishap risk significance for the potential effect of the identified hazard, given that mitigation techniques and safety requirements are applied to the hazard. The same values used in column 10 are also used here.
13. *Comments* This column provides a place to record useful information regarding the hazard or the analysis process that are not noted elsewhere.
14. *Status* This column states the current status of the hazard, as being either open or closed.

Note in this analysis methodology that each and every procedural task is listed and analyzed. For this reason, not every entry in the O&SHA form will constitute a hazard since not every task is hazardous. This process documents that the O&SHA considered all tasks.

8.8 HAZARD CHECKLISTS

Hazard checklists provide a common source for readily recognizing hazards. Since no single checklist is ever really adequate in itself, it becomes necessary to develop and utilize several different checklists. Utilizing several checklists may result in some repetition, but complete coverage of all hazardous elements will be more certain. If a hazard is duplicated, it should be recognized and condensed into one hazard. Remember that a checklist should never be considered a complete and final list but merely a catalyst for stimulating hazard recognition.

Chapter 4 on PHL analysis provided some example general-purpose hazard checklists applicable to system design. Figure 8.5 provides an example hazard checklist applicable to operational tasks. This example checklist is not intended to represent all hazard sources but some typical considerations for an O&SHA.

8.9 SUPPORT TOOLS

The functional flow diagram (or functional block diagram) simplifies system design and operation for clarity and understanding. Use of the FFD for O&SHA evaluation of procedures and tasks is recommended.

1. Work Area
   - Tripping, slipping, corners
   - Illumination
   - Floor load, piling
   - Ventilation
   - Moving objects
   - Exposed surfaces—hot, electric
   - Cramped quarters
   - Emergency exits
2. Materials Handling
   - Heavy, rough, sharp
   - Explosives
   - Flammable
   - Awkward, fragile
3. Clothing
   - Loose, ragged, soiled
   - Necktie, jewelry
   - Shoes, high heels
   - Protective
4. Machines
   - Cutting, punching, forming
   - Rotating shafts
   - Pinch points
   - Flying pieces
   - Projections
   - Protective equipment
5. Tools
   - No tools
   - Incorrect tools
   - Damaged tools
   - Out of tolerance tools
6. Emergency
   - Plans, procedures, numbers
   - Equipment
   - Personnel
   - Training
7. Safety Devices
   - Fails to function
   - Inadequate

Figure 8.5 *Operational hazard checklist.*

Indentured equipment lists were defined in Chapter 1 as a valuable aid in understanding systems and performing hazard analyses. ITLs are also developed to assist in the design and development of operations.

Operational sequence diagrams (OSDs) are a special type of diagram used to define and describe a series of operations and tasks using a graphical format. The OSD plots a flow of information, data, or energy relative to time (actual or sequential) through an operationally defined system using standard symbols to relate actions taken. Actions in the OSD may include inspections, data transmittal/receipt,

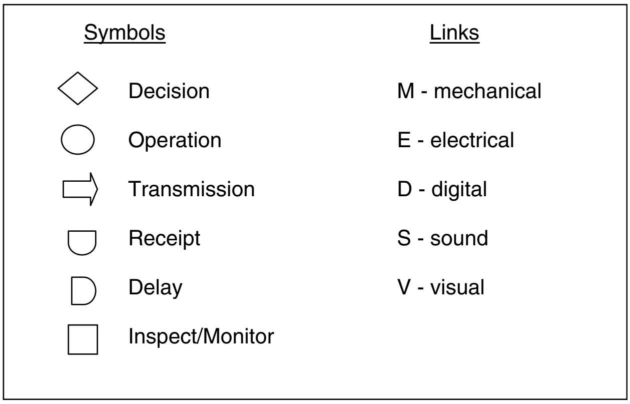


Figure 8.6 *Operational sequence diagram symbols.*

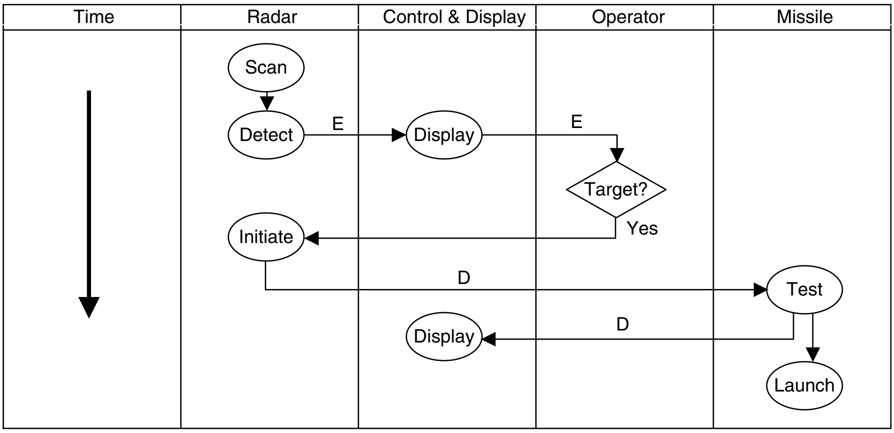


Figure 8.7 *Example operational sequence diagram.*

storage, repair, decision points, and so forth. The OSD helps to display and simplify activities in a highly complex system and identify procedurally related hazards.

Symbols used in the OSD are adapted from the American Society of Mechanical Engineers (ASME) flowchart standards, as shown in Figure 8.6. The OSD methodology was originally defined in MIL-H-46855 [1].

An example OSD is shown in Figure 8.7 for a missile system. Note that the subsystems are denoted along the top, and time is denoted in the left-hand column.

8.10 GUIDELINES

The following are some basic guidelines that should be followed when completing the O&SHA worksheet:

1. Remember that the objective of the O&SHA is to evaluate the system design and operational procedures to identify hazards and to eliminate or mitigate operational task hazards.
2. Start the O&SHA by populating the O&SHA worksheet with the specific tasks under investigation.
3. A hazard write-up in the O&SHA worksheet should be clear and understandable with as much information necessary to understand the hazard.
4. The O&SHA hazard column does not have to contain all three elements of a hazard: hazardous element (HE), initiating mechanisms (IMs), and outcome (O). The combined columns of the SSHA worksheet can contain all three components of a hazard. For example, it is acceptable to place the HE in the hazard section, the IMs in the cause section and the O in the effect section. The hazard, causes, and effects columns should together completely describe

the hazard. These columns should provide the three sides of the hazard triangle (see Chapter 2).

8.11 EXAMPLES

8.11.1 Example 1

To demonstrate the O&SHA methodology, a hypothetical procedure will be analyzed. The selected example procedure is to replace an electrical outlet receptacle in a weapons maintenance facility. The receptacle contains 220 VAC, so the procedure is a hazardous operation. The detailed set of tasks to accomplish this procedure is provided in Table 8.2.

Tables 8.3, 8.4, and 8.5 contain the O&SHA worksheets for this example. The following should be noted from this example analysis:

1. Every procedural task is listed and evaluated on the worksheet.
2. Every task may not have an associated hazard.
3. Even though a task may not have an identified hazard, the task is still documented in the analysis to indicate that it has been reviewed.

8.11.2 Example 2

In order to further demonstrate the O&SHA methodology, the same hypothetical Ace Missile System from Chapters 4, 5, and 6 will be used. The system design is shown again in Figure 8.8.

Figure 8.9 shows the basic planned operational phases for the Ace Missile System. Phase 4 has been selected for O&SHA in this example. The detailed set of tasks to accomplish phase 4 procedure is provided in Table 8.6.

TABLE 8.2 Example Electrical Outlet Replacement Procedure

Step	Description of Task
1.0	Locate circuit breaker
2.0	Open circuit breaker
3.0	Tag circuit breaker
4.0	Remove receptacle wall plate—2 screws
5.0	Remove old receptacle—2 screws
6.0	Unwire old receptacle—disconnect 3 wires
7.0	Wire new receptacle—connect 3 wires
8.0	Install new receptacle—2 screws
9.0	Install old wall plate—2 screws
10.0	Close circuit breaker
11.0	Remove circuit breaker tag
12.0	Test circuit

TABLE 8.3 O&SHA Example 1—Worksheet 1

System: Missile Maintenance Facility Operation: Replace 220V Electrical Outlet			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
1.0 Locate CB. Locate panel and correct circuit breaker (CB) inside panel.	OHA-1	Wrong CB is selected.	Human error	Circuit is not deenergized, live contacts are touched later in procedure resulting in electrocution.	1D	Warning note to test contacts prior to touching wires in task 6.	1E		Open
2.0 Open CB. Manually open the CB handle.	OHA-2	CD is not actually opened.	Internal CB contacts are failed closed; human error	Circuit is not deenergized, live contacts are touched later in procedure resulting in electrocution.	1D	Warning note to test contacts prior to touching wires in task 6.	1E		Open
3.0 Tag CB. Place tag on CB indicating that it's not to be touched during maintenance.	OHA-3	Wrong CB is tagged and untagged CB is erroneously closed.	Another person closes unmarked CB.	Circuit is not deenergized, resulting in electrocution.	1D	Warning note to test contacts prior to touching wires in task 6.	1E		Open
4.0 Remove wall plate. Remove two screws from outlet wall plate; remove wall plate.	—	None							
							Page: 1 of 3		

TABLE 8.4 O&SHA Example 1—Worksheet 2

System: Missile Maintenance Facility Operation: Replace 220V Electrical Outlet			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
5.0 Remove receptacle. Remove two screws from old outlet receptacle; pull receptacle out from wall.	—	None							
6.0 Unwire old receptacle. Disconnect the 3 wires from old receptacle wire mounts.	OHA-4	High voltage (220 VAC) is still on circuit.	CB not opened; wires are energized.	Electrocution	1D	Warning note to test contacts prior to touching	1E		Open
7.0 Wire new receptacle. Connect the 3 wires to the new receptacle wire mounts.	—	Wires are incorrectly connected to wrong wire mounts.	Human error; error in manual	Does not matter since AC current					
8.0 Install receptacle. Install new receptacle into wall and install 2 receptacle screws.	—	None							
							Page: 2 of 3		

TABLE 8.5 O&SHA Example 1—Worksheet 3

System: Missile Maintenance Facility Operation: Replace 220V Electrical Outlet			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
9.0 Install wall plate. Install old wall plate to new receptacle by installing the 2 wall plate screws.	—	None							
10.0 Close CB. Close circuit breaker.	OSHA-5	Arcing/sparking	Wires incorrectly installed and partially touching ground	Personnel injury	2D	Warning note to visually inspect installation Require installation QA check prior to applying power	2E		Open
11.0 Remove tag. Remove CB tag.	—	None							
12.0 Test circuit. Place meter in new receptacle and test voltages.	OSHA-6	Meter settings are incorrect, causing damage to meter	Human error	Damaged test equipment	3D	Warning note in manual regarding potential meter damage	3E		Open
							Page: 3 of 3		

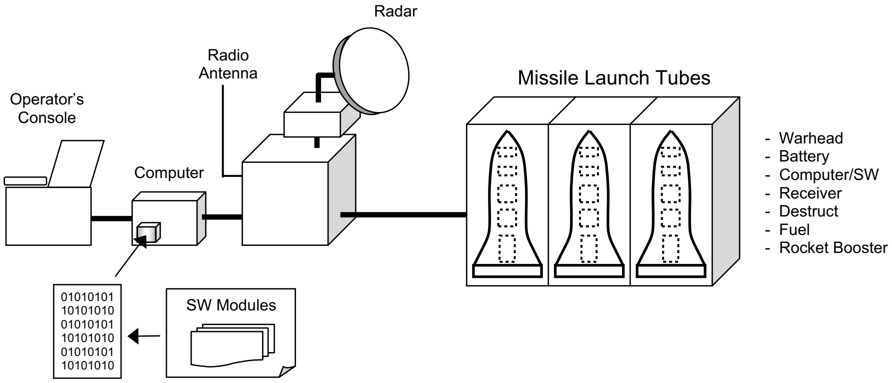


Figure 8.8 *Ace Missile System.*

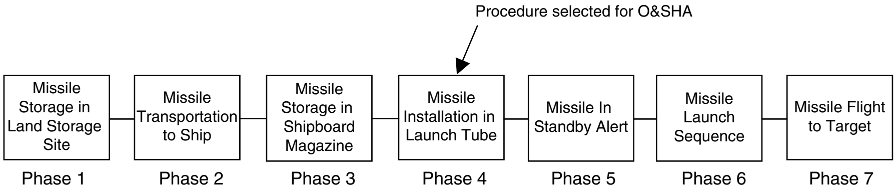

Procedure selected for O&SHA
Missile Storage in Land Storage Site
Missile Transportation to Ship
Missile Storage in Shipboard Magazine
Missile Installation in Launch Tube
Missile In Standby Alert
Missile Launch Sequence
Missile Flight to Target
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
Phase 6
Phase 7

Figure 8.9 *Ace functional flow diagram of missile operational phases.*

It should be noted that in a real-world system the steps in Table 8.3 would likely be more refined and consist of many more discrete and detailed steps. The steps have been kept simple here for purposes of demonstrating the O&SHA technique. Tables 8.7 through 8.10 contain the O&SHA worksheets for the Ace Missile System example.

TABLE 8.6 Missile Installation in Launch Tube Procedure

Step	Description of Task
4.1	Remove missile from ship storage locker.
4.2	Load missile onto handcart transporter.
4.3	Transport missile to launch tube.
4.4	Hoist missile into launch tube.
4.5	Run missile tests.
4.6	Install missile cables.
4.7	Remove S&A pins.
4.8	Place missile in standby alert.

TABLE 8.7 O&SHA Example 2—Worksheet 1

System: Ace Missile System Operation: Missile Installation in Launch Tube			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
Task 4.1: Remove missile from ship magazine.	OHA-1	Missile is dropped resulting in explosion.	Human handling error and significant shock on missile.	Shock causes ignition of W/H explosives.	1D	Require trained and qualified personnel Conduct 40-ft drop test Warning note in manual on explosives hazard	1E		Open
	OHA-2	Missile is dropped resulting in damaged missile.	Human handling error and missile hits sharp surface when dropped.	Missile skin is dented, resulting in unusable missile.	2D	Develop missile handling procedures Ensure adequate missile handling equipment is used Return all dropped missiles to depot, do not use Warning note in manual on missile damage Require trained and qualified personnel	2E		Open
Task 4.2: Load missile onto hand cart transporter.	OHA-3	Missile is dropped, resulting in personnel injury.	Human handling error and missile falls on personnel.	Personnel injury.	2D	Require trained and qualified personnel Warning note in manual on personnel hazard	2E		Open
	OHA-4	Missile is dropped, resulting in damaged missile.	Cart is overloaded causing axle failure resulting in dumping load of missiles.	Missile skin is dented, resulting in several unusable missiles.	2D	Require trained and qualified personnel Warning note in manual to not overload cart	2E		Open
							Page: 1 of 4		

TABLE 8.8 O&SHA Example 2—Worksheet 2

System: Ace Missile System Operation: Missile Installation in Launch Tube			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
Task 4.3: Transport missile to launch tube.	OHA-5	Missile falls off cart, resulting in damaged missile.	Human handling error and missile hits sharp surface when dropped.	Missile skin is dented, resulting in unusable missile.	2D	Develop missile handling procedures Ensure adequate missile handling equipment is used Return all dropped missiles to depot, do not use Warning note in manual on missile damage Require trained and qualified personnel	2E		Open
	OHA-6	Missile falls off cart, resulting in personnel injury.	Human handling error and missile falls on personnel.	Personnel injury.	2D	Require trained and qualified personnel Warning note in manual on personnel hazard	2E		Open
	OHA-7	Missile is struck by bullet or shrapnel, resulting in explosion.	Terrorist or wartime activities.	Initiation of W/H explosives, resulting in death/injury.	1D	Use insensitive munitions (IM)	1E		Open
Task 4.4: Hoist missile into launch tube.	OHA-8	Missile is dropped, resulting in a fuel fire.	Human handling error; hoist failure.	Fuel tank is ruptured with ignition source present, causing fire, resulting in death/injury.	1D	Develop procedures for fire fighting equipment (available and personnel training) Warning note in manual on fire hazard and responses Inspect hoist equipment prior to use Require trained and qualified personnel	1E		Open
							Page: 2 of 4		

TABLE 8.9 O&SHA Example 2—Worksheet 3

System: Ace Missile System Operation: Missile Installation in Launch Tube			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
Task 4.5: Run missile tests.	OHA-9	Missile test causes missile launch.	Test equipment fault; stray voltage on test lines.	Inadvertent missile launch, resulting in personnel injury.	1D	Develop test equipment procedures and inspections Require trained and qualified personnel Caution note to ensure S&A pins are installed	1E		Open
	OHA-10	Missile test causes destruct system initiation.	Test equipment fault; stray voltage on test lines.	Inadvertent missile destruct initiation, resulting in personnel injury.	1D	Develop test equipment procedures and inspections Require trained and qualified personnel Caution note to ensure S&A pins are installed	1E		Open
Task 4.6: Install missile cables.	OHA-11	Cables incorrectly installed, resulting in mismated connectors that cause wrong voltages on missile launch wire.	Human error results in incorrect connector mating that places wrong voltages on critical connector pins.	Inadvertent missile launch, resulting in personnel death/injury.	1D	Require trained and qualified personnel Caution note to ensure S&A pins are installed Design connectors to prevent mismating	1E		Open
							Page: 3 of 4		

TABLE 8.10 O&SHA Example 2—Worksheet 4

System: Ace Missile System Operation: Missile Installation in Launch Tube			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
Task 4.7: Remove S&A pins.	—	Missile launch S&A pin not removed.	Human error	Unable to launch missile; not a safety concern, dud missile.	—		—		
	OHA-12	Missile destruct S&A pin not removed.	Human error	Unable to destruct errant missile, resulting in death/injury.	1D	Require trained and qualified personnel Caution note to ensure S&A pins are removed	1E		Open
Task 4.8: Place missile in standby alert.	OHA-13	Missile is erroneously placed in training mode and system launches against false target.	Human error	Missile strikes erroneous target, resulting in death/injury.	1D	Require trained and qualified personnel Warning note in manual on system mode hazard	1E		Open
							Page: 4 of 4		

The following should be noted from the O&SHA of the Ace Missile System:

1. A total of 12 operational hazards were identified in the procedural steps for the missile installation in launch tube procedure.
2. All of the identified hazards fit within the previously established TLMs (see Chapter 5 on PHA).

8.12 ADVANTAGES AND DISADVANTAGES

The following are advantages of the O&SHA technique. The O&SHA:

1. Provides rigor for focusing on operational and procedural hazards.
2. Is cost effective in providing meaningful safety results.

There are no disadvantages of the O&SHA technique.

8.13 COMMON MISTAKES TO AVOID

The following is a list of common errors made during the conduct of an O&SHA:

1. Some procedural tasks have not been identified, are incomplete, or have been omitted.
2. The hazard description is incomplete, ambiguous, or too detailed.
3. Causal factors are not adequately identified, investigated, or described.
4. The mishap risk index (MRI) is not stated, is incomplete, or is not supported by the hazard information provided.
5. The hazard mitigation does not support the final MRI.

8.14 SUMMARY

This chapter discussed the O&SHA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The O&SHA is an analysis tool for identifying system operational hazards, causal factors, mishap risk, and system safety design requirements for mitigating risk.
2. The primary purpose of the O&SHA is to identify hazardous procedures, design conditions, failure modes, and human error that can lead to the occurrence of an undesired event or hazard during the performance of operational and support tasks.

3. The use of a specialized worksheet provides structure and rigor to the O&SHA process.
4. The use of functional flow diagrams, operational sequence diagrams, and indentured task lists greatly aids and simplifies the O&SHA process.

REFERENCE

1. MIL-H-46855, *Human Engineering Requirements for Military Systems, Equipment and Facilities*,

BIBLIOGRAPHY

Ericson, C. A., Boeing Document D2-113072-4, *System Safety Analytical Technology: Operations and Support Hazard Analysis*, 1971.

Layton, D., *System Safety: Including DOD Standards*, Weber Systems, 1989.

Roland, H. E. and B. Moriarty, *System Safety Engineering and Management*, 2nd ed., Wiley, New York, 1990.

Stephans, R. A., *System Safety for the 21st Century*, Wiley, Hoboken, NJ, 2004.

Stephenson, J., *System Safety 2000*, Wiley, New York, 1991.

System Safety Society, *System Safety Analysis Handbook*, System Safety Society.

Vincoli, J. W., *A Basic Guide to System Safety*, Van Nostrand Reinhold, New York, 1993.

Chapter 9

Health Hazard Assessment

9.1 INTRODUCTION

The health hazard assessment (HHA) is an analysis technique for evaluating the human health aspects of a system's design. These aspects include considerations for ergonomics, noise, vibration, temperature, chemicals, hazardous materials, and so forth. The intent is to identify human health hazards during design and eliminate them through design features. If health hazards cannot be eliminated, then protective measures must be used to reduce the associated risk to an acceptable level. Health hazards must be considered during manufacture, operation, test, maintenance, and disposal.

On the surface, the HHA appears to be very similar in nature to the operating and support hazard analysis (O&SHA), and the question often arises as to whether they both accomplish the same objectives. The O&SHA evaluates operator tasks and activities for the identification of hazards, whereas the HHA focuses strictly on human health issues. There may occasionally be some overlap, but they each serve different interests.

9.2 BACKGROUND

This analysis technique falls under the health design hazard analysis type (HD-HAT). The basic analysis types are described in Chapter 3. The HHA is performed over a period of time, continually being updated and enhanced as more design information becomes available.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

The purpose of the HHA is to:

1. Provide a design safety focus from the human health viewpoint.
2. Identify hazards directly affecting the human operator from a health standpoint.

The intent of the HHA is to identify human health hazards and propose design changes and/or protective measures to reduce the associated risk to an acceptable level. Human health hazards can be the result of exposure to ergonomic stress, chemicals, physical stress, biological agents, hazardous materials, and the like. As previously stated, phases where human operators can be exposed to health hazards occur during manufacture, operation, test, maintenance, and disposal of the system.

The HHA is applicable to analysis of all types of systems, equipment, and facilities that include human operators. The HHA evaluates operator health safety during production, operation, maintenance, and disposal. The HHA technique, when applied to a given system by experienced safety personnel, should provide a thorough and comprehensive identification of the human health hazards that exist in a given system. A basic understanding of hazard analysis theory is essential as well as system safety concepts. Experience with the particular type of system is helpful in generating a complete list of potential hazards. The technique is uncomplicated and easily learned. Standard, easily followed HHA worksheets and instructions are provided in this chapter.

The HHA concentrates on human health hazards during the production, test, and operational phases of the system in order to eliminate or mitigate human health hazards through the system design. The HHA should be completed and system risk known prior to the conduct of any of the production or operational phases. Although some of the hazards identified through the HHA may have already been identified by the preliminary hazard list (PHL), preliminary hazard analysis (PHA), or subsystem hazard analysis (SSHA) techniques, the HHA should not be omitted since it may catch hazards overlooked by these other analyses. Use of this technique by a system safety program (SSP) is highly recommended.

9.3 HISTORY

The HHA technique was established very early in the history of the system safety discipline. It was formally instituted and promulgated by the developers of MIL-STD-882.

9.4 THEORY

The HHA focuses on the identification of potential human health hazards resulting from a system operator's exposure to known human health hazard sources. In

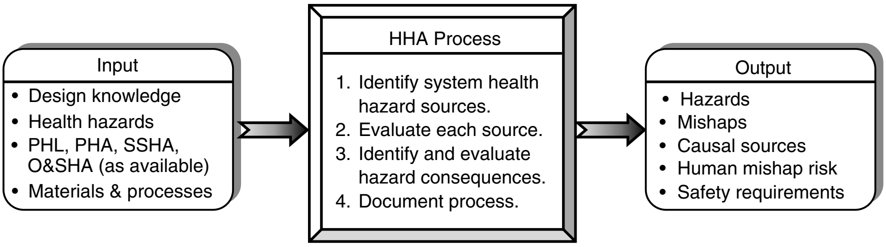


Figure 9.1 *HHA overview.*

general terms, these hazard sources stem from system tasks, processes, environments, chemicals, and materials. Specific health hazards and their impact on the human are assessed during the HHA.

Figure 9.1 shows an overview of the basic HHA process and summarizes the important relationships involved in the HHA process. This process consists of utilizing both design information and known hazard information to identify hazards. Known hazardous elements and mishap lessons learned are compared to the system design to determine if the design concept contains any of these potential hazard elements.

The HHA process involves:

1. Identifying the human hazard sources agents (noise, radiation, heat stress, cold stress, etc.) involved with the system and its logistical support
2. Determining the critical quantities or exposure levels involved, based on the use, quantity, and type of substance/agent used
3. Establishing design mitigation methods to eliminate or reduce exposures to acceptable levels

9.5 METHODOLOGY

Table 9.1 lists and describes the basic steps of the HHA process, which involves performing a detailed analysis of all potentially hazardous human health hazard sources.

The thought process behind the HHA methodology is shown in Figure 9.2. The idea supporting this process is that different kinds of design information are used to facilitate human health hazard identification. The analysis begins with hazards identified from the PHL and PHA, which is the starting point for the HHA. The next step is to once again employ the use of hazard checklists and undesired mishap checklists. Of particular interest are hazard checklists dealing with human health issues. Also, data on human limitations and regulatory requirements are used to identify human health hazards.

TABLE 9.1 HHA Process

Step	Task	Description
1	Acquire design information.	Acquire all of the design, operational, and manufacturing data for the system.
2	Acquire health hazard checklists.	Acquire checklists of known health hazard sources, such as chemicals, materials, processes, etc. Also, acquire checklists of known human limitations in the operation of systems, such as noise, vibration, heat, etc.
3	Acquire regulatory information.	Acquire all regulatory data and information that are applicable to human health hazards.
4	Identify health hazard sources.	Examine the system and identify all potentially hazardous health sources and processes within the system. Include quantity and location when possible. Utilize the checklists.
5	Identify hazards.	Identify and list potential hazards created in the system design resulting from the health hazard sources.
6	Identify safety barriers.	Identify design mitigation methods or barriers in the path of the health hazard source. Also, identify existing design features to eliminate or mitigate the hazard.
7	Evaluate system risk.	Identify the level of mishap risk presented to personnel, both with and without design controls in the system design.
8	Recommend corrective action.	Determine if the design controls present are adequate and, if not, recommend controls that should be added to reduce the mishap risk.
9	Track hazards.	Transfer newly identified hazards into the HTS. Update the HTS as hazards, hazard causal factors, and risk are identified in the HHA.
10	Document HHA.	Document the entire HHA process on the worksheets. Update for new information as necessary.

The HHA is strongly dependent upon the use of health hazard checklists. Hazard checklists are generic lists of known hazardous items and potentially hazardous designs or situations and should not be considered complete or all-inclusive. Checklists are intended as a starting point to help trigger the analyst's recognition of potential hazard sources from past lessons learned.

Typical health hazard checklist categories include:

1. Ergonomics
2. Noise
3. Vibration
4. Temperature
5. Chemicals
6. Biological
7. Hazardous materials
8. Physical stress

When performing the HHA, the following factors should be given consideration:

1. Toxicity, quantity, and physical state of materials
2. Routine or planned uses and releases of hazardous materials or physical agents

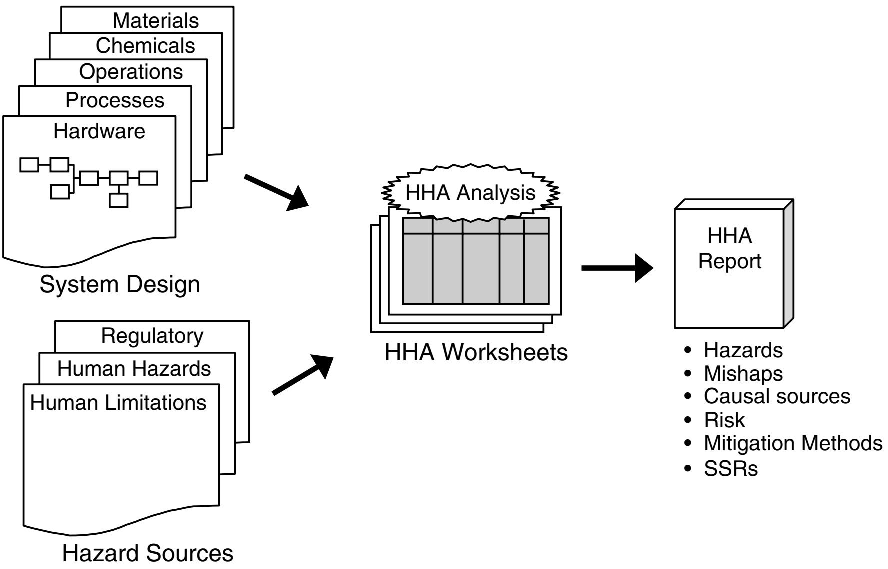


Figure 9.2 *HHA methodology.*

3. Accidental exposure potentials
4. Hazardous waste generated
5. Hazardous material handling, transfer, and transportation requirements
6. Protective clothing/equipment needs
7. Detection and measurement devices required to quantify exposure levels
8. Number of personnel potentially at risk
9. Design controls that could be used, such as isolation, enclosure, ventilation, noise or radiation barriers, and so forth
10. Potential alternative materials to reduce the associated risk to users/operators
11. The degree of personnel exposure to the health hazard
12. System, facility, and personnel protective equipment design requirements (e.g., ventilation, noise attenuation, radiation barriers, etc.) to allow safe operation and maintenance
13. Hazardous material and long-term effects (such as potential for personnel and environmental exposure, handling and disposal issues/requirements, protection/control measures, and life-cycle costs)
14. Means for identifying and tracking information for each hazardous material
15. Environmental factors that effect exposure (wind, temperature, humidity, etc.)

When hazardous materials must be used in the system, the following considerations must be evaluated and documented:

1. Identify hazardous materials data:
   a. Name
   b. Stock number
   c. Affected system components and processes
   d. Quantity, characteristics, and concentrations of the materials in the system
   e. Source documents relating to the materials
2. Determine under which conditions the hazardous materials can pose a health threat.
3. Characterize material hazards and determine reference quantities and hazard ratings (e.g., acute health, chronic health, carcinogenic, contact, flammability, reactivity, and environmental hazards).
4. Estimate the expected usage rate of each hazardous material.
5. Recommend the disposition (disposal, recycle, etc.) of each hazardous material identified.

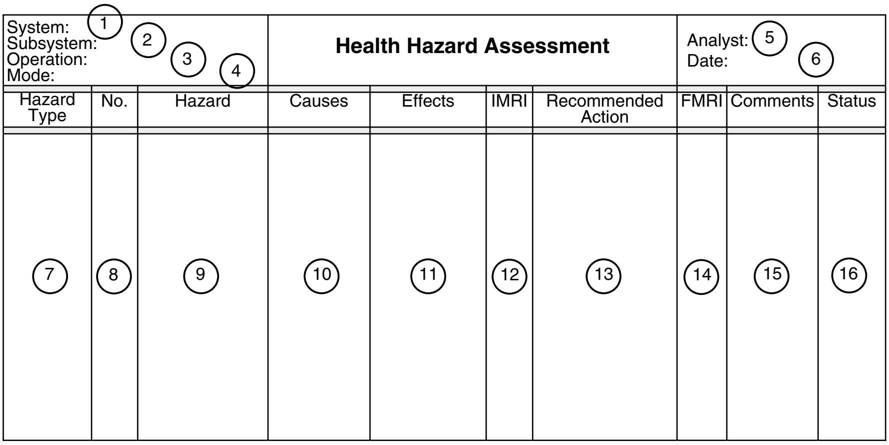
When feasible engineering designs are not available to reduce hazards to acceptable levels, alternative protective measures must be specified (e.g., protective clothing, specific operation, or maintenance practices to reduce risk to an acceptable level). Identify potential nonhazardous or less hazardous alternatives to hazardous materials if they exist or provide a justification why an alternative cannot be used.

9.6 WORKSHEET

The HHA is a detailed hazard analysis utilizing structure and rigor. It is desirable to perform the HHA using a specialized worksheet. Although the format of the analysis worksheet is not critical, typically, matrix or columnar-type worksheets are used to help maintain focus and structure in the analysis. Sometimes a textual document layout worksheet is utilized. As a minimum, the following basic information is required from the HHA:

1. Personnel health hazards
2. Hazard effects (mishaps)
3. Hazard causal factors (materials, processes, excessive exposures, etc.)
4. Risk assessment (before and after design safety features are implemented)
5. Derived safety requirements for eliminating or mitigating the hazards.

The recommended HHA worksheet is shown in Figure 9.3. This particular HHA worksheet utilizes a columnar-type format and has been proven to be effective in many applications. The worksheet can be modified as found necessary by the SSP.



System: ① Subsystem: ② Operation: ③ Mode: ④			**Health Hazard Assessment**				Analyst: ⑤ Date: ⑥		
Hazard Type	No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯

Figure 9.3 *Recommended HHA worksheet.*

The information required under each column entry of the worksheet is described below:

1. *System* This column identifies the system under analysis.
2. *Subsystem* This column identifies the subsystem under analysis.
3. *Operation* This column identifies the operation under analysis.
4. *Mode* This column identifies the system mode under analysis.
5. *Analyst* This column identifies the name of the HHA analyst.
6. *Date* This column identifies the date of the analysis.
7. *Hazard Type* This column identifies the type of human health concern being analyzed, such as vibration, noise, thermal, chemical, and so forth.
8. *Hazard No.* This column identifies the number assigned to the identified hazard in the HHA (e.g., HHA-1, HHA-2, etc.). This is for future reference to the particular hazard source and may be used, for example, in the hazard action record (HAR) and the hazard tracking system (HTS).
9. *Hazard* This column identifies the particular human health hazard. It should describe the hazard source, mechanism, and outcome. The specific system mode or phase of concern should also be identified.
10. *Cause* This column identifies conditions, events, or faults that could cause the hazard to exist and the events that can trigger the hazardous elements to become a mishap or accident.
11. *Effect/Mishap* This column identifies the effect and consequences of the hazard, should it occur. Generally the worst-case result is the stated effect.
12. *Initial Mishap Risk Index (IMRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard,

given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values are shown below:

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

13. *Recommended Action* This column establishes recommended preventive measures to eliminate or control identified hazards. Safety requirements in this situation generally involve the addition of one or more barriers to keep the energy source away from the target. The preferred order of precedence for design safety requirements is as shown below:

Order of Precedence
1. Eliminate hazard through design selection.
2. Control hazard through design methods.
3. Control hazard through safety devices.
4. Control hazard through warning devices.
5. Control hazard through procedures and training.

14. *Final Mishap Risk Index (FMRI)* This column provides a qualitative measure of mishap risk significance for the potential effect of the identified hazard, given that mitigation techniques and safety requirements are applied to the hazard. The same values used in column 12 are also used here.
15. *Comments* This column provides a place to record useful information regarding the hazard or the analysis process that are not noted elsewhere.
16. *Status* This column states the current status of the hazard, as either being open or closed. This follows the hazard tracking methodology established for the program. A hazard can only be closed when it has been verified through analysis, inspection, and/or testing that the safety requirements are implemented in the design and successfully tested for effectiveness.

9.7 CHECKLIST

Table 9.2 provides a list of typical health hazard sources that should be considered when performing an HHA.

TABLE 9.2 Typical Human Health Hazard Sources

HHA Category	Examples
Acoustic Energy	
Potential energy existing in a pressure wave transmitted through the air may interact with the body to cause loss of hearing or internal organ damage.	• Steady-state noise from engines • Impulse noise from shoulder-fired weapons
Biological Substances	
Exposures to microorganisms, their toxins, and enzymes.	• Sanitation concerns related to waste disposal
Chemical Substances	
Exposure to toxic liquids, mists, gases, vapors, fumes, or dusts.	• Combustion products from weapon firing • Engine exhaust products • Degreasing solvents
Oxygen Deficiency	
Hazard may occur when atmospheric oxygen is displaced in a confined/enclosed space and falls below 21% by volume. Also used to describe the hazard associated with the lack of adequate ventilation in crew spaces.	• Enclosed or confined spaces associated with shelters, storage tanks, and armored vehicles • Lack of sufficient oxygen and pressure in aircraft cockpit cabins • Carbon monoxide in armored tracked vehicles
Ionizing Radiation Energy	
Any form of radiation sufficiently energetic to cause ionization when interacting with living matter.	• Radioactive chemicals used in light sources for optical sights and instrumented panels
Nonionizing Radiation	
Emissions from the electromagnetic spectrum that has insufficient energy to produce ionization, such as lasers, ultraviolet, and radio frequency radiation sources.	• Laser range finders used in weapons systems; microwaves used with radar and communication equipment
Shock	
Delivery of a mechanical impulse or impact to the body. Expressed as a rapid acceleration or deceleration.	• Opening forces of a parachute harness • Back kick of firing a handheld weapon
Temperature Extremes	
Human health effects associated with hot or cold temperatures.	• Increase to the body's heat burden from wearing total encapsulating protective chemical garments • Heat stress from insufficient ventilation to aircraft or armored vehicle crew spaces

(*continued*)

TABLE 9.2 ***Continued***

HHA Category	Examples
Trauma	
Injury to the eyes or body from impact or strain.	• Physical injury cause by blunt or sharp impacts • Musculo-skeletal trauma caused by excessive lifting
Vibration	
Adverse health effects [e.g., back pain, hand-arm vibration syndrome (HAVS), carpel tunnel syndrome, etc.] caused by contact of a mechanically oscillating surface with the human body.	• Riding in and/or driving/piloting armored vehicles or aircraft • Power hand tools • Heavy industrial equipment
Human–Machine Interface	
Various injuries such as musculo-skeletal strain, disk hernia, carpel tunnel syndrome, etc. resulting from physical interaction with system components.	• Repetitive ergonomic motion • Manual material handling—lifting assemblies or subassemblies • Acceleration, pressure, velocity, and force
Hazardous Materials	
Exposures to toxic materials hazardous to humans.	• Lead • Mercury

9.8 EXAMPLE

In order to demonstrate the HHA methodology, an HHA is performed on an example system. The particular system for this example is a hypothetical diesel submarine system. An HHA is performed on the diesel engine room of this system. Tables 9.3 through 9.5 contain the HHA worksheets for this example.

9.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the HHA technique:

1. Is easily and quickly performed.
2. Does not require considerable expertise for technique application.
3. Is relatively inexpensive yet provides meaningful results.
4. Provides rigor for focusing on system health hazards.
5. Quickly provides an indication of where major system health hazards will exist.

There are no disadvantages of the HHA technique.

TABLE 9.3 Example HHA—Worksheet 1

System: Subsystem: Operation: Mode:			**Health Hazard Analysis**				Analyst: Date:		
HH Type	No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
Noise	HH-1	Excessive exposure to engine noise causes operator ear damage	Constant engine noise above xx dB	Ear damage; loss of hearing	3C	Ear protection; limit exposure time	3E		Open
Vibration	—	No hazard; within limits	Engine vibration	None	4E	None	4E		Closed
Temperature	—	No hazard; within limits	Engine room temperature	None	4E	None	4E		Closed
Oxygen deficiency	HH-2	Loss of oxygen in engine room, causing operator death	Closed compartment and faults cause oxygen loss	Operator death	1C	Sensors and warning devices	1E		Open
							Page: 1 of 3		

TABLE 9.4 Example HHA—Worksheet 2

System: Subsystem: Operation: Mode:			**Health Hazard Analysis**				Analyst: Date:		
HH Type	No.	Hazard	Causes	Effects	MRI	Recommended Action	FMRI	Comments	Status
Biological substance	—	None present; no hazard	None	None	4E	None	4E		Closed
Chemical substance	HH-3	Exposure to diesel fuel fumes	Operator sickness	Operator sickness	3B	Sensors and air purge	3E		Open
Ergonomic	—	None	None	None	4E	None	4E		Closed
Physical stress	HH-4	Operator injury from lifting heavy objects	Operator injury	Operator injury	3C	All items must not exceed one-man weight limit	3E		Open
								Page: 2 of 3	

TABLE 9.5 Example HHA—Worksheet 3

System: Subsystem: Operation: Mode:			**Health Hazard Analysis**				Analyst: Date:		
HH Type	No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
Ionizing radiation	—	No hazard; none present	None	None	4E	None	4E		Closed
Nonionizing radiation	—	No hazard; none present	None	None	4E	None	4E		Closed
Hazardous Material	HH-5	Exposure to asbestos causes operator death	Exposure to asbestos particles	Operator death	1C	Prohibit use of asbestos in system	1E		Open
								Page: 3 of 3	

9.10 COMMON MISTAKES TO AVOID

When first learning how to perform an HHA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of an HHA.

1. The hazard identified is other than a human health hazard.
2. The hazard description is not detailed enough.
3. Design mitigation factors are not stated or provided.
4. Design mitigation factors do not address the actual causal factor(s).
5. Overuse of project-specific terms and abbreviations.

9.11 SUMMARY

This chapter discussed the HHA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of HHA is to identify human health hazards.
2. The use of a human health hazard checklist greatly aids and simplifies the HHA process.
3. The use of the recommended HHA worksheet aids the analysis process and provides documentation of the analysis.

BIBLIOGRAPHY

There are no significant references for the HHA technique that describe it in detail. Many textbooks on system safety discuss the methodology in general but do not provide detailed explanation with examples. Refer to the *Safety Analysis Handbook* published by the System Safety Society for a short description of HHA. DoD Data Item Description DI-SAFT-80106, *Occupational Health Hazard Assessment Report*, provides information on an HHA.

Chapter 10

Safety Requirements/ Criteria Analysis

10.1 INTRODUCTION

The safety requirement/criteria analysis (SRCA) is an analysis for evaluating system safety requirements (SSRs). As the name implies, SRCA evaluates SSRs and the criteria behind them. SRCA has a twofold purpose: (1) to ensure that every identified hazard has at least one corresponding safety requirement and (2) to verify that all safety requirements are implemented and are validated successfully. The SRCA is essentially a traceability analysis to ensure that there are no holes or gaps in the safety requirements and that all identified hazards have adequate and proven design mitigation coverage. The SRCA applies to hardware, software, firmware, and test requirements.

The SRCA also applies to the traceability of design criteria and guidelines to SSRs, such as those specified in the DoD *Joint Software System Safety Handbook* (DoDJSSSH) [1] and Electronic Industries Association SEB6-A for software [2], and MIL-STD-1316 for fuze systems [3]. Guideline traceability ensures that the appropriate safety guidelines and criteria are incorporated into the SSRs.

10.2 BACKGROUND

This analysis technique falls under the requirements design hazard analysis type (RD-HAT). The basic analysis types are described in Chapter 3. Alternate names

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

for this technique are requirements hazard analysis (RHA) and requirements traceability analysis.

The purpose of the SRCA is to ensure that all identified hazards have corresponding design safety requirements to eliminate or mitigate the hazard and that the safety requirements are verified and validated as being successful in the system design and operation. The intent is to ensure that the system design requirements have no "safety" gaps (i.e., no hazard has been left unmitigated) and to verify that all safety requirements are adequately implemented or created as necessary.

The SRCA is applicable to analysis of all types of systems, facilities, and software where hazards and safety requirements are involved during development. SRCA is particularly useful when used in a software safety program. The SRCA technique, when applied to a given system by experienced safety personnel, is very thorough in providing an accurate traceability of safety design requirement verification and safety test requirement validation.

A basic understanding of system safety and the design requirement process is essential. Experience with the particular type of system is helpful. The technique is uncomplicated and easily learned. Standard easily followed SRCA worksheets and instructions are provided in this chapter.

The SRCA is very useful for ensuring that design safety requirements exist for all hazards and that the safety requirements are in the design and test specifications. SRCA provides assurance that safety requirements exist for all identified hazards and ensures that all safety requirements are incorporated into the design and test specifications. The application of the SRCA to software development has proven to be very effective for successfully evaluating software to ensure compliance with safety requirements.

10.3 HISTORY

The SRCA technique was established very early in the history of the system safety discipline. It was formally instituted and promulgated by the developers of MIL-STD-882.

10.4 THEORY

As previously stated, the purpose of the SRCA is to ensure that safety requirements exist for all identified hazards, that all safety requirements are incorporated into the design and test specifications and that all safety requirements are successfully tested. Figure 10.1 shows an overview of the basic SRCA process and summarizes the important relationships involved in the SRCA process. This process consists of comparing the SSRs to design requirements and identified hazards. In this way any missing safety requirements will be identified. In addition, SSRs are traced into the test requirements to ensure that all SSRs are tested.

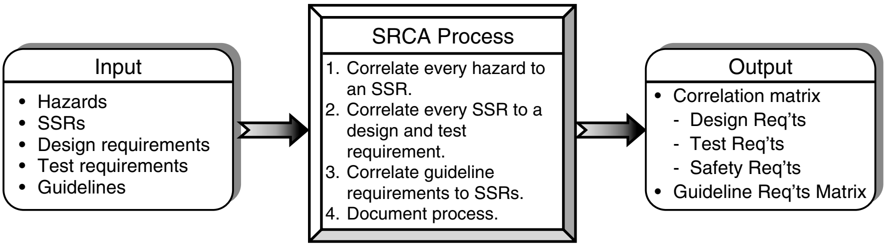


Figure 10.1 *SRCA overview.*

10.5 METHODOLOGY

Figure 10.2 shows an overview of the SRCA thought process for the SRCA technique. The idea behind this thought process is that a matrix worksheet is used to correlate safety requirements, with design requirements, test requirements, and identified hazards. If a hazard does not have a corresponding safety requirement, then there is an obvious gap in the safety requirements. If a safety requirement is not included in the design requirements, then there is a gap in the design requirements. If a safety requirement is missing from the test requirements, then that requirement cannot be verified and validated. If an SSR cannot be shown to have passed testing, then the associated hazard cannot be closed.

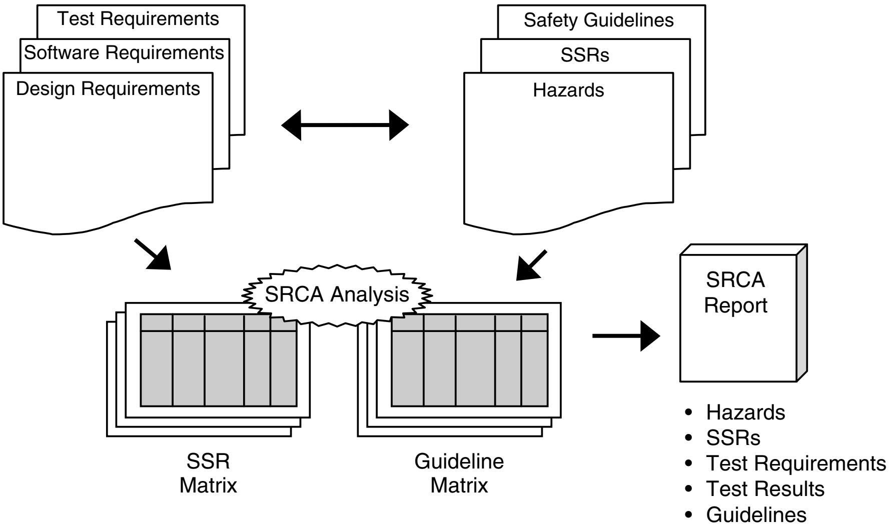


Figure 10.2 *SRCA methodology.*

TABLE 10.1 SRCA Process

Step	Task	Description
1	Acquire requirements.	Acquire all of the design (hardware and software) and test requirements for the system.
2	Acquire safety data.	Acquire all of the hazards and SSRs for the system.
3	Acquire safety guidelines.	Acquire all safety guidelines that are applicable to the system.
4	Establish an SSR traceability matrix.	Correlate SSRs with hazards, design requirements, and test requirements.
5	Establish guideline traceability matrix.	Correlate safety guidelines and criteria with SSRs.
6	Identify requirement gaps.	Identify hazards that have no corresponding safety requirement.
7	Recommend corrective action.	Determine if the design controls present are adequate and, if not, recommend controls that should be added to reduce the mishap risk.
8	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
9	Document SRCA.	Document the entire SRCA process on the worksheets. Update for new information as necessary.

The SRCA is a detailed correlation analysis, utilizing structure and rigor to provide traceability for all SSRs. The SRCA begins by acquiring the system hazards, SSRs, design requirements, and test requirements. A traceability matrix is then constructed that correlates the hazards, SSRs, design requirements, and test requirements together. The completed traceability matrix ensures that every hazard has a corresponding safety requirement and that every safety requirement has a corresponding design and test requirement.

The SRCA consists of two separate correlation traceability analyses: (1) an SSRs correlation and (2) a guideline compliance correlation. The guideline correlation only applies to systems where guidelines exist and are applied to the system design. For example, the safety guideline requirements from the DoDJSSSH are generally applied to the design of software, and the guideline requirements from MIL-STD-1316 are applied to fuze system designs. Table 10.1 lists and describes the basic steps of the SRCA process.

10.6 WORKSHEETS

The SRCA is a detailed hazard analysis utilizing structure and rigor. It is desirable to perform the SRCA using specialized worksheets. Although the format of the analysis worksheet is not critical, typically, matrix or columnar-type worksheets are used to help maintain focus and structure in the analysis. Software packages are available to aid the analyst in preparing these worksheets.

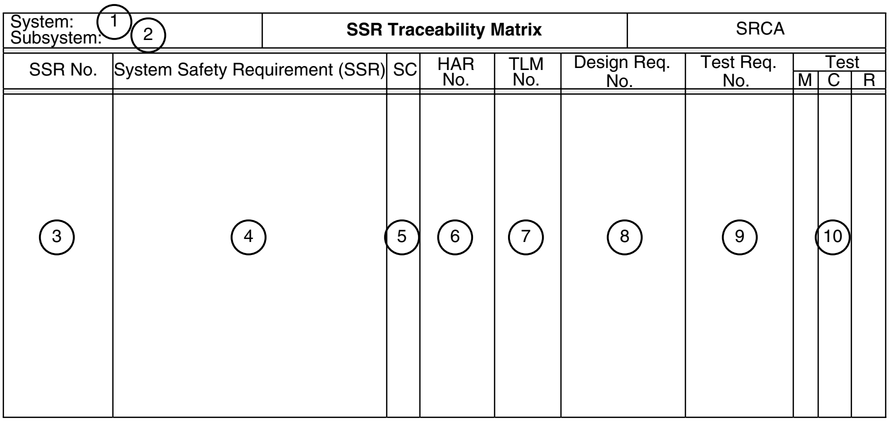
The purposes of the SRCA are to establish traceability of SSRs and to assist in the closure of mitigated hazards. As a minimum, the following basic information is required from the SRCA:

1. Traceability matrix of all identified hazards to corresponding SSRs
2. Traceability matrix of all safety design requirements to test requirements and test results
3. Identification of new safety design requirements and tests necessary to cover gaps discovered by items 1 and 2 above
4. Traceability matrix of all safety guidelines and criteria to SSRs
5. Data from items 1, 2, 3, and 4 above supporting closure of hazards

The specific worksheet to be used may be determined by the managing authority, the safety working group, the safety team, or the safety analyst performing the analysis. Figures 10.3 contains an example SRCA requirements correlation worksheet for the traceability of SSRs.

The information required under each column of the requirements correlation matrix worksheet is described below:

1. *System* This column identifies the system under analysis.
2. *Subsystem* This column identifies the subsystem under analysis.
3. *System Safety Requirement (SSR) Number* This column identifies the SSR number.
4. *SSR* This column states the actual verbiage of the SSR.
5. *Safety Critical (SC)* Place a Yes in this column to indicate that the SSR is an SC requirement.



System: 1 Subsystem: 2	SSR Traceability Matrix					SRCA			
SSR No.	System Safety Requirement (SSR)	SC	HAR No.	TLM No.	Design Req. No.	Test Req. No.	Test		
							M	C	R
3	4	5	6	7	8	9		10	

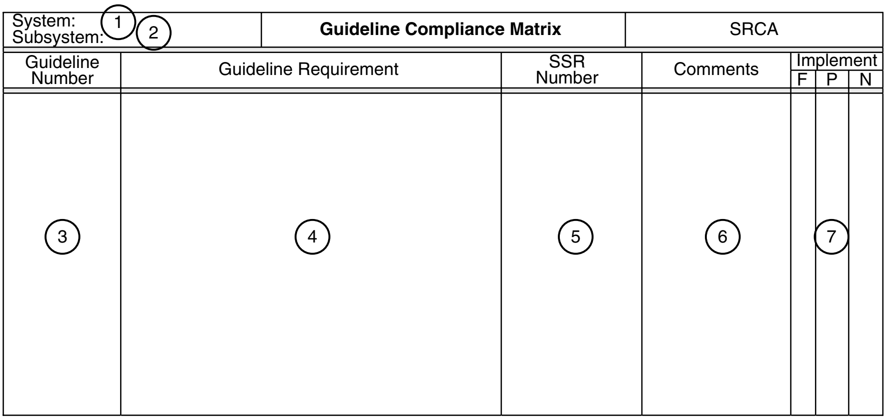
Figure 10.3 SRCA requirements correlation matrix worksheet.

6. *Hazard Action Record (HAR) Number* This column identifies the HAR or HARs associated with the SSR. The SSR may be providing mitigation for one or more hazards.
7. *Top-Level Mishap (TLM) Number* This column identifies the TLM associated with the SSR.
8. *Design Requirement Number* This column identifies the specific design requirement that implements the SSR.
9. *Test Requirement Number* This column identifies the specific test requirement or requirements that test the SSR.
10. *Test* This column provides information regarding testing of the SSR. Three different types of information are provided:
    a. M This column identifies the test method used: test (T), analysis (A), inspection (I), and not (N) done.
    b. C This column identifies the test coverage: explicitly (E) tested by a specific test or implicitly (I) tested through another test.
    c. R This column identifies the test results: pass (P) or fail (F).

Figure 10.4 contains the recommended SRCA correlation worksheet for the traceability of SSR compliance with safety guideline and criteria.

The information required under each column of the guideline correlation matrix worksheet is described below:

1. *System* This column identifies the system under analysis.
2. *Subsystem* This column identifies the subsystem under analysis.
3. *Guideline Number* This column identifies the requirement number from the guideline or criteria document.



System: 1 Subsystem: 2	**Guideline Compliance Matrix**	SRCA

Guideline Number	Guideline Requirement	SSR Number	Comments	Implement		
				F	P	N
3	4	5	6		7	

Figure 10.4 *Guideline correlation matrix worksheet.*

4. *Guideline Requirement* This column contains the actual text of the guideline requirement.
5. *SSR Number* This column identifies the specific SSR that implements the design guideline requirement.
6. *Comments* This column provides for any necessary discussion associated with the guideline requirement. For example, if the guideline is only partially implemented or not implemented at all, sufficient rationale and justification must be provided.
7. *Implement* This column provides information regarding implementation of the design guideline. Check the particular column that is applicable:
   a. Full (F) implementation by the SSR
   b. Partial (P) implementation by the SSR
   c. Not (N) implemented (not applicable or not possible)

10.7 EXAMPLE

This example involves a fuze subsystem for a missile weapon system, which includes both hardware and software. In these examples, not all of the SSRs or design requirements are included, only a small example portion of the overall requirements to demonstrate the technique.

Note from this example that more than one safety requirement may exist for a particular hazard. Also, note that the hazard action record (HAR) number is provided for each hazard. The identified design requirement is derived from the program design specification document, and the test requirement is derived from the program test requirements document.

Table 10.2 provides an SRCA requirements traceability matrix for this example system. Note that only a single page is shown for this example. A typical SRCA would consist of many pages.

Table 10.3 provides a compliance matrix for the DoDJSSSH software guidelines [1]. A software SRCA correlation compliance would include the review of each of these guidelines, determine if it were applicable to the system design, provide rationale for those not applicable, and provide the corresponding safety requirement reference in the specification for those found to be applicable.

Table 10.4 provides a MIL-STD-1316 (Series) compliance matrix for this example system. Table 10.5 provides a MIL-HDBK-454 (Series) compliance matrix for this example system.

10.8 ADVANTAGES AND DISADVANTAGES

The following are advantages of the SRCA technique:

1. SRCA is easily and quickly performed.
2. SRCA correlates SSRs to hazards and design requirements and specifications.

TABLE 10.2 SRCA Requirements Traceability Matrix Example

System: Lark Missile Subsystem: Fire Control System		**SSR Traceability Matrix**				Safety Requirements/Criteria Analysis			
SSR Number	System Safety Requirement (SSR)	SC	HAR Number	TLM Number	Design Req't Number	Test Req't Number	Test		
							T/A/I/N	E/I	P/F
SSR 31	No single point failure can result in missile launch.	Y	21	1	SS 7.7.21	TS 4.7.21	T	E	P
SSR 32	Three separate and independent means are required for missile arming.	Y	81, 95	1	SS 7.7.22	TS 4.7.22	T	E	P
SSR 33									
SSR 34									
							Page:		

TABLE 10.3 DoDJSSSH Compliance Matrix Example

System: Subsystem:	**DoDJSSSH Software Compliance Matrix**		Safety Requirements/Criteria Analysis			
DoDJSSSH Number	DoDJSSSH Requirement	SSR Number	Comments	Compliance		
				F	P	N
E.4.3	Primary computer failure. The system shall be designed such that a failure of the primary control computer will be detected and the system returned to a safe state.	SSR 71		X		
E.5.2	CPU selection. CPUs, microprocessors, and computers that can be fully represented mathematically are preferred to those that cannot.		Not possible for program to obtain a CPU meeting this requirement. Intel Pentium II has been selected and approved. This requirement is too stringent for program.			X
E.6.4	Operational checks. Operational checks of testable safety critical system elements shall be made immediately prior to performance of a related safety critical operation.	SSR 72		X		
E.9.4	Safety critical displays. Safety critical operator displays, legends, and other interface functions shall be clear, concise, and unambiguous and, where possible, be duplicated using separate display devices.	SSR 73		X		
E.11.2	Modular code. Software design and code shall be modular. Modules shall have one entry and one exit point.	SSR 74		X		
E.11.18	Variable declaration. Variables or constants used by a safety critical function will be declared/initialized at the lowest possible level.	SSR 75		X		
E.11.19	Unused executable code. Operational program loads shall not contain unused executable code.	SSR 76		X		
				Page:		

TABLE 10.4 MIL-STD-1316E Compliance Matrix Example

System: Subsystem:	**MIL-STD-1316E Compliance Matrix**		Safety Requirements/Criteria Analysis			
1316E Number	MIL-STD-1316E Requirement	SSR Number	Comments	Compliance		
				F	P	N
4.2.2	*Arming delay*. A safety feature of the fuze shall provide arming delay, which assures that a safe separation distance can be achieved for all defined operational conditions.	SSR 47		X		
4.2.3	*Manual arming*. An assembled fuze shall not be capable of being armed manually.	SSR 48		X		
4.3	*Safety system failure rate*. The fuze safety system failure rate shall be calculated for all logistical and tactical phases from manufacture to safe separation. The safety system failure rate shall be verified to the extent practical by test and analysis during fuze evaluation and shall not exceed the rates given for the following phases:	SSR 49	Verified by FTA	X		
4.3a	Prior to intentional initiation of the arming sequence: 1×10^{-6} to prevent arming or functioning.					
4.3b	Prior to the exit (for tubed launch munitions): 1×10^{-4} to prevent arming 1×10^{-6} to prevent functioning					
4.3c	Between initiation of arming sequence and safe separation: 1×10^{-3} to prevent arming ALARP[a] with established risk to prevent functioning					
				Page:		

[a]ALARP, as low as reasonably practical.

TABLE 10.5 MIL-HDBK-454 Compliance Matrix Example

System: Subsystem:	**MIL-HDBK-454 Compliance Matrix**		Safety Requirements/Criteria Analysis			
454 Number	MIL-STD-454 Requirement	SSR Number	Comments	Compliance		
				F	P	N
4.1	The equipment shall provide fail-safe features for safety of personnel during installation, operation, maintenance, and repair or interchanging of a complete assembly or component parts.	SSR 101		X		
4.2	Electric equipment shall be bonded in accordance with MIL-B-5087, Class R/L/H.	SSR 102		X		
4.3a	At an ambient temperature of 25°C, the operating temperature of control panels and operating controls shall not exceed 49°C (120°F).	SSR 103		X		
4.3b	At an ambient temperature of 25°C (77°F), exposed parts subject to contact by personnel (other than control panels and operating controls) shall not exceed 60°C (140°F).	SSR 104		X		
				Page:		

Source: MIL-HDBK-454M, *general guidelines for Electrical Equipment, guideline 1—Safety Design Criteria for Personnel Hazards.*

3. SRCA verifies and validates SSRs through correlation of test results.
4. Software packages are available to aid the analyst in preparing SRCA worksheets.

There are no major disadvantages of the SRCA technique.

10.9 COMMON MISTAKES TO AVOID

When first learning how to perform an SRCA, it is commonplace to commit some typical errors. The following is a list of common errors made during the conduct of an SRCA:

1. Failing to put all safety guidelines and requirements into SSRs
2. Failing to perform a traceability compliance analysis on all safety guidelines and requirements SSRs

10.10 SUMMARY

This chapter discussed the SRCA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of the SRCA is to assess the SSRs and:
   - Identify hazards without associated SSRs (gaps in the design SSRs).
   - Identify requirements that are not in the system design requirements.
   - Identify requirements that are not tested and validated for effectiveness.
   - Identify safety guidelines and requirements that are not implemented in the SSRs.
2. The SRCA relates the identified hazards to the design SSRs to ensure that all identified hazards have a least one safety requirement, whose implementation will mitigate the hazard.
3. The SRCA relates the design SSRs to the test requirements to ensure all safety requirements are verified and validated by test.
4. The SRCA is also used to incorporate safety guidelines and requirements that are specifically safety related but not tied to a specific hazard.
5. The SRCA process ensures that the design safety requirements are properly developed and translated into the system hardware and software requirement documents.
6. The use of the recommended SRCA worksheets simplifies the process and provides documentation of the analysis.

REFERENCES

1. DoD, *DoD Joint Software System Safety Handbook* (DoDJSSSH), Appendix E—Generic Requirements and Guidelines, 1999.
2. Electronic Industries Association, EIA SEB6-A, *System Safety Engineering in Software Development*, Appendix A—Software System Safety Checklist, Electronic Industries Association, 1990.
3. MIL-STD-1316 (Series), *Safety Criteria for Fuze Design—DoD Design Criteria Standard*.
4. MIL-HDBK-454M (Series), *General Guidelines for Electronic Equipment, Guideline 1—Safety Design Criteria for Personnel Hazards*.

Chapter 11

Fault Tree Analysis

11.1 INTRODUCTION

Fault tree analysis (FTA) is a systems analysis technique used to determine the root causes and probability of occurrence of a specified undesired event. FTA is employed to evaluate large complex dynamic systems in order to understand and prevent potential problems. Using a rigorous and structured methodology, FTA allows the systems analyst to model the unique combinations of fault events that can cause an undesired event to occur. The undesired event may be a system hazard of concern or a mishap that is under accident investigation.

A fault tree (FT) is a model that logically and graphically represents the various combinations of possible events, both faulty and normal, occurring in a system that lead to an undesired event or state. The analysis is deductive in that it transverses from the general problem to the specific causes. The FT develops the logical fault paths from a single undesired event at the top to all of the possible root causes at the bottom. The strength of FTA is that it is easy to perform, easy to understand, provides useful system insight, and shows all of the possible causes for a problem under investigation.

Fault trees are graphical models using logic gates and fault events to model the cause–effect relationships involved in causing the undesired event. The graphical model can be translated into a mathematical model to compute failure probabilities and system importance measures. FT development is an iterative process, where the initial structure is continually updated to coincide with design development.

In the analysis of systems there are two applications of FTA. The most commonly used application is the proactive FTA, performed during system development to influence design by predicting and preventing future problems. The other

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

application is the reactive FTA, performed after an accident or mishap has occurred. The techniques used for both applications are identical except the reactive FTA includes the use of mishap evidence and the evidence event gate.

When used as a system safety analysis tool, the FT results in a graphic and logical representation of the various combinations of possible events, both faulty and normal, occurring within a system, which can cause a predefined undesired event. An undesired event is any event that is identified as objectionable and unwanted, such as a potential accident, hazardous condition, or undesired failure mode. This graphic presentation exposes the interrelationships of system events and their interdependence upon each other, which results in the occurrence of the undesired event.

The completed FT structure can be used to determine the significance of fault events and their probability of occurrence. The validity of action taken to eliminate or control fault events can be enhanced in certain circumstances by quantifying the FT and performing a numerical evaluation. The quantification and numerical evaluation generates three basic measurements for decision making relative to risk acceptability and required preventive measures:

1. The probability of occurrence of the undesired event
2. The probability and significance of fault events (cut sets) causing the undesired event
3. The risk significance or importance of components

In most circumstances a qualitative evaluation of the fault tree will yield effective results at a reduced cost. Careful thought must be given in determining whether to perform a qualitative or a quantitative FTA. The quantitative approach provides more useful results, however, it requires more time and experienced personnel. The quantitative approach also requires the gathering of component failure rate data for input to the FT.

Since a FT is both a graphic and a logical representation of the causes or system faults leading to the undesired event, it can be used in communicating and supporting decisions to expend resources to mitigate hazards. As such, it provides the required validity in a simple and highly visible form to support decisions of risk acceptability and preventive measure requirements.

The FT process can be applied during any lifecycle phase of a system—from concept to usage. However, FTA should be used as early in the design process as possible since the earlier necessary design changes are made, the less they cost.

An important time- and cost-saving feature of the FT technique is that only those system elements that contribute to the occurrence of the undesired event need to be analyzed. During the analysis, noncontributing elements are ruled out and are, thus, not included in the analysis. This means that a majority of the effort is directed toward the elimination or control of the source or sources of the problem area. However, system elements not involved with the occurrence of one undesired event may be involved with the occurrence of another undesired event.

In summary, the FT is used to investigate the system of concern, in an orderly and concise manner, to identify and depict the relationships and causes of the undesired event. A quantitative evaluation may be performed in addition to a qualitative evaluation to provide a measure of the probability of the occurrence of the top-level event and the major faults contributing to the top-level event. The analyst may use the results of a FTA as follows:

1. Verification of design compliance with established safety requirements
2. Identification of design safety deficiencies (subtle or obvious) that have developed in spite of existing requirements
3. Identification of common mode failures
4. Establishment of preventive measures to eliminate or mitigate identified design safety deficiencies
5. Evaluation of the adequacy of the established preventive measures
6. Establishment or modification of safety requirements suitable for the next design phase

11.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (SD-HAT). Refer to Chapter 3 for a description of the analysis types. The FTA technique has been referred to as logic tree analysis and logic diagram analysis.

Fault tree analysis has several basic purposes, which include the following:

1. Find the root causes of a hazard or undesired event during design development in order that they can be eliminated or mitigated.
2. Establish the root causes of a mishap that has occurred and prevent them from recurring.
3. Identify the undesired event causal factor combinations and their relative probability.
4. Determine high-risk fault paths and their mechanisms.
5. Identify risk importance measures for components and fault events.
6. Support a probabilistic risk assessment (PRA) of system designs.

The FTA technique can be used to model an entire system, with analysis coverage given to subsystems, assemblies, components, software, procedures, environment, and human error. FTA can be conducted at different abstraction levels, such as conceptual design, top-level design, and detailed component design. FTA has been successfully applied to a wide range of systems, such as missiles, ships, spacecraft, trains, nuclear power plants, aircraft, torpedoes, medical equipment, and chemical plants. The technique can be applied to a system very early in design development and thereby identify safety issues early in the design process. Early application helps system developers to design in safety of a system during early development rather than having to take corrective action after a test failure or a mishap.

A basic understanding of FTA theory is essential to developing FTs of small and noncomplex systems. In addition it is crucial for the analyst to have a detailed understanding of the system regardless of complexity. As system complexity increases, increased knowledge and experience in FTA is also required. Overall, FTA is very easy to learn and understand. Proper application depends on the complexity of the system and the skill of the analyst.

Applying FTA to the analysis of a system design is not a difficult process. It is more difficult than an analysis technique such as a PHA, primarily because it requires a logical thought process, an understanding of FTA construction methodology, and a detailed knowledge of system design and operation. FTA does not require knowledge of high-level mathematics compared to Markov or Petri net analyses.

The FTA technique enjoys a favorable reputation among system safety analysts in all industries utilizing the technique. In some industries it is the only tool that can provide the necessary probability calculations for verification that numerical requirements are being met. Many commercial computer programs are available to assist the analyst in building, editing, and mathematically evaluating FTs.

Some analysts criticize the FTA tool because it does not always provide probabilities to six-decimal-place accuracy when modeling certain designs. However, comparison of FT model results to those of other tools, such as Markov analysis (MA) show that FTA provides very comparable results with much greater simplicity in modeling difficulty. In addition, six-digit accuracy is sometime meaningless when the input data is not precise.

Although FTA is classified as a hazard analysis, it is primarily used as a root cause analysis tool to identify and evaluate the causal factors of a hazard. In addition, it can provide a probability risk assessment.

Markov analysis could be utilized in place of FTA for probability calculations; however, MA has limitations that FTA does not (refer to Chapter 18). For example, it is difficult to model large complex systems, the mathematics are more cumbersome, it is difficult to visualize fault paths in an MA model, and an MA model does not produce cut sets.

11.3 HISTORY

The FTA technique was invented and developed by H. Watson and Allison B. Mearns of Bell Labs for use on the Minuteman Guidance System. Dave Haasl of the Boeing Company recognized the power of FTA and applied it for quantitative safety analysis of the entire Minuteman Weapon System. The analytical power and success of the technique was recognized by the commercial aircraft industry and the nuclear power industry, and they then began using it for safety evaluations.

Many individuals in each of these industries contributed to enhancing the state-of-the-art in fault tree mathematics, graphics, and computer algorithms.

11.4 THEORY

Fault tree analysis is a robust, rigorous, and structured methodology requiring the application of certain rules of Boolean algebra, logic, and probability theory. The FT itself is a logic diagram of all the events (failure modes, human error, and normal conditions) that can cause the top undesired event to occur.

When the FT is complete, it is evaluated to determine the critical cut sets (CSs) and probability of failure. The cut sets are the combination of failure events that can cause the top to occur. The FT evaluation provides the necessary information to support risk management decisions.

As shown in Figure 11.1 the theory behind FTA is to start with a top undesired event (UE) (e.g., hazard) and model all of the system faults that can contribute to this top event. The FT model is a reflection of the system design, from a failure state viewpoint. In this example the UE might be “inadvertent warhead initiation due to system faults.”

The FTs are developed in layers, levels, and branches using a repetitive analysis process. Figure 11.2 demonstrates an FT developed in layers, with each major layer representing significant aspects of the system. For example, the top FT structure usually models the system functions and phases, the intermediate FT structure

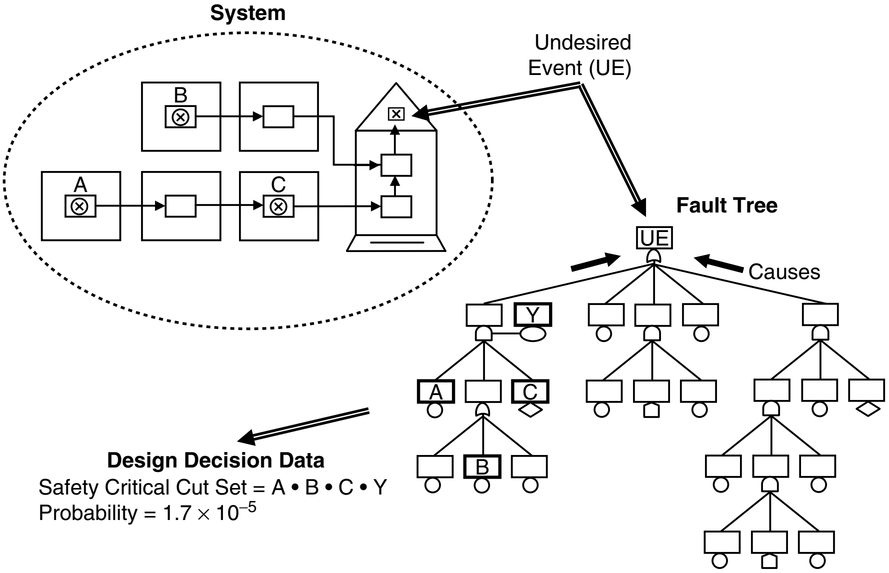


Figure 11.1 FTA overview.

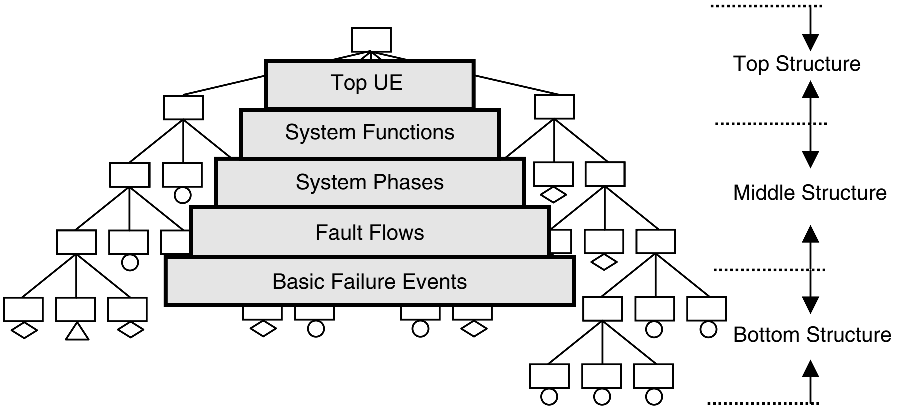


Figure 11.2 *Major levels of a fault tree.*

models subsystem fault flows, and the bottom FT structure models assembly and component fault flows.

11.5 METHODOLOGY

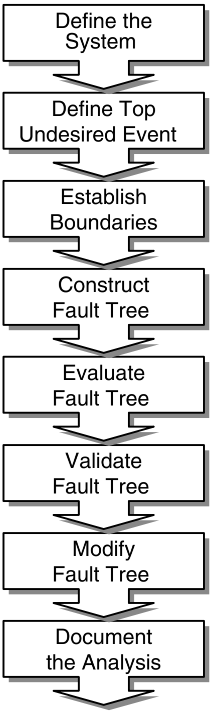
There are eight basic steps in the FTA process, as shown in Figure 11.3. These are the steps required to perform a complete and accurate FTA. Some analysts may combine or expand some of the steps, but these are the basic procedures that must be followed.

11.5.1 Building Blocks

Fault trees consists of nodes interlinked together in a treelike structure. The nodes represent fault/failure paths and are linked together by Boolean logic and symbols. The FT symbols form the basic building blocks of FTA and consist of four categories:

1. Basic events
2. Gate events
3. Conditional events
4. Transfer events

Figure 11.4 shows the standard symbols for basic event (BE), condition event (CE), and transfer event (TE) as they would appear on an FT and their associated definitions. Note that the rectangle is nothing more than a placeholder for text. When FTA was first developed, the text was placed directly in the BE symbols



1. Understand system design and operation. Acquire current design data (drawings, schematics, procedures, diagrams, etc.).

2. Descriptively define problem and establish the correct undesired event for the analysis.

3. Define analysis ground rules and boundaries. Scope the problem and record all ground rules.

4. Follow construction process, rules, and logic to build FT model of the system.

5. Generate cut sets and probability. Identify weak links and safety problems in the design.

6. Check if the FT model is correct, complete, and accurately reflects system design.

7. Modify the FT as found necessary during validation or due to system design changes.

8. Document the entire analysis with supporting data. Provide as customer product or preserve for future reference.

Figure 11.3 *FTA process.*

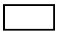
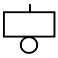
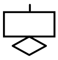
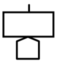
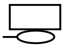
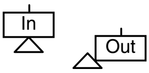
Symbol	Type	Description
	Node Text Box	Contains the text for all FT nodes. Text goes in the box, and the node symbol goes below the box.
	Primary Failure (BE)	A basic component failure; the primary, inherent, failure mode of a component. A random failure event.
	Secondary Failure (BE)	An externally induced failure or a failure mode that could be developed in more detail if desired.
	Normal Event (BE)	An event that is expected to occur as part of normal system operation.
	Condition (CE)	A conditional restriction or probability.
	Transfer (TE)	Indicates where a branch or sub-tree is marked for the same usage elsewhere in the tree. In and Out or To/From symbols.

Figure 11.4 *FT symbols for basic events, conditions, and transfers.*

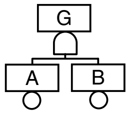
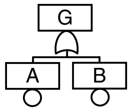
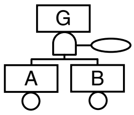
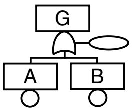
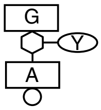
Symbol	GateType	Description
	AND Gate	The output occurs only if all of the inputs occur together. $P = P_A \bullet P_B = P_A P_B$ (2 input gate) $P = P_A \bullet P_B \bullet P_C = P_A P_B P_C$ (3 input gate)
	OR Gate	The output occurs only if at least one of the inputs occurs. $P = P_A + P_B - P_A P_B$ (2 input gate) $P = (P_A + P_B + P_C) - (P_{AB} + P_{AC} + P_{BC}) + (P_{ABC})$ (3 input gate)
	Priority AND Gate	The output occurs only if all of the inputs occur together, and A must occur before B. The priority statement is contained in the Condition symbol. $P = (P_A P_B) / N!$ Given $\lambda_A \approx \lambda_B$ and N = number of inputs to gate
	Exclusive OR Gate	The output occurs if either of the inputs occurs, but not both. The exclusivity statement is contained in the Condition symbol. $P = P_A + P_B - 2(P_A P_B)$
	Inhibit Gate	The output occurs only if the input event occurs and the attached condition is satisfied. $P = P_A \bullet P_Y = P_A P_Y$

Figure 11.5 FT symbols for gate events.

and the rectangle was only used for gate nodes, but with the advent of computer graphics this became cumbersome, so the rectangle was adopted for all nodes.

Figure 11.5 shows the gate event symbols, definitions, and probability calculation formulas. It is through the gates that the FT logic is constructed and the tree grows in width and depth. The symbols shown in Figures 11.4 and 11.5 are generally considered the standard FT symbols, however, some FT software programs do utilize slightly different symbols. Figure 11.6 shows some alternative and additional symbols that might be encountered.

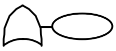
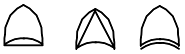
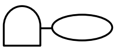
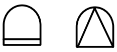
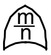
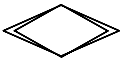
Typical Symbol	Action	Description	Alternate Symbol
	Exclusive OR Gate	Only one of the inputs can occur, not both. Disjoint events.	
	Priority AND Gate	All inputs must occur, but in given order, from left to right.	
	M of N Gate	M of N combinations of inputs causes output to occur. Voting gate.	
	Double Diamond	User-defined event for special uses.	

Figure 11.6 Alternative FT symbols.

11.5.2 Definitions

In addition to the FT symbol definitions, the following definitions define important concepts utilized in FTA:

Cut set (CS) Set of events that together cause the top UE to occur. Also referred to as a fault path.

Minimal cut set (MinCS or MCS) Cut set that has been reduced to the minimum number of events that cause the top UE to occur. The CS cannot be further reduced and still guarantee occurrence of the top UE.

CS order Number of items in a CS. A one-order CS is a single-point failure (SPF). A two-order CS has two items ANDed together.

Multiple occurring event (MOE) FT basic event that occurs in more than one place in the FT.

Multiple occurring branch (MOB) FT branch that is used in more than one place in the FT. This is one place in the FT where the transfer symbol is used. All BEs below the MOB are automatically MOEs.

Failure Occurrence of a basic inherent component failure, for example, "resistor fails open."

Fault Occurrence or existence of an undesired state of a component, subsystem, or system. For example, "light off" is an undesired fault state that may be due to light bulb failure, loss of power, or operator action. (Note that all failures are faults, but not all faults are failures.)

Primary fault/failure Independent *component failure that cannot be further defined* at a lower level. For example, "diode inside a computer fails (due to materiel flaw)."

Secondary fault/failure Independent component *failure that is caused by an external force* on the system. For example, "diode fails due to excessive RF/EMI energy in system." Failure due to out-of-tolerance operational or environmental conditions.

Command fault/failure Item that is "commanded" to fail or forced into a fault state by system design. For example, "light off" is the command fault for the light, that is, it is commanded to fail off if certain system faults cause loss of power. A command fault can be the normal operational state, but, at the wrong time, and sometimes it is lack of the desired normal state when desired or intended. (This is the "transition" to look for in the analysis.)

Exposure time (ET) Length of time a component is effectively exposed to failure during system operation. ET has a large effect on FT probability calculations ($P = 1.0 - e^{-\lambda T}$). Exposure time can be controlled by design, repair, circumvention, testing, and monitoring.

Critical path Highest probability CS that drives the top UE probability. The most dramatic system improvement is usually made by reducing the probability of this CS.

Importance measure Measure of the relative importance (sensitivity) of a BE or CS in the overall FT.

Figure 11.7 demonstrates the usage of FT transfer symbols and the MOE/MOB concepts. This figure shows an example of three FT pages. On page 1, the node with a triangle at the bottom with the name A represents a transfer in. This means that a duplicate of branch A should also go here, but it is drawn somewhere else, page 2 in this case. In this case, A is not an MOB but merely the transfer of tree

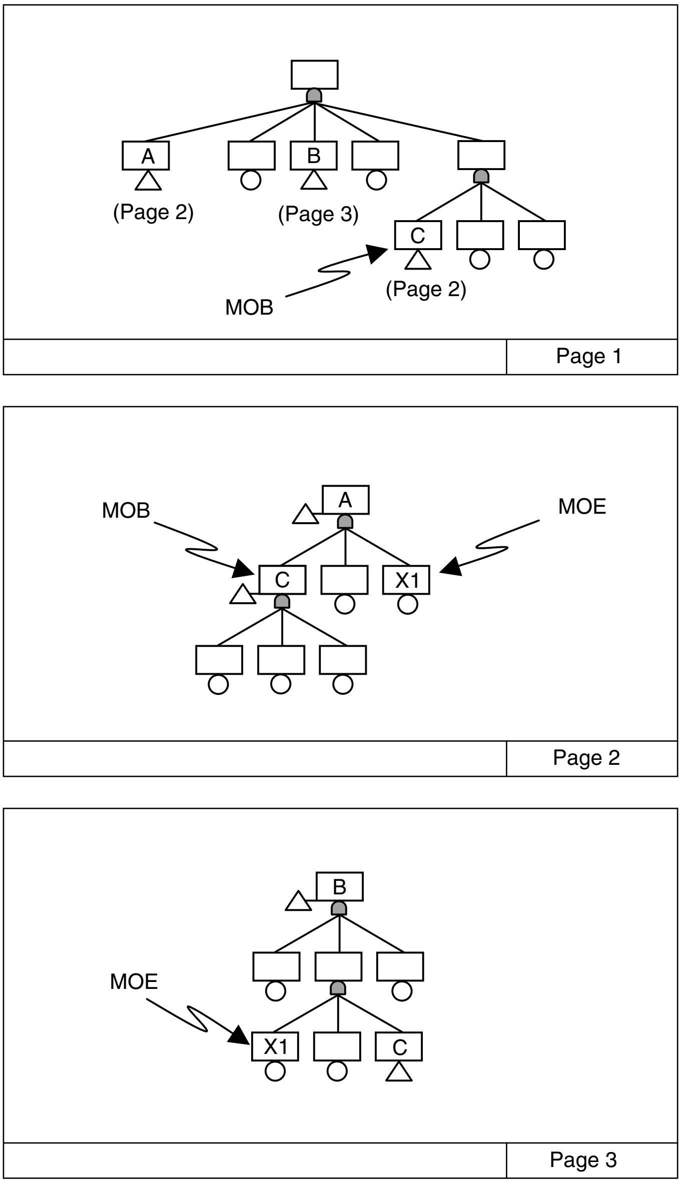


Figure 11.7 *FT transfers and MOE/MOB.*

to start on a new page, due to lack of space on page 1. Transfer C represents an MOE, as it is intended to be repeated in two different places in the FT.

11.5.3 Construction—Basics

Fault tree construction is an iterative process that begins at the treetop and continues down through all of the tree branches. The same set of questions and logic is applied on every gate, moving down the tree. After identifying the top UE, sub-undesired events are identified and structured into what is referred to as the *top fault tree* layer. The actual deductive analysis begins with the development of the *fault flow* or cause-and-effect relationship of fault and normal events through the system. This deductive reasoning involves determining the type of gate and the particular inputs to this gate at each gate level of the FT. The fault flow links the flow of events from the system level, through the subsystem level, to the component level.

The FT development proceeds through the identification and combination of the system normal and fault events, until all events are defined in terms of basic identifiable hardware faults, software faults, and human error. This is the level of basic events in the FT structure and is the end point for construction of the FT.

In developing the structure of the FT, certain procedures must consistently be followed in a repetitive manner. These procedures are necessary at each gate level to determine the type of gate to be used and the specific inputs to the gate. The established procedure evolves around three principal concepts:

1. The I–N–S concept
2. The SS–SC concept
3. The P–S–C concept

I–N–S Concept This concept involves answering the question "What is immediate (I), necessary (N), and sufficient (S) to cause the event?" The I–N–S question identifies the most immediate cause(s) of the event; the causes that are absolutely necessary; and only includes the causes that are absolutely necessary and sufficient. For example, water is necessary to maintain a green lawn and rain is sufficient to provide it, or a sprinkler system is sufficient.

This seems like an obvious question to ask, but too often it is forgotten in the turmoil of analysis. There are several reasons for stressing this question:

1. It helps keep the analyst from jumping ahead.
2. It helps focus on identifying the next element in the cause–effect chain.
3. It is a reminder to only include the minimum sufficient causes necessary and nothing extraneous.

SS–SC Concept The SS–SC concept differentiates between the failure being "state-of-the-system" (SS) and "state-of-the-component" (SC). If a fault in the event box can be caused by a component failure, classify the event as an SC fault. If the fault cannot be caused by a component failure, classify the fault as an

SS fault. If the fault event is classified as SC, then the event will have an OR gate with P–S–C inputs. If the fault event is classified as SS, then the event will be further developed using I–N–S logic to determine the inputs and gate type.

P–S–C Concept This concept involves answering the question "What are the primary (P), secondary (S), and command (C) causes of the event?" The P–S–C question forces the analyst to focus on specific causal factors. The rationale behind this question is that every component fault event has only three ways of failing: a primary failure mode, a secondary failure mode, or a command path fault. Figure 11.8 demonstrates this concept. An added benefit of this concept is that if more than two of the three elements of P–S–C are present, then an OR gate is automatically indicated.

Figure 11.8 depicts how a system element is subdivided into primary, secondary, and command events for the FT structure. Two types of system events exist—those that are intended and those that are not intended. The intended events follow the desired intended mode of system operation, while the command path faults follow the undesired modes of operation.

A primary failure is the inherent failure of a system element (e.g., a resistor fails open). The primary failure is developed only to the point where identifiable internal component failures will directly cause the fault event. The failure of one component is presumed to be unrelated to the failure of any other component (i.e., independent).

A secondary failure is the result of external forces on the component (e.g., a resistor fails open due to excessive external heat exposure). Development of the secondary failure event requires a thorough knowledge of all external influences affecting system components (e.g., excessive heat, vibration, EMI, etc.). The failure of one

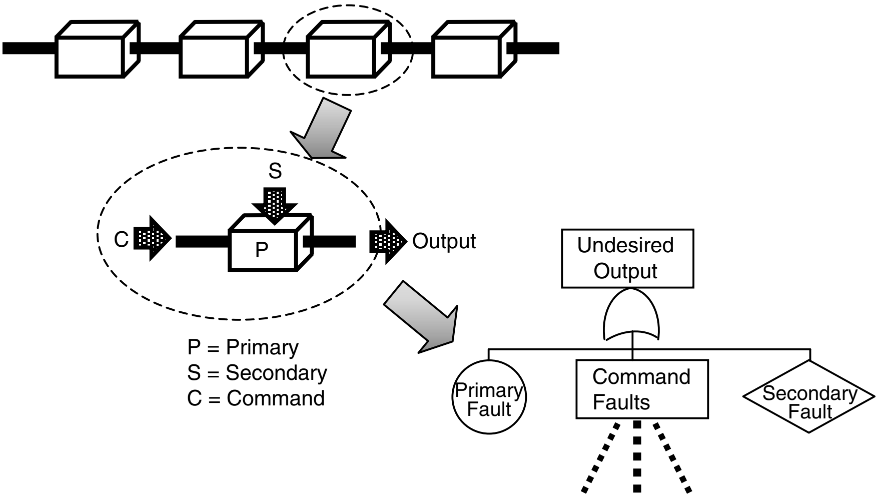


Figure 11.8 *P–S–C concept.*

component may be related to the failure of other components (i.e., dependent). This type of component failure is due to any cause other than its own primary failure.

A command failure is an expected, or intended, event that occurs at an undesired time due to specific failures. For example, missile launch is an intended event at a certain point in the mission. However, this event can be "commanded" to occur prematurely by certain failures in the missile arm and fire functions. Failures and faults in this chain of events are referred to as the *command path* faults.

The command path is a chain of events delineating the path of command failure events through the system. Analysis of command path events creates an orderly and logical manner of fault identification at each level of the FT. A path of command events through the FT corresponds to the signal flow through the system. In developing command events, the question "what downstream event commands the event to occur?" is asked for each event being analyzed. At the finish of each FT branch, the command path will terminate in primary and/or secondary events.

Note that the command path is primarily a guideline for analysis of fault event development through a system. Once an analysis is completed, comparison between the FT and the system signal flow diagram will show that the FT command path represents the signal flow through the system along a single thread.

For another example of a command path fault, consider a relay. When the relay coil is energized, the relay contacts will automatically close, as designed and intended. If a failure down stream of the relay provides inadvertent power to the relay coil, then the closing of the relay contacts is considered as a "command" failure. The relay operates as normally intended, except at the wrong time.

11.5.4 Construction—Advanced

As previously mentioned, FT building is a repetitive process. Figure 11.9 displays this iterative process; for every logic gate on the FT, the same set of three questions is asked: I–N–S, P–S–C, and SS–SC.

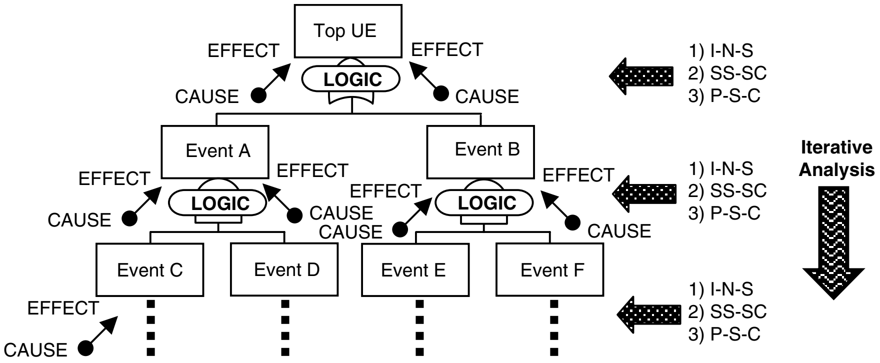


Figure 11.9 *FT building steps.*

Answering these questions provides the gate input events and the gate logic involved. As can be seen from this diagram, as the iterative analysis proceeds downward, the cause–effect relationships are linked in an upward manner.

The basic steps to follow when constructing the FT include:

1. Review and understand the fault event under investigation.
2. Identify all the possible causes of this event via the questions:
   a. Immediate, necessary, and sufficient?
   b. State of component or state of system?
   c. Primary, secondary, and command?
3. Identify the relationship or logic of the cause–effect events.
4. Structure the tree with the identified gate input events and gate logic.
5. Double check logic to ensure that a jump in logic has not occurred.
6. Keep looking back to ensure identified events are not repeated.
7. Repeat for next fault event (i.e., gate).

Some critical items to remember while performing this process:

1. When possible, start analyzing in the design at the point where the undesired event occurs.
2. Work backward (through the system) along signal or logic flow.
3. Keep node wording clear, precise, and complete.
4. Check to ensure all text boxes have unique text, no repeated text.
5. Ensure you do not jump ahead of a possible fault event.
6. Look for component or fault event transition states (e.g., “no output signal from component A,” “no input fluid to valve V1”).

11.5.5 Construction Rules

Some basic rules for FT construction and development include:

1. Complete basic required data for each FT node (node type, node name, and text).
2. Give every node a unique identifying name.
3. No gate-to-gate connections are allowed (always have text box).
4. Always place relevant text in text box; never leave it blank.
5. State event fault state exactly and precisely; use state transition wording.
6. Complete the definition of all inputs to a gate before proceeding.
7. Keep events on their relative level for clarity.
8. Use meaningful naming convention.

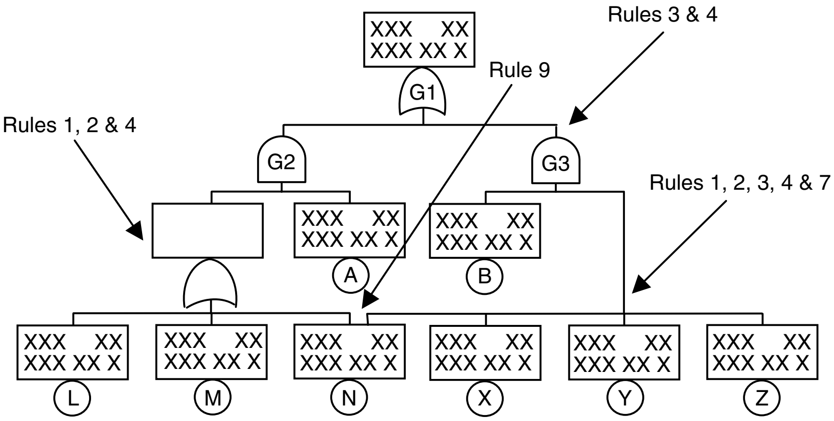


Figure 11.10 *FT construction errors.*

9. Do not draw lines from two gates to a single input (use the MOE methodology).
10. Assume no miracles (i.e., miraculous component failure blocks other failures from causing UE).
11. I–N–S, P–S–C, and SS–SC are analysis concepts; do not use these words in text boxes.

Figure 11.10 demonstrates some typical violations of the FT construction rules. Violation of these rules creates many problems. For example, if a text box is missing or has no text in it, no one reading the FT will be able to understand the logic involved.

11.6 FUNCTIONAL BLOCK DIAGRAMS

When constructing FTs, an important concept to remember is the use of functional block diagrams (FBDs). The FBD presents a simplified representation of the system design and operation for clarity and understanding. It shows the subsystem interfaces and the component relationships. The FBD shows the functions that must be performed by the system for successful operation, thereby also indicating potential modes of faulty operation. When constructing an FT it is often much easier to work from an FBD than from a large complex electrical schematic. A general rule of thumb is: *If an analyst cannot draw an FBD of the system being analyzed, then the analyst may not fully understand the system design and operation.* As shown in Figure 11.11, in many cases the FBD forms the levels and events directly for the FTA.

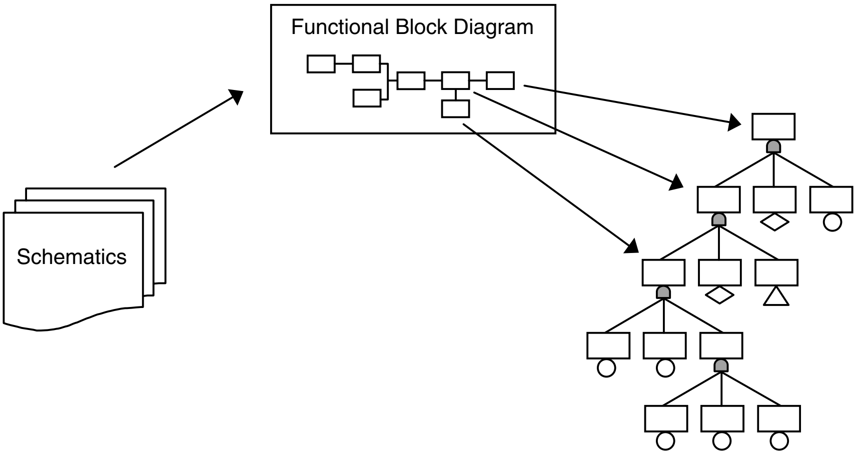


Figure 11.11 *Use of functional block diagrams.*

11.7 CUT SETS

Cut sets (CS) are one of the key products from FTA. They identify the component failures and/or event combinations that can cause the top UE to occur. CSs also provide one mechanism for probability calculations. Essentially, CSs reveal the critical and weak links in a system design by identifying safety problem components, high probability CS, and where intended safety or redundancy features have been bypassed.

Figure 11.12 shows an example FT with its resulting CSs listed on the right. Per the definition of a CS, each of these CSs can cause the top UE to occur. CSs are generated through the rules of Boolean algebra, and many different algorithms exist for generating CSs.

In general, the following observations regarding CS tend to hold true:

1. A low-order CS indicates high safety vulnerability. A single-order CS (i.e., a single-point failure) tends to cause the greatest risk.

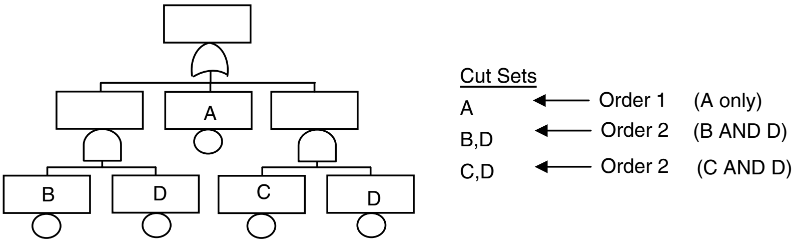


Figure 11.12 *Example FT cut sets.*

2. A high-order CS indicates low safety vulnerability. A high-order CS (e.g., a five-input AND gate) tends to have a comparatively small probability and therefore presents less system risk.
3. For a large total number of CS the analyst needs to evaluate the collective risk on the top UE. This is because all of the CS added together might reach an unacceptable value.

11.8 MOCUS ALGORITHM

One of the most common FT algorithms for generating CSs is the MOCUS (method of obtaining cut sets) algorithm, developed by J. Fussell and W. Vesely [1]. This is an effective top-down gate substitution methodology for generating CSs from an FT. MOCUS is based on the observation that AND gates increase number of elements in a CS and that OR gates increase the number of CSs.

The basic steps in the MOCUS algorithm are as follows:

1. Name or number all gates and events.
2. Place the uppermost gate name in the first row of a matrix.
3. Replace top gate with its inputs, using notation of:
   a. Replace an AND gate with its inputs, each input separated by a comma.
   b. Replace an OR gate by vertical arrangement, creating a new line for each input.
4. Reiteratively substitute and replace each gate with its inputs, moving down the FT.
5. When only basic inputs remain in the matrix, the substitution process is complete and the list of all cut sets has been estblished.
6. Remove all nonminimal CSs and duplicate CSs from the list using the laws of Boolean algebra.
7. The final list contains the minimal cut sets.

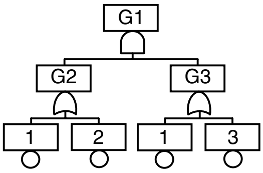
Figure 11.13 provides an example of applying the MOCUS algorithm to an FT. Figure 11.14 provides an example of applying the MOCUS algorithm to an FT using a modified technique.

11.9 BOTTOM-UP ALGORITHM

Another CS generation algorithm is the bottom-up algorithm, which is just the reverse of the MOCUS algorithm. Figure 11.15 shows how the algorithm works on the same FT used in Figure 11.14. Note that the results are identical for the two methods.

1	2	3	4	5	6
G1	G2, G3	1, G3	1, 1	1	1
			1, 3	1, 3	
		2, G3	2, 1	1, 2	
			2, 3	2, 3	2, 3

All CS MinCS



Steps:
1. Enter top gate name.
2. Replace G1 with its inputs, G1 and G2.
3. Replace G2 with its inputs, 1 and 2.
4. Replace G3 with its inputs, 1 and 3.
5. These are the total CSs, some are nonminimal.
6. Eliminate nonminimal CSs.

Figure 11.13 *MOCUS Example 1.*

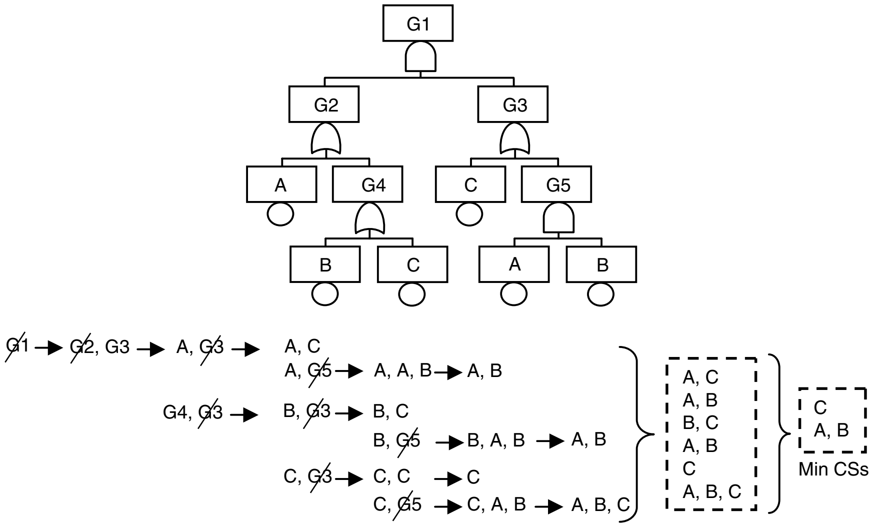

G1
G2
G3
A
G4
C
G5
B
C
A
B
~~G1~~ → ~~G2~~, G3 → A, ~~G3~~ →
A, C
A, ~~G5~~ → A, A, B → A, B
G4, ~~G3~~ →
B, ~~G3~~ → B, C
B, ~~G5~~ → B, A, B → A, B
C, ~~G3~~ → C, C → C
C, ~~G5~~ → C, A, B → A, B, C
A, C
A, B
B, C
A, B
C
A, B, C
C
A, B
Min CSs

Figure 11.14 *MOCUS Example 2.*

$$G5 = A \bullet B = AB$$
$$G3 = C + G5 = C + AB$$
$$G4 = B + C$$
$$G2 = A + G4 = A + B + C$$
$$\begin{aligned} G1 &= G2 \bullet G3 \\ &= (A + B + C)\,(C + AB) \\ &= AC + AAB + BC + BAB + CC + CAB \\ &= AC + AB + BC + AB + C + ABC \\ &= C + AC + BC + AB + ABC \\ &= C + AB \end{aligned}$$

Figure 11.15 *Example using bottom-up method.*

11.10 MATHEMATICS

Fault tree mathematics are based on Boolean algebra, probability theory, and reliability theory. The following are some definitions for mathematical terms frequently encountered in FTA.

Probability of success. Reliability (R) of a component, which is calculated by $R = e^{-\lambda T}$, where $\lambda =$ component failure rate and $T =$ component exposure time. Also, $\lambda = 1/\text{MTBF}$, where MTBF is the mean time between failure.

Probability of failure. Unreliability (Q) is the probability of failure of a component, where:

$$R + Q = 1 \quad \text{and} \quad Q = 1 - R = 1 - e^{-\lambda T}$$

When $\lambda T < 0.001$ then $Q \approx \lambda T$, which is a useful approximation for hand calculations. In safety work, Q is referred to as P, for probability of failure. Note that the longer the mission (or exposure time) the higher the probability of failure, and the smaller the failure rate the lower the probability of failure.

Boolean rules for FTA. The following Boolean laws apply directly to FTA for the reduction of CS to their minimum components. These rules are required for reducing trees with MOEs in them.

$$\begin{aligned} a \bullet a &= a \\ a + a &= a \\ a + ab &= a \\ a(a + b) &= a \end{aligned}$$

AND gate probability expansion. The probability for an AND gate is

$$P = P_A P_B P_C P_D P_E, \ldots, P_N$$

where N is equal to the number of inputs to the gate.

OR gate probability expansion. Probability for an OR gate is

$$\begin{aligned} P = &\left(\sum \text{1st terms}\right) - \left(\sum \text{2nd terms}\right) + \left(\sum \text{3rd terms}\right) \\ &- \left(\sum \text{4th terms}\right) + \left(\sum \text{5th terms}\right) - \left(\sum \text{6th terms}\right), \ldots, \\ P = &(P_A + P_B + P_C) - (P_{AB} + P_{AC} + P_{BC}) + (P_{ABC}) \\ &\gg \text{example for 3-input AND gate} \end{aligned}$$

FT probability expansion. The Boolean equation for an entire FT is all of the cut sets ORed together. This means that the probability calculation is the OR expansion formula for all of the CS.

$$\begin{aligned}\mathrm{CS} = \{&\mathrm{CS1}; \mathrm{CS2}; \mathrm{CS3}; \mathrm{CS4}; \mathrm{CS5}; \mathrm{CS6}; \mathrm{CS7}; \mathrm{CS8}; \mathrm{CS9}; \mathrm{CS10};\\ &\mathrm{CS11}; \mathrm{CS12}; \mathrm{CS13}; \mathrm{CS14}; \ldots\}\end{aligned}$$

$$\begin{aligned}P = &\left(\sum \text{1st terms}\right) - \left(\sum \text{2nd terms}\right) + \left(\sum \text{3rd terms}\right)\\ &- \left(\sum \text{4th terms}\right) + \left(\sum \text{5th terms}\right) - \left(\sum \text{6th terms}\right), \ldots,\end{aligned}$$

$$\begin{aligned}P = &(P_{\mathrm{CS1}} + P_{\mathrm{CS2}} + \cdots) - (P_{\mathrm{CS1}} \bullet P_{\mathrm{CS2}} + P_{\mathrm{CS1}} \bullet P_{\mathrm{CS3}} + \cdots)\\ &+ (P_{\mathrm{CS1}} \bullet P_{\mathrm{CS2}} \bullet P_{\mathrm{CS3}} + P_{\mathrm{CS1}} \bullet P_{\mathrm{CS2}} \bullet P_{\mathrm{CS4}} + \cdots) - \cdots\end{aligned}$$

Inclusion–exclusion approximation. Most FTs have a large number of CSs. Formulating the exact equation for a large number of cut sets would result in an unwieldy equation, even for a computer. The inclusion–exclusion approximation method has been developed to resolve this numerical problem. This approximation says that the first term in the OR gate expansion is the upper bound probability for the tree. This means the true probability will be no worse than this value. The first and second terms together compute the lower bound tree probability. This means the true probability will be no better than this value. And, as successive terms are added to the computation, the tree probability approaches the exact calculation.

Figure 11.16 shows the OR gate expansion formula along with the "terms" in the formula for just four CSs.

Figure 11.17 shows how by including each successive term in the calculation the probability will approach the exact probability.

11.11 PROBABILITY

The top FT probability is a general term for the probability calculated for the top undesired event. The top event probability is calculated from the FT using the probabilities that are input for the basic events, in terms of a failure rate and exposure time or a straight probability. Depending on the specific top event definition, the

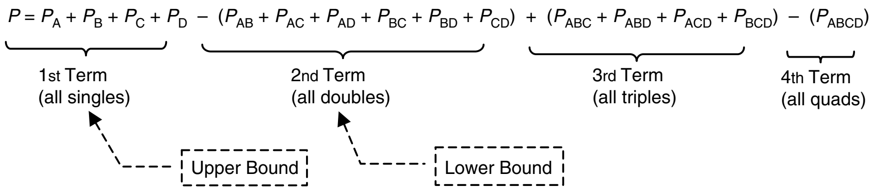

$P = P_A + P_B + P_C + P_D - (P_{AB} + P_{AC} + P_{AD} + P_{BC} + P_{BD} + P_{CD}) + (P_{ABC} + P_{ABD} + P_{ACD} + P_{BCD}) - (P_{ABCD})$
1st Term (all singles)
2nd Term (all doubles)
3rd Term (all triples)
4th Term (all quads)
Upper Bound
Lower Bound

Figure 11.16 *OR gate expansion formula.*

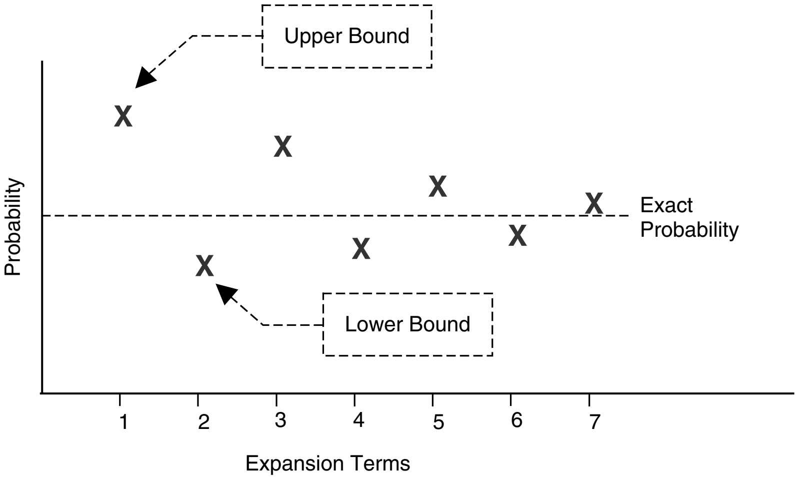


Figure 11.17 *First and second terms bound the tree probability.*

top event probability can be the probability of the top event occurring during a mission, the probability of the top event occurring in a given period of time, a pure probability number for the top event, or the top event unavailability.

A gate probability is sometimes called an intermediate event probability since it is calculated for an intermediate event below the FT top event. The gate acts like a top event for the branch of FT below it. Analysis of intermediate gate event probabilities is sometimes useful during FTA. Whatever method is used to calculate gate probabilities (top-down or bottom-up), if MOEs are not correctly mathematically accounted for (i.e., resolved) the final results can be erroneous.

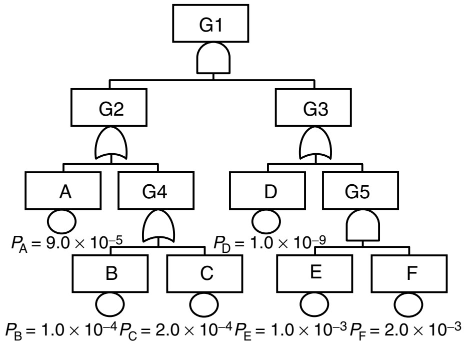
There are several different methods to compute the top FT probability. The most common approaches are the following:

1. Direct analytical calculation using the FT CSs
2. Bottom-up gate-to-gate calculation
3. Simulation

The direct analytical calculation using the FT CSs approach merely sums all of the CSs using the OR gate expansion explained above. When the number of CSs becomes very large, it becomes too time consuming and unwieldy to make an exact calculation, and the inclusion–exclusion approximation method explained above is then utilized.

The simulation method employees Monte Carlo techniques to simulate the random failure of events in the FT. Millions of trials are generally run, and then statistical calculations are made to compute the top FT probability.

The bottom-up gate-to-gate calculation method starts at the bottom of the FT and calculates each gate up the tree in a step-by-step process. Each gate is calculated


G1
G2
G3
A
G4
D
G5
$P_A = 9.0 \times 10^{-5}$
$P_D = 1.0 \times 10^{-9}$
B
C
E
F
$P_B = 1.0 \times 10^{-4}$
$P_C = 2.0 \times 10^{-4}$
$P_E = 1.0 \times 10^{-3}$
$P_F = 2.0 \times 10^{-3}$

$$P_{G4} = P_B + P_C - P_B P_C$$
$$P_{G4} = 1.0 \times 10^{-4} + 2.0 \times 10^{-4} - (1.7 \times 10^{-4})\ (2.1 \times 10^{-4})$$
$$P_{G4} = 3.0 \times 10{-4}$$

$$P_{G5} = P_E \bullet P_F$$
$$P_{G5} = 1.0 \times 10^{-3} + 2.0 \times 10^{-3}$$
$$P_{G5} = 2.0 \times 10^{-6}$$

$$P_{G2} = P_A + P_{G4} - P_A P_{G4}$$
$$P_{G2} = 9.0 \times 10^{-5} + 3.0 \times 10^{-6} - (1.7 \times 10^{-6})\ (3.0 \times 10^{-6})$$
$$P_{G2} = 3.9 \times 10^{-4}$$

$$P_{G3} = PD + PG5 - PDPG5$$
$$P_{G3} = 1.0 \times 10^{-9} + 2.0 \times 10^{-6} - (1.7 \times 10^{-9})\ (2.0 \times 10^{-6})$$
$$P_{G3} = 2.0 \times 10^{-6}$$

$$P_{G1} = P_{G2} \bullet P_{G3}$$
$$P_{G1} = 3.9 \times 10^{-4} + 2.0 \times 10^{-6}$$
$$P_{G1} = 7.8 \times 10^{-10}$$

Figure 11.18 *Example bottom-up gate to gate calculation.*

using the appropriate gate probability formula. A lower level gate calculation is used as an input value to a higher level gate. There is one important caution with this technique, if the FT contains MOEs or MOBs the calculation will be incorrect unless the MOEs and MOBs are correctly accounted for (i.e., Boolean reduction), which usually means falling back on the CS calculation. An example bottom-up gate-to-gate calculation is shown in Figure 11.18.

11.12 IMPORTANCE MEASURES

One of the most important outputs of an FTA is the set of importance measures that are calculated for the FT events and CSs. Importance measures help to identify weak links in the system design and the components that will provide the most cost-effective mitigation. The FT importance measures establish the significance for all the events in the fault tree in terms of their contributions to the FT top event probability. Both intermediate gate events as well as basic events can be prioritized according to their importance. Top event importance measures can also be calculated that give the sensitivity of the top event probability to an increase or decrease in the probability of any event in the fault tree. Both absolute and relative importance measures can be calculated.

What is often useful about the top event importance measures is that they generally show that relatively few events are important contributors to the top event probability. In many FTs, less than 20 percent of the basic events in the fault tree are important contributors, contributing more than 80 to 90 percent of the top event probability. Moreover, the importance measures of events in the FT generally cluster in groups that differ by orders of magnitude from one another. In these cases, the importance measures are so dramatically different that they are generally not dependent on the preciseness of the data used in the FTA.

The FT top importance measures can be used to allocate program resources by identifying the significant areas for design improvement. Trade studies can be performed to show how much probability improvement can be achieved for various design change costs.

The basic importance measures that can be calculated for each event in the FT are:

Cut set (CS) importance. Evaluates the contribution of each min CS to the FT top event probability. This importance measure provides a method for ranking the impact of each CS. The CS importance is calculated by calculating the ratio of the CS probability to the overall FT top probability. The calculation is performed as follows:

Given the Following Min Cut Sets

2
2, 3
2, 4 $\ggg$ $I_{2,4} = (P_2 \bullet P_4)/P_{\mathrm{TOP}}$ (for cut set 2, 4)
7
8, 9

Fussell–Vesely (FV) importance. Evaluates the contribution of each event to the FT top event probability. This importance measure is sometimes called the *top contribution importanc*e. Both the absolute and the relative FV importance are determinable for every event modeled in the fault tree, not only for the basic events, but for every higher level event and contributor as well. This provides a numerical significance of all the fault tree elements and allows them to be prioritized. The FV importance is calculated by summing all of the minimal cut sets (causes) of the top event involving the particular event and calculating the ration to the top FT probability. The calculation is performed as follows:

Given the Following Min Cut Sets

2 $\ggg$
2, 3 $\ggg$ $I_2 = [(P_2) + (P_2 \bullet P_3)\ (P_2 \bullet P_4)]/\mathrm{P_{TOP}}$ (for event 2)
2, 4 $\ggg$
7
8, 9

Risk Reduction Worth (RRW). Evaluates the decrease in the probability of the top event if a given event is assured not to occur. This importance measure can also be called the *top decrease sensitivity.* This measure is related to the previous FV importance. The RRW for a basic event shows the decrease in the probability of the top event that would be obtained if the lower level event (i.e., the failure) did not occur. It thus gives the maximum reduction in the top probability for the upgrade of an item. Both the absolute value and relative value of the RRW are determinable for every event and contributor modeled in the fault tree. The RRW is normally calculated by requantifying the fault tree or the minimum cut sets with the probability of the given event set to 0.0. This calculation and that for risk achievement worth and Birnbaum's importance measure (below) are similar to a partial derivative, in that all other event probabilities are held constant.

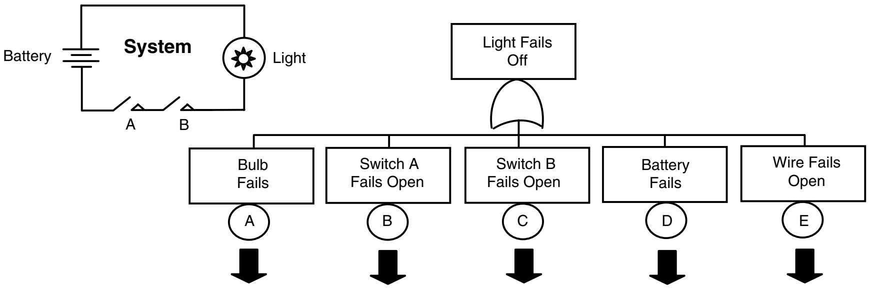
Risk Achievement Worth (RAW). Evaluates the increase in the top event probability if a given event occurs. This importance measure can also be called the *top increase sensitivity.* The RAW shows where prevention activities should be focused to assure failures do not occur. Since the failures with the largest RAW have the largest system impacts, these are the failures that should be prevented. The RAW also shows the most significant events for contingency planning. Both the absolute and relative RAW are obtainable for every event and contributor modeled in the fault tree. The RAW is normally calculated by requantifying the fault tree or the minimum cut sets with the probability of the given event set to 1.0.

Birnbaum's importance measure (BB). Evaluates the rate of change in the top event probability as a result of the change in the probability of a given event. The BB measure is equivalent to a sensitivity analysis and can be calculated by first calculating the top event probability with the probability of the given event set to 1.0 and then subtracting the top event probability with the probability of the given event set to 0.0. Because of the way BB measure is formulated, it does not account for the probability of an event. BB is related to RAW and RRW; when these are expressed on an interval scale (absolute value), $\mathrm{BB} = \mathrm{RAW} + \mathrm{RRW}$.

The above importance and sensitivity measures can be calculated not only for the FT but also for its equivalent success tree. When applied to the success tree, the measures give the importance of an event not occurring. The top event is now the nonoccurrence of the undesired event, and each event is the event nonoccurrence. Therefore, when applied to an event in the success tree, the FV importance gives the contribution of the nonoccurrence of the event to the nonoccurrence of the top event. The RRW gives the decrease in the nonoccurrence probability of the top event if the event nonoccurrence probability were zero, that is, if the event did occur. The RAW gives the increase in the nonoccurrence probability of the top event if the nonoccurrence probability of the event were 1.0, that is, if the event were assured not to occur. The importance measures for the success tree give equivalent information as for the FT, but from a nonoccurrence, or success, standpoint.

11.13 EXAMPLE 1

Figure 11.19 is a summary example showing a sample system, with its corresponding FT, CS, and probability calculation.



Event A	Event B	Event C	Event D	Event E
$\lambda = 1.0 \times 10^{-6}$	$\lambda = 1.0 \times 10^{-7}$	$\lambda = 1.0 \times 10^{-7}$	$\lambda = 1.0 \times 10^{-8}$	$\lambda = 1.0 \times 10^{-9}$
$T = 2$ hr	$T = 2$ hr	$T = 2$ hr	$T = 2$ hr	$T = 2$ hr
$P = 2.0 \times 10^{-6}$	$P = 2.0 \times 10^{-7}$	$P = 2.0 \times 10^{-7}$	$P = 2.0 \times 10^{-8}$	$P = 2.0 \times 10^{-9}$

where $P = 1.0 - e^{-\lambda T} \approx \lambda T$

$$
\begin{aligned}
P = {} & P_A + P_B + P_C + P_D + P_E \\
& - (P_AP_B + P_AP_C + P_AP_D + P_AP_E + P_BP_C + P_BP_D + P_BP_E + P_CP_D + P_CP_E + P_DP_E) \\
& + (P_AP_BP_C + P_AP_BP_D + P_AP_BP_E + P_BP_CP_D + P_BP_CP_E + P_BP_DP_E + P_CP_DP_E) \\
& - (P_AP_BP_CP_D + P_AP_BP_CP_E + P_BP_CP_DP_E) \\
& + P_AP_BP_CP_DP_E
\end{aligned}
$$

$P = (2.0 \times 10^{-6}) + (2.0 \times 10^{-7}) + (2.0 \times 10^{-7}) + (2.0 \times 10^{-8}) + (2.0 \times 10^{-9})$ [upper bound only]

$P = 2.422 \times 10^{-6}$

CUT SETS
A
B
C
D
E

Figure 11.19 *Example FT with CS and probability calculation.*

11.14 EXAMPLE 2

Figure 11.20 is a example fire and arming circuit for a missile system, simplified for the purpose of demonstrating FT construction. This figure shows a basic electrical diagram of the functions for this system. Note that this example is a contrived and simplified system for purposes of demonstrating FT construction. The purpose of this example is to demonstrate construction and evaluation of a proactive-type FTA that is performed during system design.

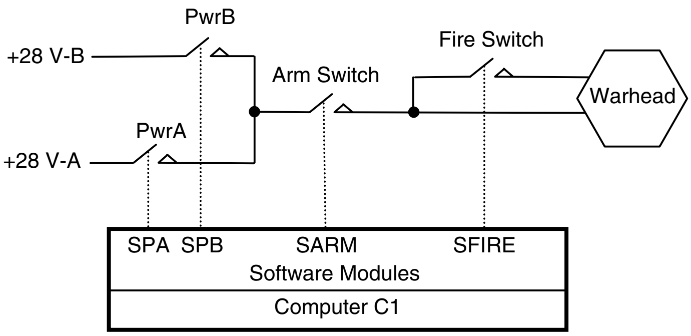


Figure 11.20 *Example missile arm–fire system.*

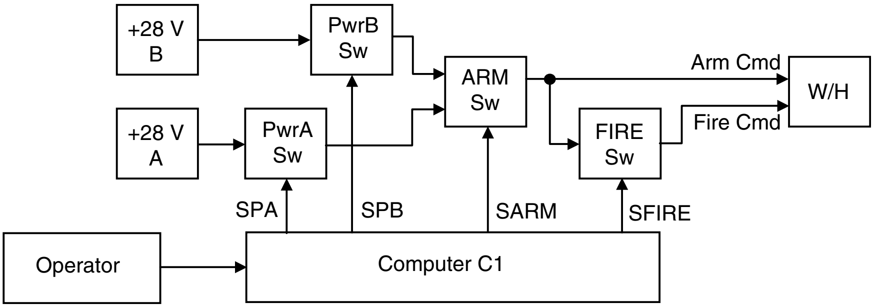


Figure 11.21 *System FBD.*

Simplifying detailed circuits into block diagrams aids the FTA construction process significantly. Figure 11.21 shows the functional block diagram (FBD) for the example missile arm–fire system circuit.

Figure 11.22 demonstrates the FT construction process by developing the first three levels of the FT from the FBD. The FTA begins at the warhead and progresses backward down the command path of the system.

In Figure 11.22 the top-level construction of the FT is depicted through steps 1, 2, and 3. These steps are explained as follows:

Step 1 In step 1 the FT analysis begins where the UE begins, at the missile warhead. When asking what could cause inadvertent warhead ignition, examine the inputs to the warhead (and ignoring the internals to the warhead itself). In this case there are two input signals, warhead arm and warhead fire commands. The I–N–S causes of warhead ignition are (a) warhead arm signal present AND (b) warhead fire signal present. This is a state-of-the-system fault event requiring an AND gate.

Step 2 Step 2 evaluates the fault event “arm signal at warhead input.” The question that must be answered is: What is I–N–S to provide an arm signal to the warhead? This step involves tracing the arm signal backwards to its source. The arm signal could be inadvertently provided (command fault) from the arm switch, or there could be a wire short to +28 VDC in the wiring. This is a state-of-the-system fault event requiring an OR gate.

Step 3 Step 3 evaluates the fault event “power is output from the arm switch.” The question that must be answered is: What is I–N–S to provide power output from the arm switch? Examination of the arm switch diagram shows that it has two power inputs, an input command that opens or closes the switch. This means that power can only be output when (a) power is present at the input of the arm switch an (b) when the arm switch is closed. This is a state-of-the-system fault event requiring an AND gate.

Step 4 (not shown in the figure) Step 4 evaluates the fault event “arm switch is closed.” The question that must be answered is: What is I–N–S to cause the arm switch to close. This is a state-of-the-component fault event requiring an OR gate because the analysis is at a component level. There are three ways a component can fail: primary, secondary, and command (P–S–C). If each of these ways is feasible, they are enumerated under the OR gate. The command fault would be expanded as the next step in the analysis.

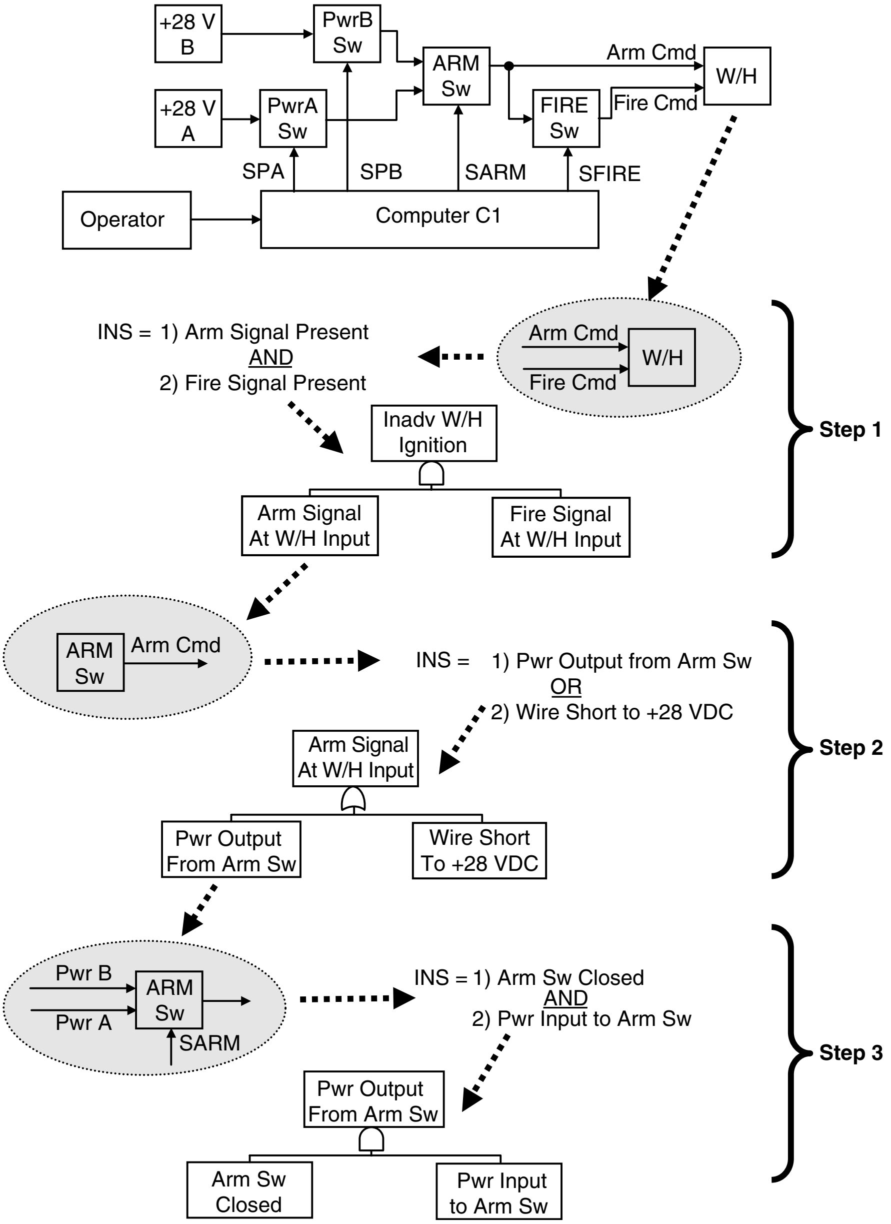


Figure 11.22 *System FBD and start of FT.*

The FT for this system is shown in Figures 11.23(*a–c*). The three FT sections constructed in Figure 11.22 are combined together, and the rest of the FT is then completed.

After the FT is constructed, failure data must be collected for the components in the FT. Table 11.1 contains the failure data for the example missile system. This data is used in the FT probability calculation. Note that since this is a small and simple FT, a very simple node naming convention is used whereby the first letter represents a specific node type, as follows:

X: represent primary failures (circles)

Z: represents secondary failures (diamonds)

H: represents normal events (houses)

G: represents a gate event

Table 11.2 contains the list of minimum CSs generated from the FT. Each CS is shown with the probability just for that CS. In this table the CSs are ordered by probability. Note that this FT yields 216 CSs for just 22 components in the FT. The CS list shows that there are no CSs of order 1 (i.e., SPF). It also shows that there are 2 CSs of order 2 and 205 CSs of order 3.

The computed top probability for this FT is $P = 5.142 \times 10^{-6}$. As a quick check, by mentally summing the probability of the top probability CSs and comparing that value to the FT probability, this overall FT probability looks reasonable.

Note that some 3-order CSs have a higher probability than some of the 2-order CSs. But, closer examination shows that many of these 3-order CSs have a house in them with $P = 1.0$, thus making them 2-order CSs.

Figure 11.24 is an FT of the CS with the highest probability (CS-1). This CS-1 FT displays the basic events involved and the path taken to the top of the FT. The important item to note from this CS-1 FT is that contrary to the CS list, there is a SPF in the FT. CS-1 involves events Z10 AND H1. But, since the house event H1 is a normal event with probability equal to 1.0, it does not count as a failure. Therefore, only event Z10 is necessary and sufficient to cause the top undesired event. Another important item to note from this FT is that event Z10 is an MOE, which occurs on both sides of an AND gate, thereby effectively bypassing intended system redundancy. Note also from the CS list that some 3-order CSs have a higher probability than 2-order CSs. This short CS analysis demonstrates that it is important to fully evaluate each CS.

11.15 EXAMPLE 3

This example involves a reactive-type FTA that is performed after the undesired event has already occurred. This example shows how to use the evidence event gate (EEG) when performing an FTA for an accident investigation. Figure 11.25 shows the EEG definition. As the FT is developed downward, fault event B is

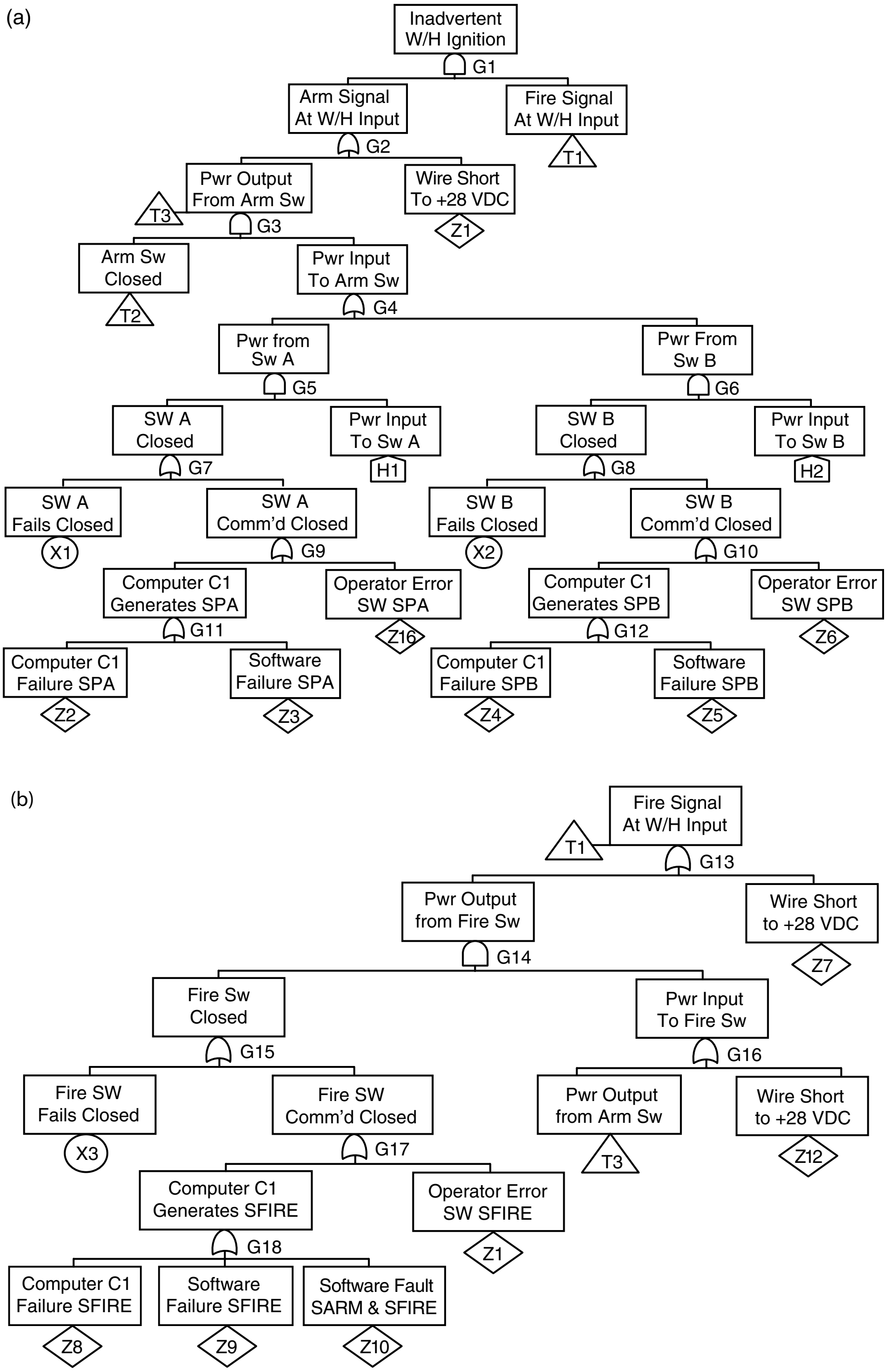


Figure 11.23 *(a) Inadvertent warhead ignition FT. (b) FT branch T1. (c) FT branch T2.*

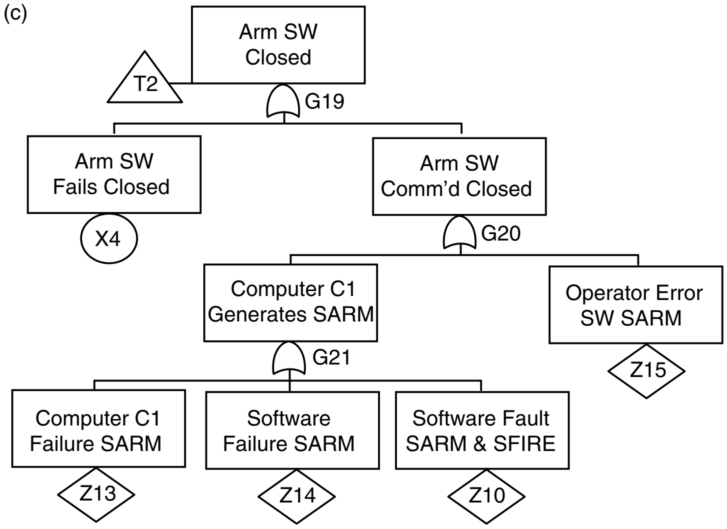


Figure 11.23 Continued.

TABLE 11.1 Basic Event Data

Name	Lambda	ET[a]	Prob	Text	Notes
X1	1.100×10^{-5}	10		Switch A fails closed	
X2	1.100×10^{-5}	10		Switch B fails closed	
X3	1.100×10^{-5}	10		Fire switch fails closed	
X4	1.100×10^{-5}	10		Arm switch fails closed	
Z1	1.100×10^{-9}	10		Wire short arm wire to +28 VDC	
Z2	1.100×10^{-7}	10		Computer C1 failure SPA	
Z3	1.100×10^{-7}	10		Software failure SPA	
Z4	1.100×10^{-7}	10		Computer C1 failure SPB	
Z5	1.100×10^{-7}	10		Software failure SPB	
Z6	1.100×10^{-4}	10		Operator error switch SPB	
Z7	1.100×10^{-9}	10		Wire short to +28 VDC	
Z8	1.100×10^{-7}	10		Computer C1 failure SFIRE	
Z9	1.100×10^{-7}	10		Software failure SFIRE	
Z10	1.100×10^{-7}	10		Software fault SARM & SFIRE	MOE
Z11	1.100×10^{-4}	10		Operator error switch SFIRE	
Z12	1.100×10^{-9}	10		Wire short to +28 VDC	
Z13	1.100×10^{-7}	10		Computer C1 failure SARM	
Z14	1.100×10^{-7}	10		Software failure SARM	
Z15	1.100×10^{-4}	10		Operator error switch SARM	
Z16	1.100×10^{-4}	10		Operator error switch SPA	
H1			1.0	Power input to switch A	
H2			1.0	Power input to switch B	

[a] ET, exposure time.

TABLE 11.2 FT Cut Sets

1	1.10×10^{-6}	H1	Z10	
2	1.10×10^{-6}	H2	Z10	
3	1.21×10^{-6}	H1	Z11	Z15
4	1.21×10^{-6}	H2	Z11	Z15
5	1.21×10^{-7}	H1	X3	Z15
6	1.21×10^{-7}	H1	X4	Z11
7	1.21×10^{-7}	H2	X3	Z15
8	1.21×10^{-7}	H2	X4	Z11
9	1.21×10^{-8}	H1	X3	X4
10	1.21×10^{-8}	H2	X3	X4
11	1.21×10^{-9}	H1	Z11	Z13
12	1.21×10^{-9}	H1	Z11	Z14
13	1.21×10^{-9}	H1	Z15	Z8
14	1.21×10^{-9}	H1	Z15	Z9
15	1.21×10^{-9}	H2	Z11	Z13
16	1.21×10^{-9}	H2	Z11	Z14
17	1.21×10^{-9}	H2	Z15	Z8
18	1.21×10^{-9}	H2	Z15	Z9
19	1.21×10^{-9}	Z10	Z16	
20	1.21×10^{-9}	Z10	Z6	
21	1.33×10^{-9}	Z11	Z15	Z16
22	1.33×10^{-9}	Z11	Z15	Z6
23	1.21×10^{-10}	H1	X3	Z13
24	1.21×10^{-10}	H1	X3	Z14
25	1.21×10^{-10}	H1	X4	Z8
26	1.21×10^{-10}	H1	X4	Z9
27	1.21×10^{-10}	H2	X3	Z13
28	1.21×10^{-10}	H2	X3	Z14
29	1.21×10^{-10}	H2	X4	Z8
30	1.21×10^{-10}	H2	X4	Z9
31	1.21×10^{-10}	X1	Z10	
32	1.21×10^{-10}	X2	Z10	
33	1.33×10^{-10}	X1	Z11	Z15
34	1.33×10^{-10}	X2	Z11	Z15
35	1.33×10^{-10}	X3	Z15	Z16
36	1.33×10^{-10}	X3	Z15	Z6
37	1.33×10^{-10}	X4	Z11	Z16
38	1.33×10^{-10}	X4	Z11	Z6
39	1.21×10^{-11}	H1	Z15	Z7
40	1.21×10^{-11}	H2	Z15	Z7
41	1.33×10^{-11}	X1	X3	Z15
42	1.33×10^{-11}	X1	X4	Z11
43	1.33×10^{-11}	X2	X3	Z15
44	1.33×10^{-11}	X2	X4	Z11
45	1.33×10^{-11}	X3	X4	Z16
46	1.33×10^{-11}	X3	X4	Z6
47	1.21×10^{-12}	H1	X4	Z7
48	1.21×10^{-12}	H1	Z13	Z8
49	1.21×10^{-12}	H1	Z13	Z9
50	1.21×10^{-12}	H1	Z14	Z8
51	1.21×10^{-12}	H1	Z14	Z9
52	1.21×10^{-12}	H2	X4	Z7
53	1.21×10^{-12}	H2	Z13	Z8
54	1.21×10^{-12}	H2	Z13	Z9
55	1.21×10^{-12}	H2	Z14	Z8
56	1.21×10^{-12}	H2	Z14	Z9
57	1.21×10^{-12}	Z10	Z2	
58	1.21×10^{-12}	Z10	Z3	
59	1.21×10^{-12}	Z10	Z4	
60	1.21×10^{-12}	Z10	Z5	
61	1.33×10^{-12}	X1	X3	X4
62	1.33×10^{-12}	X2	X3	X4
63	1.33×10^{-12}	Z11	Z13	Z16
64	1.33×10^{-12}	Z11	Z13	Z6
65	1.33×10^{-12}	Z11	Z14	Z16
66	1.33×10^{-12}	Z11	Z14	Z6
67	1.33×10^{-12}	Z11	Z15	Z2
68	1.33×10^{-12}	Z11	Z15	Z3
69	1.33×10^{-12}	Z11	Z15	Z4
70	1.33×10^{-12}	Z11	Z15	Z5
71	1.33×10^{-12}	Z15	Z16	Z8
72	1.33×10^{-12}	Z15	Z16	Z9
73	1.33×10^{-12}	Z15	Z6	Z8
74	1.33×10^{-12}	Z15	Z6	Z9
75	1.33×10^{-13}	X1	Z11	Z13
76	1.33×10^{-13}	X1	Z11	Z14
77	1.33×10^{-13}	X1	Z15	Z8
78	1.33×10^{-13}	X1	Z15	Z9
79	1.33×10^{-13}	X2	Z11	Z13
80	1.33×10^{-13}	X2	Z11	Z14
81	1.33×10^{-13}	X2	Z15	Z8
82	1.33×10^{-13}	X2	Z15	Z9
83	1.33×10^{-13}	X3	Z13	Z16
84	1.33×10^{-13}	X3	Z13	Z6
85	1.33×10^{-13}	X3	Z14	Z16
86	1.33×10^{-13}	X3	Z14	Z6
87	1.33×10^{-13}	X3	Z15	Z2
88	1.33×10^{-13}	X3	Z15	Z3
89	1.33×10^{-13}	X3	Z15	Z4
90	1.33×10^{-13}	X3	Z15	Z5
91	1.33×10^{-13}	X4	Z11	Z2
92	1.33×10^{-13}	X4	Z11	Z3
93	1.33×10^{-13}	X4	Z11	Z4
94	1.33×10^{-13}	X4	Z11	Z5
95	1.33×10^{-13}	X4	Z16	Z8
96	1.33×10^{-13}	X4	Z16	Z9
97	1.33×10^{-13}	X4	Z6	Z8
98	1.33×10^{-13}	X4	Z6	Z9
99	1.21×10^{-14}	H1	Z13	Z7
100	1.21×10^{-14}	H1	Z14	Z7

(*continued*)

TABLE 11.2 *Continued*

101	1.21×10^{-14}	H2	Z13	Z7
102	1.21×10^{-14}	H2	Z14	Z7
103	1.33×10^{-14}	X1	X3	Z13
104	1.33×10^{-14}	X1	X3	Z14
105	1.33×10^{-14}	X1	X4	Z8
106	1.33×10^{-14}	X1	X4	Z9
107	1.33×10^{-14}	X2	X3	Z13
108	1.33×10^{-14}	X2	X3	Z14
109	1.33×10^{-14}	X2	X4	Z8
110	1.33×10^{-14}	X2	X4	Z9
111	1.33×10^{-14}	X3	X4	Z2
112	1.33×10^{-14}	X3	X4	Z3
113	1.33×10^{-14}	X3	X4	Z4
114	1.33×10^{-14}	X3	X4	Z5
115	1.33×10^{-14}	Z15	Z16	Z7
116	1.33×10^{-14}	Z15	Z6	Z7
117	1.33×10^{-15}	X1	Z15	Z7
118	1.33×10^{-15}	X2	Z15	Z7
119	1.33×10^{-15}	X4	Z16	Z7
120	1.33×10^{-15}	X4	Z6	Z7
121	1.33×10^{-15}	Z11	Z13	Z2
122	1.33×10^{-15}	Z11	Z13	Z3
123	1.33×10^{-15}	Z11	Z13	Z4
124	1.33×10^{-15}	Z11	Z13	Z5
125	1.33×10^{-15}	Z11	Z14	Z2
126	1.33×10^{-15}	Z11	Z14	Z3
127	1.33×10^{-15}	Z11	Z14	Z4
128	1.33×10^{-15}	Z11	Z14	Z5
129	1.33×10^{-15}	Z13	Z16	Z8
130	1.33×10^{-15}	Z13	Z16	Z9
131	1.33×10^{-15}	Z13	Z6	Z8
132	1.33×10^{-15}	Z13	Z6	Z9
133	1.33×10^{-15}	Z14	Z16	Z8
134	1.33×10^{-15}	Z14	Z16	Z9
135	1.33×10^{-15}	Z14	Z6	Z8
136	1.33×10^{-15}	Z14	Z6	Z9
137	1.33×10^{-15}	Z15	Z2	Z8
138	1.33×10^{-15}	Z15	Z2	Z9
139	1.33×10^{-15}	Z15	Z3	Z8
140	1.33×10^{-15}	Z15	Z3	Z9
141	1.33×10^{-15}	Z15	Z4	Z8
142	1.33×10^{-15}	Z15	Z4	Z9
143	1.33×10^{-15}	Z15	Z5	Z8
144	1.33×10^{-15}	Z15	Z5	Z9
145	1.21×10^{-16}	Z1	Z7	
146	1.33×10^{-16}	X1	X4	Z7
147	1.33×10^{-16}	X1	Z13	Z8
148	1.33×10^{-16}	X1	Z13	Z9
149	1.33×10^{-16}	X1	Z14	Z8
150	1.33×10^{-16}	X1	Z14	Z9
151	1.33×10^{-16}	X2	X4	Z7
152	1.33×10^{-16}	X2	Z13	Z8
153	1.33×10^{-16}	X2	Z13	Z9
154	1.33×10^{-16}	X2	Z14	Z8
155	1.33×10^{-16}	X2	Z14	Z9
156	1.33×10^{-16}	X3	Z13	Z2
157	1.33×10^{-16}	X3	Z13	Z3
158	1.33×10^{-16}	X3	Z13	Z4
159	1.33×10^{-16}	X3	Z13	Z5
160	1.33×10^{-16}	X3	Z14	Z2
161	1.33×10^{-16}	X3	Z14	Z3
162	1.33×10^{-16}	X3	Z14	Z4
163	1.33×10^{-16}	X3	Z14	Z5
164	1.33×10^{-16}	X4	Z2	Z8
165	1.33×10^{-16}	X4	Z2	Z9
166	1.33×10^{-16}	X4	Z3	Z8
167	1.33×10^{-16}	X4	Z3	Z9
168	1.33×10^{-16}	X4	Z4	Z8
169	1.33×10^{-16}	X4	Z4	Z9
170	1.33×10^{-16}	X4	Z5	Z8
171	1.33×10^{-16}	X4	Z5	Z9
172	1.33×10^{-17}	Z13	Z16	Z7
173	1.33×10^{-17}	Z13	Z6	Z7
174	1.33×10^{-17}	Z14	Z16	Z7
175	1.33×10^{-17}	Z14	Z6	Z7
176	1.33×10^{-17}	Z15	Z2	Z7
177	1.33×10^{-17}	Z15	Z3	Z7
178	1.33×10^{-17}	Z15	Z4	Z7
179	1.33×10^{-17}	Z15	Z5	Z7
180	1.33×10^{-18}	X1	Z13	Z7
181	1.33×10^{-18}	X1	Z14	Z7
182	1.33×10^{-18}	X2	Z13	Z7
183	1.33×10^{-18}	X2	Z14	Z7
184	1.33×10^{-18}	X4	Z2	Z7
185	1.33×10^{-18}	X4	Z3	Z7
186	1.33×10^{-18}	X4	Z4	Z7
187	1.33×10^{-18}	X4	Z5	Z7
188	1.33×10^{-18}	Z13	Z2	Z8
189	1.33×10^{-18}	Z13	Z2	Z9
190	1.33×10^{-18}	Z13	Z3	Z8
191	1.33×10^{-18}	Z13	Z3	Z9
192	1.33×10^{-18}	Z13	Z4	Z8
193	1.33×10^{-18}	Z13	Z4	Z9
194	1.33×10^{-18}	Z13	Z5	Z8
195	1.33×10^{-18}	Z13	Z5	Z9
196	1.33×10^{-18}	Z14	Z2	Z8
197	1.33×10^{-18}	Z14	Z2	Z9
198	1.33×10^{-18}	Z14	Z3	Z8
199	1.33×10^{-18}	Z14	Z3	Z9
200	1.33×10^{-18}	Z14	Z4	Z8
201	1.33×10^{-18}	Z14	Z4	Z9
202	1.33×10^{-18}	Z14	Z5	Z8
203	1.33×10^{-18}	Z14	Z5	Z9
204	1.33×10^{-19}	Z1	Z11	Z12

(*continued*)

TABLE 11.2 ***Continued***

205	1.33×10^{-20}	X3	Z1	Z12
206	1.33×10^{-20}	Z13	Z2	Z7
207	1.33×10^{-20}	Z13	Z3	Z7
208	1.33×10^{-20}	Z13	Z4	Z7
209	1.33×10^{-20}	Z13	Z5	Z7
210	1.33×10^{-20}	Z14	Z2	Z7
211	1.33×10^{-20}	Z14	Z3	Z7
212	1.33×10^{-20}	Z14	Z4	Z7
213	1.33×10^{-20}	Z14	Z5	Z7
214	1.33×10^{-22}	Z1	Z10	Z12
215	1.33×10^{-22}	Z1	Z12	Z8
216	1.33×10^{-22}	Z1	Z12	Z9

hypothesized as a possible cause of the accident. If there is data from the accident investigation indicating that event B did not happen, that evidence is stated in E, and event B is not developed further because it has been proven as a false cause. If evidence indicates that B did occur, then event B is analyzed further because it is a positive cause. This is a method for quickly following productive causal paths. Figure 11.26 shows an FTA of the *Titanic* sinking. This FT uses the EEG and shows where collected evidence can be utilized in the FTA. It should be noted that this type of FT with the EEG is a qualitative-type analysis not a quantitative-type analysis. Note in this FT that transfer events A and B would be further developed as a result of this analysis, however; the information is not available.

11.16 PHASE- AND TIME-DEPENDENT FTA

Typical FT quantification provides a single value for the probability of the top event for a system mission. This top event probability is not partitioned into contributions over different mission phases or time intervals. If the mission under consideration has different phases, which are reflected in the FT, then the top event probability obtained is the total probability for the mission. Similarly, if a system fault event is modeled over a time interval, then the top probability obtained is the total system failure probability over the time interval. In this case, individual probabilities for different segments of the time interval are not obtainable.

Most FT software cannot produce phase-dependent or time-dependent results. This is not the limitation of the fault tree model itself, but a limitation of the available software. Different mission phases can be modeled in an FT. Also, individual failure rates and time intervals can be provided for each component. However, typical FT software calculates the total probability only and does not have the capability of breaking the probability into more detailed contributions.

This limitation of FT software is not generally a problem because most applications only require a single mission probability. If phase-dependent or time-dependent results are desired, then there are two options:

1. Use specialized software that has the capability to perform these calculations.
2. Break the FT model into phase-dependent or time-dependent segments and then perform the calculations with standard FT software.

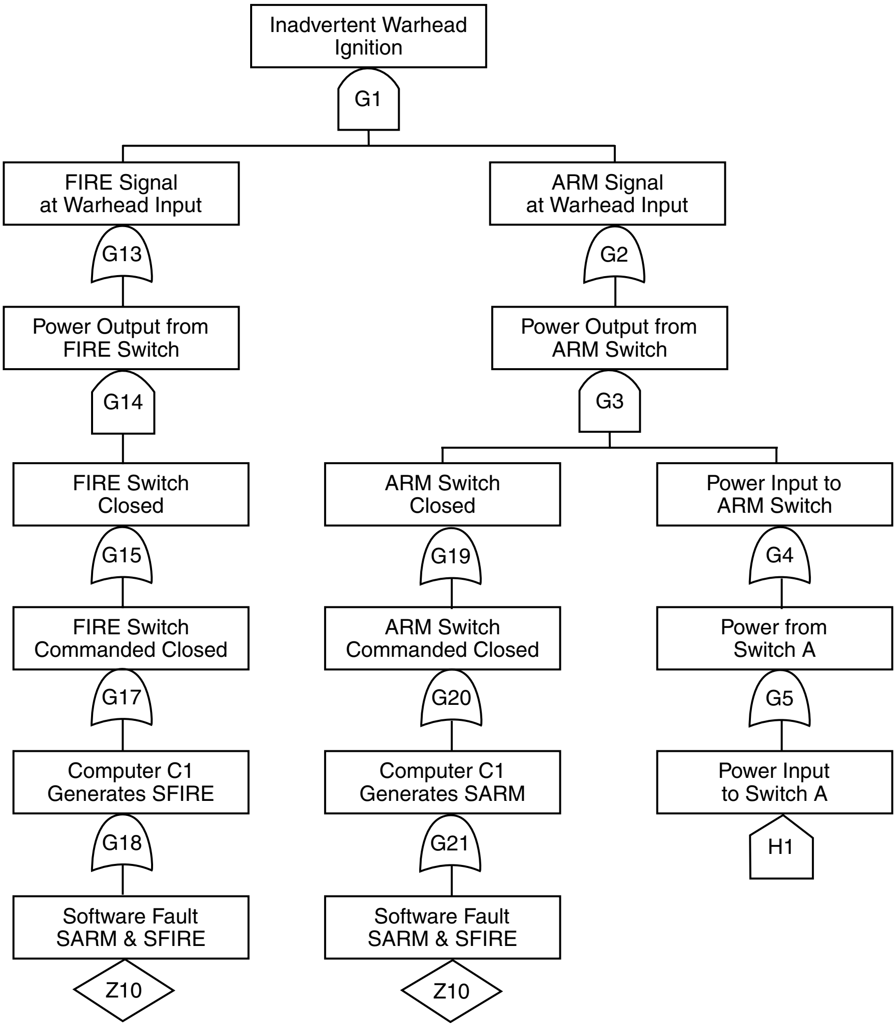

Inadvertent Warhead Ignition
G1
FIRE Signal at Warhead Input
G13
Power Output from FIRE Switch
G14
FIRE Switch Closed
G15
FIRE Switch Commanded Closed
G17
Computer C1 Generates SFIRE
G18
Software Fault SARM & SFIRE
Z10
ARM Signal at Warhead Input
G2
Power Output from ARM Switch
G3
ARM Switch Closed
G19
ARM Switch Commanded Closed
G20
Computer C1 Generates SARM
G21
Software Fault SARM & SFIRE
Z10
Power Input to ARM Switch
G4
Power from Switch A
G5
Power Input to Switch A
H1

Figure 11.24 *FT of highest probability CS.*

The second method involves modeling time dependence into the FT by dividing (partitioning) the top undesired event into smaller time segments. The top undesired event is divided into time interval events using an OR gate. This modeling technique is illustrated in Figure 11.27, whereby the top undesired event is divided into three mission phases, with each phase representing a different time interval.

In the mission-phased FT model the basic event occurrences, such as component failures, have been separated into more specific phased events. The OR gate is more correctly a mutually exclusive OR gate since the event cannot occur in both intervals 1, 2, and 3. If the FT software cannot handle mutually exclusive OR gates, then the

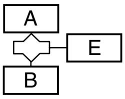
Symbol	GateType	Description
	Evidence Event	This gate does not show a logical combination, it is used to indicate that evidence is present to prove or disprove a particular path. Event B is developed only if evidence event E is true. Not used for a quantitative analysis.

Figure 11.25 *Evidence event gate definition.*

simple OR gate can be used provided the minimal cut sets can be scanned to remove any minimal cut sets that contain both of the events.

This approach is both tedious and tricky. It is tedious because the number of basic events in the FT is expanded and hence can greatly expand the number of minimal CSs that are generated. It is tricky because ORing the three phases together is not entirely correct and only provides an approximation. The reason it is not entirely correct is because cross-phase CSs are not accounted for. For example, say that the three-phase FT had only one CS comprised of A and B, as shown in Figure 11.28. Equation (1) in the figure shows the probability calculation for the single-phase FT. Equation (2) shows the calculation for the FT when the two phases are ORed together. Equation (3) shows the correct probability calculation, which must include the two additional cross-phase CSs (e.g., A fails in phase 1 and B fails in phase 2).

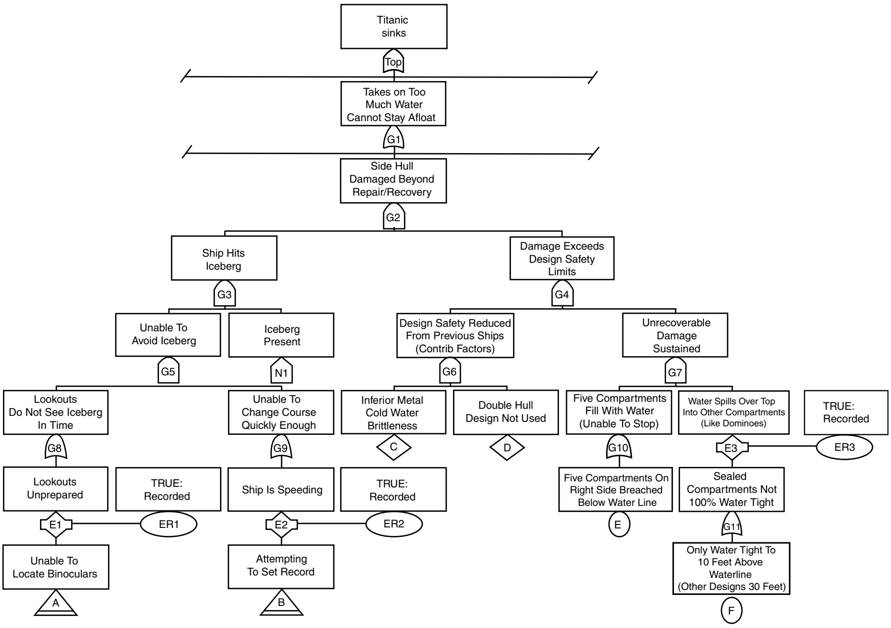

Titanic sinks
Top
Takes on Too Much Water Cannot Stay Afloat
G1
Side Hull Damaged Beyond Repair/Recovery
G2
Ship Hits Iceberg
G3
Damage Exceeds Design Safety Limits
G4
Unable To Avoid Iceberg
G5
Iceberg Present
N1
Design Safety Reduced From Previous Ships (Contrib Factors)
G6
Unrecoverable Damage Sustained
G7
Lookouts Do Not See Iceberg In Time
G8
Unable To Change Course Quickly Enough
G9
Inferior Metal Cold Water Brittleness
C
Double Hull Design Not Used
D
Five Compartments Fill With Water (Unable To Stop)
G10
Water Spills Over Top Into Other Compartments (Like Dominoes)
E3
TRUE: Recorded
ER3
Lookouts Unprepared
TRUE: Recorded
E1
ER1
Ship Is Speeding
TRUE: Recorded
E2
ER2
Five Compartments On Right Side Breached Below Water Line
E
Sealed Compartments Not 100% Water Tight
G11
Unable To Locate Binoculars
A
Attempting To Set Record
B
Only Water Tight To 10 Feet Above Waterline (Other Designs 30 Feet)
F

Figure 11.26 *FTA of Titanic sinking.*

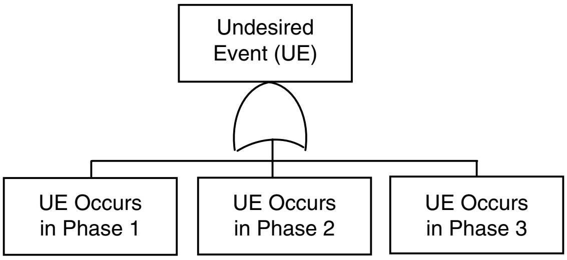
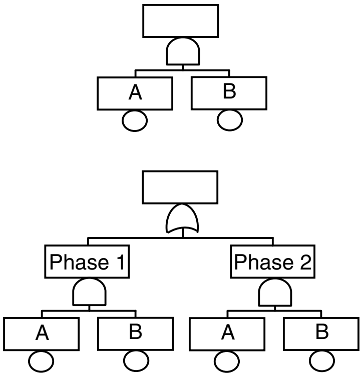


Figure 11.27 *Mission phased FT.*

11.17 DYNAMIC FTA

Dynamic fault tree (DFT) is an extension of the standard FT analysis methodology and was developed specifically for the analysis of computer-based systems. Two special gates are part of the DFT methodology, the functional dependency (FDEP) gate and the spares gate. The DFT methodology was developed to provide a means for combining FTA with Markov analysis for sequence-dependent problems. Markov chains are commonly used to assess the reliability and performance of fault-tolerant computer-based systems. Markov models have the advantage of easily modeling the sequence-dependent behavior that is typically associated with fault-tolerant systems. However, Markov models have the disadvantage of being large and cumbersome, and the generation of a Markov model for many systems can be tedious and error prone. Thus, DFT combines the best of both techniques.

Dynamic fault tree works well with sequence-dependent failures. For example, suppose a system uses two redundant components, one of which operates as the primary unit and the other serves as a standby backup in case the first fails. Also, suppose the design uses a switch to change to the backup when the primary fails. If the switch controller fails after the primary unit fails (and thus the standby spare is



$$P = A \bullet B \qquad \text{[Eq.1]}$$

$$P = A_1 \bullet B_1 + A_2 \bullet B_2 \qquad \text{[Eq.2]}$$

$$P = A_1 \bullet B_1 + A_2 \bullet B_2 + A_1 \bullet B_2 + A_2 \bullet B_1 \qquad \text{[Eq. 3]}$$

Figure 11.28 *Example of phased FT cut sets.*

already in use), the system can continue to operate. However, if the switch controller fails before the primary unit fails, then the standby spare unit cannot be switched into active operation, and the system fails when the primary unit fails. The order in which the primary and switch fail determines whether the system continues to operate, and thus the FT model is sequence dependent. The standard FT approach would be to model this situation using a priority AND gate. In standard FTA the priority AND gate mathematical calculation provides a very good approximation but not an exact answer.

If the inputs to a priority AND gate are not simple basic events (i.e., they are gate events), this calculation is more difficult and in general requires the solution of a set of integral equations or some approximations. The DFT methodology can relieve the analyst of the need to perform the calculation of the probability of the order of occurrence of the inputs to a priority AND gate. The DFT methodology automatically generates and solves the set of integral equations needed to solve the priority AND system via a built-in Markov algorithm.

Standard FT methodology will model everything that the DFT approach can model. The benefit of the DFT approach is that it provides increased accuracy in the final probability calculation. The disadvantage of DFT is that it is sometimes more difficult to understand the DFT model, and special software is required that can handle the special DFT gates. For further information on this approach see Ref. 2, 3, and 4.

11.18 ADVANTAGES AND DISADVANTAGES

The following are advantages of the FTA technique:

1. Structured, rigorous, and methodical approach.
2. A large portion of the work can be computerized.
3. Can be effectively performed on varying levels of design detail.
4. Visual model displays cause–effect relationships.
5. Relatively easy to learn, do, and follow.
6. Models complex system relationships in an understandable manner.
7. Follows fault paths across system boundaries.
8. Combines hardware, software, environment, and human interaction.
9. Permits probability assessment.
10. Scientifically sound; based on logic theory, probability theory, Boolean algebra, and reliability theory.
11. Commercial software is available.
12. FTs can provide value despite incomplete information.
13. A proven technique with many years of successful use.
14. FT approximations can provide excellent decision-making information.

Although a strong and powerful technique, FTA does have the following disadvantages:

1. Can easily become time consuming if not careful.
2. Can become the goal rather than the tool.
3. Modeling sequential timing and repair is more difficult.
4. Modeling multiple phases is more difficult.
5. Requires an analyst with some training and practical experience.

11.19 COMMON MISTAKES TO AVOID

When first learning how to perform an FTA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of an FTA:

1. Not including human error in the FT
2. Not fully understanding the system design and operation
3. Jumping ahead in the system design further than the fault logic warrants
4. Not placing text in every tree node
5. Not placing sufficient descriptive text in every tree node
6. Forgetting the correct FT definitions (incorrect event usage)
7. Incorrectly accounting for MOEs in FT mathematics

11.20 SUMMARY

This chapter discussed the FTA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of FTA is to identify all events (failures, errors, environments, etc.) that can lead to the occurrence of a UE and show how they logically occur and relate to each other.
2. FTA is an analysis tool that provides:
   - An evaluation of complex systems and system relationships
   - A graphical model
   - A probability model
3. FTA is for system evaluation:
   - Safety—hazardous and catastrophic events
   - Reliability—system unavailability
   - Performance—unintended functions

4. FTA is for decision making:
   - Root cause analysis
   - Risk assessment
   - Design assessment
5. There are two types of FTA:
   - Design evaluation (proactive; prevents accident)
   - Accident investigation (reactive; postaccident)
6. The established FT construction procedure evolves around three principal concepts:
   - I–N–S concept
   - SS–SC concept
   - P–S–C concept
7. The use of a functional block diagram greatly aids and simplifies the FTA process.

REFERENCES

1. J. B. Fussell, and W. E. Vesely, A New Method for Obtaining Cutsets for Fault Trees, *Trans. ANS*, **15**, 262–263 (1972).
2. J. Dugan, S. Bavuso, and M. Boyd, Dynamic Fault Tree Models For Fault Tolerant Computer Systems, *IEEE Trans. Reliability*, **41**(3, September): 363–377 (1992).
3. J. D. Andrews, and J. B. Dugan, Dependency Modeling Using Fault Tree Analysis, Proceedings of the 17th International System Safety Conference, 1999, pp. 67–76.
4. L. Meshkat, J. B. Dugan, and J. D. Andrews, Dependability Analysis of Systems With On-Demand and Active Failure Modes, Using Dynamic Fault Trees, *IEEE Trans. Reliability*, **51**(2): 240–251 (2002).

BIBLIOGRAPHY

Andrews, J. D. and T. R. Moss, *Reliability and Risk Assessment*, 2nd ed., Longman Scientific & Technical, 2002.

Fussell, J. B., et al., MOCUS—A Computer Program to Obtain Minimal Cutsets, Aerojet Nuclear ANCR-1156, 1974.

Henley, E. J. and H. Kumamoto, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed., IEEE Press, 1996.

NASA, *Fault Tree Handbook with Aerospace Applications*, version 1.1, NASA, August 2002.

Roberts, N. H., W. E. Vesely, D. F. Haasl, and F. F. Goldberg, *Fault Tree Handbook*, NUREG-0492, U.S. Government Printing Office, Washington, DC, 1981.

Schneeweiss, W. G., *The Fault Tree Method*, LiLoLe, 1999.

Chapter 12

Event Tree Analysis

12.1 INTRODUCTION

Event tree analysis (ETA) is an analysis technique for identifying and evaluating the sequence of events in a potential accident scenario following the occurrence of an initiating event. ETA utilizes a visual logic tree structure known as an event tree (ET). The objective of ETA is to determine whether the initiating event will develop into a serious mishap or if the event is sufficiently controlled by the safety systems and procedures implemented in the system design. An ETA can result in many different possible outcomes from a single initiating event, and it provides the capability to obtain a probability for each outcome.

12.2 BACKGROUND

The ETA technique falls under the system design hazard analysis type (SD-HAT) and should be used as a supplement to the SD-HAT analysis. Refer to Chapter 3 for a description of the analysis types. The ETA is a very powerful tool for identifying and evaluating all of the system consequence paths that are possible after an initiating event occurs. The ETA model will show the probability of the system design resulting in a safe operation path, a degraded operation path, and an unsafe operation path.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

The purpose of ETA is to evaluate all of the possible outcomes that can result from an initiating event. Generally, there are many different outcomes possible from an initiating event, depending upon whether design safety systems work properly or malfunction when needed. ETA provides a probabilistic risk assessment (PRA) of the risk associated with each potential outcome.

The ETA technique can be used to model an entire system, with analysis coverage given to subsystems, assemblies, components, software, procedures, environment, and human error. ETA can be conducted at different abstraction levels, such as conceptual design, top-level design, and detailed component design. ETA has been successfully applied to a wide range of systems, such as nuclear power plants, spacecraft, and chemical plants. The technique can be applied to a system very early in design development and thereby identify safety issues early in the design process. Early application helps system developers to design in safety of a system during early development rather than having to take corrective action after a test failure or a mishap.

The ETA technique, when applied to a given system by an experienced analyst, is thorough at identifying and evaluating all of the possible outcomes resulting from an initiating event (IE). A basic understanding of ETA and FTA theory is essential to developing an ETA model. In addition it is crucial for the analyst to have a detailed understanding of the system. Overall, ETA is very easy to learn and understand. Proper application depends on the complexity of the system and the skill of the analyst. Applying the ETA technique to the evaluation of a system design is not a difficult process; however, it does require an understanding of FTA and probability theory.

A cause–consequence analysis (CCA) is very similar to ETA and is a possible alternative technique. Additionally, multiple FTAs could be performed to obtain the same results as an ETA. The ETA produces many different potential outcomes from a single event, whereas the FTA only evaluates the many causes of a single outcome.

The use of an ETA is recommended for a PRA of the possible outcomes resulting from an initiating event. The resulting risk profiles provide management and design guidance on areas requiring additional safety countermeasure design methods.

12.3 HISTORY

Event tree analysis is a binary form of a decision tree for evaluating the various multiple decision paths in a given problem. ETA appears to have been developed during the WASH-1400 [1] nuclear power plant safety study (circa 1974). The WASH-1400 team realized that a nuclear power plant PRA could be achieved by FTA; however, the resulting fault trees (FTs) would be very large and cumbersome, and they therefore established ETA to condense the analysis into a more manageable picture, while still utilizing FTA.

12.4 DEFINITIONS

The ETA technique is based on the following definitions:

Accident scenario Series of events that ultimately result in an accident. The sequence of events begins with an initiating event and is (usually) followed by one or more pivotal events that lead to the undesired end state.

Initiating event (IE) Failure or undesired event that initiates the start of an accident sequence. The IE may result in a mishap, depending upon successful operation of the hazard countermeasure methods designed into the system. Refer to Chapter 2 on hazard theory for information on the components of a hazard.

Pivotal events Intermediary events between the IE and the final mishap. These are the failure/success events of the design safety methods established to prevent the IE from resulting in a mishap. If a pivotal event works successfully, it stops the accident scenario and is referred to as a mitigating event. If a pivotal event fails to work, then the accident scenario is allowed to progress and is referred to as an aggravating event.

Probabilistic risk assessment (PRA) Comprehensive, structured, and logical analysis method for identifying and evaluating risk in a complex technological system. The detailed identification and assessment of accident scenarios, with a quantitative analysis, is the PRA goal.

Event tree (ET) Graphical model of an accident scenario that yields multiple outcomes and outcome probabilities. ETs are one of the most used tools in a PRA.

A common definition of risk in the PRA discipline is that risk is based upon a set of triplets:

1. Accident scenarios—what can go wrong?
2. Scenarios frequencies—how likely is it?
3. Scenarios consequences—What are the consequences?

12.5 THEORY

When performing a PRA, identifying and developing accident scenarios is fundamental to the concept of risk evaluation. The process begins with a set of IEs that perturb the system (i.e., cause it to change its operating state or configuration). For each IE, the analysis proceeds by determining the additional failure modes necessary to lead to the undesirable consequences. The consequences and frequencies of each scenario are computed for the individual IEs and the collection of probabilities form a risk profile for the system.

Event trees are used to model accident scenarios. An ET starts with the IE and progresses through the scenario via a series of pivotal events (PEs) until an end state is reached. The PEs are failures or events that are mitigating or aggravating to the scenario. The frequency (i.e., probability) of the PE can be obtained from an FTA of the event.

The PRA theory relates very closely with standard system safety terminology. An accident scenario is equivalent to a hazard; scenario frequency is equivalent to hazard probability; scenario outcome is equivalent to hazard severity.

Risk management involves the identification and prevention or reduction of adverse accident scenarios and the promotion of favorable scenarios. Risk management requires understanding the elements of adverse scenarios so that their components can be prevented or reduced, and an understanding of favorable scenarios in order that their components can be enhanced or promoted.

An accident scenario contains an IE and (usually) one or more pivotal events leading to an end state as shown in Figure 12.1.

As modeled in most PRAs, an IE is a perturbation that requires some kind of response from operators and/or one or more systems to prevent an undesired consequence. The pivotal events include successes or failures of these responses or possibly the occurrence or nonoccurrence of external conditions or key phenomena. The end states are formulated according to the decisions being supported by the analysis. Scenarios are classified into end states according to the kind and severity of consequences, ranging from completely successful outcomes to losses of various kinds, such as:

- Loss of life or injury/illness to personnel
- Damage to or loss of equipment or property (including software)
- Unexpected or collateral damage as a result of tests
- Failure of mission
- Loss of system availability
- Damage to the environment

An ET distills the pivotal event scenario definitions and presents this information in a tree structure that is used to help classify scenarios according to their consequences. The headings of the ET are the IE, the pivotal events, and the end states. The tree structure below these headings shows the possible scenarios ensuing from the IE, in terms of the occurrence or nonoccurrence of the pivotal events. Each distinct path through the tree is a distinct scenario. According to a widespread but informal convention, where pivotal events are used to specify system success or failure, the “down” branch is considered to be “failure.” The ET concept is shown in Figure 12.2.

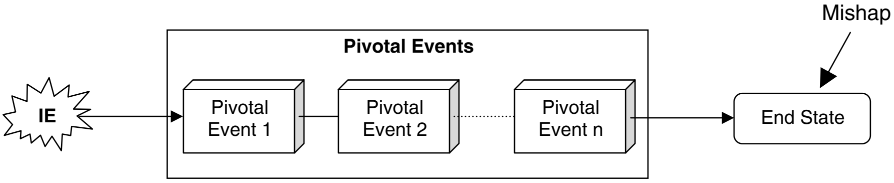


Figure 12.1 *Accident scenario concept.*

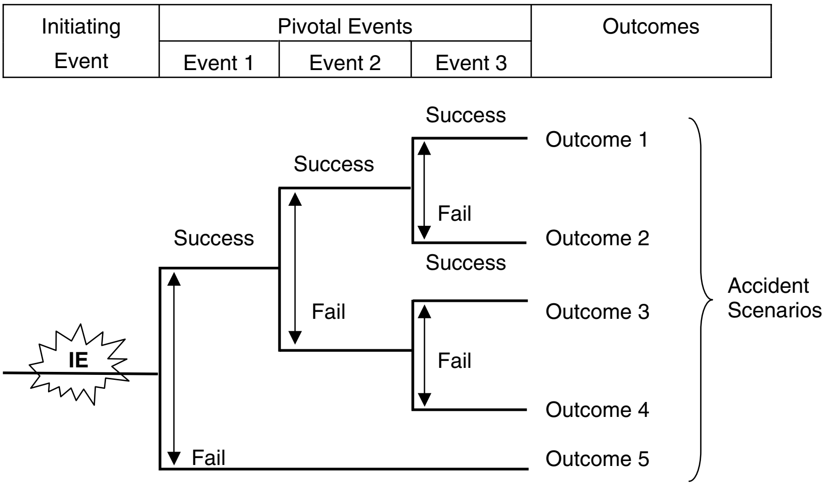


Figure 12.2 *Event tree concept.*

In most ETs, the pivotal event splits are binary: A phenomenon either does or does not occur; a system either does or does not fail. This binary character is not strictly necessary; some ETs show splits into more than two branches. What is necessary is that distinct paths be mutually exclusive and quantified as such (at least to the desired level of accuracy).

An example of ET structure with quantitative calculations is displayed in Figure 12.3. The ET model logically combines all of the system design safety countermeasure methods intended to prevent the IE from resulting in a mishap. A side effect of the analysis is that many different outcomes can be discovered and evaluated. Note how the ET closely models the scenario concept shown in Figure 12.1.

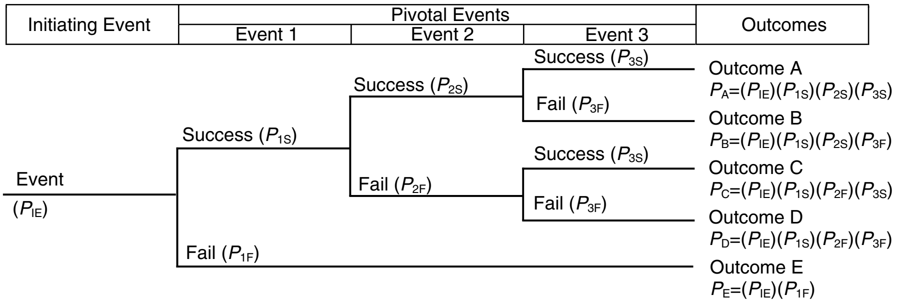


Figure 12.3 *ETA concept.*

12.6 METHODOLOGY

Figure 12.4 shows an overview of the basic ETA process and summarizes the important relationships involved in the ETA process. The ETA process involves utilizing detailed design information to develop event tree diagrams (ETDs) for specific IEs. In order to develop the ETD, the analyst must have first established the accident scenarios, IEs, and pivotal events of interest. Once the ETD is constructed, failure frequency data can be applied to the failure events in the diagram. Usually this information is derived from FTA of the failure event. Since $1 = P_S + P_F$, the probability of success can be derived from the probability of failure calculation. The probability for a particular outcome is computed by multiplying the event probabilities in the path.

Table 12.1 lists and describes the basic steps of the ETA process, which involves performing a detailed analysis of all the design safety features involved in a chain of events that can result from the initiating event to the final outcome.

Complex systems tend to have a large number of interdependent components, redundancy, standby systems, and safety systems. Sometimes it is too difficult or cumbersome to model a system with just an FT; so, PRA studies have combined the use of FTs and ETDs. The ETD models accident/mishap cause–consequence scenarios, and FTs model complex subsystems to obtain the probability of these subsystems failing. An accident scenario can have many different outcomes, depending on which PEs fail and which function correctly. The ET/FT combination models this complexity very well.

The goal of ETA is to determine the probability of all the possible outcomes resulting from the occurrence of an IE. By analyzing all possible outcomes, it is possible to determine the percentage of outcomes that lead to the desired result and the percentage of outcomes that lead to the undesired result.

Event trees can be used to analyze systems in which all components are continuously operating or for systems in which some or all of the components are in standby mode—those that involve sequential operational logic and switching. The starting point (referred to as the initiating event) disrupts normal system operation. The event tree displays the sequences of events involving success and/or failure of the system components.

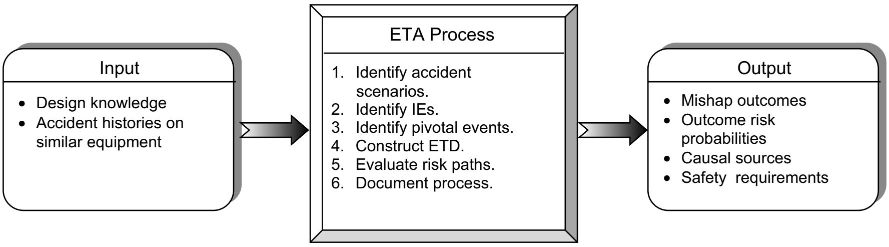


Figure 12.4 *ETA overview.*

TABLE 12.1 ETA Process

Step	Task	Description
1	Define the system.	Examine the system and define the system boundaries, subsystems, and interfaces.
2	Identify the accident scenarios.	Perform a system assessment or hazard analysis to identify the system hazards and accident scenarios existing within the system design.
3	Identify the initiating events.	Refine the hazard analysis to identify the significant IEs in the accident scenarios. IEs include events such as fire, collision, explosion, pipe break, toxic release, etc.
4	Identify the pivotal events.	Identify the safety barriers or countermeasures involved with the particular scenario that are intended to preclude a mishap.
5	Build the event tree diagram.	Construct the logical ETD, starting with the IE, then the PEs, and completing with the outcomes of each path.
6	Obtain the failure event probabilities.	Obtain or compute the failure probabilities for the PEs on the ETD. It may be necessary to use FTs to determine how a PE can fail and to obtain the probability.
7	Identify the outcome risk.	Compute the outcome risk for each path in the ETD.
8	Evaluate the outcome risk.	Evaluate the outcome risk of each path and determine if the risk is acceptable.
9	Recommend corrective action.	If the outcome risk of a path is not acceptable, develop design strategies to change the risk.
10	Document ETA.	Document the entire ETA process on the ETDs. Update for new information as necessary.

In the case of standby systems and, in particular, safety and, mission-oriented systems, the ET is used to identify the various possible outcomes of the system following a given IE, which is generally an unsatisfactory operating event or situation. In the case of continuously operated systems, these events can occur (i.e., components can fail) in any arbitrary order. In the event tree analysis, the components can be considered in any order since they do not operate chronologically with respect to each other.

The ETA is based on binary logic in which an event either has or has not happened or a component has or has not failed. It is valuable in analyzing the consequences arising from a failure or undesired event. An ET begins with an IE, such as a component failure, increase in temperature/pressure, or a release of a hazardous substance that can lead to an accident. The consequences of the event are followed through a series of possible paths. Each path is assigned a probability of occurrence and the probability of the various possible outcomes can be calculated.

The ETD is a diagram modeling all of the possible events that follow an originating failure or undesired event. The originating event can be a technical failure or an operational human error. The objective is to identify the chain of events following one or more specified basic events, in order to evaluate the consequences and determine whether the event will develop into a serious accident or are sufficiently controlled by

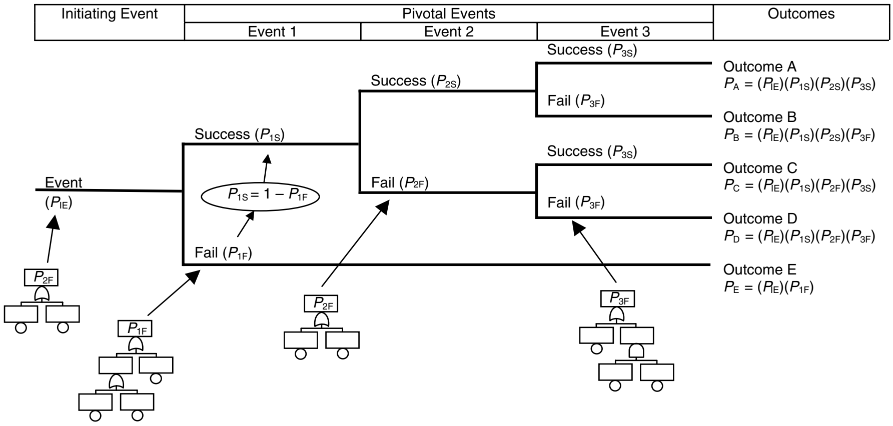


Figure 12.5 *ETD development.*

the safety systems and procedures implemented. The results can therefore be recommendations to increase the redundancy or to modifications to the safety systems.

The ETA begins with the identified IE listed at the left side of the diagram in Figure 12.5. All safety design methods or countermeasures are then listed at the top of the diagram as contributing events. Each safety design method is evaluated for the contributing event: (a) operates successfully and (b) fails to operate. The resulting diagram combines all of the various success/failure event combinations and fans out to the right in a sideways tree structure. Each success/failure event can be assigned a probability of occurrence, and the final outcome probability is the product of the event probabilities along a particular path. Note that the final outcomes can range from safe to catastrophic, depending upon the chain of events.

12.7 WORKSHEET

The primary worksheet for an ETA is the event tree diagram (ETD), which provides the following information:

1. Initiating event
2. System pivotal events
3. Outcomes
4. Event and outcome probabilities

Figure 12.5 demonstrates the typical ETD. Each event is divided into two paths, success and failure. The success path always is the top path and the failure path is the lower path. The ETD has only one IE, which is identified at the far left of the diagram. As many contributing events as necessary to fully describe the system are listed at the top of the diagram. The more contributing events involved the larger the resulting ETD and the more tree branches required.

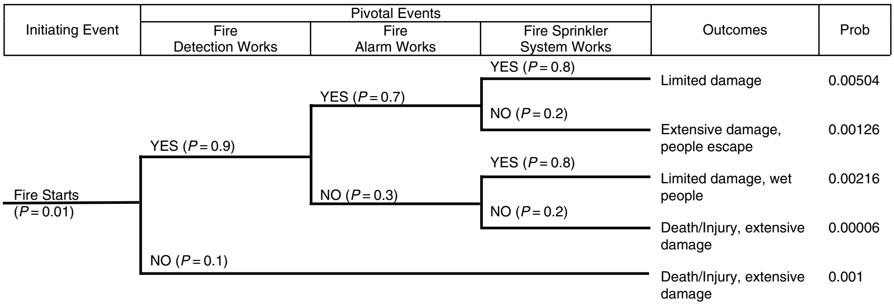


Figure 12.6 *ETA example 1.*

12.8 EXAMPLE 1

Figure 12.6 contains an example ETA for a fire detection and suppression system in an office building. This ETA analyzes all the possible outcomes of a system fire. The IE for the ET is “fire starts.” Note the range of outcomes resulting from the success or failure of the safety subsystems (pivotal events).

Note from this example that when computing the success/fail probability for each contributing PE that the PE states must always sum to 1.0, based on the reliability formula that $P_{\text{SUCCESS}} + P_{\text{FAILURE}} = 1$. Also note that in this case there are three contributing PEs that generate five possible different outcomes, each with a different probability.

12.9 EXAMPLE 2

Figure 12.7 contains an example ETA for an automobile system, where the car battery has failed. The dead battery is the IE that begins the scenario analysis.

12.10 EXAMPLE 3

Figure 12.8 contains an example ETA for a missile system. The IE is the missile being dropped during handling or transportation.

12.11 EXAMPLE 4

Figure 12.9 contains an example ETA for a nuclear power plant system. The IE is a pipe break in the cooling subsystem.

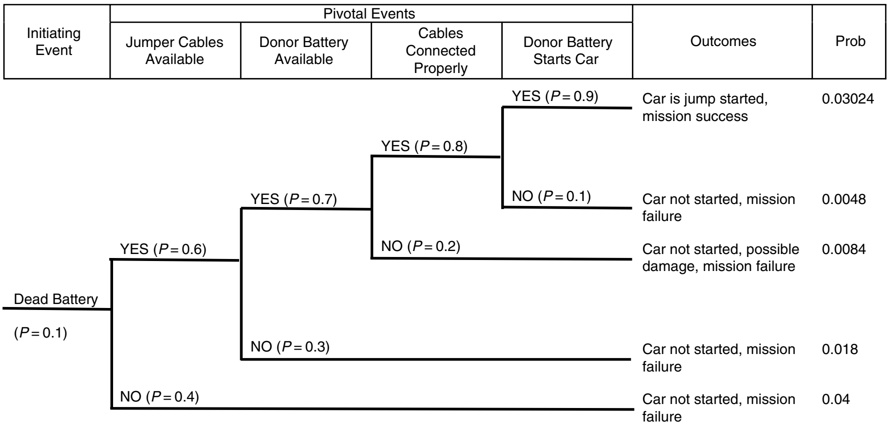


Figure 12.7 *ETA example 2.*

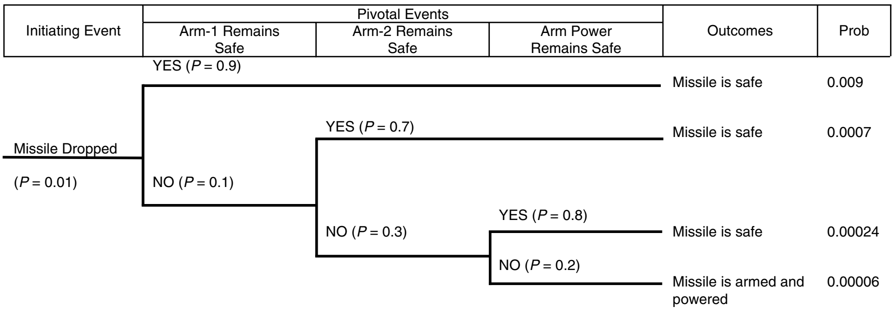


Figure 12.8 *ETA example 3.*

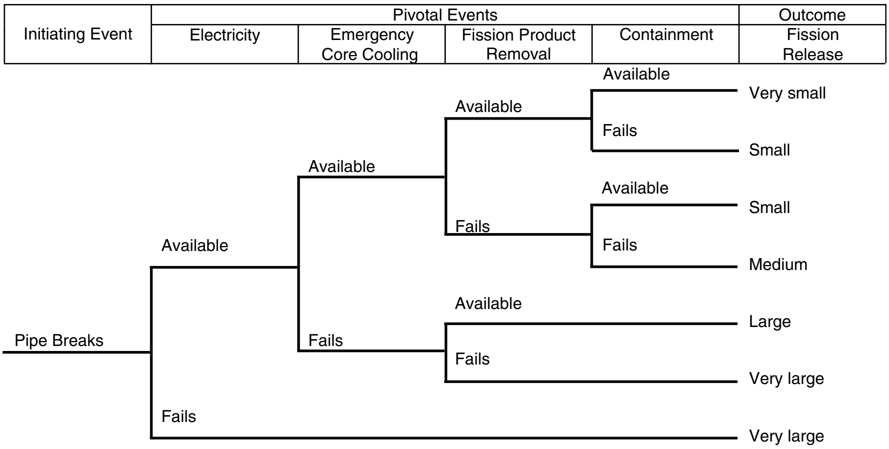


Figure 12.9 *ETA example 4.*

12.12 ADVANTAGES AND DISADVANTAGES

The following are advantages of the ETA technique:

1. Structured, rigorous, and methodical approach.
2. A large portion of the work can be computerized.
3. Can be effectively performed on varying levels of design detail.
4. Visual model displaying cause/effect relationships.
5. Relatively easy to learn, do, and follow.
6. Models complex system relationships in an understandable manner.
7. Follows fault paths across system boundaries.
8. Combines hardware, software, environment, and human interaction.
9. Permits probability assessment.
10. Commercial software is available.

The following are disadvantages of the ETA technique:

1. An ETA can only have one initiating event, therefore multiple ETAs will be required to evaluate the consequence of multiple initiating events.
2. ETA can overlook subtle system dependencies when modeling the events.
3. Partial successes/failures are not distinguishable.
4. Requires an analyst with some training and practical experience.

12.13 COMMON MISTAKES TO AVOID

When first learning how to perform an ETA, it is commonplace to commit some typical errors. The following is a list of typical errors made during the conduct of an ETA:

1. Not identifying the proper IE
2. Not identifying all of the contributing pivotal events

12.14 SUMMARY

This chapter discussed the ETA technique. The following are basic principles that help summarize the discussion in this chapter:

1. ETA is used to model accident scenarios and to evaluate the various outcome risk profiles resulting from an initiating event.
2. ETA is used to perform a PRA of a system.

3. The ETA diagram provides structure and rigor to the ETA process.
4. ETA can be a supplement to the SD-HAT.
5. Fault trees are often used to determine the causal factors and probability for failure events in the ETA.

REFERENCE

1. N. C. Rasmussen, *Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, WASH-1400, Nuclear Regulatory Commission, Washington, DC, 1975.

BIBLIOGRAPHY

Andrews, J. D. and S. J. Dunnett, Event Tree Analysis Using Binary Decision Diagrams, *IEEE Trans. Reliability*, **49**(2):230–238 (2000).

Henley, E. J. and H. Kumamoto, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed., IEEE Press, 1996.

Kapan, S. and B. J. Garrick, On the Quantitative Definition of Risk, *Risk Analysis*, **1**:11–37 (1981).

NASA, *Fault Tree Handbook with Aerospace Applications*, version 1.1. NASA, August 2002.

Papazoglou, I. A., Functional Block Diagrams and Automated Construction of Event Trees, *Reliability Eng. System Safety*, **61**(3):185–214 (1998).

Chapter 13

Failure Mode and Effects Analysis

13.1 INTRODUCTION

Failure mode and effects analysis (FMEA) is a tool for evaluating the effect(s) of potential failure modes of subsystems, assemblies, components, or functions. It is primarily a reliability tool to identify failure modes that would adversely affect overall system reliability. FMEA has the capability to include failure rates for each failure mode in order to achieve a quantitative probabilistic analysis. Additionally, the FMEA can be extended to evaluate failure modes that may result in an undesired system state, such as a system hazard, and thereby also be used for hazard analysis.

A more detailed version of the FMEA is known as failure mode, effects and criticality analysis (FMECA). The FMECA requires that more information be obtained from the analysis, particularly information dealing with the criticality and detection of the potential failure modes.

The FMEA method is a disciplined bottom-up evaluation technique that focuses on the design or function of products and processes in order to prioritize actions to reduce the risk of product or process failures. In addition, the FMEA is a tool for documenting the analysis and capturing recommended design changes. Time and resources for a comprehensive FMEA must be allotted during design and process development, when design and process changes can most easily and inexpensively be implemented.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

13.2 BACKGROUND

The FMEA technique falls under the detailed design hazard analysis type (DD-HAT) because it is a detailed analysis done at the component or functional level. The basic hazard analysis types are described in Chapter 3. An alternate name for this technique is FMECA. FMECA is basically the same as FMEA except it adds criticality evaluation to each failure mode, as well as the evaluation of possible failure mode detection methods.

The purpose of FMEA is to evaluate the effect of failure modes to determine if design changes are necessary due to unacceptable reliability, safety, or operation resulting from potential failure modes. When component failure rates are attached to the identified potential failure modes, a probability of subsystem or component failure can be derived. FMEA was originally developed to determine the reliability effect of failure modes, but it can also be used to identify mishap hazards resulting from potential failure modes.

The FMEA is applicable to any system or equipment, at any desired level of design detail—subsystem, assembly, unit, or component. FMEA is generally performed at the assembly or unit level because failure rates are more readily available for the individual embedded components. The FMEA can provide a quantitative reliability prediction for the assembly or unit that can be used in a quantitative safety analysis (e.g., fault tree). FMEA tends to be more hardware and process oriented but can be used for software analysis when evaluating the failure of software functions.

The technique is thorough for evaluating potential individual failure modes and providing reliability information. However, for safety purposes, an FMEA is limited because it considers only single item failures and not the combination of items failing together; generally, mishaps result from failure combinations. Also an FMEA does not identify hazards arising from events other than failures (e.g., timing errors, radiation, high voltage, etc.).

The technique can be easily performed and mastered; however, a basic understanding of failures and failure mode theory and hazard analysis theory is necessary as well as knowledge of system safety concepts. Additionally a detailed understanding of the system design and operation is required.

The methodology is uncomplicated and easily learned. Standard FMEA forms and instructions are included in this chapter.

The FMEA technique is a valuable reliability tool for analyzing potential failure modes and calculating subsystem, assembly, or unit failure rates. Severity and probability evaluation of failure modes provides a prioritized list for corrective actions. FMEA can also be extended to identify hazards resulting from potential failure modes and evaluating the resulting mishap risk. Note, however, that an FMEA will likely not identify all system hazards because it is only looking at single component failure modes, while hazards can be the result of multiple hazards and events other than failure modes. For this reason, FMEA is not recommended as the sole tool for hazard identification. FMEA should only be used for hazard analysis when done in conjunction with other hazard analysis techniques.

A modified FMEA for hazard identification is recommended for evaluation of failure modes, when done in support of other hazard analyses. However, the FMEA is not recommended as the sole hazard analysis to be performed, since the FMEA primarily looks at single failure modes only, while a hazard analysis considers many additional system aspects.

13.3 HISTORY

The FMEA was developed for the U.S. military as a formal analysis technique. Military procedure MIL-P-1629 (now MIL-STD-1629A) [1], titled "Procedures for Performing a Failure Mode, Effects and Criticality Analysis," is originally dated November 9, 1949. It was used as a reliability evaluation technique to determine the effect of system and equipment failures. Failures were classified according to their impact on mission success and personnel/equipment safety. The term *personnel/equipment*, taken directly from an abstract of military standard MIL-P-1629, is notable because of the significance given to personnel. Used for aerospace/rocket development, the FMEA and the more detailed FMECA were helpful in avoiding errors on small sample sizes of costly rocket technology.

Use of the FMEA was encouraged in the 1960s for space product development and served well on getting a man on the moon. Ford Motor Company reintroduced FMEA in the late 1970s for safety and regulatory consideration after multiple Pinto automobile exploding gas tank accidents. Ford Motor Company has also used FMEAs effectively for production improvement, as well as design improvement.

The Automotive Industry Action Group (AIAG) and the American Society for Quality Control (ASQC) copyrighted industrywide FMEA standards, in February of 1993, that are the technical equivalent of the Society of Automotive Engineers procedure SAE J-1739 [2]. The standards are presented in an FMEA manual [3] approved and supported by all three U.S. auto makers, which provides general guidelines for preparing an FMEA.

13.4 DEFINITIONS

In order to facilitate a better understanding of FMEA, some definitions for specific terms are in order. The following are basic FMEA terms:

Failure Departure of an item from its required or intended operation, function, or behavior; problems that users encounter. The inability of a system, subsystem, or component to perform its required function. The inability of an item to perform within previously prescribed limits.

Failure mode Manner by which an item fails; the mode or state the item is in after it fails. The way in which the failure of an item occurs.

Failure cause Process or mechanism responsible for initiating the failure mode. The possible processes that can cause component failure include physical failure, design defects, manufacturing defects, environmental forces, and so forth.

Failure effect Consequence(s) a failure mode has on the operation, function, or status of an item and on the system.

Fault Undesired anomaly in the functional operation of an equipment or system. The occurrence of an undesired state, which may be the result of a failure.

Critical item list (CIL) List of items that are considered critical for reliable and/or safe operation of the system. The list is generated from the FMEA.

Indenture level Levels of system hierarchy that identify or describe the relative complexity of a system. The levels progress from the more complex (system) to the simpler (part/component) divisions level (MIL-STD-1629A [1] on FMEAs). The hierarchy is the organizational structure defining dominant and subordinate relationships between subsystems down to the lowest component/piece part.

Risk priority number (RPN) Risk ranking index for reliability. RPN = (probability of occurrence) × (severity ranking) × (detection ranking).

13.5 THEORY

The FMEA technique is a qualitative and quantitative analysis method used for the evaluation of potential failure modes. The FMEA is a technique that answers a series of questions:

- What can fail?
- How does it fail?
- How frequently will it fail?
- What are the effects of the failure?
- What is the reliability/safety consequence of the failure?

To conduct an FMEA, it is necessary to know and understand certain system characteristics:

- Mission
- System design
- Operational constraints
- Success and failure boundaries
- Credible failure modes and a measure of their probability of occurrence

Figure 13.1 depicts the FMEA concept. The subsystem being analyzed is divided into its relevant indenture levels, such as unit 1, unit 2, unit 3, and so forth. Each unit

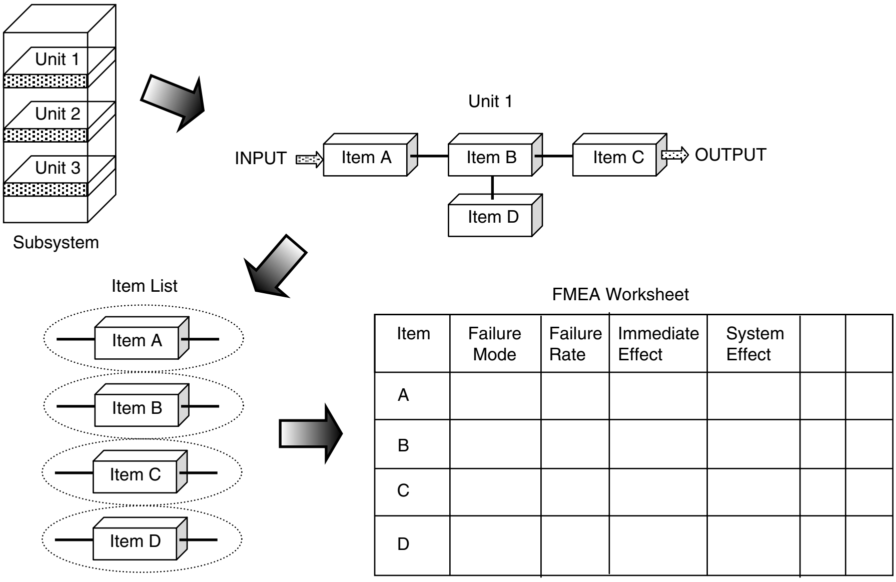


Figure 13.1 *FMEA concept.*

is then further subdivided into its basic items. Each item is listed down the left-hand column of the FMEA worksheet and individually analyzed. The concept is to break-down the "entity" being analyzed into individual items. In effect, the subsystem is analyzed *top-down* when it is divided into indenture levels, and then it is analyzed *bottom-up* when each item is individually evaluated. An item can be a hardware part or component, or it can be a function. Each item is then singularly isolated and all potential failure modes for this item are listed in the first column of the FMEA. Each item is then evaluated in detail.

The primary building blocks of a system that an FMEA analyzes are the system hardware and the system functions, referred to as the system structural aspect and the system functional aspect. Figure 13.2 depicts the functional vs. structural concept of a system, which is relevant for FMEA. The functional aspect defines how the system must operate and the functional tasks that must be performed. The structural aspect defines how the functions will be implemented via the hardware that actually carries out the system operations. System design and implementation progresses from the system functions down to the hardware piece parts.

Conceptually, there are three approaches to performing an FMEA:

1. *Functional Approach* The functional FMEA is performed on functions. The functions can be at any functional indenture level for the analysis: system, subsystem, unit, or assembly. This approach focuses on ways in which functional objectives of a system go unsatisfied or are erroneous. The functional approach is also applicable to the evaluation of software through the

evaluation of required software functions. The functional approach tends to be more of a system-level analysis.

2. *Structural Approach* The structural FMEA is performed on hardware and focuses on potential hardware failure modes. The hardware can be at any hardware indenture level for the analysis: subsystem, unit, assembly, or part (component). The structural approach tends to be a detailed analysis at the component level.
3. *Hybrid Approach* The hybrid FMEA is a combination of the structural and the functional approaches. The hybrid approach begins with the functional analysis of the system and then transitions to a focus on hardware, especially hardware that directly contributes to functional failures identified as safety critical.

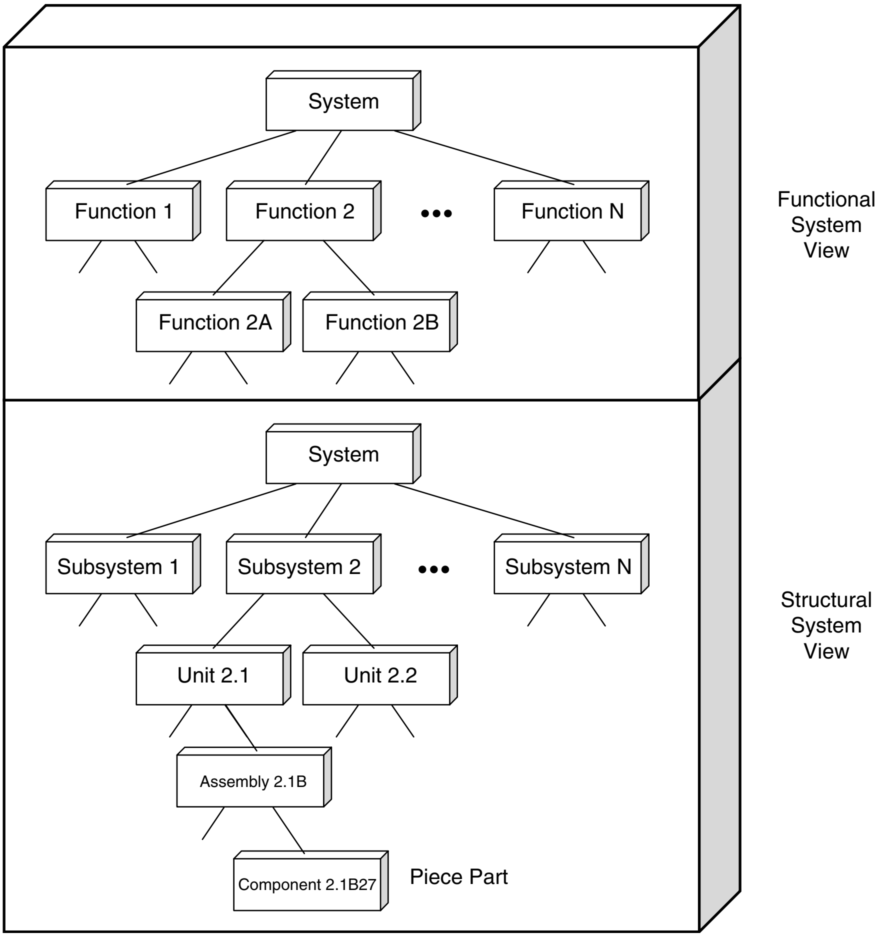


Figure 13.2 *Functional vs. structural levels.*

The functional approach is performed when the system is being defined by the functions that are to be accomplished. The structural hardware approach is performed when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. The hybrid approach combines both aspects, beginning with identification of important system functional failures and then identifying the specific equipment failure modes that produce those system functional failures.

13.5.1 Structural and Functional Models

The purpose of an FMEA is to evaluate potential design failure modes early in the development program to cost effectively implement safety design corrections. To attain this objective the FMEA must closely track the design as it progresses from conceptual to detailed.

Design depth and detail correlates to structural and functional decomposition of the system. A structural model of the system captures the static structure of the system comprised of the hardware components. A functional model of the system captures the functions that must be performed in order for the system to achieve its goals and objectives. These two system views contrast what must be done (function) with how it is to be done (structure).

Figure 13.3 provides a brief example of a structural model and a functional model for a radio system and the failure modes that might be considered. These models also depict indenture levels for each type of model.

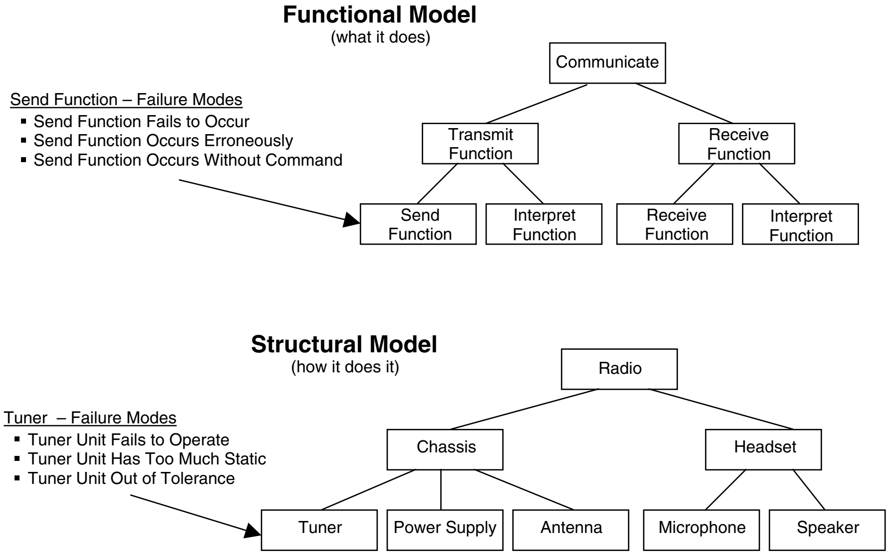


Figure 13.3 *Functional and structural models.*

13.5.2 Product and Process FMEA

The FMEA is classified as a product FMEA or a process FMEA, depending upon the application. The product FMEA analyzes the design of a product or system by examining the way that the item's failure modes affect the operation of the product or system. The process FMEA analyzes the processes involved in the manufacture, use, and maintenance of a product. It examines the way that process methods affect the operation of the product or system. Both types of FMEA focus on design—design of the product or design of the process. The FMEA classification types, along with general failure mode areas, are presented in Figure 13.4.

13.5.3 Functional Failure Modes

Functional-type FMEAs evaluate system, subsystem, and unit functions. Functional failure modes are a little more abstract than hardware failure modes. The key is to consider each adverse state that is possible for each function.

Example functional failure modes may include, but are not limited to, the following:

1. Function fails to perform.
2. Function performs incorrectly.
3. Function performs prematurely.
4. Function provides incorrect or misleading information.
5. Function does not fail safe.

13.5.4 Hardware Failure Modes

Hardware-type FMEAs consider both component catastrophic and component out-of-tolerance modes of failure. Catastrophic failure means complete component functional failure in the required mode of operation. For example, a resistor failing open or shorted means that it no longer functions as intended. Out-of-tolerance failure refers to a failure mode where the component is functional but not within specified

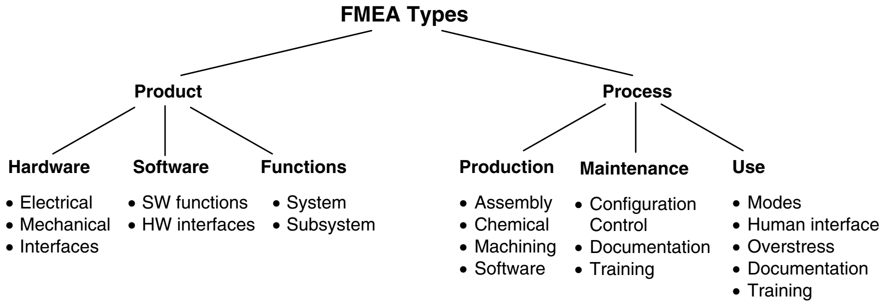


Figure 13.4 *FMEA types—product and process.*

operating boundaries. Example modes for a resistor might include too low resistance or too high resistance, but it still provides some level of resistance. An intermittent failure is a failure that is not continuous; the failure occurs in a cyclic on/off fashion.

The basic failure categories for hardware items include:

1. Complete failure
2. Partial failure (e.g., out of tolerance)
3. Intermittent failure

In a typical FMEA, these basic failure modes may be expressed by the following examples:

1. Open circuit
2. Short circuit
3. Out of tolerance
4. Leak
5. Hot surface
6. Bent
7. Oversize/undersize
8. Cracked
9. Brittle
10. Misaligned
11. Binding
12. Corroded
13. Failure to operate
14. Intermittent operation
15. Degraded operation
16. Loss of output

13.5.5 Software Failure Modes

Performing an FMEA on a mechanical or electrical system is generally more straightforward than performing an FMEA on software. Failure modes of components such as relays and resistors are generally well understood. Mechanical and electrical components fail due to aging, wear, or stress. For software the situation is different because software modules do not fail per se, they only display incorrect behavior. A software-oriented FMEA can only address incorrect behavior of software (i.e., the software fails to perform as intended).

A software FMEA (SFMEA) normally involves performing an analysis of the software functions. An SFMEA would follow the same basic steps as a hardware FMEA: set up a starting point, understand the design, make a list of typical failure modes, and then perform the analysis. Software failure modes would be seen as types of erroneous behavior and not typos in the code. Distinguishing characteristics between the hardware and software FMEA are shown in Table 13.1.

Example software functional failure modes may include, but are not limited to, the following:

1. Software function fails.
2. Function provides incorrect results.
3. Function occurs prematurely.
4. Unsent messages.
5. Messages sent too early or too late.

TABLE 13.1 Hardware/Software FMEA Characteristics

Hardware	Software
Is performed at a part (component) level where failure rates can be obtained.	Is only practical at the functional level.
System is considered free of failures at start of operation.	System is assumed to contain software faults at start of operation.
Postulates failure modes due to aging, wear, or stress.	Postulates failure modes according to functional failure.
Analyzes failure consequence at the item level and the system level.	Analyzes failure consequence at the system level.
States the criticality in measures of consequence severity and probability.	States the criticality in measures of consequence severity, but probability cannot be determined.
States hardware measures taken to prevent or mitigate failure consequence.	States software measures taken to prevent or mitigate failure consequence.
Software can cause hardware to fail.	Hardware can cause software to fail.

6. Faulty message.
7. Software stops or crashes.
8. Software hangs.
9. Software exceeds internal capacity.
10. Software startup failure.
11. Software function has slow response.

13.5.6 Quantitative Data Sources

When performing a quantitative FMEA/FMECA, component failure rates are required. Although many models are available for performing reliability prediction analyses, each of these models was originally created with a particular application in mind. Table 13.2 describes the most widely used reliability prediction models in terms of their intended applications, noting both their advantages and disadvantages. Note that there is no available failure rate data for software as there are no defined failure modes.

13.6 METHODOLOGY

Figure 13.5 shows an overview of the basic FMEA process and summarizes the important relationships involved. Based on reliability theory, all components have inherent failure modes. The FMEA process evaluates the overall impact of each and every component failure mode. The primary FMEA goal is to determine the effect on system reliability from component failures, but the technique can be extended to determine the effect on safety.

Input data for the FMEA includes detailed hardware/function design information. Design data may be in the form of the design concept, the operational

TABLE 13.2 Comparison of Reliability Prediction Models

Reliability Prediction Model	Application and Originating Country	Advantages	Disadvantages
MIL-HDBK-217, *The Military Handbook for the Reliability Prediction of Electronic Equipment*	Military and commercial, United States	Provides for both parts stress and parts count analysis of electronic parts. Can easily move from preliminary design stage to complete design stage by progressing from parts count to parts stress. Includes models for a broad range of part types. Provides many choices for environment types. Well-known and widely accepted.	Does not consider other factors that can contribute to failure rate such as burn-in data, lab testing data, field test data, designer experience, wear-out, etc. Considers only electronic parts.
Telcordia (Bellcore), *Reliability Prediction Procedure for Electronic Equipment* (Technical Reference #TR-332 or Telcordia Technologies Special Report SR-332), AT&T Bell Labs	Commercial, United States	Offers analysis ranging from parts count to full parts stress through the use of calculation methods. Considers burn-in data, lab testing data, and field test data. Well-known and accepted.	Considers only electronic parts. Supports only a limited number of ground environments. Fewer part models compared to MIL-HDBK-217. Does not account for other factors such as designer experience, wear-out, etc.
The Handbook of Reliability Prediction Procedures for Mechanical Equipment (NSWC-98/LE1), Navy	Military and commercial, United States	Provides for analyzing a broad range of mechanical parts (seals, springs, solenoids, bearings, gears, etc.)	Limited to mechanical parts.
HRD5, *The Handbook for Reliability Data for Electronic Components Used in Telecommunication Systems*	Telecommunications, United Kingdom	Similar to Telcordia. Fairly broad range of part types modeled.	Considers only electronic parts. Not widely used.

(*continued*)

TABLE 13.2 ***Continued***

Reliability Prediction Model	Application and Originating Country	Advantages	Disadvantages
PRISM, *System Reliability Assessment Methodology* developed by the Reliability Analysis Center (RAC)	Military and commercial, United States	Incorporates NPRD/EPRD database of failure rates. Enables the use of process grading factors, predecessor data, and test or field data. Small, limited set of part types modeled.	Newer standard, still gaining acceptance. Considers only electronic parts. Cannot model hybrids. No reference standard available.
NPRD/EPRD, Nonelectronics Parts Reliability (NPRD) and Electronic Parts Reliability (EPRD) databases by RAC	Military and commercial, United States	Broad array of electronic and nonelectronic parts. Based completely on field data.	Consists entirely of databases of failure rates, not mathematical models.

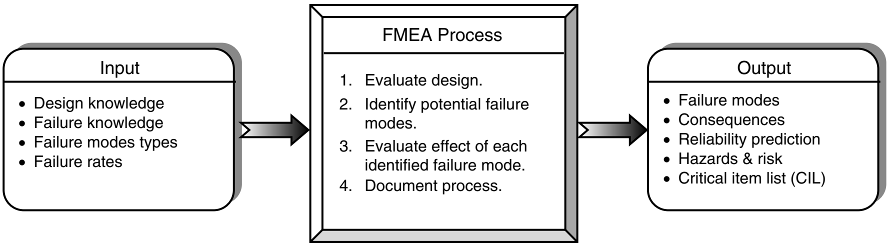


Figure 13.5 *FMEA overview.*

concept, and major components planned for use in the system and major system functions. Sources for this information include design specifications, sketches, drawings, schematics, function lists, functional block diagrams (FBDs), and/or reliability block diagrams (RBDs). Input data also includes known failure modes for components and failure rates for the failure modes. FMEA output information includes identification of failure modes in the system under analysis, evaluation of the failure effects, identification of hazards, and identification of system critical items in the form of a critical items list (CIL).

Table 13.3 lists the basic steps in the FMEA process, which involves performing a detailed analysis of all item failure modes. A worksheet is utilized to document the FMEA as identified in the next section.

13.7 WORKSHEET

The FMEA is a detailed analysis of potential failure modes. It is desirable to perform the FMEA using a form or worksheet to provide analysis structure, consistency, and documentation. The specific format of the analysis worksheet is not critical. Typically, matrix-, columnar- or text-type forms are utilized to help maintain focus and structure in the analysis. An FMEA that supports system safety and hazard analysis should contain the following information, as a minimum:

1. Failure mode
2. System effect of failure mode
3. System-level hazards resulting from failure
4. Mishap effect of hazards
5. Failure mode and/or hazard causal factors
6. How the failure mode can be detected
7. Recommendations (such as safety requirements/guidelines that can be applied)
8. The risk presented by the identified hazard

TABLE 13.3 FMEA Process

Step	Task	Description
1	Define system.	Define, scope, and bound the system. Define the mission, mission phases, and mission environments. Understand the system design and operation. Note that all steps are applicable for an SFMEA.
2	Plan FMEA.	Establish FMEA goals, definitions, worksheets, schedule, and process. Start with functional FMEA then move to FMEA of hardware that is safety critical (identified from functional FMEA). Divide the system under analysis into the smallest segments desired for the analysis. Identify items to be analyzed and establish indenture levels for items/functions to be analyzed.
3	Select team.	Select all team members to participate in FMEA and establish responsibilities. Utilize team member expertise from several different disciplines (e.g., design, test, manufacturing, etc.).
4	Acquire data.	Acquire all of the necessary design and process data needed (e.g., functional diagrams, schematics, and drawings) for the system, subsystems, and functions for FMEA. Refine the item indenture levels for analysis. Identify realistic failure modes of interest for the analysis and obtain component failure rates.
5	Conduct FMEA.	a. Identify and list the items to be evaluated. b. Obtain concurrence on the list and level of detail. c. Transfer the list to the FMEA worksheet. d. Analyze each item on the list by completing the FMEA worksheet questions. e. Have the FMEA worksheets validated by a system designer for correctness.
6	Recommend corrective action.	Recommend corrective action for failure modes with unacceptable risk. Assign responsibility and schedule for implementing corrective action.
7	Monitor corrective action.	Review test results to ensure that safety recommendations and system safety requirements are effective in mitigating hazards as anticipated.
8	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
9	Document FMEA.	Document the entire FMEA process on the worksheets. Update for new information and closure of assigned corrective actions.

Many different FMEA worksheet formats have been proposed by different programs, projects, and disciplines over the years. Some different examples are shown below. Each form provides a different amount and type of information to be derived from the analysis. The specific form to be used may be determined by the customer, the system safety working group, the safety manager, the reliability group, or the reliability/safety analyst performing the analysis. Typically a program stays with the same FMEA worksheet over the life of the program. Therefore it is important to ensure that relevant safety-related information is included in the FMEA worksheet. Figure 13.6 uses a very basic FMEA worksheet format, primarily for use by the reliability organization.

Failure Mode and Effects Analysis						
Component	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	RPN

RPN = Risk Priority Number (Reliability)

Figure 13.6 *Example FMEA worksheet 1—reliability.*

Figure 13.7 illustrates a more complex FMEA worksheet format, which is also primarily for use by the reliability organization but provides needed system safety information.

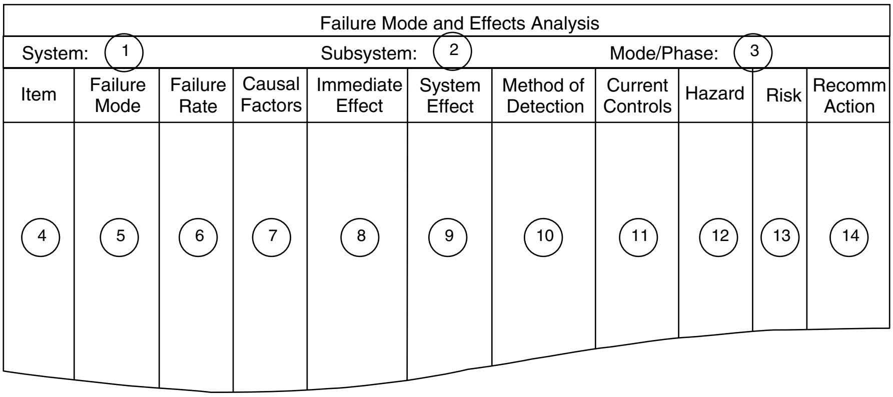
Figure 13.8 is the preferred worksheet format for systems safety as it includes workspace for relevant safety-related information as well as reliability information. Other worksheet formats may exist because different organizations often tailor their FMEA worksheet to fit their particular needs.

The FMEA steps for this recommended worksheet are as follows:

1. *System* This column identifies the system under analysis.
2. *Subsystem* This column identifies the subsystem under analysis.
3. *Mode/Phase* This column identifies the system mode or life-cycle phase under analysis.

Failure Mode and Effects Analysis									
Item	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	RPN	Method of Detection	Current Controls	Recomm Action

Figure 13.7 *Example FMEA worksheet 2—reliability.*



Failure Mode and Effects Analysis

System: 1 Subsystem: 2 Mode/Phase: 3

Item	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recomm Action
4	5	6	7	8	9	10	11	12	13	14

Figure 13.8 *Example FMEA worksheet 3—safety/reliability.*

4. *Item* This column identifies the component, item, or function being analyzed. For hardware components, the component part number and descriptive title should be identified when possible. A description of the item's purpose or function is also useful and should be included.
5. *Failure Mode* This column identifies all credible failure modes that are possible for the identified component, item, or function. This information can be obtained from various sources, such as historical data, manufacturer's data, experience, or testing. Since some components may have more than one failure mode, each mode must be listed and analyzed for its effect on the assembly and then on the subsystem.
6. *Failure Rate* This column provides the failure rate or failure probability for the identified mode of failure. Some quantitative data sources are noted in Table 13.2. The source of the failure rate should also be provided, for future reference. These can be best judgments that are revised as the design process goes on. Care must be taken to make sure that the probability represents that of the particular failure mode being evaluated.
7. *Causal Factors* This column identifies all of the possible factors that can cause the specific failure mode. Causal factors may include many different sources, such as physical failure, wear out, temperature stress, vibration stress, and the like. All conditions that affect a component or assembly should be listed to indicate whether there are special periods of operation, stress, personnel action, or combinations of events that would increase the probabilities of failure or damage.
8. *Immediate Effect* This column identifies the most immediate and direct effect of the indicated failure mode. This is the low-level effect that occurs on the next item in the design.
9. *System Effect* This column identifies the ultimate effect of the specific failure mode on the system. This is the high-level effect.

10. *Method of Detection* This column identifies how the specific failure mode might be detected after it has occurred and before resulting in any serious consequence. If a method of detection is possible, it may be used in the mitigating design.
11. *Current Controls* This column identifies how the specific failure mode is prevented from happening, or how it is safely mitigated should it occur.
12. *Hazard* This column identifies the specific hazard that is created as a result of the indicated failure mode. (Remember: Document all hazard considerations, even if they are later proven to be nonhazardous.)
13. *Risk* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, in terms of severity and probability. Note that reliability organizations use a risk priority number (RPN); however, an RPN is not useful for safety risk assessment. For system safety, the generally followed mishap risk index from MIL-STD-882 is used.

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

14. *Recommended Action* This column identifies methods for eliminating or mitigating the effects of the potential failure mode.

13.8 EXAMPLE 1: HARDWARE FMEA

This is an example of a hardware-type FMEA used to evaluate the system design during the design development process. Figure 13.9 depicts a missile battery that

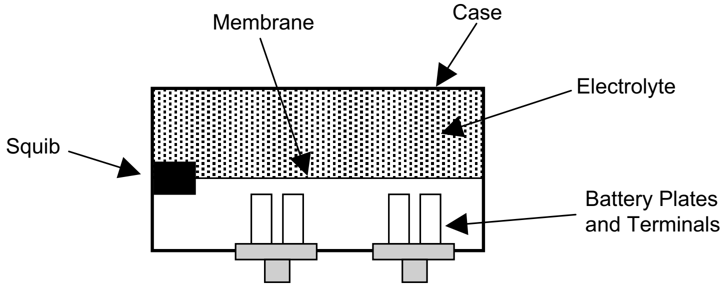


Figure 13.9 *FMEA example 1—battery.*

is inactive and inert until activated by a pyrotechnic squib. In this design, the electrolyte is separated from the battery plates by a frangible membrane. When battery power is desired, the squib is fired to break the membrane, and the released electrolyte energizes the battery.

The battery subsystem is comprised of the following components:

1. Case
2. Electrolyte
3. Battery plates and terminals
4. Membrane (separates electrolyte from battery plates)
5. Squib (breaks open the membrane)

The FMEA worksheets for this battery design are shown in Tables 13.4 and 13.5.

13.9 EXAMPLE 2: FUNCTIONAL FMEA

This is an example of a functional-type FMEA method that concentrates on system and software functions, by evaluating the various functional failure modes. Figure 13.10 depicts a generic aircraft landing gear system.

The GDnB button in Figure 13.10 is pressed to lower the landing gear and the GupB button is pressed to raise the gear. When the gear is up, switch S1 sends a true signal to the computer, otherwise it sends a false signal. When the gear is down, switch S2 sends a true signal to the computer, otherwise it sends a false signal. The purpose of the switches is for the system to know what position the landing gear is actually in and prevent conflicting commands. S_{WOW} is the weight-on-wheels switch.

The major functions of the landing gear, for both hardware and software functions, include:

1. Gear up
2. Gear down
3. Perform self-test
4. Report system malfunction
5. Record self-test results

Tables 13.6 and 13.7 contain the FMEA worksheets evaluating the functions involved with the aircraft landing gear. Note that in the functional FMEA the failure rate column is blank since rates are not available for functions.

13.10 LEVEL OF DETAIL

The FMEA level of detail applies to the function/hardware indenture level at which failures are postulated. Failures can be considered at any level, from the top system

TABLE 13.4 Hardware FMEA of Battery—Worksheet 1

Failure Mode and Effects Analysis										
System: Missile				Subsystem: Missile Battery			Mode/Phase: Operation			
Component	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recommended Action
Case	Cracks	3.5×10^{-5} Manuf. data	Manufacturing defect	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2D	Add system sensor
	Pinholes	1.1×10^{-9} Manuf. data	Material defect	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2E	Add system sensor
Electrolyte	Leaks out of case	4.1×10^{-6} Manuf. data	Case defect; pinholes	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2D	Add system sensor
	Wrong electrolyte used	1.0×10^{-5} Manuf. data	Human error	Does not react with battery plates	No power output from battery	Inspection	QA	Unsafe battery reaction	2D	
Battery plates and terminals	Cracks	2.2×10^{-6} Manuf. data	Material defect	Inadequate battery reaction	Insufficient power output from battery	None	None	None	4D	
	Breaks	1.0×10^{-9} Manuf. data	Material defect	Inadequate battery reaction	No power output from battery	None	None	None	4E	
Analyst:				Date:			Page: 1/2			

TABLE 13.5 Hardware FMEA of Battery—Worksheet 2

Failure Mode and Effects Analysis										
System: Missile				Subsystem: Missile Battery			Mode/Phase: Operation			
Component	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recommended Action
Membrane	Cracks	3.5×10^{-5} Manuf. data	Materiel defect	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2D	Add system sensor
	Pinholes	1.1×10^{-9} Manuf. data	Materiel defect	Electrolyte leakage	No power output from battery	Inspection	QA	Fire source	2E	Add system sensor
	Fails to rupture	4.1×10^{-6} Manuf. data	Materiel defect	No electrolyte to battery plates	No power output from battery	Inspection	QA	None	2D	Add system sensor
Squib	Fails to fire	4.1×10^{-9} Manuf. data	Materiel defect	No electrolyte to battery plates	No power output from battery	Inspection	None	None	2E	
	Fires prematurely	4.1×10^{-9} Manuf. data	Materiel; RF energy; dropped	Premature electrolyte to battery plates	Premature battery activation	System sensor for power	System sensor for power	Premature missile power	2E	Add system sensor
Analyst:				Date:			Page: 2/2			

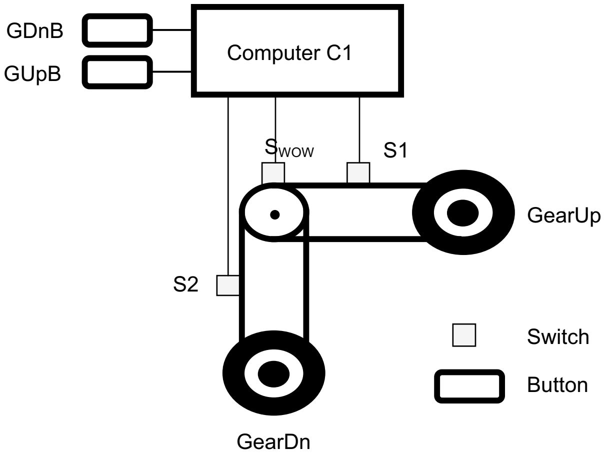


Figure 13.10 *FMEA example 2—aircraft landing gear system.*

functions down to individual components. During the conceptual phase of system development, a high-level functional approach is particularly appropriate for eliminating design inadequacies. In later system development phases, more detailed hardware or functional approaches are more appropriate for adequately implementing the design concept. Thus, the FMEA level of detail is affected by the phase of system development in which it is performed.

A less detailed analysis, completed at a time when it can contribute measurably to the adequacy of the system design, may be much more valuable than a more detailed analysis delivered at such a late date that implementation costs make changes unfeasible.

The functional approach is the system-level approach conducting an FMEA, is normally used when system hardware definition has not reached the point of identifying specific hardware items, and requires a less detailed analysis. This method of analysis is more adaptable to considering multiple failures and external influences such as software functions and human error. The hardware approach is the more rigorous and detailed method of conducting an FMEA and is normally used whenever the hardware items can be identified from engineering drawings. While the hardware approach is normally utilized from the part level up, it can be initiated at almost any indenture level.

13.11 ADVANTAGES AND DISADVANTAGES

The following are advantages of the FMEA technique. The FMEA:

1. Is easily understood and performed.
2. Is relatively inexpensive to perform, yet provides meaningful results.

TABLE 13.6 Functional FMEA of Landing Gear—Worksheet 1

Failure Mode and Effects Analysis

System: Aircraft Subsystem: Landing Gear Mode/Phase: Flight

Function	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recommended Action
Gear up	Fails to issue	N/A	Computer; software; wiring	Landing gear	Aircraft flight with gear down	Sensor		Damage from drag	4C	
	Issues prematurely	N/A	Computer; software	If down, landing gear raises prematurely	Gear raises during taxi or takeoff	Sensor		Aircraft damage during taxi	2C	
Gear down	Fails to issue	N/A	Computer; software; wiring	Unable to lower landing gear	Aircraft must land with landing gear up	Sensor		Damage or injury during landing	2C	
	Issues prematurely	N/A	Computer; software	If up, landing gear lowers prematurely	Aircraft flight with gear down	Sensor		Damage from drag	2C	
Gear self-test (BIT = built-in-test)	Fails to occur	N/A	Computer; software; electronic faults	Landing gear fault not detected	Unable to raise or lower gear when desired, no warning	None		Possible unsafe state	4C	
	Occurs erroneously	N/A	Computer; software; electronic faults	Landing gear fault self-test data incorrect	No warning or incorrect warning regarding landing gear status	None		Possible unsafe state	4C	

Analyst: Date: Page: 1/2

TABLE 13.7 Functional FMEA of Landing Gear—Worksheet 2

Failure Mode and Effects Analysis										
System: Aircraft				Subsystem: Landing Gear				Mode/Phase: Flight		
Function	Failure Mode	Failure Rate	Causal Factors	Immediate Effect	System Effect	Method of Detection	Current Controls	Hazard	Risk	Recommended Action
Report system malfunction	Fails to occur	N/A	Computer; software; electronic faults	BIT data not reported	No warning of fault state	Pilot report		None	4D	
	Occurs erroneously	N/A	Computer; software; electronic faults	BIT data reported incorrectly	No warning of fault state, or incorrect warning	Pilot report		None	4D	
Record self-test results	Fails to occur	N/A	Computer; software; electronic faults	BIT data not recorded	No recording of fault state	Data analysis		None	4D	
	Occurs erroneously	N/A	Computer; software; electronic faults	BIT data recorded incorrectly	No recording of fault state, or incorrect recording	Data analysis		None	4D	
Analyst:				Date:			Page: 2/2			

3. Provides rigor for focusing the analysis.
4. Provides a reliability prediction of the item being analyzed.
5. Has commercial software available to assist in the FMEA process.

The following are disadvantages of the FMEA technique. The FMEA:

1. Focuses on single failure modes rather than failure mode combinations.
2. Not designed to identify hazards unrelated to failure modes.
3. Provides limited examination of human error.
4. Provides limited examination of external influences and interfaces.
5. Requires expertise on the product or process under analysis.

13.12 COMMON MISTAKES TO AVOID

When first learning how to perform an FMEA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of an FMEA.

1. Not utilizing a structured approach with a standardized worksheet
2. Not having a design team participate in the analysis in order to obtain all possible viewpoints
3. Not fully investigating the complete effect of a failure mode

13.13 SUMMARY

This chapter discussed the FMEA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of an FMEA is to identify potential failure modes and to evaluate the effect of these failures should they occur. The FMEA is primarily for reliability but can also be used for safety evaluations with some modification.
2. An FMEA is a qualitative and/or quantitative analysis tool. It can be used quantitatively to predict the failure rate of an assembly, unit, or subsystem.
3. The FMEA generally requires detailed design information.
4. FMEAs can be used to evaluate the design of hardware, software, functions, and processes.
5. The FMEA should not be the sole analysis for the identification of hazards but should be used in conjunction with other hazard analyses. FMEA should be a supplement to the DD-HAT and SD-HAT analyses.

6. FMEAs are most effectively performed through a team effort, involving all the disciplines involved with the product or process.
7. A safety-oriented FMEA provides the following information:
   - Failure modes
   - The immediate and system effect of the failure modes
   - Failure rates
   - Hazards resulting from the failure modes
   - Mishap risk assessment

REFERENCES

1. MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, 1980.
2. SAE Standard J-1739, Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA), August 2002.
3. AIAG, *FMEA-3 Potential Failure Mode and Effects Analysis*, 3rd ed., Automotive Industry Action Group (AIAG), July 2002 (equivalent of SAE J-1739).

BIBLIOGRAPHY

IEC 60812, *Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA)*, 2nd ed., 2001.

McDermott, R., R. Mikulak, and M. Beauregard, *The Basics of FMEA*, Productivity, Inc., 1996.

OLB-71, Failure Mode and Effects Analysis, Engineering Industry Training Board (EITB), Watford, England, 1986.

SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Appendix G—Failure Mode and Effects Analysis, 1996.

SAE ARP5580, Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications, July 2001.

Stamatis, D. H., *Failure Mode and Effect Analysis: FMEA from Theory to Execution*, Quality Press, American Society for Quality, 1995.

STUK-YTO-TR 190, Failure Mode and Effects Analysis of Software-Based Automation Systems, August 2002, Finish Radiation and Nuclear Safety Authority.

Chapter 14

Fault Hazard Analysis

14.1 INTRODUCTION

Fault hazard analysis (FaHA) is an analysis technique for identifying those hazards arising from component failure modes. It is accomplished by examining the potential failure modes of subsystems, assemblies, or components and determining which failure modes can form undesired states that could result in a mishap.

14.2 BACKGROUND

The FaHA technique falls under the detailed design hazard analysis type (DD-HAT) analysis. The basic hazard analyses types are described in Chapter 3. The purpose of FaHA is to identify hazards through the analysis of potential failure modes in the hardware that comprises a subsystem.

The FaHA is applicable to analysis of all types of systems and equipment. FaHA can be implemented on a subsystem, a system, or an integrated set of systems. The FaHA can be performed at any level from the component level through the system level. It is hardware oriented and not suited for software analysis.

The FaHA is a thorough technique for evaluating potential failure modes. However, it has the same limitations as the FMEA. It looks at single failures and not combinations of failures. FaHAs generally overlook hazards that do not result entirely from failure modes, such as poor design, timing errors, and the like.

The conduct of an FaHA requires a basic understanding of hazard analysis theory, failure modes, and a detailed understanding of the system under analysis. The methodology is similar to failure mode and effects analysis (FMEA). Although the FaHA

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

is a valuable hazard analysis technique, the subsystem hazard analysis (SSHA) has replaced the FaHA. The SSHA methodology includes considering failure modes for safety implications, and thus it accomplishes the same objective as the FaHA.

The FaHA technique is not recommended for general usage. Other safety analysis techniques are more cost effective for the identification of hazards and root causes, such as the SSHA. The FaHA should be used only when a rigorous analysis of all component failure modes is required. The FaHA technique is uncomplicated and easily mastered using the worksheets and instructions provided in this chapter.

14.3 HISTORY

The Boeing Company developed the FaHA in 1965 for the Minuteman program as a variation of the FMEA technique. It was developed to allow the analyst to stop the analysis at a point where it becomes clear that a failure mode did not contribute to a hazard, whereas the FMEA requires complete evaluation of all failure modes.

14.4 THEORY

The FaHA is a qualitative and/or quantitative analysis method. The FaHA can be used exclusively as a qualitative analysis or, if desired, expanded to a quantitative one for individual component failure modes. The FaHA requires a detailed investigation of the subsystems to determine which components can fail leading to a hazard and resultant effects to the subsystem and its operation.

The FaHA answers a series of questions:

- What can fail?
- How it can fail?
- How frequently will it fail?
- What are the effects of the failure?
- What hazards result as a consequence of failure?

The FaHA considers total functional and out-of-tolerance modes of failure. For example, a 5 percent, 5000-Ω (±250-Ω) resistor can have as functional failure modes “failing open” or “failing short,” while the out-of-tolerance modes might include “too low a resistance” or “too high a resistance.”

To conduct an FaHA, it is necessary to know and understand the following system characteristics:

- Equipment mission
- Operational constraints
- Success and failure boundaries
- Realistic failure modes and their probability of occurrence

The general FaHA approach involves the following:

- Analyzing each component
- Analyzing all component failure modes
- Determining if failure mode directly causes hazard
- Determining the failure mode effect on subsystem and system
- Determining if the component failure can be induced by another component

The FaHA approach utilizing a columnar form with specially selected entries provides optimum results. This approach establishes a means for systematically analyzing a system or subsystem design for the identification of hazards. In addition to identifying hazards, data in the FaHA form provides useful information for other safety analyses, such as the fault tree analysis.

The purpose of the FaHA is to identify hazards existing within a subsystem due to potential hardware component failure. This is accomplished by examining the causes and effects of subsystem component failures.

14.5 METHODOLOGY

Table 14.1 lists the basic steps in the FaHA process. The FaHA methodology is demonstrated in Figure 14.1 which contains a hypothetical system, consisting of two subsystems, shown in functional block diagram format. In performing an FaHA, the idea is to break each subsystem into major components or black boxes, whose failure modes can be evaluated.

The next step is to identify and evaluate all credible failure modes for each component within the black box or subsystem. For instance, in subsystem 1, component B may fail "open." The effects of this failure mode upon components A and C are determined and also the effects at the subsystem interface with subsystem 2.

Secondary factors that could cause component B to fail open are identified. For instance, excessive heat radiated from component C may cause component B to fail open.

Events "upstream" of component B that could directly command component B to fail open are identified. These types of events are usually a part of the normal sequence of planned events, except they occur at the wrong time and may not be controllable once they occur on their own. For example, a short circuit in component A may output from component A the signal that commands component B to respond in the open mode.

When the FaHA is completed, the effects of failures in subsystem 1 will terminate at the interface, and the upstream events commanding failures in subsystem 2 will begin from the interface. Hence, it is possible to determine interface hazards by comparing the "effects" of subsystem 1 with the "upstream events" of subsystem 2. This is an indirect result of the FaHA.

TABLE 14.1 FaHA Process

Step	Task	Description
1	Define system.	Define, scope, and bound system. Establish indenture levels for items to be analyzed.
2	Plan FaHA.	Establish FaHA goals, definitions, worksheets, schedule, and process. Define credible failures of interest for the analysis.
3	Acquire data.	Acquire all of the necessary design and process data needed for the FaHA. Refine the item indenture levels for analysis. Data can include functional diagrams, schematics, and drawings for the system, subsystems, and functions. Sources for this information could include design specifications, functional block diagrams, sketches, drawings, and schematics.
4	Partition system.	Divide the system under analysis into smaller logical and manageable segments, such as subsystems, units, or functional boxes.
5	Conduct FaHA.	For analyses performed down to the component level, a complete component list with the specific function of each component is prepared for each module as it is to be analyzed. Perform the FaHA on each item in the identified list of components. This step is further expanded in the next section. Analysis identifies: • Failure mode • Immediate failure effect • System-level failure effect • Potential hazard and associated risk
6	Recommend corrective action.	Recommend corrective action for failure modes with unacceptable risk or criticality to program manager for action.
7	Monitor corrective action.	Review the FaHA at scheduled intervals to ensure that corrective action is being implemented.
8	Document FaHA.	Documentation of the entire FaHA process, including the worksheets. Update for new information and closure of assigned corrective actions.

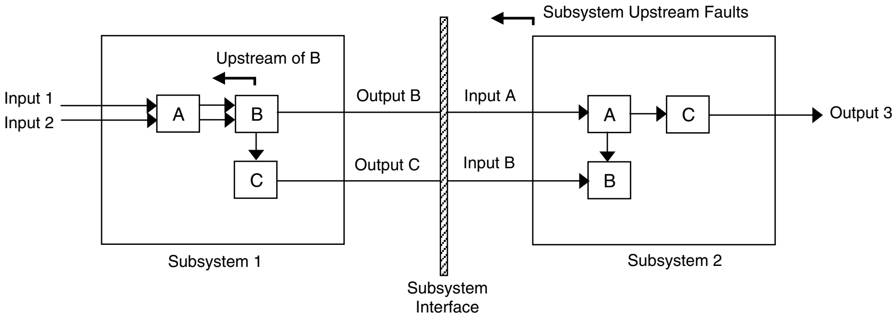


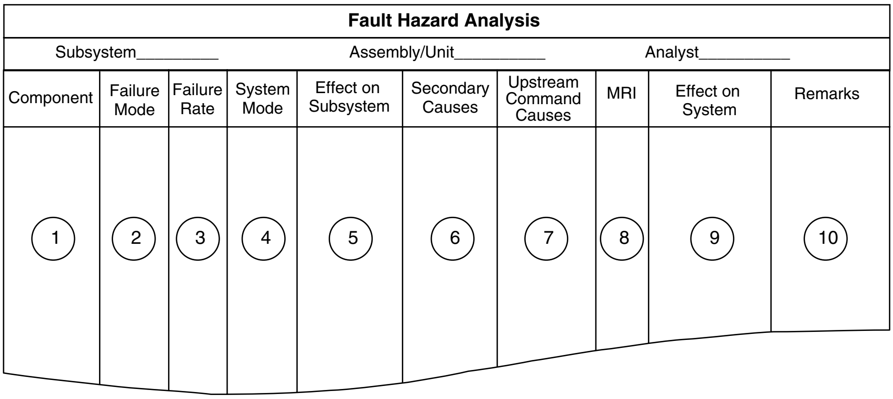
Figure 14.1 *Example system interface.*

14.6 WORKSHEET

The FaHA is a formal and detailed hazard analysis utilizing structure and rigor. It is desirable to perform the FaHA using a worksheet. Although the format of the analysis worksheet is not critical, a recommended FaHA format is shown in Figure 14.2. This is the form that was successfully used on the Minuteman missile weapon system program.

The intended content for each column is described as follows:

1. *Component* This column identifies the major functional or physical hardware components within the subsystem being analyzed. The component should be identified by part number and descriptive title.
2. *Failure Mode* This column identifies all credible failure modes that are possible for the identified component. This information can be obtained from the FMEA, manufacturer's data or testing. (Note: This column matches the "primary" cause question in an FTA.)
3. *Failure Rate* This column provides the failure rate or failure probability for the identified mode of failure. The source of the failure rate should also be provided for future reference.
4. *Operational Mode* This column identifies the system phase or mode of operation during the indicated failure mode.
5. *Effect on Subsystem* This column identifies the direct effect on the subsystem and components within the subsystem for the identified failure mode.
6. *Secondary Causes* This column identifies secondary factors that may cause the component to fail. Abnormal and out-of-tolerance conditions may cause the component failure. Component tolerance levels should be provided. Also, environmental factors or common cause events may be a secondary cause for failure. (Note: This column matches the "secondary" cause question in an FTA.)



Fault Hazard Analysis

Subsystem_________ Assembly/Unit_________ Analyst_________

Component	Failure Mode	Failure Rate	System Mode	Effect on Subsystem	Secondary Causes	Upstream Command Causes	MRI	Effect on System	Remarks
①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩

Figure 14.2 Recommended FaHA worksheet.

7. *Upstream Command Causes* This column identifies those functions, events, or failures that directly force the component into the indicated failure mode. (Note: This column matches the "command" cause question in an FTA.)
8. *Mishap Risk Index (MRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values from MIL-STD-882 are shown below.

Severity	Probability
I. Catastrophic	A. Frequent
II. Critical	B. Probable
III. Marginal	C. Occasional
IV. Negligible	D. Remote
	E. Improbable

9. *Effect on System* This column identifies the direct effect on the system of the indicated component failure mode.
10. *Remarks* This column provides for any additional information that may be pertinent to the analysis.

14.7 EXAMPLE

In order to demonstrate the FaHA technique, the same hypothetical small missile system from Chapter 4 on preliminary hazard list (PHL) analysis will be used. The basic preliminary component and function design information from the PHL is provided again in Figure 14.3.

Components	Functions
Missile Body	Storage
Warhead	Transportation
Engine (Jet)	Handling
Fuel (Liquid)	Standby
Computer	Alert
Software	Launch
Navigation	Flight
Communications	Command
Guidance	Response
Battery	Impact

Figure 14.3 *Missile system component list and function list.*

Typically, an FaHA would be performed on each of the component subsystem designs. For this FaHA example, the battery subsystem has been selected for evaluation using the FaHA technique. The battery design is shown in Figure 14.4.

In this design the electrolyte is contained separately from the battery plates by a frangible membrane. When battery power is desired, the squib is fired, thereby breaking the electrolyte housing and releasing electrolyte into the battery, thus energizing the battery.

The battery subsystem is comprised of the following components:

1. Case
2. Electrolyte
3. Battery plates
4. Frangible container separating electrolyte from battery plates
5. Squib that breaks open the electrolyte container

The battery FaHA is shown in Table 14.2.

The following conclusions can be derived from the FaHA worksheet contained in Table 14.2:

1. The failures with a risk level of 2C indicate that the failure mode leaves the system in an unsafe state, which will require further analysis to evaluate the unsafe state and design mitigation to reduce the risk.
2. The failures with a risk level of 4C indicate that the failure mode leaves the missile in a state without power, resulting in a dud missile (not a safety problem).

14.8 ADVANTAGES AND DISADVANTAGES

The following are advantages of the FaHA technique:

1. FaHAs are more easily and quickly performed than other techniques (e.g., FTA).
2. FaHAs can be performed with minimal training.
3. FaHAs are inexpensive.
4. FaHAs forces the analyst to focus on system elements and hazards.

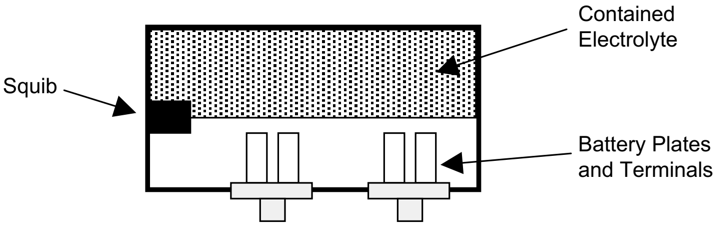


Figure 14.4 *Example missile battery design.*

TABLE 14.2 FaHA Worksheet for Battery

Fault Hazard Analysis

Subsystem: Missile Assembly/Unit: Battery Analyst: Date:

Component	Failure Mode	Failure Rate	System Mode	Effect on Subsystem	Secondary Causes	Upstream Command Causes	MRI	Effect On System	Remarks
Battery squib	Squib fails to ignite	3.5×10^{-5} Manuf. data	Flight	No power output from battery	Excessive shock	No ignition command	4C	Dud missile	Safe
	Squib ignites inadvertently	1.1×10^{-9} Manuf. data	Ground operations	Battery power is inadvertently applied	Heat; shock	Inadvertent ignition command	2C	Unsafe system state	Further analysis required
Battery electrolyte	Electrolyte leakage	4.1×10^{-6} Manuf. data	Ground operations	Corrosion; gases; fire	Excessive shock; puncture	Manufacturing defect	2C	Unsafe system state	Further analysis required
Battery power	Premature power output	1.0×10^{-10} Manuf. data	Ground operations	Power is inadvertently applied to missile electronics	None	Electrolyte leakage into battery cells	2C	Unsafe system state	Further analysis required
	No power output	2.2×10^{-6} Manuf. data	Flight	No power output to missile electronics	Battery damage	Broken cables	4C	Dud missile	Safe
Battery case	Case leaks	1.0×10^{-12} Manuf. data	Flight	No power output	Excessive shock		4C	Dud missile	Safe
			Ground operations	Corrosion; gases; fire	Excessive shock		2C	Unsafe state	Further analysis required
							Page: 1 of 1		

The following are disadvantages of the FaHA technique:

1. FaHAs focus on single failure modes and not combinations of failure modes.
2. The FaHA focuses on failure modes, overlooking other types of hazards (e.g., human errors).
3. FaHAs are not applicable to software since software has no failure modes.

14.9 COMMON MISTAKES TO AVOID

When first learning how to perform an FaHA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of an FaHA:

1. Not fully understanding the FaHA technique
2. Using the FaHA technique when another technique might be more appropriate

14.10 SUMMARY

This chapter discussed the FaHA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of the FaHA is to identify hazards by focusing on potential hardware failure modes. Every credible single failure mode for each component is analyzed to determine if it can lead to a hazard.
2. FaHA is a qualitative and/or quantitative analysis tool.
3. The use of a functional block diagram greatly aids and simplifies the FaHA process.

BIBLIOGRAPHY

Ericson, C. A., Boeing Document D2-113072-2, *System Safety Analytical Technology—Fault Hazard Analysis*, 1972.

Harris, R. W., Fault Hazard Analysis, USAF—Industry System Safety Conference, Las Vegas, Feb., 1969.

Chapter 15

Functional Hazard Analysis

15.1 INTRODUCTION

Functional hazard analysis (FuHA) is a tool for identifying hazards through the rigorous evaluation of system and/or subsystem functions including software. Systems are designed to perform a series of functions, which can be broken into subfunctions, sub-subfunctions, and so forth. Functional objectives are usually well understood even when detailed design details are not available or understood. FuHA is an inductive hazard analysis approach (inductively determines effect of fault events) that evaluates the functional failure, corruption, and malfunction of functions.

15.2 BACKGROUND

This analysis technique does not uniquely fit into any one of the basic hazard analyses types described in Chapter 3 because the primary focus of this technique is on the analysis of functions only. It could be performed during preliminary design in support of a preliminary design hazard analysis type (PD-HAT), or it could be performed during detailed design in support of a system design hazard analysis type (SD-HAT).

Within the safety community the acronym FHA has been used for both functional hazard analysis and fault hazard analysis. Within this book fault hazard analysis will be referred to as FaHA and functional hazard analysis as FuHA.

The purpose of FuHA is to identify system hazards by the analysis of functions. Functions are the means by which a system operates to accomplish its mission or goals. System hazards are identified by evaluating the safety impact of a function failing to operate, operating incorrectly, or operating at the wrong time. When a

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

function's failure can be determined hazardous, the casual factors of the malfunction should be investigated in greater detail.

The FuHA method is applicable to the analysis of all types of systems, equipment, and software. FuHA can be implemented on a single subsystem, a complete functional system, or an integrated set of systems. The level of analysis detail can vary, depending upon the level of functions being analyzed. For example, analysis of high-level system functions will result in a high-level hazard analysis, whereas analysis of low-level (detailed design) subsystem functions will yield a more detailed functional analysis.

The technique, when methodically applied to a given system by experienced safety personnel, is thorough in identifying system functional hazards. Through logical analysis of the way a system is functionally intended to operate, the FuHA provides for the identification of hazards early in the design process. A basic understanding of system safety concepts and experience with the particular type of system is essential to create a correct list of potential hazards. The technique is uncomplicated and easily learned. Standard, easily followed FuHA forms and instructions are provided in this chapter.

The FuHA method is a powerful, efficient, and comprehensive system safety analysis technique for the discovery of hazards. It is especially powerful for the safety assessment of software. After a functional hazard is identified, further analysis of that hazard may be required to determine if the causal factors of the functional failure are possible. Since the FuHA focuses on functions, it might overlook other types of hazards, such as those dealing with hazardous energy sources, sneak circuit paths, hazardous material, and the like. For this reason the FuHA should not be the sole hazard analysis performed but should be done in support of other types of hazard analysis, for example, preliminary hazard analysis (PHA) or subsystem hazard analysis (SSHA).

15.3 HISTORY

The exact history of this technique is unknown. The technique seems to have naturally evolved over the years for the early analysis of systems when functional design information is available prior to the development of detailed design.

15.4 THEORY

Figure 15.1 shows an overview of the basic FuHA process and summarizes the important relationships involved. This process involves the evaluation of system functions for the identification and mitigation of hazards.

Input information for the FuHA consists of all design information relating to functional system operation. Typically the following types of information are available and utilized in the FuHA:

1. System design and operation information

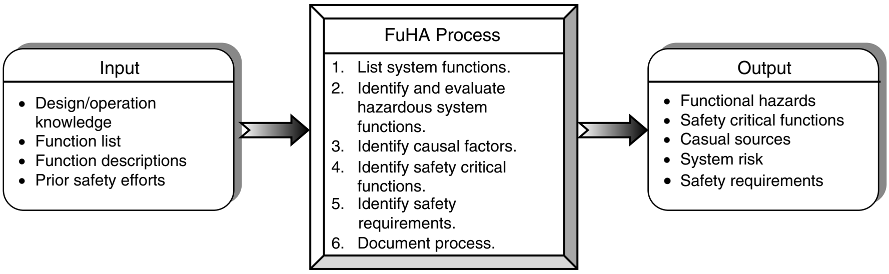

Input
• Design/operation knowledge
• Function list
• Function descriptions
• Prior safety efforts
FuHA Process
1. List system functions.
2. Identify and evaluate hazardous system functions.
3. Identify causal factors.
4. Identify safety critical functions.
5. Identify safety requirements.
6. Document process.
Output
• Functional hazards
• Safety critical functions
• Casual sources
• System risk
• Safety requirements

Figure 15.1 *FuHA overview.*

2. A developed list of all system functions
3. Information from the preliminary hazard list (PHL), PHA, and SSHA (if previously performed)
4. Functional flow diagrams of system operation
5. Hazard checklists (hazardous functions, tasks, etc.)

The primary purpose of the FuHA is to identify and mitigate hazards resulting from the malfunction or incorrect operation of system functions. As such, the following information is typically output from the FuHA:

1. Functional hazards
2. Identification of safety critical functions
3. Hazard causal factors (failures, design errors, human errors, etc.)
4. Risk assessment
5. Safety requirements to mitigate the hazard

15.5 METHODOLOGY

Table 15.1 lists and describes the basic steps in the FuHA process. This process involves performing a detailed analysis focused on system functions.

Figure 15.2 depicts the overall FuHA methodology. A key element of this methodology is to identify and understand all system functions. A function list must be created, and the use of functional flow diagrams is recommended because they provide an invaluable aid to the analysis. Checklists are applied against the function list to help identify hazards.

Figure 15.3 provides an example checklist of common failure states used for the analysis of functions. Each of the system functions should be evaluated for the effect of the failure state on the system.

TABLE 15.1 FuHA Process

Step	Task	Description
1	Define operation.	Define, scope, and bound the operation to be performed. Understand the operation and its objective.
2	Acquire data.	Acquire all of the necessary design and operational data needed for the analysis. This includes both schematics and manuals.
3	List functions.	Make a detailed list of all the functions to be considered in the FuHA. This might be taken directly from a design document that is already written. It is important that all functions are considered.
4	Conduct FuHA.	Perform the FuHA on each item in the function list. This involves evaluating the effect of each functional failure mode. It is important that all functional failure modes be identified, along with the mission phase under analysis. Utilize existing hazard analyses results to assist in identifying hazards. Also, use hazard checklists to assist in hazard recognition. Identify hazards and any existing design features to eliminate or mitigate the hazard.
5	Evaluate system risk.	Identify the level of mishap risk presented by the identified hazards.
6	Identify safety critical functions.	Based on level of risk criticality, identify those functions that are considered safety critical.
7	Recommend corrective action.	Recommend corrective action for hazards with unacceptable risk. Develop derived safety requirements to mitigate identified hazards. Also, identify safety features already in the design or procedures for hazard mitigation.
8	Monitor corrective action.	Review design requirements to ensure that corrective action is being implemented.
9	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
10	Document FuHA.	Document the entire FuHA process on the worksheets. Update for new information and closure of assigned corrective actions.

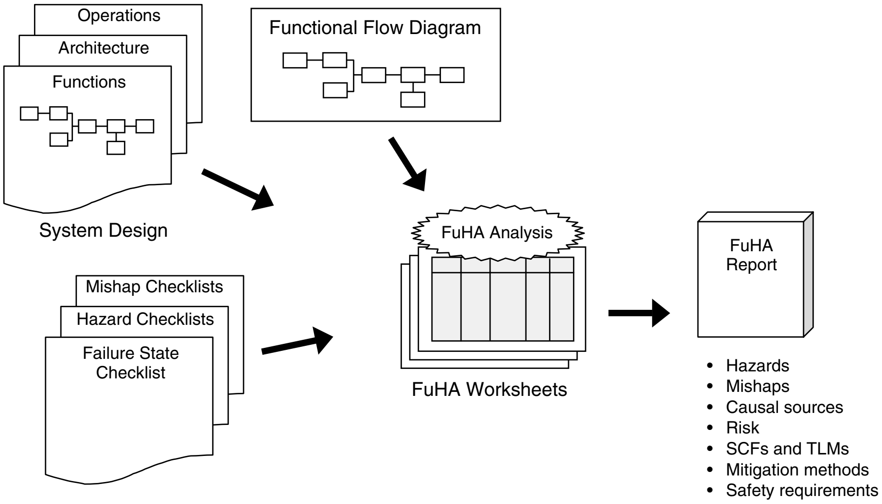


Figure 15.2 FuHA methodology.

1. Fails to operate
2. Operates incorrectly/erroneously
3. Operates inadvertently
4. Operates at wrong time (early, late)
5. Unable to stop operation
6. Receives erroneous data
7. Sends erroneous data
8. Conflicting data or information

Figure 15.3 *Example of hazard checklist for failure states.*

15.6 WORKSHEETS

It is desirable to perform the FuHA analysis using a worksheet. The worksheet will help to add structure and rigor to the analysis, record the process and data, and help support justification for the identified hazards. The format of the analysis worksheet is not critical, and typically columnar-type worksheets are utilized.

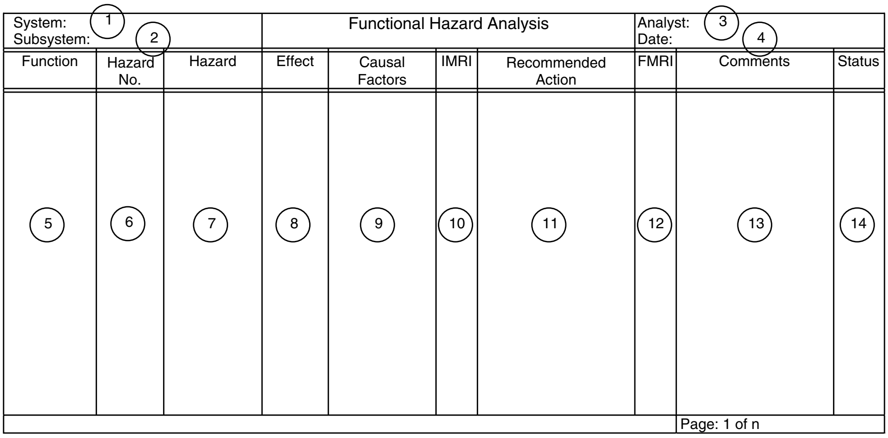
The following basic information should be obtained from the FuHA analysis worksheet:

1. Hazards
2. Hazard effects (mishaps)
3. Hazard causal factors (to subsystem identification)
4. Safety critical factors or parameters
5. Risk assessment (before and after design safety features are implemented)
6. Derived safety requirements for eliminating or controlling the hazards

A recommended FuHA analysis worksheet is shown in Figure 15.4. This particular FuHA analysis worksheet utilizes a columnar-type format. Other worksheet formats may exist because different organizations often tailor their FuHA analysis worksheet to fit their particular needs. The specific worksheet to be used may be determined by the system safety program (SSP), system safety working group, or the FuHA customer.

The following instructions describe the information required under each column entry of the FuHA worksheet:

1. *System* This column identifies the system under analysis.
2. *Subsystem* This column identifies the subsystem under analysis.
3. *Analyst* This column identifies the analyst performing the analysis.
4. *Date* This column identifies the date of the analysis.
5. *Function* This column identifies the design function. List and describe each of the system functions to be performed. If possible, include the purpose and the mode or phase of operation being performed.



System: 1 Subsystem: 2			Functional Hazard Analysis				Analyst: 3 Date: 4		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
5	6	7	8	9	10	11	12	13	14
								Page: 1 of n	

Figure 15.4 *Recommended FuHA worksheet.*

6. *Hazard Number* This column identifies the number assigned to the identified hazard in the FuHA (e.g., FuHA-1, FuHA-2). This hazard number is for future reference to the particular hazard source and will be recorded in the associated hazard action record (HAR).
7. *Hazard* This column identifies the specific hazard being postulated and evaluated for the stated functional failure. (Remember: Document all hazard considerations, even if they are later proven to be nonhazardous.) Generally, a hazard is identified by considering the effect of function failure, erroneous function, incorrect function timing, and the like.
8. *Effect* This column identifies the effect and consequences of the hazard, should it occur. Generally, the worst-case mishap result is the stated effect.
9. *Causal Factors* This column identifies the causal factors involved in causing the functional failure and in causing the final effect resulting from the failure.
10. *Initial Mishap Risk Index (IMRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values from MIL-STD-882 are shown below.

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

11. *Recommended Action* This column establishes recommended preventive measures to eliminate or control identified hazards. Safety requirements in this situation generally involve the addition of one or more barriers to keep the energy source away from the target. The preferred order of precedence for design safety requirements is as shown below.

Order of Precedence
1. Eliminate hazard through design selection.
2. Control hazard through design methods.
3. Control hazard through safety devices.
4. Control hazard through warning devices.
5. Control hazard through procedures and training.

12. *Final Mishap Risk Index (FMRI)* This column provides a qualitative measure of mishap risk significance for the potential effect of the identified hazard, given that mitigation techniques and safety requirements are applied to the hazard. The same metric definitions used in column 10 are also used here.
13. *Comments* This column provides a place to record useful information regarding the hazard or the analysis process that are not noted elsewhere.
14. *Status* This column states the current status of the hazard, as either being open or closed. This follows the hazard tracking methodology established for the program. A hazard can only be closed when it has been verified through analysis, inspection, and/or testing that the safety requirements are implemented in the design and successfully tested for effectiveness.

Note in this analysis methodology that every system function is listed and analyzed. For this reason, not every entry in the FuHA form will constitute a hazard since not every function is hazardous. The analysis documents, however, that all functions were considered by the FuHA. Note also that the analysis becomes a traceability matrix, tracing each function and its safety impact.

In filling out the columnar FuHA form, the dynamic relationship between the entries should be kept in mind. The hazard, cause, and effect columns should completely describe the hazard. These columns should provide the three sides of the hazard triangle (see Chapter 2): source, mechanism, and outcome. Also, the FuHA can become somewhat of a living document that is continually being updated as new information becomes available.

15.7 EXAMPLE 1: AIRCRAFT FLIGHT FUNCTIONS

Table 15.2 provides a list of aircraft functions derived from the initial design concept for the aircraft system. This table also identifies the major failure condition of concern for each of the functions. These high-level functions are analyzed by FuHA.

Tables 15.3 and 15.4 contain the FuHA worksheets for this example.

TABLE 15.2 Basic Aircraft Functions

No.	Function	Failure Condition
1	Control flight path	Inability to control flight path
2	Control touchdown and rollout	Inability to control touchdown and rollout
3	Control thrust	Inability to control thrust
4	Control cabin environment	Inability to control cabin environment
5	Provide spatial orientation	Inability to control to provide spatial orientation
6	Fire protection	Loss of fire protection

15.8 EXAMPLE 2: AIRCRAFT LANDING GEAR SOFTWARE

Figure 15.5 provides an example generic landing gear system that is computer driven using software. In this example FuHA analyzes the software functions. The GDnB button is pressed to lower the landing gear, and the GupB button is pressed to raise the gear. When the gear is up, switch S1 sends a true signal to the computer; otherwise it sends a false signal. When the gear is down, switch S2 sends a true signal to the computer; otherwise it sends a false signal. The purpose of the switches is for the system to know what position the landing gear is actually in and prevent conflicting commands. S_{WOW} is the weight-on-wheels switch.

The major software functions for the landing gear are listed in Figure 15.5. These functions have been identified early in the design but have not yet been actually developed. Even though software code modules are yet to be developed to perform these functions, they can still be analyzed by FuHA.

Tables 15.5 and 15.6 contain the FMEA worksheets evaluating the functions involved with the aircraft landing gear.

15.9 EXAMPLE 3: ACE MISSILE SYSTEM

In order to demonstrate the FuHA methodology, the same hypothetical small missile system from Chapters 4 and 5 will be used. The basic system design information provided in the PHA is shown again in Figure 15.6.

Figure 15.7 lists the major system components, functions, phases, and energy sources that should be considered for any system analysis. The major segments of the system are the missile and the weapon control system (WCS). FuHA will analyze the functions in this chart.

The FuHA worksheets for the Ace Missile System are shown in Tables 15.7 and 15.8.

15.10 ADVANTAGES AND DISADVANTAGES

The following are advantages of the FuHA technique:

1. Is easily and quickly performed.
2. Does not require considerable expertise.

TABLE 15.3 FuHA Example 1—Worksheet 1

System: Aircraft Subsystem: Critical Functions			Functional Hazard Analysis				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
Control flight path (pitch and yaw)	F-1	Fails to occur, causing aircraft crash	Inability to control flight path (e.g., elevator hard over)	Loss of hydraulics; flight controls; software	1C			Safety critical function	Open
	F-2	Occurs erroneously, causing aircraft crash	Elevator hard over	Software	1C				Open
Control touchdown and rollout	F-3	Fails to occur, causing aircraft crash	Inability to control flight path	Loss of hydraulics; flight controls; software	1C			Safety critical function	Open
	—	Occurs erroneously, causing aircraft crash	Not applicable						Open
Control thrust (engine speed and power)	F-4	Fails to occur, causing aircraft crash	Loss of aircraft thrust when needed	Engine hardware; software	1C			Safety critical function	Open
	F-5	Occurs erroneously, causing aircraft crash	Incorrect aircraft thrust	Engine hardware; software	1C				Open
							Page: 1 of 2		

TABLE 15.4 FuHA Example 1—Worksheet 2

System: Aircraft Subsystem: Critical Functions			**Functional Hazard Analysis**				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
Control cabin environment	F-6	Fails to occur, causing passenger becomes sick	Passenger comfort	Computer fault; software	2D				Open
	F-7	Occurs erroneously, causing passenger becomes sick	Passenger comfort	Computer fault; software	2D				Open
Provide spatial orientation	F-8	Fails to occur, causing aircraft crash	Pilot loses spatial orientation during critical flight	Computer fault; software; displays fail	1C	Provide three independent displays		Safety critical function	Open
	F-9	Occurs erroneously, causing aircraft crash	Pilot loses spatial orientation during critical flight	Computer fault; software; displays fail	1C				Open
Fire protection	F-10	Fails to occur, causing aircraft crash	Unable to extinguish onboard fire	Computer fault; software	1C			Safety critical function	Open
	F-11	Occurs erroneously, causing equipment damage	Equipment damage	Computer fault; software; displays fail	3C				Open
							Page: 2 of 2		

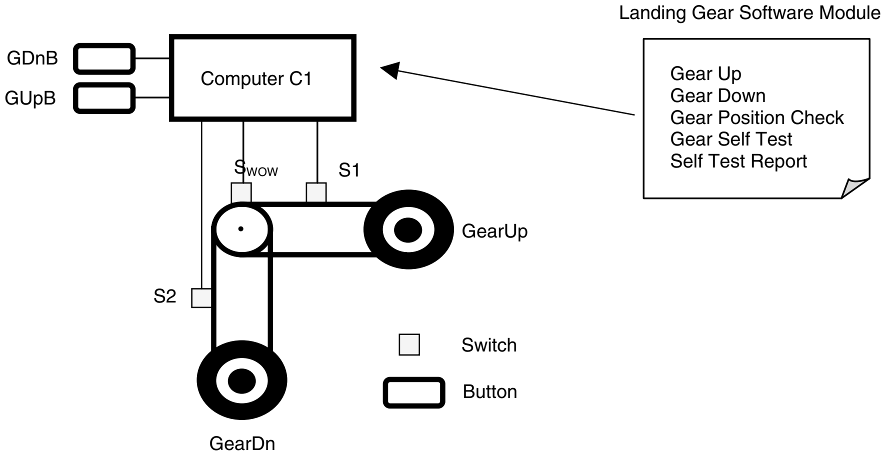


Figure 15.5 *Example aircraft landing gear system.*

3. Is relatively inexpensive, yet provides meaningful results.
4. Provides rigor for focusing on hazards associated with system functions.
5. Good tool for software safety analysis.

The following are disadvantages of the FuHA technique:

1. Since the technique focuses on functions, it might overlook other types of hazards, such as those dealing with hazardous energy sources or sneak circuit paths.
2. After a functional hazard is identified, further analysis is required to identify the specific causal factors.

15.11 COMMON MISTAKES TO AVOID

When first learning how to perform an FuHA, it is commonplace to commit some typical errors. The following is a list of common errors made during the conduct of an FuHA.

1. Each system function is not evaluated and documented.
2. The hazard description is incomplete, ambiguous, or too detailed.
3. Causal factors are not adequately identified or investigated.
4. The mishap risk index (MRI) is not stated or is incomplete.
5. The hazard mitigation method is insufficient for hazard risk.
6. The hazard is closed prematurely or incorrectly.
7. Modes other than operation are often overlooked, for example, maintenance, training, and testing.

TABLE 15.5 FuHA Example 2—Worksheet 1

System: Aircraft Subsystem: Landing Gear Software Functions			**Functional Hazard Analysis**				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
Gear up	F-1	Fails to issue after takeoff, causing damage from drag	Aircraft flight with gear down	Computer; software; wiring	2C				Open
	F-2	Issues prematurely, causing aircraft damage during taxi	Gear raises during taxi or takeoff	Computer; software	2C				Open
Gear down	F-3	Fails to issue for landing, causing damage or injury during landing	Unable to lower landing gear and aircraft must land with landing gear up	Computer; software; wiring	1C	Provide redundant design Provide multiple sensors for software logic tests		Gear down is safety critical function	Open
		Issues prematurely during flight, causing damage from drag	Aircraft flight with gear down	Computer; software	2C				Open
Gear position check	F-4	Function fails, resulting in unknown gear position, causing system to not lower gear for landing	Unable to lower landing gear and aircraft must land with landing gear up	Computer; software; electronic faults	1C				Open
	F-5	Function error that reports incorrect gear position, causing system to not lower gear for landing	Unable to lower landing gear and aircraft must land with landing gear up	Computer; software; electronic faults	1C				Open
								Page: 1 of 2	

TABLE 15.6 FuHA Example 2—Worksheet 2

System: Aircraft Subsystem: Landing Gear Software Functions			**Functional Hazard Analysis**				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
Gear self-test	F-6	Self-test fails, resulting in gear fault not reported prior to takeoff, causing system to not lower gear for landing	Landing gear fault not detected. Unable to raise or lower gear when desired, no warning	Computer; software; electronic faults	1C				Open
	F-7	Self-test error, resulting in gear fault erroneously reported prior to takeoff, causing unnecessary maintenance delay	Incorrect landing gear status reported	Computer; software; electronic faults	3C				Open
Self-test report	F-7	Self-test report fails, resulting in gear fault not reported prior to takeoff, causing system to not lower gear for landing	BIT data not reported. No warning of fault state	Computer; software; electronic faults; memory fault	1C			System may still be correctly operational	Open
	F-8	Self-test report error, resulting in gear fault erroneously reported prior to takeoff, causing unnecessary maintenance delay	BIT data reported incorrectly. No warning of fault state, or incorrect warning	Computer; software; electronic faults; memory fault	3C			System may still be correctly operational	Open
								Page: 2 of 2	

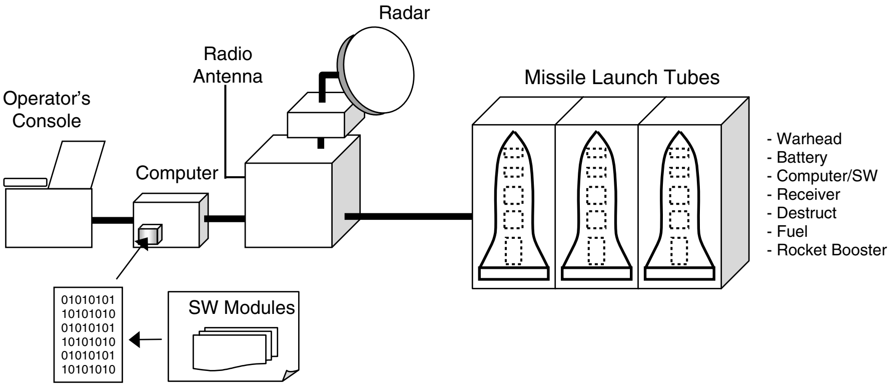
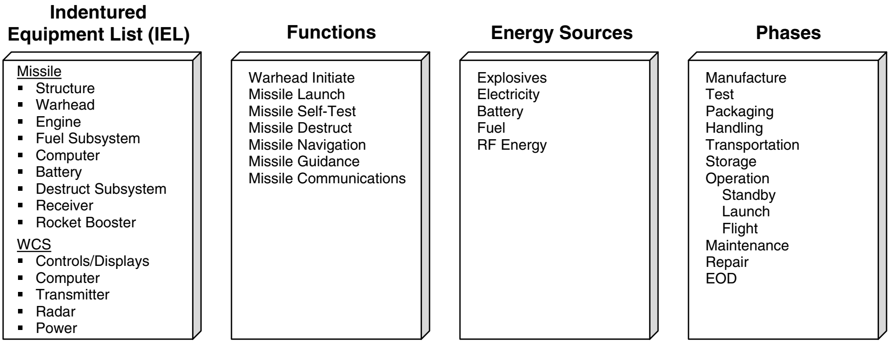


Figure 15.6 Ace missile system.

15.12 SUMMARY

This chapter discussed the FuHA technique. The following are basic principles that help summarize the discussion in this chapter:

1. FuHA is a qualitative analysis tool for the evaluation of system functions.
2. The primary purpose of FuHA is to identify functions that can lead to the occurrence of an undesired event or hazard.
3. FuHA is useful for software analysis.
4. The use of a functional block diagram greatly aids and simplifies the FuHA process.



Indentured Equipment List (IEL)

Missile
▪ Structure
▪ Warhead
▪ Engine
▪ Fuel Subsystem
▪ Computer
▪ Battery
▪ Destruct Subsystem
▪ Receiver
▪ Rocket Booster

WCS
▪ Controls/Displays
▪ Computer
▪ Transmitter
▪ Radar
▪ Power

Functions

Warhead Initiate
Missile Launch
Missile Self-Test
Missile Destruct
Missile Navigation
Missile Guidance
Missile Communications

Energy Sources

Explosives
Electricity
Battery
Fuel
RF Energy

Phases

Manufacture
Test
Packaging
Handling
Transportation
Storage
Operation
Standby
Launch
Flight
Maintenance
Repair
EOD

Figure 15.7 Missile system component list and function list.

TABLE 15.7 **Ace Missile System FuHA—Worksheet 1**

System: Ace Missile System Subsystem: System Functions			**Functional Hazard Analysis**				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
W/H Arm-1	F-1	Missile W/H Arm-1 function occurs inadvertently	Inadvertent W/H initiation	Faults cause inadvertent missile W/H Arm-1 function	1C	Design for multiple events being required before initiation can occur (i.e., Arm-1 and Arm-2 and power).	1E		Open
	F-2	Missile W/H Arm-1 function fails to occur	Unable to initiate W/H	Faults cause failure of missile W/H Arm-1 function	4E		4E	Dud weapon; not a safety concern	Closed
W/H Arm-2	F-3	Missile W/H Arm-2 function occurs inadvertently	Inadvertent W/H initiation	Faults cause inadvertent missile W/H Arm-2 function	1C	Design for multiple events being required before initiation can occur (i.e., Arm-1 and Arm-2 and power).	1E	Dud weapon; not a safety concern	Open
	F-4	Missile W/H Arm-2 function fails to occur	Unable to initiate W/H	Faults cause failure of missile W/H Arm-2 function	4E		4E		Closed

(*continued*)

TABLE 15.7 ***Continued***

System: Ace Missile System Subsystem: System Functions			Functional Hazard Analysis				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
Missile launch	F-5	Inadvertent missile launch function occurs	Inadvertent missile launch	Faults cause inadvertent missile launch signal	1C	Review software code Design for safe HMI Launch must require multiple design events	1E		Open
	F-6	Missile launch function fails to occur when intended	Missile battery may have been activated; unsafe missile state	Faults prevent missile launch when intended	2C	Use redundant design	2E		Open
	F-7	Incorrect missile is launched	Inadvertent missile launch	Incorrect missile is selected and launched	1C	Design for safe HMI Review code for software safety	1E		Open
								Page: 1 of 2	

TABLE 15.8 Ace Missile System FuHA—Worksheet 2

System: Ace Missile System Subsystem: System Functions			Functional Hazard Analysis				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
Missile self-test	F-8	Missile launch self-test function fails, resulting in unknown missile status	Unsafe missile state	Faults cause erroneous missile data to WCS operator and system	2C	Use redundant design Design for safe HMI	2E		Open
Missile destruct	F-9	Missile destruct function inadvertently occurs	Missile strikes undesired target	Faults cause inadvertent missile destruct signal	1C	Launch must require multiple events Review software code Design for safe HMI	1E	Dud weapon; not a safety concern	Closed
	F-10	Missile destruct function fails to occur when requested	Missile fails to destruct when necessary to avoid undesired target	Faults prevent missile destruct when destruct has been elected	1C	Use redundant design	1E		Open
Missile navigation	F-11	Navigation function error occurs, causing undesired target strike, resulting in death/injury	Missile strikes undesired target	Faults cause incorrect missile navigation, resulting in striking undesired target	1C	Design for safe HMI Review code for software safety	1E		Open

(*continued*)

TABLE 15.8 ***Continued***

System: Ace Missile System Subsystem: System Functions			**Functional Hazard Analysis**				Analyst: Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Action	FMRI	Comments	Status
Missile guidance	F-12	Guidance function error occurs, causing undesired target strike, resulting in death/injury	Missile striking undesired target	Faults cause incorrect missile guidance, resulting in striking undesired target	1C	Use redundant design Design for safe HMI Analyze guidance system	1E		Open
								Page: 2 of 2	

BIBLIOGRAPHY

SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Appendix A—Functional Hazard Assessment, 1996.

Chapter 16

Sneak Circuit Analysis

16.1 INTRODUCTION

Sneak circuit analysis (SCA) is an analysis technique for identifying a special class of hazards known as *sneak circuits.* SCA is accomplished by examining electrical circuits (or command/control functions) and searching out unintended electrical paths (or control sequences) that, without component failure, can result in:

1. Undesired operations
2. Desired operations but at inappropriate times
3. Inhibited desired operations

A sneak circuit is a latent path or condition in an electrical system that inhibits a desired condition or initiates an unintended or unwanted action. This condition is not caused by component failures but has been inadvertently designed into the electrical system to occur as normal operation. Sneak circuits often exist because subsystem designers lack the overall system visibility required to electrically interface all subsystems properly. When design modifications are implemented, sneak circuits frequently occur because changes are rarely submitted to the rigorous testing that the original design undergoes. Some sneak circuits are evidenced as "glitches" or spurious operational modes and can be manifested in mature, thoroughly tested systems after long use. Sometimes sneaks are the real cause of problems thought to be the result of electromagnetic interference or grounding "bugs." SCA can be applied to both hardware and software designs.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

16.2 BACKGROUND

This analysis technique falls under the detailed design hazard analysis type (DD-HAT) and/or the system design hazard analysis type (SD-HAT) (refer to Chapter 3). The purpose of the SCA is to identify latent paths that can cause the occurrence of unwanted functions or inhibit desired functions, assuming all components are functioning properly. Sneak paths are of concern because they may result in unintended paths or control sequences in electrical/electronic systems that might result in hazards, undesired events, or inappropriately timed events.

The SCA technique is applicable to control and energy delivery circuits of all kinds (e.g., electrical, hydraulic, pneumatic, etc.), although electronic/electrical are the most common. Systems benefiting from SCA include solid-state electronic devices, relay logic systems, and digital systems. It has been used extensively for the evaluation of rocket propulsion, spacecraft, missiles, aircraft, and computers.

The SCA method can be implemented on a limited subsystem, a complete functional system, or an integrated set of systems. Analysis is based on "as-built" documentation, in the form of final schematics and drawings. The preferred start time to begin SCA is during engineering development and prior to critical design review (CDR). However, SCA can be performed during any phase of the program where sufficiently detailed design drawings are available. If performed too early, the results may be meaningless, and, if performed too late, design changes may be too costly.

The technique, when applied to a given system, is thorough at identifying all previously known types of sneak circuits. The sneak types form the sneak clue list, and as new sneak types are identified, they are added to the clue list. The SCA will not be able to identify paths that lie outside the known clue list; however, a skilled analyst may be able to do so.

The SCA method is a somewhat difficult technique to learn, understand, and master, primarily due to the lack of public domain information on the topic. The technique must be mastered, the material understood, and there must be detailed requisite knowledge of the process being modeled. Detailed knowledge of the SCA process, along with all of the clues for identifying sneak paths, is required. SCA is not an analysis for the uninitiated. There is commercially available software that evaluates a computer-aided design (CAD) electrical schematic for sneak circuits, thereby making it a slightly simpler process.

The SCA technique enjoys a favorable reputation among control system designers who recognize it as a disciplined approach to the discovery of inadvertent design flaws. A disadvantage is that the technique lends itself to application after significant design and developmental engineering effort has been expended. This makes any sizable design change a relatively expensive consideration. Even with its good reputation, its usage seems to be infrequent and limited to a few programs, primarily due to the costs involved. The use of SCA is not widespread in the system safety discipline because of the proprietary sneak clues, the large amount of effort required, and its focus on sneak hazards. SCA must generally be subcontracted to companies that have the capability, or it must be performed using commercial software packages that are available.

The actual methodology is very straightforward and simple in concept. However, the "clues" used for identifying sneak paths are considered proprietary by each company that has developed SCA capability. Even the companies selling commercial SCA applications will not reveal the clues used; they are built into the program for automatic usage by the program. A company creating its own SCA technology will not know if its capability is 100 percent successful without significant research and experience.

As an alternative to an SCA, a hazard analysis that identifies safety critical circuits, followed by a detailed analysis of those circuits, may be performed. However, it may not be possible to identify all sneaks without a clue list.

Although a very powerful analysis tool, the benefits of an SCA are not as cost effective to the system safety analyst as other tools. Other safety analysis techniques, such as SSHA and fault tree analysis, are more cost effective for the identification of hazards and root causes. SCA is highly specialized and only assists in a certain niche of potential safety concerns dealing with timing and sneak paths. The technique is not recommended for every day safety analysis usage and should be used when required for special design or safety critical concerns. Specific reasons for performing an SCA include:

1. The system is safety critical or high consequence and requires significant analysis coverage to provide safety assurance (e.g., safe and arm devices, fuzes, guidance systems, launch commands, fire control system, etc.).
2. When an independent design analysis is desired.
3. The cause of unresolved problems (e.g., accidents, test anomalies, etc.) cannot be found via other analysis techniques.

It is important to perform an SCA as early as possible in order to cost effectively influence system design. Yet, there is a trade-off involved since SCA can be somewhat costly; it should be done only once on a mature design.

16.3 HISTORY

The original SCA technique using topographs and sneak clues was invented and developed by the Boeing Company in Houston, Texas. Beginning in 1967 Boeing developed the methodology for use on the Apollo and Skylab systems for NASA. As the technique proved successful, it was applied to many other types of systems and software.

16.4 DEFINITIONS

In order to facilitate a better understanding of SCA, some definitions for specific terms are in order. The following are basic SCA terms:

Sneak Latent path or condition in an electrical system that inhibits a desired condition or initiates an unintended or unwanted action through normal system operation, without failures involved.

Sneak clues Checklist of items or clues that helps the analyst identify a sneak. The analyst compares the clues to the network tree and topograph to recognize sneaks. The clue list has been developed from past experience and research.

Node Electrical circuit component, such as a resistor, transistor, switch, etc.

Nodal sets Set of interconnected nodes that make up each circuit.

Paths Route that results when all of the nodes in a nodal set are connected together.

Network trees Diagram that represents a simplified version of the system circuitry, created by selective deletion of extraneous circuitry detail to reduce system complexity, while retaining all pertinent circuit elements.

Topograph Topological patterns that appear in each network tree.

16.5 THEORY

The purpose of SCA is to identify sneak paths in electrical circuits, software, and the like that result in unintended operation or inhibited operation of a system function. There are several ways by which this can be achieved, such as systematic inspection of detailed circuit diagrams, manually drawing simplified diagrams for manual examination, or by using the automated topograph-clue method developed by Boeing. This chapter focuses on the topograph-clue method because it is more structured and rigorous, and it was the genesis for the SCA concept.

The theory behind the automated topograph-clue method of SCA is conceptually very simple and is portrayed in Figure 16.1. Electrical circuit diagrams are transformed into network trees through the use of special computer programs. The network trees are then reduced down into topographs. The topographs are evaluated in conjunction with clue lists to identify sneak circuits. Although the concept appears to be very simple, there is much more complexity actually involved in the process.

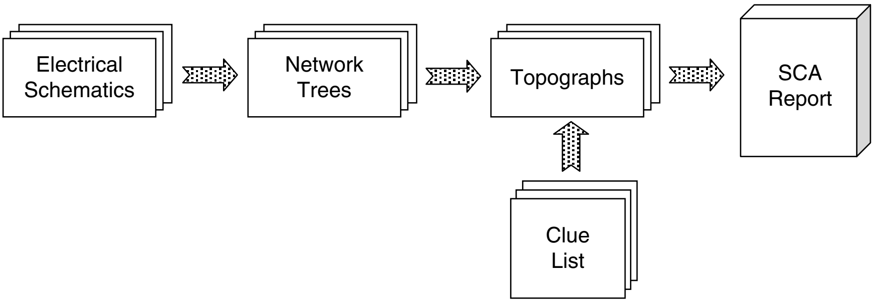


Figure 16.1 SCA concept.

16.6 METHODOLOGY

Figure 16.2 shows an overview of the basic SCA process and summarizes the important relationships involved. The input data primarily consists of detailed electrical schematics and wire lists. The output from the SCA consists of a sneak report identifying all of the identified sneak-type problems and concerns.

The basic definition for a sneak circuit is that it is a designed in signal or current path that causes unwanted functions or modes of operation to occur or that inhibits a desired function from occurring. Sneak circuit conditions are latent in nature; that is, they are always present but not always active, and they are not dependent upon component failures.

The analysis method is accomplished by examining circuits (or command/control functions), searching out unintended paths (or control sequences) that, without component failure, can result in undesired operations, or in desired operations at inappropriate times, or that can inhibit desired operations.

Experienced SCA analysts indicate the sneak circuits are primarily caused by:

1. *Design Oversight* Large and complex systems make complete overview extremely difficult. As a result, latent sneak paths are accidentally built into the design and are not immediately recognized.
2. *Changes* Revision to the original design that corrects one design problem but inadvertently creates a new sneak path in the design.
3. *Incompatible Design* Designs prepared by independent designers or design organizations may be incompatible with respect to the inadvertent creation of a sneak circuit in the integrated system.
4. *Fixes* Malfunctions observed during testing are occasionally corrected by field fixes that fix the immediate problem but also generate a sneak condition that is not immediately recognized.
5. *Human Error* Human error can contribute to a sneak condition when specified tasks are performed improperly, out of sequence, or when unanticipated modes of operation are performed.

In general, the SCA process involves seven basic steps, as shown in Table 16.1. These are the major tasks that must be performed in order to conduct an SCA. If a

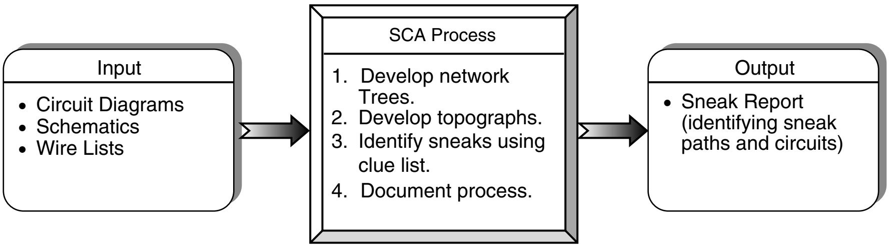

Input
• Circuit Diagrams
• Schematics
• Wire Lists
SCA Process
1. Develop network Trees.
2. Develop topographs.
3. Identify sneaks using clue list.
4. Document process.
Output
• Sneak Report (identifying sneak paths and circuits)

Figure 16.2 *SCA overview.*

TABLE 16.1 Sneak Circuit Analysis Process

Step	Task	Description
1	Acquire data.	Understand system; acquire current design data.
2	Code data.	Format data for computer.
3	Process data.	Computer processing of input data.
4	Produce network trees.	Generate network tree diagrams of system.
5	Identify topographs.	Identify various topographs within network trees.
6	Perform analysis.	Apply clues and identify sneak problems.
7	Generate report.	Report problems and recommended solutions, and document the entire SCA process.

commercial software package is used, it will perform some of the steps for the analyst. Each of these seven steps is described in greater detail in the following sections.

16.6.1 Step 1: Acquire Data

The first step is to acquire data that represents the "as-built" circuitry of the system as closely as possible. Functional schematics, integrated schematics, and system-level schematics do not always accurately represent the constructed hardware. Detailed manufacturing and installation schematics must be used because these drawings specify exactly what is built, contingent upon quality control checks, tests, and inspections. The final analysis results are only as good as the input data that is used. The data requirements necessitate performance of an SCA after the detail level circuitry design is available, typically after a program's preliminary design review. If the analysis is performed earlier in the program, subsequent design changes can invalidate much of the analysis results. On the other hand, while SCA is applicable to mature operational systems, the analysis ideally should be applied at very early stages of the system development for it to minimize integration problems and to permit design changes early in the development process before manufactured hardware requires modifications. The most cost-effective period in a project's life cycle for performing an SCA is after the detailed circuit design has been completed but before all hardware assembly and testing have been accomplished.

16.6.2 Step 2: Code Data

Computer automation has played a major role in SCA from its inception. Computer programs have been developed to allow for encoding of schematics and wire lists into simple "to–from" connections. The analyst must first study the system intensively and partition it at key points, such as power and ground buses, to avoid large and unnecessarily cumbersome network trees. Once partitioned, rigorous encoding rules for both schematic and wire list data are used to ensure that an accurate representation of the circuitry is maintained. The same rules are applied on all electrical continuity data regardless of source, format, or encoding analyst. The single resultant format for all continuity data ensures that the computer can tie all connected nodes together accurately to produce nodal sets. Note that the coding rules are either proprietary or part of a commercial computer program that is utilized.

16.6.3 Step 3: Process Data

When the system schematics are encoded and input into the computer, the computer program performs all the necessary checks, calculations, and SCA processing to generate the needed data. At this stage, the computer may discover errors in the coded data and require the analyst to make corrections in the input data.

The SCA program recognizes each reference designator/item/pin as a single point or node. This node is tied to other nodes as specified by the input data. The computer connects associated nodes into paths and collects associated paths into nodal sets. The nodal sets represent the interconnected nodes that make up each circuit. Each node is categorized by the computer as "special" or "nonspecial." Special nodes include all active circuit elements such as switches, loads, relays, and transistors; nonspecial nodes are interconnecting circuit elements such as connectors, terminal boards, and tie points. Before a nodal set can be output for analysis, the set is simplified by the elimination of the nonspecial nodes. This simplification removes all nonactive circuit elements from the nodal sets while leaving the circuit functionally intact. This simplified nodal set is then output from the computer.

First, the SCA program generates plots of each nodal set. Then the program generates other output reports including: (a) Path reports wherein every element of each path is listed in case the analyst needs to trace a given path node by node, (b) an output data index that lists every item and pin code and provides the nodal set and path numbers in which each appears, and (c) matrix reports that list each node of a nodal set, list all labels associated with active circuit elements of that nodal set, and provide cross references to other related circuitry (e.g., a relay coil in one nodal set will be cross referenced to its contacts, which may appear in another nodal set). Once these subsidiary reports are generated, the reports and the nodal set plots are turned over to sneak circuit analysts for the next stage of the analysis, network tree production.

16.6.4 Step 4: Produce Network Trees

Network trees are the end result of all data manipulation activities undertaken in preparation for the actual analysis. The SCA program derives network trees from the circuit under analysis. The network trees represent a simplified version of the system circuitry by employing selective deletion of extraneous circuitry detail to reduce system complexity, while retaining all circuit elements pertinent to an understanding of all system operational modes. All power sources are drawn at the top of each network tree with grounds appearing at the bottom. The circuit is oriented on the page such that current flow would be directed from top to bottom down the page.

To produce completed network trees, the analyst begins with the computer nodal set plots. Occasionally, these must be redrawn to ensure "down-the-page" current flow, then thoroughly labeled and cross referenced with the aid of matrix reports and the other computer output reports. If these simple guidelines are followed in the production of network trees, identification of the basic topographs (step 5) is greatly simplified.

16.6.5 Step 5: Identify Topographs

The analyst must next identify the basic topological patterns (topographs) that appear in each network tree. There are five basic topograph patterns: (a) single line (no node), (b) ground dome, (c) power dome, (d) combination dome, and (e) "H" pattern, as illustrated in Figure 16.3.

One of these patterns, or several together, will characterize the circuitry of any given network tree. Although at first glance a given circuit may appear more complex than these basic patterns, closer inspection reveals that the circuit is composed of these basic patterns in combination. While examining each intersect node in the network tree, the SCA analyst must identify the pattern or patterns containing that node and apply the basic clues that have been found to typify sneak circuits involving that particular pattern. When every intersect node in the topograph has been examined, all sneak circuit conditions within the network tree will have been uncovered.

16.6.6 Step 6: Perform Analysis

Associated with each topograph pattern is a list of clues to help the analyst identify sneak circuit conditions. These lists were first generated by Boeing during the original study of historical sneak circuits and were updated and revised during the first several years of applied SCA. Now, the lists provide a guide to all possible design flaws that can occur in a circuit containing one or more of the five basic topograph patterns, subject to the addition of new clues associated with new technological developments. The clue list consists of a series of questions, either imbedded in

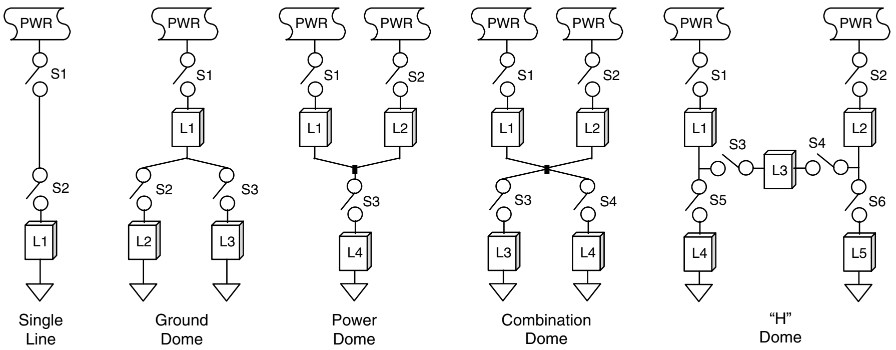


Figure 16.3 General SCA topograph patterns.

the SCA program or known to the analyst, used to identify sneak paths. As an example, the single-line topograph shown Figure 16.4 would have clues such as:

1. Is switch Sl open when load Ll is desired?
2. Is switch Sl closed when load L1 is not desired?
3. Does the label Sl reflect the true function of Ll?

Sneak circuits are rarely encountered in single-line topographs because of its simplicity. This is an elementary example given primarily as the default case, which covers circuitry not included by the other topographs. With each successive topograph, the clue list becomes longer and more complicated. The clue list for the H pattern includes over 100 clues. This pattern, because of its complexity, is associated with more sneak circuits than any other pattern. Almost half of the critical sneak circuits identified to date can be attributed to the H pattern. Such a design configuration should be avoided whenever possible. The possibility of current reversal through the H crossbar is the most commonly used clue associated with H pattern sneak circuits.

16.6.7 Step 7: Generate Report

Sneak circuit analysis of a system produces the following four general categories of outputs: (a) drawing error reports, (b) design concern reports, (c) sneak circuit reports, and (d) network trees and supplementary computer output reports.

Drawing error reports disclose document discrepancies identified primarily during the data-encoding phase of the sneak circuit analysis effort. Design concern reports describe circuit conditions that are unnecessary or undesirable but that are not actual sneak circuits. These would include single failure points, unsuppressed inductive loads, unnecessary components, and inadequate redundancy provisions. A number of such conditions usually are identified whenever an analyst examines a circuit at the level of detail required for a formal sneak circuit analysis.

Sneak circuit reports delineate the sneak conditions identified during the analysis. These reports fall into the following broad categories:

1. Sneak paths
2. Sneak timing
3. Sneak labels
4. Sneak indications
5. Sneak procedures

Sneak Paths Latent paths in designed circuitry that even without component failures permit unwanted functions to occur or inhibit desired functions from occurring. A sneak path is one that permits current or energy to flow along an unsuspected path or in an unintended direction.

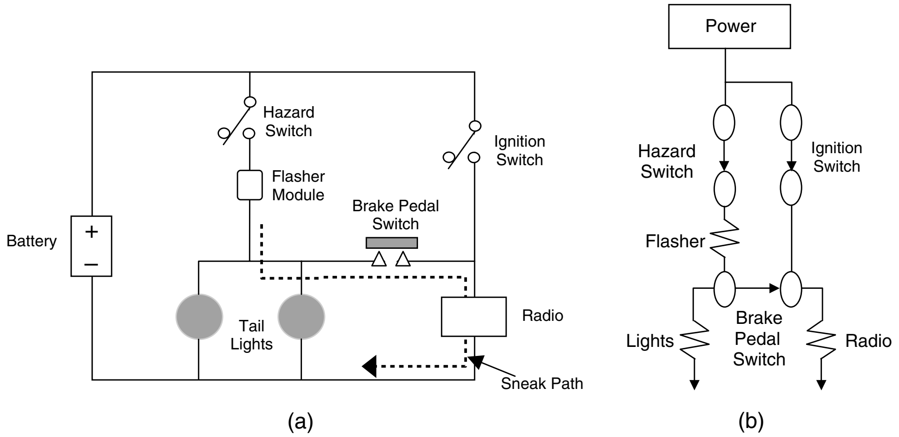


Figure 16.4 *Sneak Path Example (Automotive Circuit)*

Sneak Timing A latent path that modifies the intended timing or sequencing of a signal, creating an inappropriate system response. Functions are inhibited or occur at an unexpected or undesired time. For example, faulty ignition timing can ruin the performance of an automobile engine.

Sneak Labels Lack of precise nomenclature or instructions on controls or operating consoles that can lead to operator error. A label on a switch or control device could cause incorrect actions to be taken by operators.

Sneak Indicators An indication that causes ambiguous or incorrect operator displays. A false or ambiguous system status resulting from an improper connection or control of display devices. For example, a warning light might glow while the item it monitors is not failed or vice versa.

Sneak Procedures Ambiguous wording, incomplete instructions, lack of caution notes, or similar deficiencies that might result in improper operator action under contingency operations.

16.7 EXAMPLE 1: SNEAK PATH

Figure 16.4 illustrates an automotive circuit with a sneak path. Note the H topograph pattern in this example. Design intent was for the car radio to be powered only through the ignition switch, and for the taillights to be powered from the ignition through the brake switch or via the hazard light switch. A reverse current condition occurs when the hazard switch is closed and the brake switch closes. The radio blinks on and off even though the ignition switch is off. Although not a hazardous situation, this demonstrated how sneak circuits could exist through design errors.

16.8 EXAMPLE 2: SNEAK LABEL

Figure 16.5 illustrates a sneak label example that was discovered on an aircraft radar system. In this example the circuit breaker provides power to two disparate systems, but the circuit breaker label reflects only one of the systems. An operator attempting to remove power from the liquid coolant pump would inadvertently remove power from the entire radar system.

16.9 EXAMPLE 3: SNEAK INDICATOR

Figure 16.6 illustrates a sneak indicator example that was discovered on a sonar power supply system. In this example the indicator lamps for motor ON and OFF do not truly monitor and reflect the actual status of the motor. Switch S3 could be in the position shown, providing motor ON indication even though switches S1 or S2, or relay contacts K1 or K2, could be open and inhibiting motor operation.

16.10 EXAMPLE SNEAK CLUES

Clues are applied to the software network trees and topographs to identify design problems and sneak circuits. Table 16.2 shows a few example clues that are used in the analysis. Companies that are experienced in SCA generally have a much longer list of clues, which they usually consider proprietary. The list of clues is one of the strengths behind SCA.

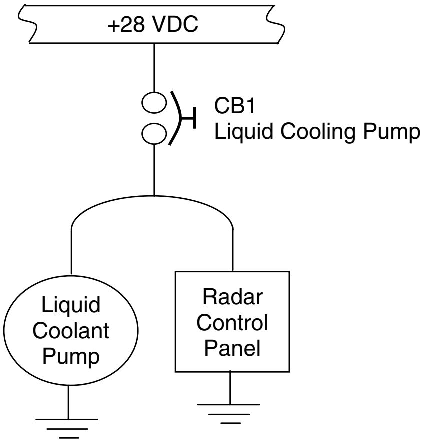


Figure 16.5 *Sneak label example.*

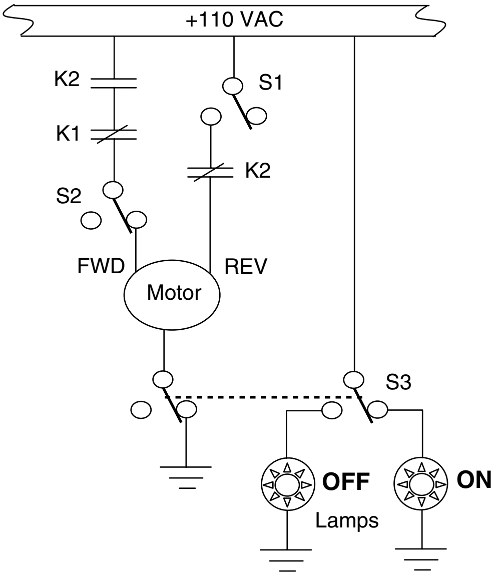


Figure 16.6 *Sneak indicator example.*

TABLE 16.2 Example Electrical SCA Clues

No.	Clue Questions
1	Can a switch be open when a load is required?
2	Can a switch be closed when a load is not required?
3	Can the clocks be unsynchronized when they are required to be synchronized?
4	Does the label indicate the true condition?
5	Is anything else expected to happen that is not indicated by the label?
6	Can current flow in the wrong direction? Current reversal concern
7	Can a relay open prematurely under certain conditions?
8	Can power be cut off at a wrong time because of an energized condition in the interfacing circuit?
9	Can a circuit lose its ground because of interfacing circuits?
10	Is relay race possible?
11	Is feedback possible?
12	Are conflicting commands possible?
13	Are ambiguous labels possible?
14	Are false indicators possible?
15	Are intermittent signals possible?
16	Are incorrect signal polarities possible?
17	Does load exceed drive capabilities?
18	Are incorrect wiring interconnections possible?
19	Are improper voltage levels possible?
20	Is counter initialized (inaccurate count concern)?
21	Is latch initialized (initial system state undefined concern)?

16.11 SOFTWARE SNEAK CIRCUIT ANALYSIS

Software sneak circuit analysis (SSCA) is the extension of the hardware sneak circuit analysis technique to analyze software, because sneak paths can also exist within computer software code. A software sneak path is a latent path or condition in software code that inhibits a desired condition or initiates an unintended or unwanted action.

The purpose of SSCA is to discover software code logic that could cause undesired program outputs, incorrect program operation, or incorrect sequencing/timing. When software controls a safety critical function, an SSCA can help detect sneak paths that would result in a mishap.

The technique was invented and developed by the Boeing Company in Houston, Texas. Following the successful application of SCA on hardware, Boeing research in 1975 showed that the same methodology could also be applied to software.

The following are significant advantages of the SSCA technique:

1. Is a rigorous approach based on the actual software code.
2. Permits large portions of the work to be computerized.
3. Can locate sneak paths that are difficult to find via other techniques.
4. Works equally well on different programming languages.
5. Does not require the execution of the software.

The overall methodology is identical to that of hardware SCA. The same basic seven-step SCA process applies, except the system and data consists of software code instead of electrical circuits. The program source code is converted into network trees and topographs, which the analyst evaluates using software clues. In this case the network trees are based on electrical pseudocircuit models.

Figure 16.7 shows example software sneak that is often cited in various SCA literature. The intended design is shown on the left as a flow diagram. The topographs

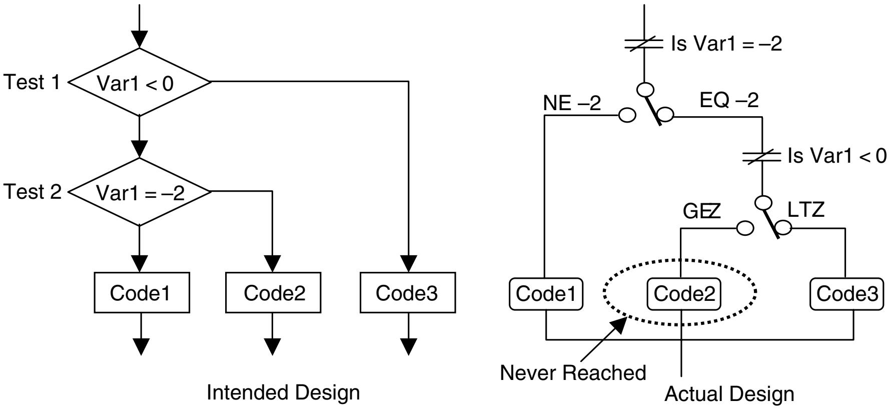


Figure 16.7 *Software SCA example.*

TABLE 16.3 Example Software SCA Clues

No.	Clue
1	Unused paths
2	Inaccessible paths
3	Improper initialization
4	Lack of data storage/usage synchronization
5	Bypass of desired paths
6	Improper branch sequencing
7	Potential undesirable loops
8	Infinite looping
9	Incorrect sequencing of data processing
10	Unnecessary (redundant) instructions

developed from a network tree is shown on the right. This SSCA discovered that the actual code was not implemented correctly as designed. Test 1 and test 2 were inadvertently interchanged in the code and thus the circled branch would never be executed.

Although SSCA did discover this code error without actually exercising the code, it might also have been found through peer code review or through the analysis of a flow diagram generated from the code. Also, module testing might have also discovered the error.

Clues are applied to the software network trees and topographs just as is done in hardware SCA. Table 16.3 shows a few example software clues that are used in the analysis. Companies that are experienced in SSCA generally have a much longer list of clues, which they consider proprietary.

16.12 ADVANTAGES AND DISADVANTAGES

The following are advantages of the SCA technique:

1. Rigorous approach based on detailed schematics.
2. A large portion of the analysis can be computerized.
3. Can locate sneak paths that are difficult to find via manual techniques.
4. Commercial CAD/SCA software packages are available for performing SCA.

Although a strong and powerful technique, SCA has the following disadvantages:

1. SCA is somewhat of a proprietary technique. Only corporations that have researched and developed the tool have the clues that are necessary for identifying the sneak paths. The clues are not available in any public domain form. Therefore, the cost of SCA can be considerable.
2. Entering the data for the SCA is a time-consuming process. Therefore, it is usually only done once during the program development, and this is usually with detailed

design information. Consequently, any identified design changes can be more costly than if identified earlier in the program development life cycle.

3. SCA does not identify all system hazards, only those dealing with sneak paths.
4. SCA requires an experienced analyst to actually recognize the sneak paths from the clues and topological diagrams.
5. SCA only considers normal component operation, it does not consider component failures.

16.13 COMMON MISTAKES TO AVOID

When first learning how to perform an SCA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of an SCA:

1. Not obtaining the necessary training
2. Using the complex SCA technique when a simpler technique might be more appropriate
3. Trying to apply the SCA technique without all of the established clues

16.14 SUMMARY

This chapter discussed the SCA technique. The following are basic principles that help summarize the discussion in this chapter:

1. SCA is a specialized tool for identifying specific classes of hazards, such as those dealing with hardware timing issues and sneak electrical paths in the hardware.
2. SCA simplifies a complex circuit into network tree diagrams and topographs that can be easily analyzed using a set of clues (usually proprietary) available to the SCA analyst.
3. SCA and SSCA requires special computer programs to generate the networks and topographs for the analysis.
4. The SCA analyst must have a complete set of sneak clues in order to ensure a complete analysis.
5. SSCA simplifies complex computer programs into network tree diagrams and topographs that can be analyzed using a set of clues (generally proprietary) available to the SSCA analyst.

BIBLIOGRAPHY

Browne, J., Jr., Benefits of Sneak Circuit Analysis for Defense Programs, Proceedings of the Third International System Safety Conference, Oct., 1977, pp. 303–320.

Buratti, D. L., W. E. Pinkston, and R. O. Simkins, Sneak Software Analysis, RADC-TR-82–179, June, 1982, pp. 1–6.

Carter, A. H., K. T. Budnik, and S. R. Douglass, Computer Produced Drawings for Circuit Analysis, Proceedings Annual R & M Symposium, 1985, pp. 224–229.

Clardy, R. C., Sneak Circuit Analysis Development and Application, *IEEE Conference Digest*, April 1976.

Clardy, R. C., Sneak Circuit Analysis: An Integrated Approach, Proceedings of the Third International System Safety Conference, Oct., 1977, pp. 377–387.

Clardy, R. C., Sneak Circuit Analysis, in *Reliability and Maintainability of Electronic Circuits*, Computer Science Press, 1980, pp. 223–241.

Forrest, M., Software Safety, *Hazard Prevention*, **24**(4) July–September: (1988).

Godoy, S. G. and G. J. Engels, Sneak Circuit and Software Sneak Analysis, *J. Aircraft*, **15**(8): 509–513 (1978).

Hill, E. J., Sneak Circuit Analysis of Military Systems, Proceedings of the Second International System Safety Conference, July, 1975, pp. 351–372.

NASA, Apollo Spacecraft Sneak Circuit Analysis Plan, NASA; SB08-P-108; NASW-1650, 1968.

NASA, Sneak Circuit Analysis Guideline for Electro-Mechanical Systems, NASA Practice No. PD-AP-1314, Oct. 1995.

Peyton, B. H. and D. C. Hess, Software Sneak Analysis, Seventh Annual Conference of the IEEE/Engineering in Medicine and Biology Society, 1985, pp. 193–196.

Price, C. J., N. Snooke, and J. Landry, Automated Sneak Identification, *Eng. Appl. Artificial Intelligence*, **9**(4): 423–427 (1995).

Rankin, J. P., Sneak Circuit Analysis, *Nuclear Safety*, **15**(5): 461–468 (1973).

Rankin, J. P., Sneak Circuit Analysis, Proceedings of the 1st International System Safety Conference, 1973, pp. 462–482.

Rankin, J. P. Origins, Application and Extensions of Sneak Circuit Analysis on Space Projects, *Hazard Prevention*, **33**(2): 24–30 (1997).

Chapter 17

Petri Net Analysis

17.1 INTRODUCTION

Petri net analysis (PNA) is an analysis technique for identifying hazards dealing with timing, state transitions, sequencing, and repair. PNA consists of drawing graphical Petri net (PN) diagrams and analyzing these diagrams to locate and understand design problems.

Models of system performance, dependability, and reliability can be developed using PN models. PNA is very useful for analyzing properties such as reachability, recoverability, deadlock, and fault tolerance. The biggest advantage of Petri nets, however, is that they can link hardware, software, and human elements in the system.

The PNA technique may be used to evaluate safety critical behavior of control system software. In this situation the system design and its control software is expressed as a timed PN. A subset of the PN states are designated as possible unsafe states. The PN is augmented with the conditions under which those states are unsafe. A PN reachability graph will then determine if those states can be reached during the software execution.

17.2 BACKGROUND

The PNA technique falls under the system design hazard analysis type (SD-HAT) and should be used as a supplement to the SD-HAT analysis. Refer to Chapter 3 for a description of the analysis types. The purpose of the PNA is to provide a technique to graphically model systems components at a wide range of abstraction levels

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

in order to resolve system reliability, safety, and dependency issues. The graphical model can then be translated into a mathematical model for probability calculations.

Petri nets can be used to model a system, subsystem, or a group of components. PNA can be used to model hardware or software operation or combinations thereof. To date, the application of PNA for system safety use has been limited to the examination of software control systems. Its use has rarely been applied to large systems. PNA can be used to develop reliability models of system operation.

The significant advantage of the technique is that it can be applied to a system very early in development and thereby identify timing issues that may effect safety early in the design process. PNA application helps system developer's design in safety and system quality during early development, eliminating the need to take corrective action after a test failure or mishap.

The PNA method is somewhat difficult to learn, understand, and master. A graduate-level understanding of mathematics and computer science is needed for the application of PNA. The analyst must master the technique and have a detailed knowledge of the process being modeled. The PNA technique is suited for use by theoretical mathematicians. The PN model quickly becomes large and unwieldy as system size increases and is therefore usually only used on small system applications.

The use of PNA is not widespread in the system safety discipline because of its difficulty to use, its limitation to smaller problems, and its limitation in scope to timing-type problems. PNA is highly specialized and only assists in a certain niche of potential safety concerns dealing with timing and state reachability. The technique is only recommended for special design safety concerns.

17.3 HISTORY

The concept of Petri nets has its origin in Carl Adam Petri's doctoral dissertation Kommunikation mit Automaten submitted in 1962 to the faculty of Mathematics and Physics at the Technische Universität Darmstadt, Germany. His thesis developed this graph-based tool for modeling the dynamics of systems incorporating switching. Subsequent research by many individuals has provided the means for using Petri's concepts as the basis for system modeling in many different applications, such as reliability, dependency, safety, and business models.

17.4 DEFINITIONS

In order to facilitate a better understanding of PNA, some definitions for specific terms are in order. The following are basic PNA terms:

Transition Represents a system event that must occur. Transitions contain a switching delay time. When all of the inputs to the transition have a token, the transition event is *enabled*, and it occurs or *switches* after the given delay time. The delay time represents the actual system operational design. A delay time is placed in each transition node. Immediate transitions have a delay time equal to zero ($D = 0$). When the transition node *switches* or *fires*, all input nodes lose their token, and all output nodes receive a token.

Place Used to represent the input and output nodes to a transition. Places contain the tokens.

Token Represents timing in the system logic. As a PN model develops, the tokens build sequencing into the model. Tokens are analogous to currency; they are used for transactions.

Connecting edge Connects the places and transitions together to build the logical model.

State Static condition (or state) of the PN model before and after the firing of a transition. A PN model will have a finite number of states, based on the model design.

Reachability System can have many different possible states; reachability refers to the systems capability to reach any or all of those states during operation. As designed, the system may not be able to reach some states.

Repair Refers to the capability to physically repair a failed component and restore it to an operational state.

17.5 THEORY

The PNA method utilizes a diagram or directed graph that portrays in a single diagram the operational states of the system. The state diagram is flexible in that it can serve equally well for a subsystem or an entire system. The diagram provides for representation of system states, transitions between states, and timing. Figure 17.1 illustrates the overall PNA process.

17.6 METHODOLOGY

A Petri net is a graphical and mathematical modeling tool. It consists of places, transitions, and arcs that connect them. Input arcs connect places with transitions, while

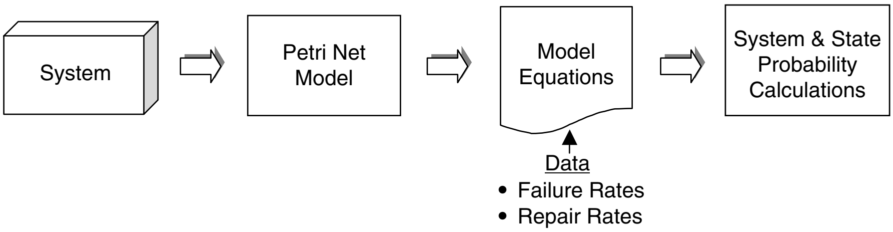


Figure 17.1 *PNA process.*

output arcs start at a transition and end at a place. There are other types of arcs, for example, inhibitor arcs. Places can contain tokens; the current state of the modeled system (the marking) is given by the number (and type if the tokens are distinguishable) of tokens in each place. Transitions are active components. They model activities that can occur (the transition fires), thus changing the state of the system (the marking of the Petri net). Transitions are only allowed to fire if they are enabled, which means that all the preconditions for the activity must be fulfilled (there are enough tokens available in the input places). When the transition fires, it removes tokens from its input places and adds some at all of its output places. The number of tokens removed/added depends on the cardinality of each arc. The interactive firing of transitions in subsequent markings is called *token game*.

Figure 17.2 shows the symbols utilized in comprising a PN model. All PN models can be constructed with just these components and using the firing rules listed below. A PN is a bipartite directed graph (digraph). It consists of two types of nodes: places (drawn as circles), which can be marked with tokens (drawn as a dot), and transitions (drawn as squares or bars), which are marked by the time, D, it takes to delay the output of tokens. If $D = 0$, the transition time is immediate; otherwise, it is timed. PNs dealing with transition times are often referred to as timed PNs. Timed Petri nets are models that consider timing issues in the sequencing. The practice of integrating timed Petri nets with software fault tree analysis has recently become popular.

The movement of tokens is governed by the *firing rules* as follows:

1. A Transition is enabled when all of the places with edges pointing to it are marked with a token.
2. After a delay $D \geq 0$ the transition switches or fires.
3. When the transition fires, it removes the token from each of its input places and adds the token to each of its output places.
4. A place can have multiple tokens.
5. The number of tokens in a PN is not necessarily constant.

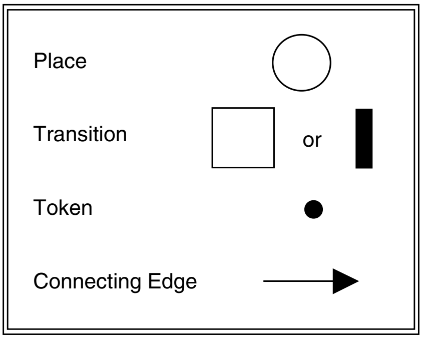


Figure 17.2 *PN model symbols.*

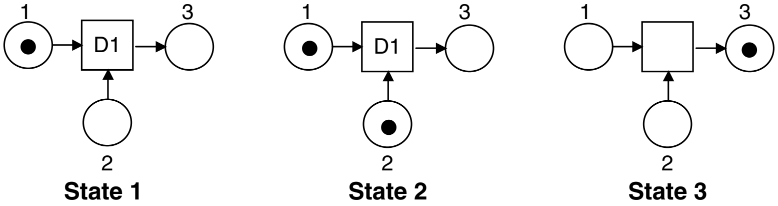


Figure 17.3 Example PN model with three transition states.

6. Tokens move along the edges at infinite speed.
7. The transition time *D* can be either random or deterministic.

The PNA method has a static part and a dynamic part. The static part consists of the places, transitions, and edges. The dynamic part involves the marking of places with the tokens when the transition firing occurs. In the PN model, places represent events that correspond to discrete system states. The transitions represent logic gates. The marking of a PN model at a given moment represents the state at that moment in time.

Figure 17.3 shows an example PN model with three transition states. In state 1, place 1 has a token but place 2 does not. Nothing can happen until place 2 receives a token. In state 2, place 2 receives a token. Now transition D1 has both inputs fulfilled, so after delay D1 it fires. State 3 shows the final transition, whereby D1 has fired, it has removed the two input tokens (places 1 and 2) and given an output token to place 3.

Figure 17.4 shows another example PN model with two transition states. This example shows how places can have multiple tokens, and how tokens are added and subtracted depending on the model. In this example, transition D1 has tokens for all input places in state 1, so it therefore fires and transitions into state 2. State 2 shows that each input place loses a token and each output place receives a token. Multiple tokens can be used for modeling counting loops or redundant components in a

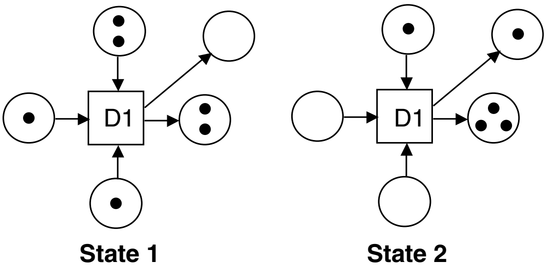


Figure 17.4 Example PN model with multiple tokens.

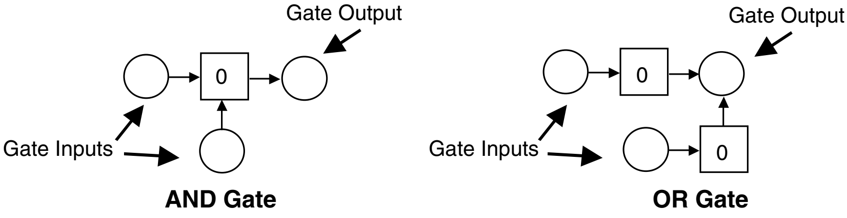


Figure 17.5 *PN model of AND gate and OR gate.*

system design. Transition D1 cannot fire again because all of its inputs do not have tokens now.

Figure 17.5 shows how AND gates and OR gates are modeled via PN models. Note that the transitions have a delay time of zero and are therefore immediate.

A powerful feature of PNs is their corresponding state graphs, otherwise referred to as reachability graphs (RG). Reachability graphs show all of the possible system states that can be reached by a PN model. Knowing which states can be reached and which cannot is valuable information for reliability and safety evaluations. For example, it is important to know if a system can reach a suspected high-risk state.

Figure 17.6 shows an example PN model along with its corresponding reachability graph. In this RG state 1 is the initial state, with places 1, 2, and 4 each having a token. State 2 shows the result of transition D1. State 3 shows the result when transition time D2 < D3, while state 4 shows the result when transition time D2 > D3.

With five places in this model, one might assume that with each place having a binary value of 0 or 1 that there would be $2^5 = 32$ possible states. But, as shown by the reachability graph only four states are actually reachable.

Figure 17.7 shows a PN model for a system design with two redundant components with repair. This system is comprised of two redundant components operating simultaneously. Successful operation requires that only one component remain functional. When a component fails, it undergoes repair. If the second component fails while the first is being repaired, then the system is failed. Note the special PN terminology in this PN model. L1 indicates life operation until random failure of component 1, while R1 indicates component 1 during repair duration. The /2 notation indicates that two tokens are required for this transition to occur.

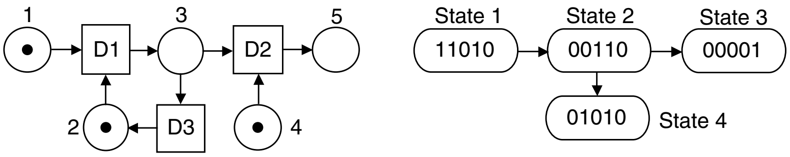


Figure 17.6 *PN with reachability graph.*

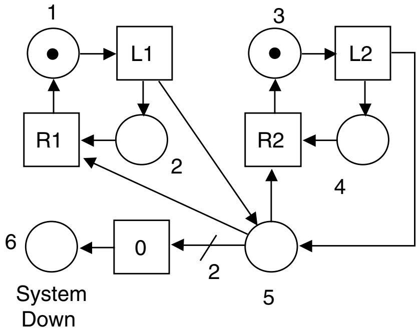


Figure 17.7 *PN of two-component system with repair.*

Figure 17.8 shows the RG for the PN model in Figure 17.7. This type of RG is referred to as a cyclic RG with an absorbing state. Note that with two components in this system, four possible states are expected, but in this case the eventual marking of place 6 defines a fifth state. Note also, that since place 5 requires two tokens for switching these state numbers are nonbinary.

The PNA method may be used to evaluate safety critical behavior of control system software. In this situation the system design and its control software is expressed as a timed PN. A subset of the PN states are designated as possible unsafe states. The PN is augmented with the conditions under which those states are unsafe. A PN reachability graph will then determine if those states can be reached. If the unsafe cannot be reached, then the system design has been proven to not have that particular safety problem.

17.7 EXAMPLES

The hypothetical missile fire control system shown in Figure 17.9 will be used to demonstrate a PN model. System operation is as follows:

1. The operator presses the arm button to initiate arming and firing process.

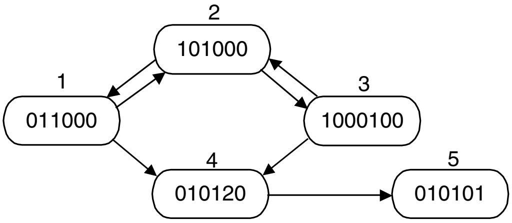


Figure 17.8 *RG for two-component system with repair.*

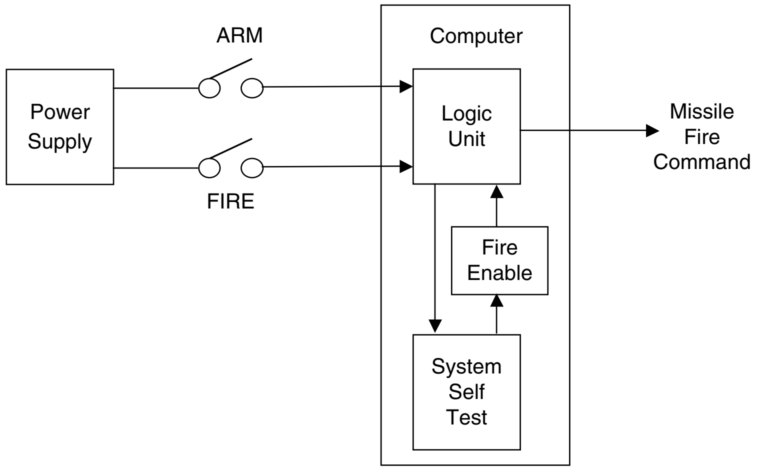


Figure 17.9 *Example missile fire sequence system.*

2. When the computer receives arm button signal, the computer initiates a system self-test to determine if the system is in a safe state and all arming and firing parameters are met.
3. If the self-test is passed, the computer generates a fire signal when the fire button is depressed; if the self-test does not pass, then firing is prohibited by the computer.

Figure 17.10 shows how a PN model might be applied to analyze an actual weapon system design.

The PN model for the missile fire sequence reveals the following safety information:

1. A valid fire signal requires three interlocks: arm command, fire command, and fire enable signal.

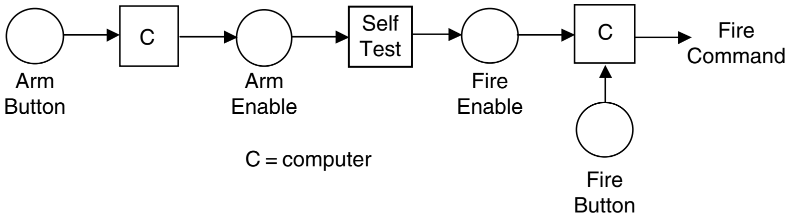


Figure 17.10 *PN for missile fire sequence system.*

2. The computer is a single-point item that processes all three interlocks and, therefore, is susceptible to single-point failures, both in hardware and software.

17.8 ADVANTAGES AND DISADVANTAGES

The following are advantages of the PNA technique:

1. PNs can be used to model an entire system, subsystem, or system components at a wide range of abstraction levels, from conceptual to detailed design.
2. When a PN model has been developed for analysis of a particular abstraction, its mathematical representation can support automation of the major portions of the analysis.
3. PNA is a good tool for modeling and understanding system operation.

The following are disadvantages of the PNA technique:

1. PNA only identifies system hazards dealing with timing and state change issues.
2. PNA is a limited hazard analysis tool because it does not identify root causes.
3. PNA requires an analyst experienced in PN graphical modeling.
4. PNA models quickly become large and complex; thus, it is more suitable to small systems or high-level system abstractions.

17.9 COMMON MISTAKES TO AVOID

When first learning how to perform a PNA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of a PNA:

1. Not obtaining the necessary training.
2. Using the complex PNA technique when a simpler technique might be more appropriate.

17.10 SUMMARY

This chapter discussed the PNA technique. The following are basic principles that help summarize the discussion in this chapter:

1. PNA models the timing and sequencing operation of the system.
2. PNA is a tool for identifying a special class of hazards, such as those dealing with timing, state transitions, and repair.

3. PNA provides both a graphical and mathematical model.
4. PNA only requires places, tokens, transitions, and connecting edges to model a system.
5. PNA can easily become too large in size for understanding, unless the system model is simplified.
6. For system safety applications, PNA is not a general-purpose hazard analysis tool and should only be used in situations to evaluate suspected timing, state transition, sequencing, and repair hazards.

BIBLIOGRAPHY

Agerwala, T., Putting Petri Nets to Work, *IEEE Computer*, Dec., 85–94 (1979).

Malhotra, M. and K. Trevedi, Dependability Modeling Using Petri Nets, *IEEE Trans. Reliability*, **44**:428–440 (1995).

Petri Nets: Properties, Analysis and Applications, *Proc. IEEE*, **77**:541–580 (1989).

Schneeweiss, W. G., *Petri Nets for Reliability Modeling*, LiLoLe, 1999.

Schneeweiss, W. G., Tutorial: Petri Nets as a Graphical Description Medium for Many Reliability Scenarios, *IEEE Trans. Reliability*, **50**(2):June, 159–164 (2001).

Chapter 18

Markov Analysis

18.1 INTRODUCTION

Markov analysis (MA) is an analysis technique for modeling system state transitions and calculating the probability of reaching various system states from the model. MA is a tool for modeling complex system designs involving timing, sequencing, repair, redundancy, and fault tolerance. MA is accomplished by drawing system state transition diagrams and examining these diagrams for understanding how certain undesired states are reached and their relative probability. MA can be used to model system performance, dependability, availability, reliability, and safety. MA describes failed states and degraded states of operation where the system is either partially failed or in a degraded mode where some functions are performed while others are not.

Markov chains are random processes in which changes occur only at fixed times. However, many of the physical phenomena observed in everyday life are based on changes that occur continuously over time. Examples of these continuous processes are equipment breakdowns, arrival of telephone calls, and radioactive decay. Markov processes are random processes in which changes occur continuously over time, where the future depends only on the present state and is independent of history. This property provides the basic framework for investigations of system reliability, dependability, and safety. There are several different types of Markov processes. In a semi-Markov process, time between transitions is a random variable that depends on the transition.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

18.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (SD-HAT) and should be used as a supplement to the SD-HAT analysis. Refer to Chapter 3 for a description of the analysis types. The purpose of MA is to provide a technique to graphically model and evaluate systems components in order to resolve system reliability, safety, and dependency issues. The graphical model can be translated into a mathematical model for probability calculations. The strength of MA is its ability to precisely model and numerically evaluate complex system designs, particularly those involving repair and dependencies.

Markov analysis can be used to model the operation, or failure, of complex system designs. MA models can be constructed on detailed component designs or at a more abstract subsystem design level. MA provides a very detailed mathematical model of system failure states, state transitions, and timing. The MA model quickly becomes large and unwieldy as system size increases and is, therefore, usually used only on small system applications or systems abstracted to a smaller more manageable model.

Markov analysis can be applied to a system early in development and thereby identify design issues early in the design process. Early application will help system developers to design in safety and reliability of a system during early development rather than having to take corrective action after a test failure or, worse yet, a mishap.

Markov analysis is a somewhat difficult technique to learn, understand, and master. A high-level understanding of mathematics is needed to apply the methodology. The technique must be mastered, the material understood, and there must be detailed requisite knowledge of the process being modeled. MA generally requires an analyst very experienced with the technique and the mathematics involved.

Although a very powerful analysis tool, MA does not appear to provide a strong benefit to the system safety analyst as do other analysis tools that are available. It is more often used in reliability for availability modeling and analysis. MA does not identify hazards; its main purpose is to model state transitions for better understanding of system operation and calculating failure state probabilities. MA models can quickly become excessively large and complex, thereby forcing simplified models of the system. MA is recommended primarily only when extremely precise probability calculations are required.

Fault tree analysis (FTA) is recommended for most analysis applications because the fault tree combinatorial model is easier to generate from the system design, and the resulting probability calculations are equal or very close to results from MA models. FTA can be used to model extremely large complex systems, which would be impossible by MA.

18.3 HISTORY

Markov chain theory derives its name from the Russian mathematician Andrei A. Markov (1856–1922), who pioneered a systematic investigation of mathematically describing random processes. The semi-Markov process was introduced in 1954 by Paul Levy to provide a more general model for probabilistic systems.

18.4 DEFINITIONS

In order to facilitate a better understanding of MA, some definitions for specific terms are in order. The following are basic MA terms:

State Condition of a component or system at a particular point in time (i.e., operational state, failed state, degraded state, etc.).

Connecting edge Line or arrow that depicts a component changing from one system state to a different state, such as transitioning from an operational state to a failed state.

State transition diagram State transition diagram is a directed graph representation of system states, transitions between states, and transition rates. These diagrams contain sufficient information for developing the state equations, which are used for probability calculations. The state transition diagram is the backbone of the technique.

Combinatorial model Graphical representation of a system that logically combines system components together according to the rules of the particular model. Various types of combinatorial models available include reliability block diagrams (RBDs), fault trees (FTs), and success trees. In MA the state transition diagram is the combinatorial model.

Deterministic process Deterministic process or model predicts a single outcome from a given set of circumstances. A deterministic process results in a sure or certain outcome and is repeatable with the same data. A deterministic model is sure or certain and is the antonym of random.

Stochastic process A stochastic process or model predicts a set of possible outcomes weighted by their likelihoods or probabilities. A stochastic process is a random or chance outcome.

Markov chain Sequence of random variables in which the future variable is determined by the present variable but is independent of the way in which the present state arose from its predecessors (the future is independent of the past given the present). The Markov chain assumes discrete states and a discrete time parameter, such as a global clock.

Markov process Assumes states are continuous. The Markov process evaluates the probability of jumping from one known state into the next logical state until the system has reached the final state. For example, the first state is everything in the system working, the next state is the first item failed, and this continues until the final system failed state is reached. The behavior of this process is that every state is memoryless, meaning that the future state of the system

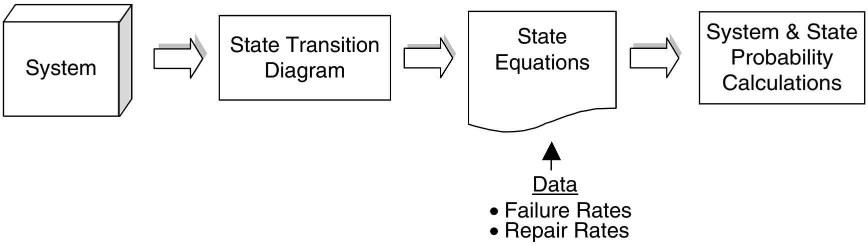


Figure 18.1 *MA process.*

depends only on its present state. In a stationary system the probabilities that govern the transitions from state to state remain constant, regardless of the point in time when the transition occurs.

Semi-Markov process Similar to that of a pure Markov model, except the transition times and probabilities depend upon the time at which the system reached the present state. The semi-Markov model is useful in analyzing complex dynamical systems and is frequently used in reliability calculations.

18.5 THEORY

Markov analysis utilizes a state transition diagram or directed graph that portrays in a single diagram the operational and failure states of the system. The state diagram is flexible in that it can serve equally well for a single component or an entire system. The diagram provides for representation of system states, transitions between states, and transition rates. These diagrams contain sufficient information for developing the state equations, which when resolved provide the probability calculations for each state. Figure 18.1 illustrates the overall MA process.

18.6 METHODOLOGY

Table 18.1 lists and describes the basic steps of the MA process.

18.6.1 State Transition Diagram Construction

Although the basic rules guiding the construction of a state diagram are simple, a good understanding of the system being analyzed is necessary. Construction of a state diagram begins with an examination of the system and a determination of the possible states in which it may exist. Figure 18.2 shows the symbols utilized in MA modeling.

TABLE 18.1 MA Process

Step	Task	Description
1	Define the system.	Examine the system and define the system boundaries, subsystems, and interfaces.
2	Identify the system states.	Establish the goals of the MA and determine the system and component states of interest.
3	Construct state diagram.	Construct the state diagram for all of the identified system states. Show the transitions between states and transition rates.
4	Develop mathematical equations.	Develop the mathematical equations from the state diagram.
5	Solve mathematical equations.	Solve the mathematical equations through manual or computer techniques.
6	Evaluate the outcome.	Evaluate the outcome of the MA analysis.
7	Recommend corrective action.	Make recommended design changes as found necessary from the MA analysis.
8	Hazard tracking.	Enter identified hazards, or hazard data, into the hazard tracking system (HTS).
9	Document MA.	Document the entire MA process, including state diagrams, equations, transition rates, and mathematical solution.

Specifically, the state diagram is constructed as follows:

1. Begin at the left of the diagram with a state (circle) identified as S1. All equipment is initially good (operational) in this state.
2. Study the consequences of failing each element (any component, circuit, or channel defined as a single failure) in each of its failure modes. Group as a common consequence any that result in removing the same or equivalent circuitry from operation.
3. Assign new states (circles) and identify as S2, S3, S4, and so on for the unique consequences of step 2.

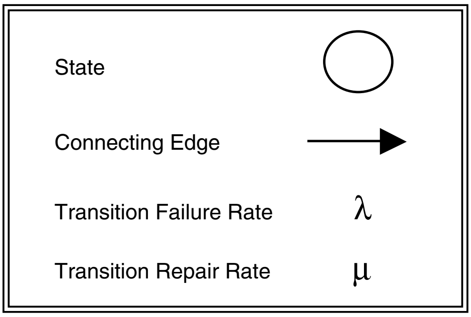


Figure 18.2 *MA symbols.*

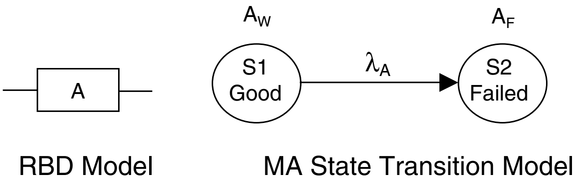


Figure 18.3 *MA model—one-component system with no repair.*

4. Connect arrows from S1, to each of the new states, and note on each arrow the failure rate or rates of the element or elements whose failure determined transition to the new state.
5. Repeat steps 2, 3, and 4 for each of the new states failing only the elements still operational in that state. Continuously observe for cases where the failures may cause transition to one of the states formerly defined.
6. Continue the process until the initial equipment is totally nonoperational.

To limit the state diagram to a reasonable size, without a major sacrifice in accuracy, longer paths between the initial operational state and the system failure state may be truncated. For example, if one path to a system failure consists of three transitions and another is five transitions, then the longer path may be truncated. The effect of this approximation must be examined in the final model to ensure minimal impact.

Figure 18.3 shows an example MA state transition model for a one-component system with no repair. The reliability block diagram (RBD) shows the system design complexity. In this MA model only two states are possible, the operational state and the failed state. The starting state is S1 in which the system is operational (good). In state S2 the system is failed. The transition from state S1 to state S2 is based on the component failure rate λ_A. Note that A_W indicates component A working and A_F indicates component A failed. The connecting edge with the notation λ_A indicates the transitional failure of component A.

Figure 18.4 shows an example MA model for a one-component system with repair. Note how component A can return from the failed stated to the operational state at the repair transition rate μ_A.

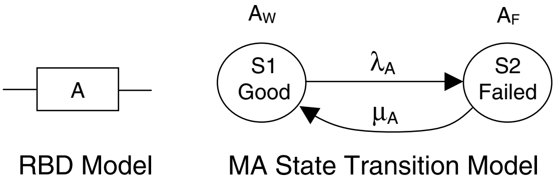


Figure 18.4 *MA model—one-component system with repair.*

$\dot{\underline{P}} = [A]\,\underline{P}$	Where P and P are n × 1 column vectors and $[A]$ is an n × n matrix.
$\underline{P} = \exp[A]t \bullet \underline{P}(0)$	Where $\exp[A]t$ is an n × n matrix and $P(0)$ is the initial probability vector describing the initial state of the system.

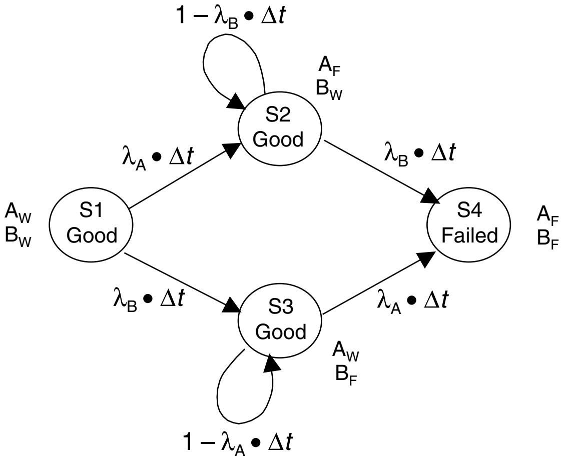
Figure 18.5 *Markov state equations.*

18.6.2 State Equation Construction

A stochastic processes is a random process controlled by the laws of probability that involve the "dynamic" part of probability theory, which includes a collection of random variables, their interdependence, their change in time, and limiting behavior. The most important variables in analyzing a dynamic process are those of rate and state. MA models are representations of a stochastic process.

A Markov process is completely characterized by its transition probability matrix, which is developed from the transition diagram. In safety and reliability work, events involve failure and repair of components. The transitional probabilities between states are a function of the failure rates of the various system components. A set of first-order differential equations is developed by describing the probability of being in each state in terms of the transitional probabilities from and to each state. The number of first-order differential equations will equal the number of system states. The mathematical formula is shown in Figure 18.5 and the solution then becomes one of solving the differential equations.

Figure 18.6 shows a Markov transition diagram for a two-component system comprised of components A and B. A_W indicates component A working and A_F indicates component A failed. States S1, S2, and S3 are noted a "good," indicating



$1 - \lambda_B \bullet \Delta t$
A_F
B_W
S2
Good
$\lambda_A \bullet \Delta t$
$\lambda_B \bullet \Delta t$
A_W
B_W
S1
Good
S4
Failed
A_F
B_F
$\lambda_B \bullet \Delta t$
S3
Good
$\lambda_A \bullet \Delta t$
A_W
B_F
$1 - \lambda_A \bullet \Delta t$

Figure 18.6 *Markov transition diagram—two-component system.*

the system is operational. State S4 is noted as "failed," meaning the system is now in the failed state.

The Markov differential equations are developed by describing the probability of being in each system state at time $t + \Delta t$ as a function of the state of the system at time t. The probability of being in state S1 at some time $t + \Delta t$ is equal to the probability of being in state S1 at time t and not transitioning out during Δt. This equation can be written as:

$$P_1(t + \Delta t) = P_1(t) \bullet [1 - (\lambda_A + \lambda_B) \bullet \Delta t]$$

The probability of being in state S2 at time $t + \Delta t$ is equal to the probability of being in state S1 at time t and transitioning to state S2 in Δt plus the probability of being in state S2 at time t and not transitioning out during Δt. This equation can be written as:

$$P_2(t + \Delta t) = P_1(t) \bullet \lambda_A \bullet \Delta t + P_2(t)(1 - \lambda_B \bullet \Delta t)$$

All of the state equations are generated in a similar manner, resulting in the following equations:

$$\begin{aligned}
P_1(t + \Delta t) &= P_1(t) \bullet [1 - (\lambda_A + \lambda_B) \bullet \Delta t] \\
P_2(t + \Delta t) &= P_1(t) \bullet \lambda_A \bullet \Delta t + P_2(t)(1 - \lambda_B \bullet \Delta t) \\
P_3(t + \Delta t) &= P_1(t) \bullet \lambda_B \bullet \Delta t + P_3(t)(1 - \lambda_A \bullet \Delta t) \\
P_4(t + \Delta t) &= P_2(t) \bullet \lambda_B \bullet \Delta t + P_3(t) \bullet \lambda_A \bullet \Delta t + P_4(t)
\end{aligned}$$

Rearranging the equations results in:

$$\begin{aligned}
[P_1(t + \Delta t) - P_1(t)]/\Delta t &= -(\lambda_A + \lambda_B) \bullet P_1(t) \\
[P_2(t + \Delta t) - P_2(t)]/\Delta t &= \lambda_A \bullet P_1(t) - \lambda_B \bullet P_2(t) \\
[P_3(t + \Delta t) - P_3(t)]/\Delta t &= \lambda_B \bullet P_1(t) - \lambda_A \bullet P_3(t) \\
[P_4(t + \Delta t) - P_4(t)]/\Delta t &= \lambda_B \bullet P_2(t) + \lambda_A \bullet P_3(t)
\end{aligned}$$

Taking the limit as $\Delta t \to 0$ results in:

$$\begin{aligned}
dP_1(t)/\Delta t &= -(\lambda_A + \lambda_B) \bullet P_1(t) \\
dP_2(t)/\Delta t &= \lambda_A \bullet P_1(t) - \lambda_B \bullet P_2(t) \\
dP_3(t)/\Delta t &= \lambda_B \bullet P_1(t) - \lambda_A \bullet P_3(t) \\
dP_4(t)/\Delta t &= \lambda_B \bullet P_2(t) + \lambda_A \bullet P_3(t)
\end{aligned}$$

In matrix form this becomes:

$$\begin{vmatrix} dP_1(t)/\Delta t \\ dP_2(t)/\Delta t \\ dP_3(t)/\Delta t \\ dP_4(t)/\Delta t \end{vmatrix} = \begin{vmatrix} -(\lambda_A + \lambda_B) & 0 & 0 & 0 \\ \lambda_A & -\lambda_B & 0 & 0 \\ \lambda_B & 0 & -\lambda_A & 0 \\ 0 & \lambda_B & \lambda_A & 0 \end{vmatrix} \bullet \begin{vmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_3(t) \end{vmatrix}$$

Solution of these equations provides the probability of being in each state.

18.7 EXAMPLES

18.7.1 Markov Chain

A Markov model can look at a long sequence of rainy and sunny days and analyze the likelihood that one kind of weather is followed by another kind. Let us say it was found that 25 percent of the time, a rainy day was followed by a sunny day, and 75 percent of the time a rainy day was followed by more rain. Additionally, sunny days were followed 50 percent of the time by rain and 50 percent by sun. Given this data, a new sequence of statistically similar weather can be generated from the following steps:

1. Start with today's weather.
2. Given today's weather, choose a random number to pick tomorrow's weather.
3. Make tomorrow's weather "today's weather" and go back to step 2.

A sequence of days would result, which might look like:

Sunny–Sunny–Rainy–Rainy–Rainy–Rainy–Sunny–Rainy–
Rainy–Sunny–Sunny . . .

The "output chain" would statistically reflect the transition probabilities derived from observed weather. This stream of events is called a Markov chain.

18.7.2 Markov Model of Two-Component Series System with No Repair

Figure 18.7 shows an example MA model for a two-component series system with no repair. The RBD indicates that successful system operation requires successful operation of both components A and B. If either component fails, the system fails.

In this MA model two states are possible. The starting state is S1, whereby the system is good (operational) when both A and B are working. Transition to state S2 occurs when either A fails or B fails. In state S2, either A and B are failed and the system is failed.

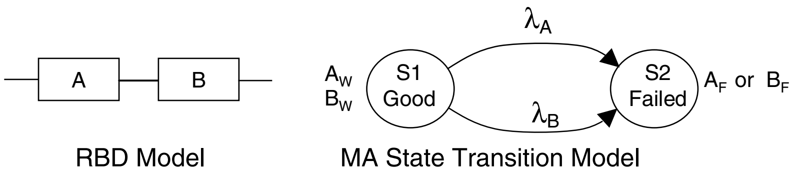


Figure 18.7 MA model—two-component series system with no repair.

18.7.3 Markov Model of Two-Component Parallel System with No Repair

Figure 18.8 shows an example MA model for a two-component parallel system with no repair. The RBD indicates that successful system operation only requires successful operation of either component A or B. Both components must fail to result in system failure.

In this MA model four states are possible. The starting state is S1, whereby the system is good (operational) when both A and B are working. Based on A failure rate λ_A, it transitions to the failed state S2. In state S2, A is failed, while B is still good. In state S3, B is failed, while A is still good. In state S4, both A and B are failed. In states S1, S2, and S3 the system is good, while in state S4 the system is failed.

18.7.4 Markov Model of Two-Component Parallel System with Component Repair

Figure 18.9 shows the MA model for a two-component parallel system with component repair but no system repair. As in the previous figure, this MA model has four possible states. In this system design and MA model, if the system transitions to state S2, but A is repaired before B fails, then the system is returned to state S1.

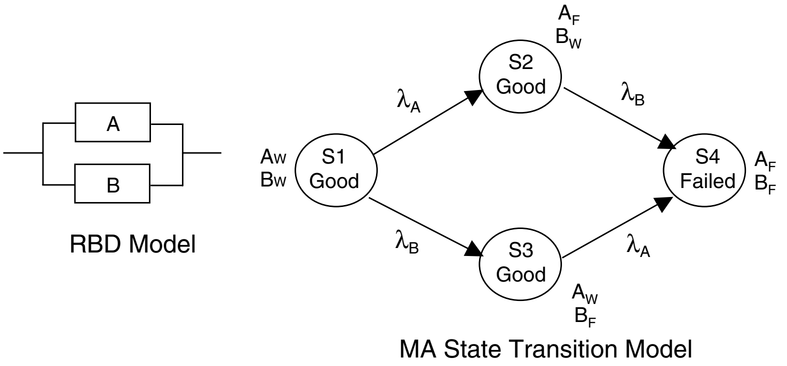


Figure 18.8 MA model—two-component parallel system with no repair.

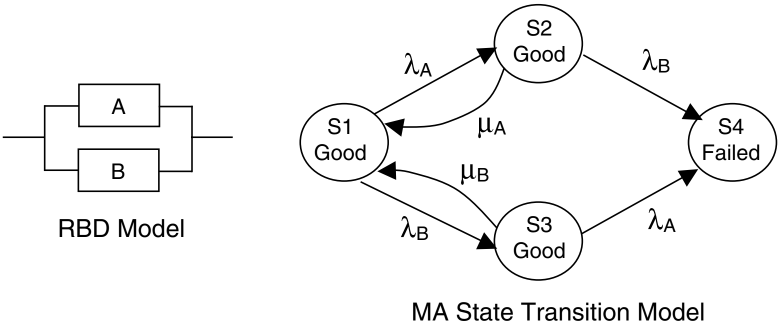


Figure 18.9 *MA model—two-component parallel system with component repair.*

Conversely, if the system is in state S3, the system returns to state S1 if component B is repaired before component A fails. The connecting edge with the notation μ_A indicates repair of component A, and μ_B indicates repair of component B.

18.7.5 Markov Model of Two-Component Parallel System with Component/System Repair

Figure 18.10 shows the MA model for a two-component parallel system with component repair and/or system repair. In this system design, even after system failure occurs, one or both components can be repaired, thereby making the system operational again.

As in the previous figure, this MA model has four possible states. In this system design, and corresponding MA model, if the system transitions to state S2, but A is repaired before B fails, then the system is returned to state S1. Conversely, if the system is in state S3, the system returns to state S1 if component B is repaired before component A fails. If state S4 is reached, the system can be repaired through repair of A and/or B.

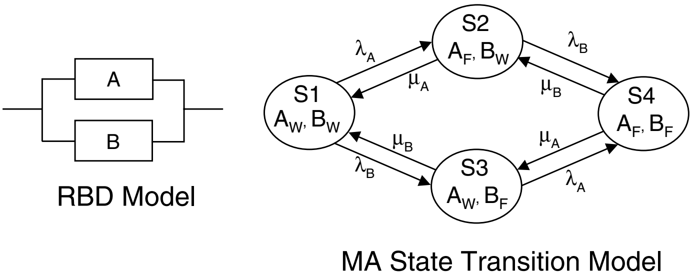


Figure 18.10 *MA model—two-component parallel system with system/component repair.*

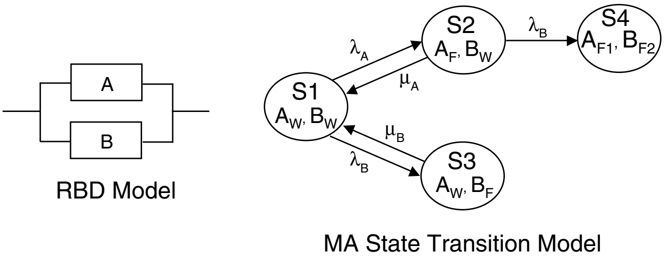


***Figure 18.11** MA model—two-component parallel system with sequencing.*

18.7.6 Markov Model of Two-Component Parallel System with Sequencing

Figure 18.11 shows the MA model for a two-component parallel system where system failure only occurs when the components fail in a specific sequence. In this system design, A monitors B such that if B fails, the fault is detected by A and is immediately repaired. If A fails before B, then it cannot detect failure of B and initiate the repair of B and system failure occurs. Note that this model assumes that B is always repaired before A can fail, thereby maintaining an operational system.

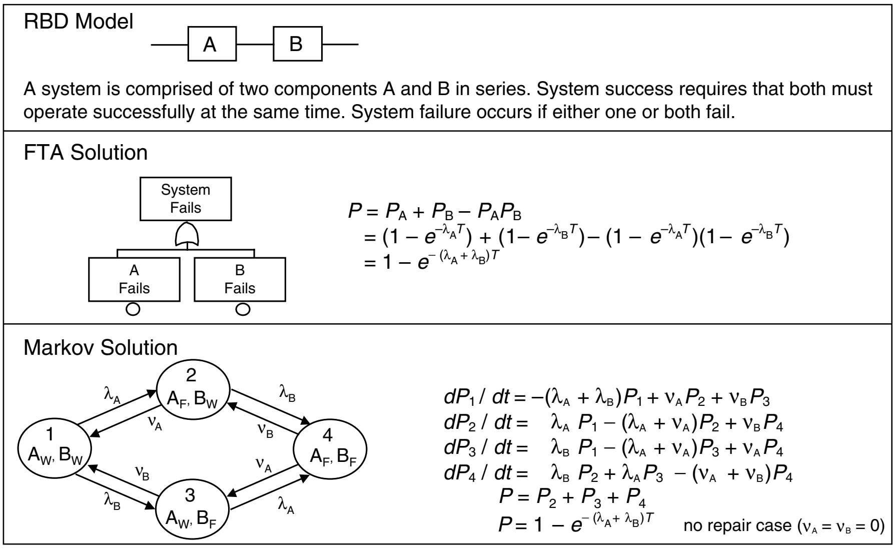
In this MA model four states are possible. The starting state is S1, whereby the system is good (operational) when both A and B are working. In state S3 component B has failed while A is still working. In this state repair is the only option, thereby taking the system back to state S1. In state S2 component A is failed while B is working. If A is repaired before B fails, the system can be restored to state S1, otherwise the system will continue to operate until component B fails, thereby taking the system to state S4, which is system failure.

18.8 MARKOV ANALYSIS AND FTA COMPARISONS

Markov analysis and FTA are often competing techniques. Each technique has its advantages and disadvantages. This section demonstrates both MA and FTA models and probability calculations for the same system design complexities. Comparing the two methods side by side helps to illustrate some of the strengths and weaknesses of each methodology.

Figure 18.12 compares MA and FTA for a two-component series system. The conclusion from this comparison is that both methods provide the same results (i.e., the equations are identical). For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.

Figure 18.13 compares MA and FTA for a two-component parallel system. The conclusion from this comparison is that both methods provide the same results (i.e., the equations are identical). For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.



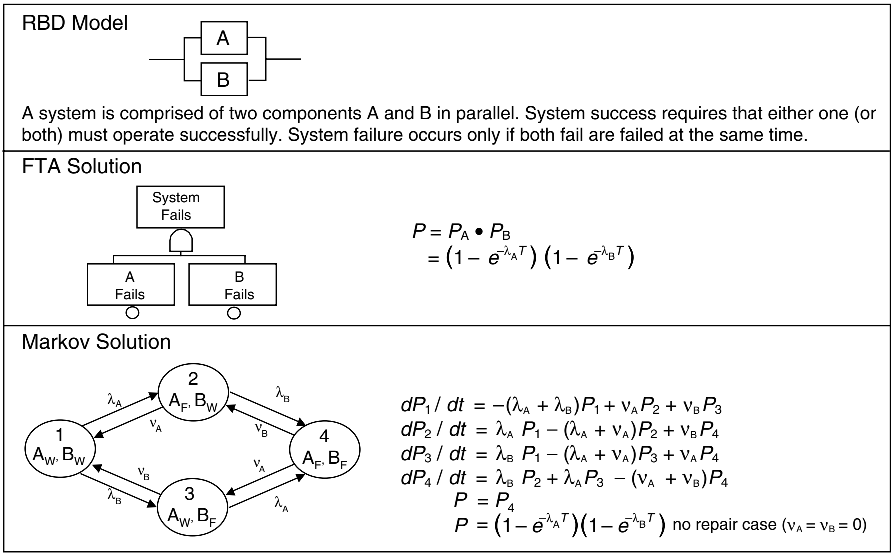
A system is comprised of two components A and B in series. System success requires that both must operate successfully at the same time. System failure occurs if either one or both fail.

$$\begin{aligned} P &= P_A + P_B - P_A P_B \\ &= (1 - e^{-\lambda_A T}) + (1- e^{-\lambda_B T}) - (1 - e^{-\lambda_A T})(1- e^{-\lambda_B T}) \\ &= 1 - e^{-(\lambda_A + \lambda_B)T} \end{aligned}$$

$$\begin{aligned} dP_1 / dt &= -(\lambda_A + \lambda_B)P_1 + \nu_A P_2 + \nu_B P_3 \\ dP_2 / dt &= \lambda_A\, P_1 - (\lambda_A + \nu_A)P_2 + \nu_B P_4 \\ dP_3 / dt &= \lambda_B\, P_1 - (\lambda_A + \nu_A)P_3 + \nu_A P_4 \\ dP_4 / dt &= \lambda_B\, P_2 + \lambda_A P_3 - (\nu_A + \nu_B)P_4 \\ P &= P_2 + P_3 + P_4 \\ P &= 1 - e^{-(\lambda_A + \lambda_B)T} \quad \text{no repair case } (\nu_A = \nu_B = 0) \end{aligned}$$

Figure 18.12 *MA and FTA comparison for a two-component series system.*

Figure 18.14 compares MA and FTA for a two-component sequence parallel system. The conclusion from this comparison is that the resulting equations for each model are different. The FT equation is an approximation. The numerical comparison table shows calculations for different time intervals using the same failure rates. The results contained in this table show that the two models produce very close

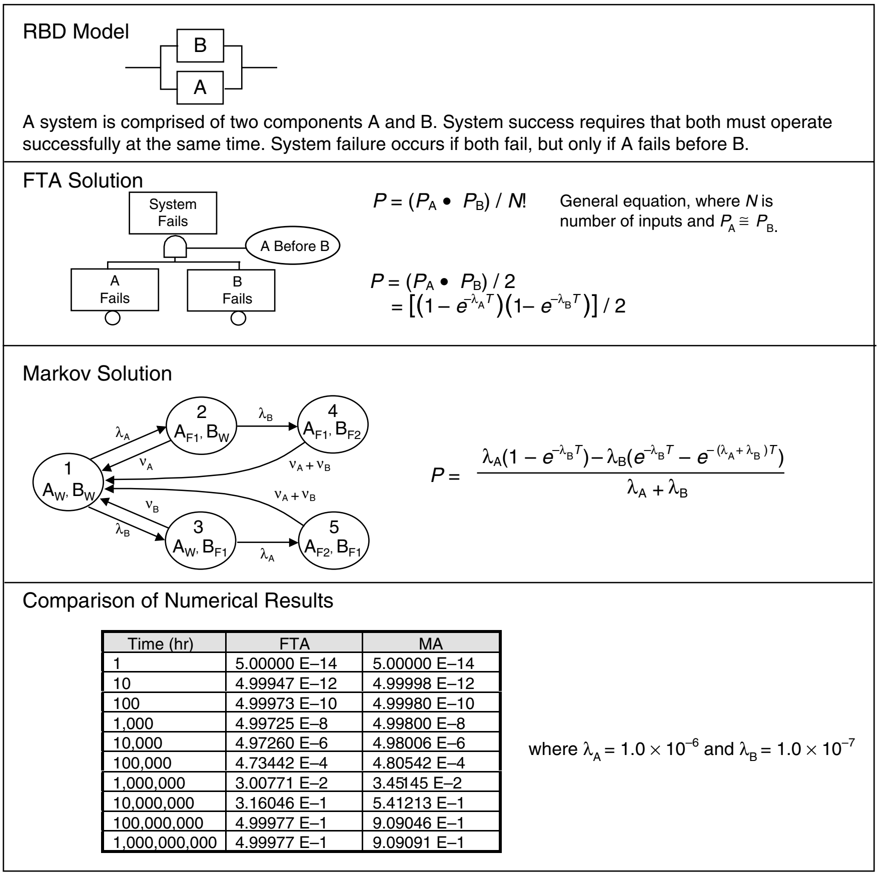


A system is comprised of two components A and B in parallel. System success requires that either one (or both) must operate successfully. System failure occurs only if both fail are failed at the same time.

$$\begin{aligned} P &= P_A \bullet P_B \\ &= \left(1- e^{-\lambda_A T}\right)\left(1- e^{-\lambda_B T}\right) \end{aligned}$$

$$\begin{aligned} dP_1 / dt &= -(\lambda_A + \lambda_B)P_1 + \nu_A P_2 + \nu_B P_3 \\ dP_2 / dt &= \lambda_A\, P_1 - (\lambda_A + \nu_A)P_2 + \nu_B P_4 \\ dP_3 / dt &= \lambda_B\, P_1 - (\lambda_A + \nu_A)P_3 + \nu_A P_4 \\ dP_4 / dt &= \lambda_B\, P_2 + \lambda_A P_3 - (\nu_A + \nu_B)P_4 \\ P &= P_4 \\ P &= \left(1 - e^{-\lambda_A T}\right)\left(1 - e^{-\lambda_B T}\right) \quad \text{no repair case } (\nu_A = \nu_B = 0) \end{aligned}$$

Figure 18.13 *MA and FTA comparison for a two-component parallel system.*



A system is comprised of two components A and B. System success requires that both must operate successfully at the same time. System failure occurs if both fail, but only if A fails before B.

$$P = (P_A \bullet P_B) / N!$$

General equation, where N is number of inputs and $P_A \cong P_B$.

$$P = (P_A \bullet P_B) / 2$$
$$= \left[\left(1 - e^{-\lambda_A T}\right)\left(1 - e^{-\lambda_B T}\right)\right] / 2$$

$$P = \frac{\lambda_A(1 - e^{-\lambda_B T}) - \lambda_B(e^{-\lambda_B T} - e^{-(\lambda_A + \lambda_B)T})}{\lambda_A + \lambda_B}$$

Time (hr)	FTA	MA
1	5.00000 E–14	5.00000 E–14
10	4.99947 E–12	4.99998 E–12
100	4.99973 E–10	4.99980 E–10
1,000	4.99725 E–8	4.99800 E–8
10,000	4.97260 E–6	4.98006 E–6
100,000	4.73442 E–4	4.80542 E–4
1,000,000	3.00771 E–2	3.45145 E–2
10,000,000	3.16046 E–1	5.41213 E–1
100,000,000	4.99977 E–1	9.09046 E–1
1,000,000,000	4.99977 E–1	9.09091 E–1

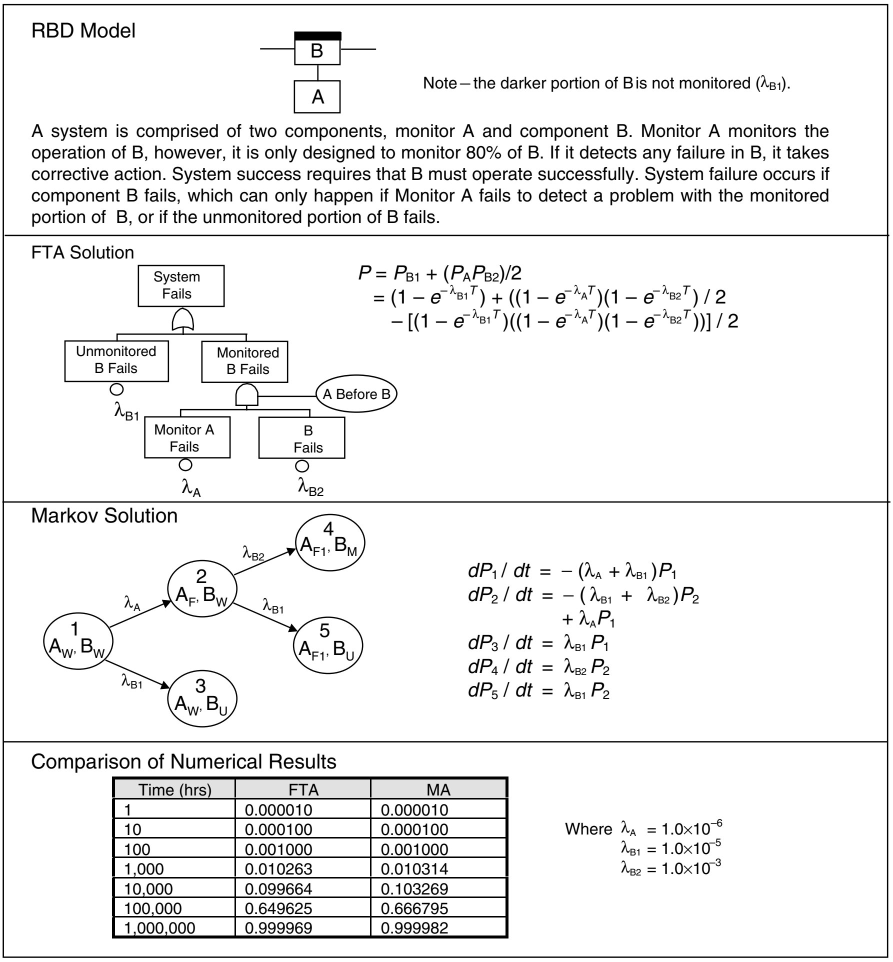
where $\lambda_A = 1.0 \times 10^{-6}$ and $\lambda_B = 1.0 \times 10^{-7}$

Figure 18.14 *MA and FTA comparison for a two-component sequence parallel system.*

results up to about 1 million hours of operation. This indicates that the FTA approximation produces very good results. For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.

Figure 18.15 compares MA and FTA for a partial monitor with coverage system. This is a coverage-type problem, whereby the monitor does not provide complete coverage of the circuit being monitored.

The conclusion from this comparison is that the resulting equations for each model are different. The FT equation is an approximation. The numerical comparison table shows calculations for different time intervals using the same failure rates. The results contained in this table show that the two models produce very close results up to about 10,000 hours of operation. This indicates that the FTA approximation produces very good results. For most analysts the FTA model is easier to understand and the FTA mathematics are easier to solve.



Note – the darker portion of B is not monitored (λ_{B1}).

A system is comprised of two components, monitor A and component B. Monitor A monitors the operation of B, however, it is only designed to monitor 80% of B. If it detects any failure in B, it takes corrective action. System success requires that B must operate successfully. System failure occurs if component B fails, which can only happen if Monitor A fails to detect a problem with the monitored portion of B, or if the unmonitored portion of B fails.

$$\begin{aligned} P &= P_{B1} + (P_A P_{B2})/2 \\ &= (1 - e^{-\lambda_{B1} T}) + ((1 - e^{-\lambda_A T})(1 - e^{-\lambda_{B2} T}) / 2 \\ &\quad - [(1 - e^{-\lambda_{B1} T})((1 - e^{-\lambda_A T})(1 - e^{-\lambda_{B2} T}))] / 2 \end{aligned}$$

$$\begin{aligned} dP_1 / dt &= -(\lambda_A + \lambda_{B1})P_1 \\ dP_2 / dt &= -(\lambda_{B1} + \lambda_{B2})P_2 \\ &\quad + \lambda_A P_1 \\ dP_3 / dt &= \lambda_{B1} P_1 \\ dP_4 / dt &= \lambda_{B2} P_2 \\ dP_5 / dt &= \lambda_{B1} P_2 \end{aligned}$$

Comparison of Numerical Results

Time (hrs)	FTA	MA
1	0.000010	0.000010
10	0.000100	0.000100
100	0.001000	0.001000
1,000	0.010263	0.010314
10,000	0.099664	0.103269
100,000	0.649625	0.666795
1,000,000	0.999969	0.999982

Where $\lambda_A = 1.0\times10^{-6}$
$\lambda_{B1} = 1.0\times10^{-5}$
$\lambda_{B2} = 1.0\times10^{-3}$

Figure 18.15 *MA and FTA comparison for a partial monitor with coverage system.*

18.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the MA technique:

1. MA provides a precise model representation for special design complexities, such as timing, sequencing, repair, redundancy, and fault tolerance.
2. MA is a good tool for modeling and understanding system operation, as well as potential system failure states and repair.
3. MA can be applied to a system very early in development and thereby identify safety issues early in the design process.

4. There are commercial software packages available to assist in MA modeling and probability calculations.

Although a strong and powerful technique, MA analysis has the following disadvantages:

1. MA does not identify system hazards; it only evaluates identified hazards in more detail.
2. MA is not a root cause analysis tool. It is a tool for evaluating the most effective methods for combining components together.
3. MA requires an experienced analyst to generate the graphical models and probability calculations.
4. The MA model quickly becomes large and complex; thus it is more limited to small systems or a high-level system abstraction.

18.10 COMMON MISTAKES TO AVOID

When first learning how to perform an MA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of an MA:

1. Not obtaining the necessary training.
2. Using the complex MA technique when a simpler technique, such as FTA, might be more appropriate.
3. Failing to recognize that the transitions (probabilities) of changing from one state to another are assumed to remain constant. Thus, a Markov model is used only when a constant failure rate and repair rate assumption is justified.
4. Failing to recognize that the transition probabilities are determined only by the present state and not the system's history. This means future states of the system are assumed to be independent of all but the current state of the system. The Markov model allows only the representation of independent states.

18.11 SUMMARY

This chapter discussed the MA technique. The following are basic principles that help summarize the discussion in this chapter:

1. MA is a tool for modeling complex system designs involving timing, sequencing, repair, redundancy, and fault tolerance.
2. MA provides both graphical and mathematical (probabilistic) system models.

3. MA models can easily become too large in size for comprehension and mathematical calculations, unless the system model is simplified. Computer tools are available to aid in analyzing more complex systems.
4. MA is recommended only when very precise mathematical calculations are necessary.
5. MA should be a supplement to the SD-HAT analysis.

BIBLIOGRAPHY

Ericson, C. A. and J. D. Andrews, Fault Tree and Markov Analysis Applied to Various Design Complexities, Proceedings of the 18th International System Safety Conference, 2000, pp. 324–335.

Faraci, V., Jr., Calculating Probabilities of Hazardous Events (Markov vs. FTA), Proceedings of the 18th International System Safety Conference, 2000, pp. 305–323.

International Electrotechnical Commission, IEC 61165, Application of Markov Techniques, 1995.

Pukite, J. and P. Pukite, *Modeling for Reliability Analysis: Markov Modeling for Reliability, Maintainability, Safety and Supportability Analyses of Complex Computer Systems*, IEEE Press, 1998.

Chapter 19

Barrier Analysis

19.1 INTRODUCTION

Barrier analysis (BA) is an analysis technique for identifying hazards specifically associated with hazardous energy sources. BA provides a tool to evaluate the unwanted flow of (hazardous) energy to targets (personnel or equipment) through the evaluation of barriers preventing the hazardous energy flow.

Barrier analysis is a powerful and efficient system safety analysis tool for the discovery of hazards associated with energy sources. The sequentially structured procedures of BA produce consistent, logically reasoned, and less subjective judgments about hazards and controls than many other analysis methods available. However, BA is not comprehensive enough to serve as the sole hazard analysis of a system, as it may miss critical human errors or hardware failures not directly associated with energy sources.

19.2 BACKGROUND

Because the BA technique is unique with a limited scope of coverage, it does not completely fulfill the requirements of any one of the seven basic hazard analyses types described in Chapter 3. However, BA is often used to support the system design hazard analysis type (SD-HAT), detailed design hazard analysis type (DD-HAT), or preliminary design hazard analysis type (PD-HAT) analyses. The BA technique is also known as the energy trace and barrier analysis (ETBA), or the energy trace analysis.

Many system designs cannot eliminate energy sources from the system since they are a necessary part of the system. The purpose of BA is to evaluate these energy

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

sources and determine if potential hazards in the design have been adequately mitigated through the use of energy barriers.

Figure 19.1 illustrates the concept of a barrier providing separation between the energy source and the target. The simple concept of barrier analysis and its graphical portrayal of accident causation is a powerful analysis tool. It should be noted that unwanted energy source from a single source may attack multiple targets. Also, in some situations multiple barriers may be required for optimum safety.

The BA technique is implemented by identifying energy flow paths that may be hazardous and then identifying or developing the barriers that must be in place to prevent the energy flow from damaging equipment or injuring personnel. There are many different types and methods of energy barriers that can be applied in a system design, that is, physical barrier (barricade), procedural barrier, or a time barrier. Barriers serve as countermeasures to control probability and/or severity of personnel injury or system damage.

Barrier analysis is a generally applicable methodology for analysis of systems of all types. It is used to ensure disciplined, consistent, and efficient procedures for the discovery of energy hazards in a system. It can also be used during accident investigations to help develop and understand damage scenarios. BA lends itself to overviews of energies in systems and guides the search for specific hazards or risks that require more detailed analysis.

Barrier analysis is capable of producing detailed analyses of hazards in new or existing systems. By meticulously and logically tracking energy flow paths sequentially, into, within, and out of a system, BA facilitates a thorough analysis for each specific energy type. A detailed understanding of energy sources in the system and their behaviors is necessary, as well as a good understanding of the system design and operation. The BA technique is uncomplicated and easily learned. Standard easily followed BA forms and instructions are provided in this chapter.

19.3 HISTORY

The BA method is based on a useful set of concepts introduced by William Haddon, Jr. [1]. These concepts have been adopted and improved upon by others until the technique has evolved into a useful safety analysis tool.

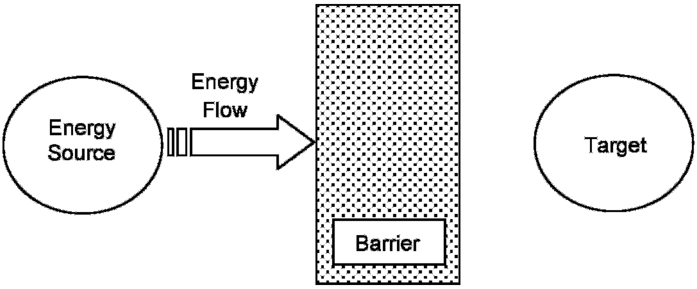


Figure 19.1 Barrier between energy source and target.

19.4 DEFINITIONS

In order to facilitate a better understanding of BA, some definitions for specific terms are in order. The following are basic BA-related terms:

Energy source Any material, mechanism, or process that contains potential energy that can be released. The concern is that the released energy may cause harm to a potential target.

Energy path Path of energy flow from source to target.

Energy barrier Any design or administrative method that prevents a hazardous energy source from reaching a potential target in sufficient magnitude to cause damage or injury. Barriers separate the target from the source by various means involving time or space. Barriers can take many forms, such as physical barriers, distance barriers, timing barriers, procedural barriers, and the like.

19.5 THEORY

The BA technique is based on the theory that when hazardous energy sources exist within a system they pose a hazardous threat to certain targets. Placing barriers between the energy source and the target can mitigate the threat to targets. This concept is illustrated in Figure 19.2, which also shows some example types of energy sources, barriers, and threats.

Barrier analysis involves the meticulous tracing of energy flows through the system. BA is based on the premise that a mishap is produced by unwanted energy exchanges associated with energy flows through barriers into exposed targets. The BA process begins with the identification of energy sources within the system design. Diagrams are then generated tracing the energy flow from its source to its potential target. The diagram should show barriers that are in place to prevent

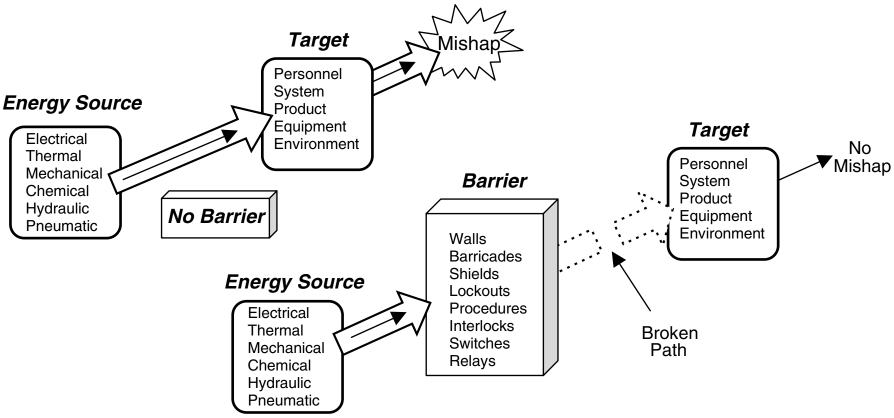


Figure 19.2 Barrier analysis concept.

damage or injury. If no barriers are in place, then safety design requirements must be generated to establish and implement effective barriers.

19.6 METHODOLOGY

Figure 19.3 shows an overview of the basic BA process and summarizes the important relationships involved.

Table 19.1 lists and describes the basic steps of the BA process and summarizes the important relationships involved. Remember that a worksheet is utilized during this analysis process.

19.6.1 Example Checklist of Energy Sources

Table 19.2 contains an example of an energy checklist. If the system design contains any energy sources in this list, then a specific energy has been identified for BA.

19.6.2 Considerations

Figure 19.4 summarizes generic components of BA: energy sources, barriers, and targets. These lists are starting points for a BA. Each component of BA must be well understood and evaluated in the system context.

After an energy source has been identified, there are a series of questions that can be answered that assist in identifying hazardous designs. Table 19.3 contains a list of some of the typical questions that must be answered by the BA.

The BA process verifies the adequacy of engineered or administrative barriers. In this context, engineered safety features are considered *hard* barriers while administrative controls such as procedures, warning signs, and supervisory checks are *soft* barriers. Because hard barriers are more difficult to bypass than soft barriers, the former is preferred. However, soft barriers may be all that can be used in some situations; therefore, an array of complementary soft barriers are often used to better ensure energy containment. Barriers may be categorized by their function, location, and/or type. Figure 19.5 provides some examples.

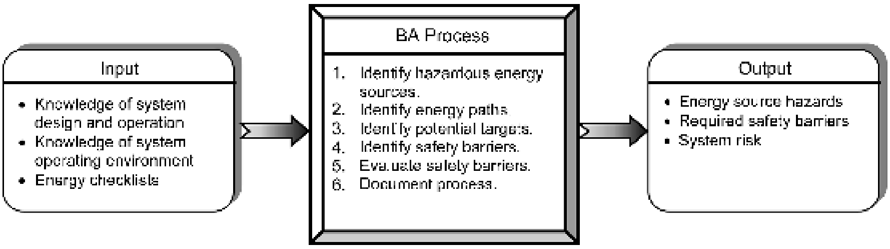

Input
• Knowledge of system design and operation
• Knowledge of system operating environment
• Energy checklists
BA Process
1. Identify hazardous energy sources.
2. Identify energy paths.
3. Identify potential targets.
4. Identify safety barriers.
5. Evaluate safety barriers.
6. Document process.
Output
• Energy source hazards
• Required safety barriers
• System risk

Figure 19.3 *Barrier analysis overview.*

TABLE 19.1 Barrier Analysis Process

Step	Task	Description
1	Identify energy sources.	Examine the system and identify all potentially hazardous energy sources. Include energy quantity and location when possible. Utilize energy source checklists. Examples include explosives, electromagnetic radiation, hazardous materials, electricity, etc.
2	Identify single energy paths.	Any potentially harmful energy flow path to the target (e.g., people, equipment, facilities, and the environment) likely to result in a mishap.
3	Identify multiple energy paths.	Multiple energy paths to the target where more than one energy path is required to reach the target and cause a mishap (e.g., both the mechanical and the electrical arm functions of a fuze).
4	Identify targets.	For each energy source, trace its travel through the system, from beginning to end. Identify all potential targets that can be injured or damaged by the hazardous energy sources. Utilize diagrams.
5	Identify the target vulnerability.	The vulnerability of the target to the unwanted energy flow. For example, an inadvertent application of +28 VDC will have little effect on a human but will destroy a microprocessor.
6	Identify safety barriers.	Identify all barriers in the path of the energy source or identify barriers that should be present. Evaluate the impact of potential failure of barriers, the lack of barriers, and/or the effectiveness of existing barriers. For example, if the heat shields on the space shuttle fall off during reentry, then the shuttle and crew could be lost.
7	Evaluate system risk.	Identify the level of mishap risk presented to the target by the energy source, both with barriers and without barriers in the system design.
8	Recommend corrective action.	Determine if the barrier controls present are adequate and, if not, recommend barriers that should be added to reduce the mishap risk. Determine if the need for more detailed analysis by other techniques (e.g., FTA) to ensure that all hazard causal factors are identified and mitigated.
9	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
10	Document BA.	Document the entire BA process on the worksheets. Update for new information as necessary.

TABLE 19.2 Energy Checklist (Sample)

Category	Energy Sources
Acoustical radiation	Equipment noise Ultrasonic cleaners Alarm devices and signal horns
Atmospheric	Wind velocity, density, direction Rain (warm, cold, freezing) Snow, hail, sleet Lightning, electrostatic Particulates, dusts, aerosols, powders Sunshine, solar Acid rain, vapor/gas clouds Air (warm, cold, freezing, inversion) Moisture, humidity

(*continued*)

TABLE 19.2 *Continued*

Category	Energy Sources
Chemical (acute and chronic sources)	Anesthetic, asphyxiant
	Corrosive/dissolving solvent/lubricating
	Decomposable, degradable
	Deposited materials/residues
	Detonable
	Oxidizing, combustible, pyrophoric
	Polymerizable
	Toxic, carcinogenic, embryo toxic
	Waste/contaminating (air, land, water)
	Water reactive
Corrosive	Chemicals, acids, caustics
	Decon solutions
	“Natural” chemicals (soil, air, water)
Electrical	Battery banks
	Diesel generators
	High lines
	Transformers
	Wiring
	Switch gear
	Buried wiring
	Cable runs
	Service outlets and fitting
	Pumps, motors, heaters
	Power tools and small equipment
	Magnetic fields
	AC or DC current flows
	Stored electrical energy/discharges
	Electromagnetic emissions/RF pulses
	Induced voltages/currents
	Control voltages/currents
Etiologic agents	Viral
	Parasitic
	Fungal
	Bacterial
	Biological toxins
EMR and particular radiations	Lasers, Masers, medical X-rays
	Radiography equipment and sources
	Welding equipment
	Electron beam
	Blacklight (e.g., Magniflux)
	Radioactive sources, contamination, waste, and scrap
	Storage areas, plug storage
	Skyshine, Bremstrahlung
	Activation products, neutrons
Explosive or pyrophoric	Caps, primer cord, explosives
	Electrical squibs
	Power metallurgy, dusts
	Hydrogen and other gases

(*continued*)

TABLE 19.2 *Continued*

Category	Energy Sources
	Nitrates, peroxides, perchlorates
	Carbides, superoxides
	Metal powders, plutonium, uranium
	Zirconium
	Enclosed flammable gases
Flammables	Chemicals, oils, solvents, grease
	Hydrogen (battery banks), gases
	Spray paint, solvent vats
	Coolants, rags, plastics, foam
	Packing materials
Kinetic—linear	Cars, trucks, railroads, carts
	Dollies, surfaces, obstructions
	Crane loads in motion, shears
	Presses, Pv blowdown
	Power-assisted driving tools
	Projectiles, missiles/aircraft in flight
	Rams, belts, moving parts
	Shears, presses
	Vehicle/equipment movement
	Springs, stressed members
Kinetic—rotational	Centrifuges, motors, pumps
	Flywheels, gears, fans
	Shop equipment (saws, grinders, drills, etc.)
	Cafeteria and laundry equipment
	Rotating machinery, gears, wheels
	Moving fan, propeller blades
Mass, gravity, height	Human effort
	Stairs, lifts, cranes
	Sling, hoists, elevators, jacks
	Bucket and ladder
	Lift truck, pits, excavations
	Vessels, canals, elevator doors
	Crane cabs, scaffolds, and ladders
	Trips and falls
	Falling/dropped objects
	Suspended objects
Noise/vibration	Noise
	Vibration
Nuclear	Vaults, temporary storage areas
	Casks, hot cells, reactor areas
	Criticality potential in process
	Laboratories, pilot plants
	Waste tanks and piping, basins, canals
	Sources and solutions, Skyshine
	Activation products, Bremstrahlung
Pressure−volume, *K* constant	Boilers, heated surge tanks
	Autoclaves
	Test loops and facilities

(*continued*)

TABLE 19.2 ***Continued***

Category	Energy Sources
	Gas bottles, pressure vessels Coiled springs, stressed members Gas receivers Overpressure ruptures, explosions thermal cycling Vacuum growth cryogenic Liquid spill, flood, buoyancy Expanding fluids, fluid jets Uncoiling object Ventilating air movement Trenching, digging, earth moving
Terrestrial	Earthquake Floods, drowning Landslide, avalanche Subsidence Compaction Cave-ins Underground water flows Glacial Volcanic
Thermal (except radiant)	Convection, furnaces Heavy metal weld preheat Gas heaters, lead melting pots Electrical wiring and equipment Exposed steam pipes and valves Steam exhausts
Thermal radiation	Furnaces, boilers Steam lines Lab and pilot plant equipment Heaters Solar Radiant, burning, molten Conductive Convective, turbulent evaporative, expansive Heat, cool
Toxic pathogenic	Toxic chemicals, check MSDS (material safety data sheets) Exhaust gases Oxygen-deficient atmosphere Sand blasting, metal plating Decon and cleaning solutions Bacteria, molds, fungi, and viruses Pesticides, herbicides, and insecticides Chemical wastes and residues

Haddon [1] originated the concept that one or more barriers can control the harmful effects of energy transfer. Expanding on Haddon's work, analysts have identified the following barrier mechanisms in order of precedence:

1. Eliminate the hazardous energy from the system (e.g., replace with alternative).

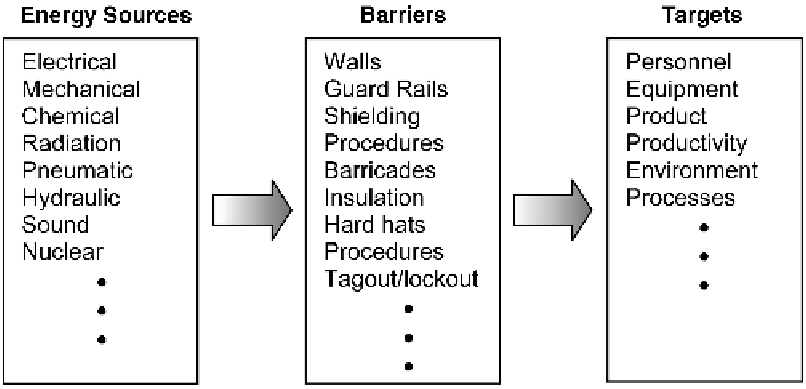


Figure 19.4 *Generic BA components.*

2. Reduce the amount of energy (e.g., voltages, fuel storage).
3. Prevent the release of energy (e.g., strength of containment of the energy).
4. Reduce the rate of release of energy (e.g., slow down burning rate, speed).
5. Prevent the buildup of released energy (e.g., pressure relief valve).
6. Control improper energy input (e.g., electrical energy through supercooled environment).
7. Separate in space or time the energy from the target (e.g., electric lines out of reach).
8. Interpose material barriers (e.g., insulation, guards, safety glasses).
9. Modify shock concentration surfaces (e.g., round off and make soft).
10. Strengthen the target to withstand the energy (e.g., earthquake-proof structures).
11. Limit the damage of energy release (e.g., prompt signals and action, sprinklers).
12. Train personnel to prevent energy release (e.g., warnings, procedures).

TABLE 19.3 BA Hazard Discovery Checklist

Energy Flow Changes	Changes in Barriers
1. Flow too much/too little/none at all	1. Barrier too strong/too weak
2. Flow too soon/too late/not at all	2. Barrier designed wrong
3. Flow too fast/too slowly	3. Barrier too soon/too late
4. Flow blocked/built up/release	4. Barrier degraded/failed completely/disturbed
5. Wrong form/wrong type input or flow	5. Barrier impedes flow/enhances flow
6. Cascading effects of release	6. Wrong barrier type selected
7. Flow conflicts with another energy flow	

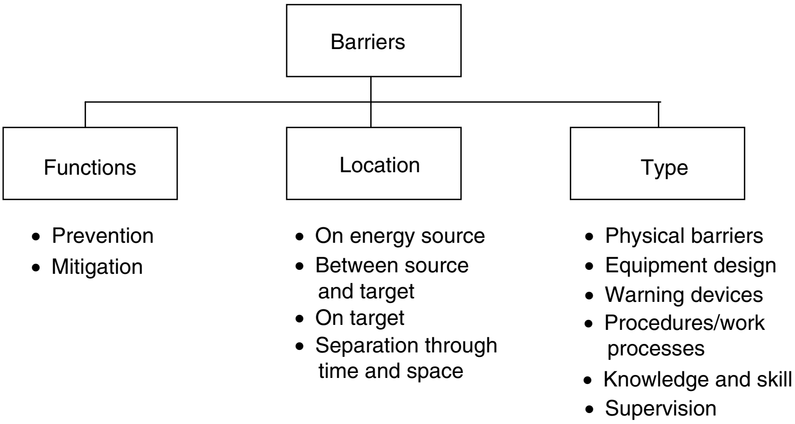


Figure 19.5 *Example barrier categorizations.*

These successive methods are called *energy barriers*. The energy barriers may be a physical obstruction or they may be a written or verbal procedure that is put into place as a means of separating the energy from the persons or objects in time or space. Substituting a less harmful energy may be a way to "limit the energy" or "prevent the buildup." These 12 barrier mechanisms are expanded in Table 19.4.

19.7 WORKSHEET

The BA process is a detailed hazard analysis of energy sources and their potential effect on system personnel and/or equipment. It is desirable to perform the BA using a form or worksheet to provide analysis structure, consistency, and documentation. The specific format of the analysis worksheet is not critical. Typically, columnar-type worksheets are utilized to help maintain focus and structure in the analysis. As a minimum, the following basic information should be obtained from the analysis worksheet:

1. System energy sources that provide a threat
2. Targets within the system that are susceptible to damage or injury from the energy sources
3. Barriers in place that will control the energy hazard
4. Barriers that are recommended to control the energy hazard
5. System risk for the energy–barrier hazard

The recommended BA worksheet is shown in Figure 19.6. This particular BA worksheet utilizes a columnar-type format. Other worksheet formats may exist because different organizations often tailor their analysis worksheet to fit their

TABLE 19.4 Barrier Mechanisms

Barrier Mechanism Strategy for Managing Harmful Energy Flow	Implementation of Mechanism
Eliminate the energy source • Exclude (remove) energy concentration	• Eliminate from design • Replace with alternate design
Reduce the amount of energy • Limit quantity and/or level of energy	• Store heavy loads on ground floors • Lower dam height • Reduce system design voltage/operating pressure • Use small(er) electrical capacitors/pressure accumulators • Reduce/control vehicle speed • Monitor/limit radiation exposure • Substitute less energetic chemicals
Prevent release of energy	• Heavy-walled pipes/vessels • Interlocks • Tagout-lockout • Double-walled tankers • Wheel chocks
Reduce the rate of release of energy • Modify rate of release of energy	• Flow restrictors in discharge lines • Resistors in discharge circuits • Fuses/circuit breakers • Ground fault circuit interrupters
Prevent the buildup of released energy	• Use pressure relief valves • Control chemical reactions
Control improper energy input • Keep energy source within specifications • Prevent the combining of energy sources	• Separate hyperbolic fuel sources
Separate energy from target in time and/or space	• Evacuate explosives test areas • Impose explosives safety quantity—distance rules • Install traffic signals • Use yellow no-passing lines on highways • Control hazardous operations remotely
Isolate by interposing a material barrier	• Concrete road barrier • Safety eyeglasses
Modify shock concentration surfaces • Modify target contact surface or basic structure	• Rounded corners • Padding
Strengthen potential target to withstand the energy	• Earthquake-proof structure • Nuclear reaction containment facility
Limit the damage of energy release	• Building sprinkler systems • Aircraft fire suppression systems
Train personnel to prevent energy release	• Warning notes • Special procedures • Safety training

Barrier Analysis

Energy Source	Energy Hazard	Target	IHRI	Barrier	FHRI	Comments
①	②	③	④	⑤	⑥	⑦

Figure 19.6 *Recommended BA worksheet.*

particular needs. The specific worksheet to be used may be determined by the system safety program (SSP), system safety working group, or the safety analysis customer.

The following instructions describe the information required under each column entry of the BA worksheet:

1. *Energy Source* This column identifies the hazardous energy source of concern.
2. *Energy Hazard* This column identifies the type of energy-related hazard (i.e., the energy path) involved with the identified energy source. The hazard should describe the hazard effect and mishap consequences and all of the relevant causal factors involved. All possibilities of hardware faults, software errors, and human error should be investigated.
3. *Target* This column identifies the target, or targets, that can be adversely affected by the energy source if barriers are not in place and a mishap occurs.
4. *Initial Mishap Risk Index (IMRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values from MIL-STD-882 are shown below.

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

5. *Barrier* This column establishes recommended preventive measures to eliminate or control identified hazards. Safety requirements in this situation

generally involve the addition of one or more barriers to keep the energy source away from the target. The preferred order of precedence for design safety requirements is as shown below.

Order of Precedence
1. Eliminate the hazard through design measures or reduce the hazard mishap risk through design measures.
2. Reduce the hazard mishap risk through the use of safety devices.
3. Reduce the hazard mishap risk through the use of warning devices.
4. Reduce the hazard mishap risk through special safety training and/or safety procedures.

6. *Final Mishap Risk Index (FMRI)* This column identifies the final mishap risk given that the barriers or safety features are in place to mitigate the hazard. This risk assessment will show the risk improvement due to barriers in the system. The same risk matrix table used to evaluate column 4 is also used here.
7. *Comments* This column provides a place to record useful information regarding the hazard or the analysis process that are not noted elsewhere.

19.8 EXAMPLE

In order to demonstrate the BA methodology, the hypothetical water heating system shown in Figure 19.7 will be analyzed for energy–barrier hazards. Table 19.5 contains a list of system components and establishes if they are energy sources of safety concern.

Figure 19.8 contains a diagram of the energy path for the propane energy source. This diagram shows all of the energy barriers in the system design.

Tables 19.6 and 19.7 contain the worksheets for a partial BA of this example system. Two of the system components, propane and water, were selected for demonstration of the BA technique.

19.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the BA technique:

1. BA is simple to grasp and use.
2. BA has a pictorial benefit that aids analysts in visualizing hazards.
3. BA is a relatively inexpensive analysis tool.
4. Most energy sources are easily recognized (e.g., explosives, electricity, springs, compressed gas).

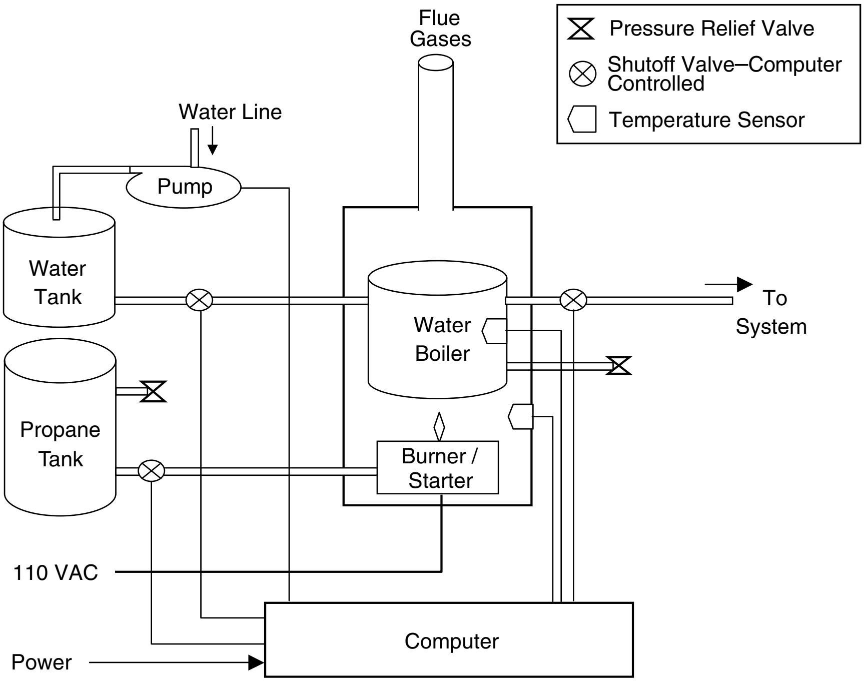


Figure 19.7 *Example water heating system.*

The following are disadvantages of the BA technique:

1. BA is limited by the ability of the analyst to identify all the hazardous energy sources.
2. BA does not identify all system hazards, only those associated with energy sources.
3. Not all sources of harm to targets are readily recognizable as energy sources (e.g., asphyxiate gases, pathogenic organisms).

TABLE 19.5 List of Energy Sources for Water Heating System

System Component	Hazardous Energy Source	Hazard Potential	Barrier
Propane tank	Yes	Yes	Yes
Propane gas	Yes	Yes	Yes
Water tank	Yes	Yes	Yes
Water	Yes	Yes	Yes
Water boiler	Yes	Yes	Yes
Electricity	Yes	Yes	Yes
Gas burner	Yes	Yes	Yes
Computer	No	Yes	Yes

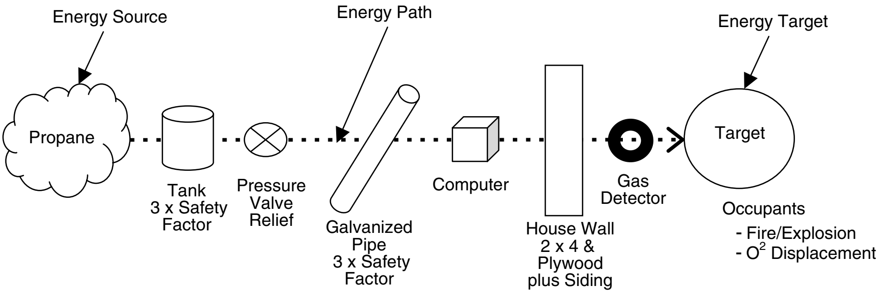


Figure 19.8 *Propane energy path with barriers.*

19.10 COMMON MISTAKES TO AVOID

When first learning how to perform a BA, it is commonplace to commit one or more of the following errors:

1. Not identifying all of the energy sources within the system
2. Not evaluating the potential failure of energy barriers
3. Not evaluating the possible cascading effects of energy sources
4. Not identifying/understanding all of the energy paths
5. Not considering the complete system (i.e., taking too narrow a view of energy paths)

TABLE 19.6 Example BA—Worksheet 1

Energy Source	Hazard	Target	IHRI	Barrier	FHRI	Comments
Propane	Fire/explosion causing death, injury and/or damage	Personnel/ facility	1C	• Isolate tank safe distance from facility • Use protected lines • Minimize ignition sources	1E	
	High-pressure release causing death, injury, and/or damage	Personnel/ facility	1C	• Isolate tank safe distance from facility • Use protected lines • Isolate lines from personnel • Use pressure relief valve	1E	
	Oxygen replacement causing death	Personnel	1C	• Use propane with smell detection (e.g., mercaptan) • Use gas detector	1E	

TABLE 19.7 Example BA—Worksheet 2

Energy Source	Hazard	Target	IHRI	Barrier	FHRI	Comments
Water	High temperature causing tank explosion, which results in death, injury, and/or damage	Personnel/ facility	1C	• Isolate boiler tank • Use protect lines	1E	
	High pressure causing tank explosion, which results in death, injury, and/or damage	Personnel/ facility	1C	• Isolate tank safe distance from facility • Use protected lines • Isolate lines from personnel • Use pressure relief valve	1E	
	Flood causing damage	Facility	2C	• Isolate tank safe distance from facility • Use water detector	2E	

19.11 SUMMARY

This chapter discussed the BA technique. The following are basic principles that help summarize the discussion in this chapter:

1. BA involves detailed focus on potentially hazardous energy sources within the system design and intentional barriers for mitigating the energy hazards.
2. BA should be a supplement to the PD-HAT, DD-HAT, and SD-HAT.
3. Some hazards identified through BA may require more detailed analysis by other techniques (e.g., FTA) to ensure that all hazard causal factors are identified and mitigated.
4. The use of worksheets provides structure and rigor to the BA process, and energy flow diagrams aid the analysis.

REFERENCE

1. W. Haddon, Energy Damage and the Ten Counter-measure Strategies, *Human Factors J.*, August, 1973.

BIBLIOGRAPHY

Barrier Analysis, DOE-76-451, SSDC-29, Safety Systems Development Center, EG&G Idaho, Inc., July 1985.

Hocevar, C. J. and C. M. Orr, Hazard Analysis by the Energy Trace Method, Proceedings of the 9th International System Safety Conference, 1989, pp. H-59–H-70.

Stephenson, J., Energy Trace and Barrier Analysis, in *System Safety 2000: A Practical Guide for Planning, Managing, and Conducting System Safety Programs*, Wiley, New York, 1991, pp. 147–152.

Chapter 20

Bent Pin Analysis

20.1 INTRODUCTION

Bent pin analysis (BPA) is an analysis technique for identifying hazards caused by bent pins within cable connectors. It is possible to improperly attach two connectors together and have one or more pins in the male connector bend sideways and make contact with other pins within the connector. If this should occur, it is possible to cause open circuits and/or short circuits to positive/negative voltages, which may be hazardous in certain system designs. For example, a certain cable may contain a specific wire carrying the fire command signal (voltage) for a missile. This fire command wire may be a long wire that passes through many connectors. If a connector pin in the fire command wire should happen to bend and make a short circuit with another connector pin containing +28 VDC, the missile fire command may be inadvertently generated. BPA is a tool for evaluating all of the potential bent pin combinations within a connector to determine if a potential safety hazard exists.

20.2 BACKGROUND

Because the BPA technique is unique with a limited scope of coverage, it does not completely fulfill the requirements of any one of the seven basic hazard analyses types described in Chapter 3. However, BPA is often used to support the system design hazard analysis type (SD-HAT), detailed design hazard analysis type (DD-HAT), or preliminary design hazard analysis type (PD-HAT) analyses. An alternate name for the BPA technique is cable failure matrix analysis (CFMA).

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

Use of this technique is recommended for identification of system hazards resulting from potential bent connector pins. BPA should always be considered for systems involving safety critical circuits with connectors. The technique is uncomplicated and easily learned. Standard easily followed BPA worksheets and instructions are provided in this chapter. An understanding of electric circuits is necessary, as well as a good understanding of the system design and operation. BPA is often overlooked as a useful tool because it is not well known.

20.3 HISTORY

The Boeing Company developed BPA circa 1965, on the Minuteman program, as a technique for identifying potential safety problems that might result from bent connector pins. The Minuteman program had been experiencing bent connector pins during system installation operations at many Minuteman sites. BPA proved to be successful in identifying potential safety problems that were subsequently eliminated through redesign.

20.4 THEORY

The purpose of BPA is to determine the potential safety effect of one or more pins bending inside a connector and making contact with other pins or the casing. If a safety critical circuit were to be short-circuited to another circuit containing positive or negative voltage, the overall effect might be catastrophic. BPA is a tool for evaluating all of the potential single pin-to-pin bent pin combinations within a connector to determine if a potential safety hazard exists, given that a bent pin occurs. Figure 20.1 is an illustration of the bent pin (BP) concept, whereby a pin can bend over within the connector and make physical contact with another pin, thereby effectively causing a short circuit and an open circuit in the wiring.

Note in Figure 20.1 that pins A and B are close enough in proximity that they can make physical contact if one of them bends in the right direction, and that pins C and D are too far apart to make physical contact should one of them bend. BPA would evaluate the two scenarios of the pins A–B combination; pin A is bent such that it makes physical contact with pin B, or pin B is bent such that it makes physical contact with pin A. Each of these two BP possibilities presents two different possible outcomes, for a total of four possible outcomes.

In this A–B and B–A scenario there are four possible outcomes:

1. Pin A makes contact with pin B; wires A and B become a short circuit, and the content of wire A has an upstream or downstream effect on wire B (depending upon the contents of both A and B).
2. Pin A makes contact with pin B; wire A becomes an open circuit after the short (downstream).

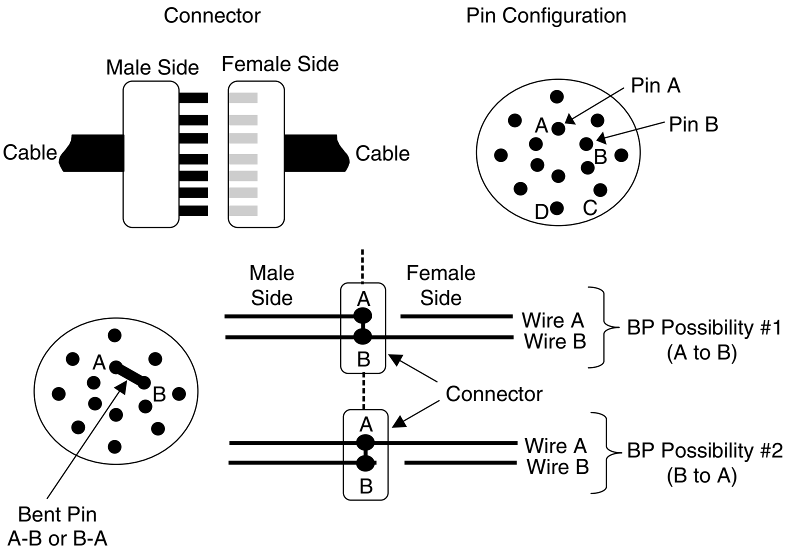


Figure 20.1 *BPA concept.*

3. Pin B makes contact with pin A; wires A and B become a short circuit, and the content of wire B has an upstream or downstream effect on wire A (depending upon the contents of both A and B).
4. Pin B makes contact with pin A; wire B becomes an open circuit after the short (downstream).

Figure 20.2 demonstrated the two possible outcomes from pin A bending and making contact with pin B. The overall system effect of these possibilities must be evaluated by the BPA. The upstream/downstream effect of the short can only be determined from the circuitry involved. Also, the overall effect of the open circuit can only be determined from the circuitry involved.

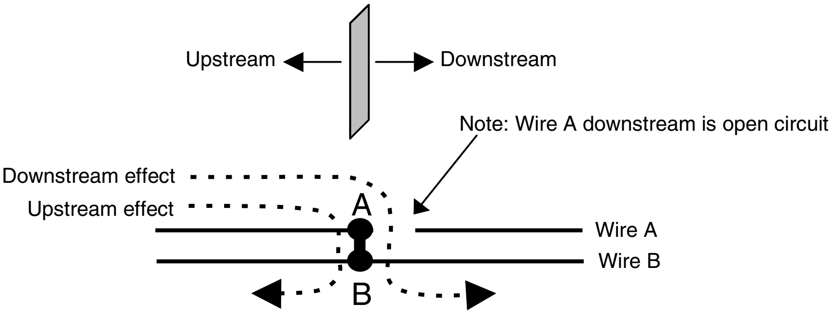


Figure 20.2 *Pin A to B short.*

20.5 METHODOLOGY

The BPA technique evaluates connector pin layouts to predict worst-case effects of failure and ultimately system consequences. BPA generally only considers and evaluates the effect of a single bent pin contacting another pin within its radius or with the connector case. BPA does not consider two pins bending and making contact with each other or with a third pin. The probability of multiple bent pins occurring is extremely small and would only be considered for high-consequence circuits.

Figure 20.3 summarizes the important relationships involved in BPA. This process consists of utilizing system design information and connector information to identify and mitigate hazards associated with potential bent connector pins.

Table 20.1 lists the basic steps in the BPA process, which involves performing a detailed analysis of all system electrical connectors. It should be noted that BPA applies to both circular and rectangular-shaped connectors. The examples in this chapter show round connectors, but the same methodology applies to rectangular connectors.

20.6 WORKSHEET

The BPA method is a detailed hazard analysis of wire connectors, utilizing structure and rigor. It is desirable to perform the BPA using a form or worksheet to provide analysis structure and consistency. The format of the analysis worksheet is not critical and can be modified to suit program requirements.

Typically, columnar-type worksheets are utilized to help maintain focus and structure in the analysis. As a minimum, the following basic information must be obtained from the analysis worksheets:

1. Possible bent pin combinations
2. The system effect to specific short or open circuits resulting from bent pins
3. The identification of bent pin combinations resulting in a hazard
4. System risk for the bent pin hazard

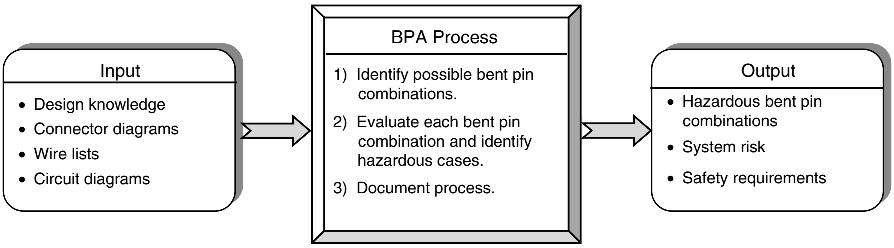
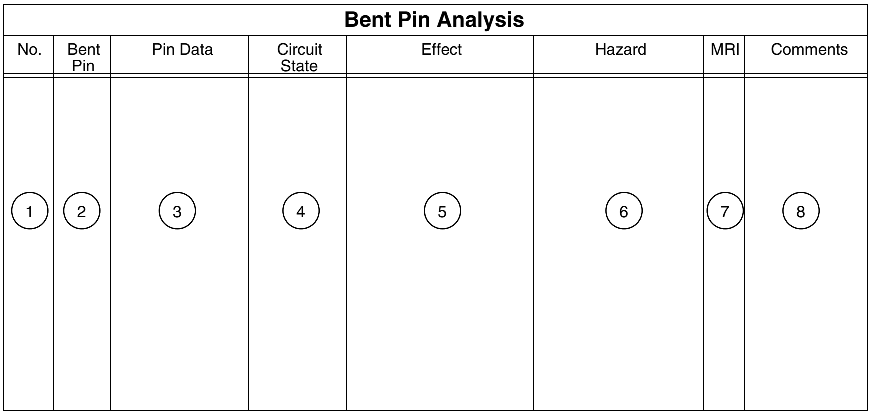


Figure 20.3 *BPA overview.*

TABLE 20.1 BPA Process

Step	Task	Description
1	Collect data.	Identify and collect data on all system wire connectors. This includes connector pin layouts and wire content descriptions.
2	Identify bent pin combinations.	Review connector pin layouts and identify all BP combinations that are physically possible, include contact with the case. Exclude BP combinations that are not possible.
3	Evaluate combinations.	Review the system design and operation to determine the effect of the potential BP combinations, should they occur. Analyze both A-B and B-A. For both A-B and B-A consider the possibilities: a. A short to B, with upstream/downstream effect on B b. A short to B, with A open from downstream side of connector c. B short to A, with upstream/downstream effect on A d. B short to B, with B open from downstream side of connector
4	Identify bent pin hazards.	Identify those BP combinations where the system effect can result in a system hazard.
5	Evaluate system risk.	Identify the level of mishap risk presented by the BP hazard.
6	Recommend corrective action.	Establish design safety requirements to mitigate the identified hazard, such as changing pin locations or changing the system design to safely accommodate the failure.
7	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
8	Document BPA.	Document the entire BPA process on the worksheets. Update for new information as necessary.

The recommended BPA matrix columnar-type worksheet is shown in Figure 20.4. This particular BPA worksheet utilizes a columnar-type format. Other worksheet formats may exist because different organizations often tailor their analysis worksheet to fit their particular needs. The specific worksheet to be used may be determined by the system safety program (SSP), system safety working group, or the safety analysis customer.



Bent Pin Analysis							
No.	Bent Pin	Pin Data	Circuit State	Effect	Hazard	MRI	Comments
1	2	3	4	5	6	7	8

Figure 20.4 *Recommended BPA worksheet.*

The following instructions describe the information required under each column entry of the BPA worksheet:

1. *No.* This column increments each BP combination in the analysis for reference purposes.
2. *Bent Pin* This column identifies the particular pin-to-pin short combination that is being analyzed. The analysis only considers a single bent pin making contact with another pin within its bend radius or a bent pin to the connector case.
3. *Pin Data* This column identifies the specific electrical or data content on each of the pins involved.
4. *Circuit State* This column identifies the two possible cases for BP analysis:
   a. Upstream and downstream effect of pin-to-pin short
   b. Downstream effect open circuit resulting from BP
5. *Effect* This column identifies the effect of the bent pin (short or open circuit), assuming it occurs, and includes the specific components impacted by the bent pin.
6. *Hazard* This column identifies the hazard that may result from the bent pin. Generally, the worst-case system effect is stated in this column.
7. *Mishap Risk Index (MRI)* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard, given that no mitigation techniques are applied to the hazard. Risk measures are a combination of mishap severity and probability, and the recommended values are shown below.

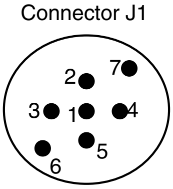
Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

8. *Comments* This column provides a place to record useful information regarding the hazard or the analysis process.

20.7 EXAMPLE

In order to demonstrate the BPA technique, the same hypothetical small missile system from Chapters 4 and 5 will be used. Figure 20.5 illustrates connector J1 for this example system, along with the connector pin layout and the pin content table. The pin content table contains a description of the electrical content of the pin (and associated wire).

Table 20.2 contains the bent pin matrix for connector J1. The bent pin matrix identifies which pins can physically make contact when one of the pins is bent. Also, a bent pin resulting in pin-to-case contact is considered.



Pin	Content Description
1	Missile Fire Command (+5 VDC)
2	+28 VDC Missile Electronics Power
3	Ground
4	+5 VDC Missile Electronics Power
5	Ground
6	Ground
7	–28 VDC Missile Electronics Power
Case	Metallic case; grounded

Figure 20.5 *Missile connector diagram and pin content table.*

The BP matrix is filled out by taking each of the pins in the left-hand column and identifying in the right-hand columns which pins it can physically contact when bent. In this BP matrix an S indicates the pin itself listed both horizontally and vertically; it is not relevant and is ignored by the analysis. An X in the matrix indicates two pins are within contact radius of one another if one of the pins is bent. These are the pin-to-pin combinations, which must then be analyzed in further detail. Connector pin layout, as well as pin length and position, is required to build this BP matrix.

The BP matrix and the pin content table are insufficient to determine the exact effect of pin-to-pin shorts. In order to determine the complete system effect of potential bent pins, it is necessary to have the complete circuit information available. Figure 20.6 contains an electrical circuit diagram for this example.

Tables 20.3–20.5 contain the BPA worksheets that evaluate each of the possible bent pin combinations generated from the bent pin matrix.

The following conclusions can be drawn from the BPA of this example missile system:

1. If pin 2 is bent and contacts pin 1 (case 2a), immediate missile launch will occur when the system is turned on and +28 VDC is applied to the launch initiator.

TABLE 20.2 Missile Connector Bent Pin Matrix

Pin	1	2	3	4	5	6	7	Case
1	S	X	X	X	X			
2	X	S						
3	X		S					
4	X			S				
5	X				S			
6						S		X
7							S	X

Code:

S—self to self (ignore).

X—possible bent pin contact.

2. If pin 4 is bent and contacts pin 1 (case 6a), immediate missile launch will occur when the system is turned on and +5 VDC is applied to the launch initiator.
3. The fire command on pin 2 is a safety critical function, and pin 2 should be isolated from other pins to avoid BP contact. If this is not possible, then pin 2 should only be in close proximity to safe short-circuit values, such as ground.

20.8 ADVANTAGES AND DISADVANTAGES

The following are advantages of the BPA technique:

1. BPA provides a pictorial aid for analysts in visualizing hazards.
2. BPA identifies hazards that might be overlooked by other techniques.

The disadvantage of the BPA technique is that it may require considerable time for obtaining detailed wire lists, electrical diagrams, and connector data.

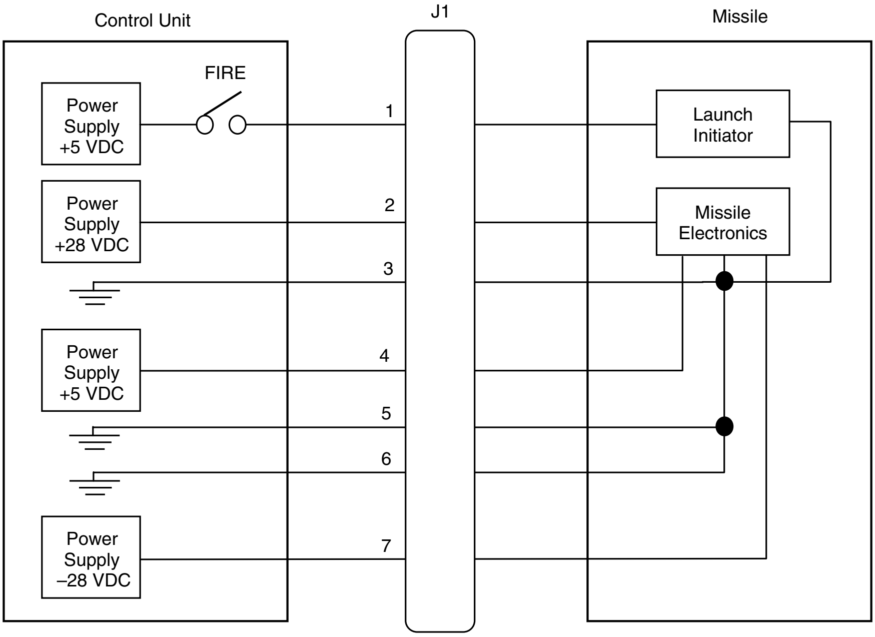


Figure 20.6 *Missile system schematic.*

TABLE 20.3 Example Bent Pin Analysis—Worksheet 1

Bent Pin Analysis							
No.	Bent Pin	Pin Data	Circuit State	Effect	Hazard	MRI	Comments
1	1 to 2	1. +5 VDC fire command	a. 1–2 short	+5 VDC short to +28 VDC when fire switch is closed	None		
		2. +28 VDC	b. 1 open	Unable to fire missile	None		
2	2 to 1	Same as 1	a. 2–1 short	+28 VDC short to missile launch initiator	Inadvertent missile launch	1C	Change pin layout
			b. 2 open	No +28 VDC power to missile electronics	Missile state unknown with loss of power	2C	Further study required
3	1 to 3	1. +5 VDC fire command	a. 1–3 short	+5 VDC short to ground when fire switch is closed	None		Unable to launch missile
		3. ground	b. 1 open	Same as 1b	None		
4	3 to 1	Same as 3	a. 3–1 short	Same as 3a	None		
			b. 3 open	Loss of ground to missile electronics and initiator	None		Has backup ground

TABLE 20.4 Example Bent Pin Analysis—Worksheet 2

Bent Pin Analysis							
No.	Bent Pin	Pin Data	Circuit State	Effect	Hazard	MRI	Comments
5	1 to 4	1. +5 VDC fire command	a. 1−4 short	+5 VDC short to +5 VDC when fire switch is closed	None		
		2. +28 VDC	b. 1 open	Same as 1b	None		
6	4 to 1	Same as 5	a. 4-1 short	+5 VDC short to missile initiator	Inadvertent missile launch	1C	Change pin layout
			b. 4 open	No +5 VDC power to missile electronics	Missile state unknown with loss of power	2C	Further study required
7	1 to 5	1. +5 VDC fire command	a. 1−5 short	Same as 3a	None		Unable to launch missile
		3. Ground	b. 1 open	Same as 1b	None		
8	5 to 1	Same as 7	a. 5−1 short	Same as 3a	None		
			b. 5 open	Same as 4b	None		Has backup ground

TABLE 20.5 Example Bent Pin Analysis—Worksheet 3

Bent Pin Analysis							
No.	Bent Pin	Pin Data	Circuit State	Effect	Hazard	MRI	Comments
9	6 to case	6. Ground case—ground	a. 6-case short	Ground to ground short	None		
			b. 1 open	Same as 4b	None		
10	7 to case	7. −28 VDC case—ground	a. 7-case short	−28 VDC short to ground	Arcs/sparks	2C	Change pin layout
			b. 7 open	No −28 VDC power to missile electronics	Missile state unknown with loss of power	2C	

20.9 COMMON MISTAKES TO AVOID

When first learning how to perform a BPA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of a BPA:

1. Not completely analyzing the system effect of both open and short circuits resulting from a bent pin
2. Not adequately determining pin length and bent pin contact radius
3. Not fully documenting the entire analysis in detail

20.10 SUMMARY

This chapter discussed the BPA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The purpose of the BPA is to identify hazards caused by electric circuits that are open or short-circuited from bent connector pins.
2. BPA should be a supplement to the PD-HAT, DD-HAT, and SD-HAT analyses.
3. BPA should always be considered whenever connectors are used to carry safety critical signals.
4. BPA generally assumes a single bent pin-to-pin contact since the probability of multiple bent pins contacting together is significantly less than the probability of a single bent pin.
5. BPA must address pin-to-case contact.
6. BPA is used to identify hazards that might be overlooked by other analyses, particularly those types of hazards involving bent connector pins causing electrical short circuits or open circuits.
7. The use of BPA worksheet forms and connector diagrams provides structure and rigor to the BPA process.

REFERENCES

There are no references for this technique that describe it in detail or provide examples. Refer to the *Safety Analysis Handbook* published by the System Safety Society for a short description of BPA.

Chapter 21

Hazard and Operability Analysis

21.1 INTRODUCTION

Hazard and operability (HAZOP) analysis is a technique for identifying and analyzing hazards and operational concerns of a system. It is a very organized, structured, and methodical process for carrying out a hazard identification analysis of a system, from the concept phase through decommissioning. Although HAZOP is a relatively simple process in theory, the steps involved must be carefully observed in order to maintain the rigor of the methodology.

The HAZOP analysis utilizes key guide words and system diagrams (design representations) to identify system hazards. Adjectives (guide words) such as *more*, *no*, *less*, and so forth are combined with process/system conditions such as *speed*, *flow*, *pressure*, and so on in the hazard identification process. HAZOP analysis looks for hazards resulting from identified potential deviations in design operational intent. A HAZOP analysis is performed by a team of multidisciplinary experts in a brainstorming session under the leadership of a HAZOP team leader.

Some of the key components to a HAZOP analysis include:

- A structured, systematic, and logical process
- A multidisciplinary team with experts in many areas
- An experienced team leader
- The controlled use of system design representations
- The use of carefully selected system entities, attributes, and guide words to identify hazards.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

21.2 BACKGROUND

This analysis technique falls under the preliminary design hazard analysis type (PD-HAT) and the detailed design hazard analysis type (DD-HAT). Refer to Chapter 3 for a discussion the analysis types. HAZOP analysis is also sometimes referred to as hazard and operability study (HAZOPS).

The purpose of HAZOP analysis is to identify the potential for system deviations from intended operational intent through the unique use of key guide words. The potential system deviations then lead to possible system hazards.

The HAZOP analysis is applicable to all types of systems and equipment, with analysis coverage given to subsystems, assemblies, components, software, procedures, environment, and human error. HAZOP analysis can be conducted at different abstraction levels, such as conceptual design, top-level design, and detailed component design. HAZOP analysis has been successfully applied to a wide range of systems, such as chemical plants, nuclear power plants, oil platforms, and rail systems. The technique can be applied to a system very early in design development and thereby identify safety issues early in the design process. Early application helps system developers to design in safety of a system during early development rather than having to take corrective action after a test failure or a mishap.

The HAZOP analysis technique, when applied to a given system by experienced personnel, should provide a thorough and comprehensive identification of hazards that exist in a given system or process. A basic understanding of hazard analysis theory is essential as well as system safety concepts. Experience with the particular type of system is helpful in generating a complete list of potential hazards, as well as experience in the HAZOP analysis process. The technique is uncomplicated and easily learned. An easily followed HAZOP analysis worksheet and instructions are provided in this chapter.

The HAZOP analysis was initially developed for the chemical process industry, and its methodology was oriented around process design and operations. The methodology can be extended to systems and functions with some practice and experience. The HAZOP analysis technique provides for an effective hazard analysis. In essence the HAZOP analysis is not much different from preliminary hazard analysis (PHA) or subsystem hazard analysis (SSHA), except for the guide words used. HAZOP analysis could be utilized for the PHA and/or SSHA techniques.

21.3 HISTORY

The HAZOP analysis was formalized as an analysis technique by the Institute of Chemical Industry (ICI) in the United Kingdom in the early 1970s to assess safety risk in chemical process plants. HAZOP analysis has been subsequently developed and improved upon and commercial software is available to assist in the HAZOP analysis process.

Although the HAZOP analysis technique was initially developed and used only by ICI, it became more widely used within the chemical process industry after the Flixborough disaster in which a chemical plant explosion killed 28 people, many of whom were residents living nearby. Through the general exchange of ideas and personnel, the methodology was then adopted by the petroleum industry, which has a similar potential for major disasters. This was then followed by the food and water industries, where the hazard potential is as great, but of a different nature, the concerns being more to do with contamination rather than explosions or chemical releases.

21.4 THEORY

The HAZOP analysis entails the investigation of deviations from design intent for a process or system by a team of individuals with expertise in different areas, such as engineering, chemistry, safety, operations, and maintenance. The approach is to review the process/system in a series of meetings during which the multidisciplinary team "brainstorms" the system design methodically by following a sequence based on prescribed guide words and the team leader's experience. The guide words are used to ensure that the design is explored in every conceivable manner. The HAZOP analysis is based on the principle that several experts with different backgrounds can interact and better identify problems when working together than when working separately and combining their results.

Fault trees may be used to complement the HAZOP analysis process. However, the use of fault trees in this context does not imply that the trees should be quantified probabilistically since the purpose is only the identification of mishap scenarios.

In many ways HAZOP analysis is similar to the PHA and SSHA in that it identifies hazards by evaluating the design by comparing system parameters to a list of key guide words that suggest modes of hazardous operation. The PHA and SSHA use hazard checklists in a manner similar to guide words.

The HAZOP analysis procedure involves taking a full description of a process/system and systematically questioning every part of it to establish how deviations from the design intent can arise. Once identified, an assessment is made as to whether such deviations and their consequences can have a negative effect upon the safe and efficient operation of the plant/system.

The HAZOP analysis is conducted through a series of team meetings led by the team leader. The key to a successful HAZOP is selection of the right team leader and the selection of the appropriate team members. This HAZOP analysis is applied in a structured way by the team, and it relies upon their imagination in an effort to discover credible causes of deviations from design intent. In practice, many of the deviations will be fairly obvious, such as pump failure causing a loss of circulation in a cooling water facility; however, the great advantage of the technique is that it encourages the team to consider other less obvious ways in which a deviation may occur. In this way the analysis becomes much more than a mechanistic checklist type of review. The result is that there is a good chance that potential failures and

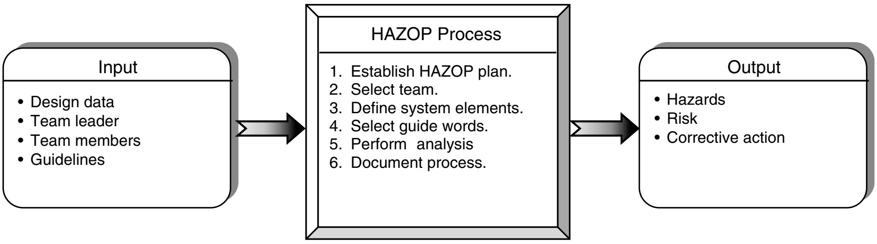


Figure 21.1 *HAZOP process.*

problems will be identified that had not previously been experienced in the type of plant/system being studied.

Figure 21.1 shows an overview of the basic HAZOP process and summarizes the important relationships involved in the HAZOP process.

21.5 METHODOLOGY

Table 21.1 lists and describes the basic steps of the HAZOP process.

Some of the key components to a HAZOP analysis include:

- A planned process that is structured, systematic, and logical.
- The correct composition of team members.
- The correct team leader (this is a critical element).
- Teamwork.
- HAZOP analysis training is vital.
- The controlled use of design representations.
- The planned use of entities, attributes, and guide words to identify hazards.

The HAZOP analysis is a time-consuming process, especially when many people are involved in the brainstorming sessions. Recommendations for avoidance or mitigation of the observed hazards cannot always be closed within the team meetings; thus, action items often result. Since the basic purpose of a HAZOP study is to identify potentially hazardous scenarios, the team should not spend any significant time trying to engineer a solution if a potential problem is uncovered. If a solution to a problem is obvious, the team should document the recommended solution in both the HAZOP and resulting HAR.

The HAZOP analysis is performed by comparing a list of system parameters against a list of guide words. This process stimulates the mental identification of possible system deviations from design intent and resulting hazards. Establishing and defining the system parameters and the guide words are key steps in the HAZOP analysis. The deviations from the intended design are generated by coupling the guide word with a variable parameter or characteristic of the plant, process,

TABLE 21.1 HAZOP Process

Step	Task	Description
1	Define system.	Define, scope, and bound the system. Define the mission, mission phases, and mission environments. Understand the system design and operation. Note that all steps are applicable for a software HAZOP.
2	Plan HAZOP.	Establish HAZOP analysis goals, definitions, worksheets, schedule, and process. Divide the system under analysis into the smallest segments desired for the analysis. Identify items to be analyzed and establish indenture levels for items/functions to be analyzed.
3	Select team.	Select team leader and all team members to participate in HAZOP analysis and establish responsibilities. Utilize team member expertise from several different disciplines (e.g., design, test, manufacturing, etc.).
4	Acquire data.	Acquire all of the necessary design and process data needed (e.g., functional diagrams, code, schematics, and drawings) for the system, subsystems, and functions. Refine the system information and design representation for HAZOP analysis.
5	Conduct HAZOP.	a. Identify and list the items to be evaluated. b. Establish and define the appropriate parameter list. c. Establish and define the appropriate guide word list d. Establish the HAZOP analysis worksheet. e. Conduct the HAZOP analysis meetings. f. Record the HAZOP analysis results on the HAZOP worksheets. g. Have the HAZOP analysis worksheets validated by a system engineer for correctness.
6	Recommend corrective action.	Recommend corrective action for hazards with unacceptable risk. Assign responsibility and schedule for implementing corrective action.
7	Monitor corrective action.	Review the HAZOP at scheduled intervals to ensure that corrective action is being implemented.
8	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
9	Document HAZOP.	Document the entire HAZOP process on the worksheets. Update for new information and closure of assigned corrective actions.

or system, such as reactants, reaction sequence, temperature, pressure, flow, phase, and the like. In other words:

$$\text{Guide word} + \text{parameter} = \text{deviation}$$

For example, when considering a reaction vessel in which an exothermic reaction is to occur and one of the reactants is to be added stepwise, the guide word *more* would be coupled with the parameter *reactant* and the deviation generated would be *thermal runaway*. Systematic examinations are made of each part of a facility or system. It should be noted that not all combinations of primary/secondary words are appropriate. For example, temperature/no (absolute zero or $-273°\text{C}$) or pressure/reverse could be considered as meaningless.

The amount of preparation required for a HAZOP analysis depends upon the size and complexity of the facility or system. Typically, the data required consist of various drawings in the form of line diagrams, flow sheets, facility layouts, isometrics and fabrication drawings, operating instructions, instrument sequence control charts, logic diagrams, and computer code. Occasionally, there are facility manuals and equipment manufacturers' manuals. The data must be accurate and sufficiently comprehensive. In particular, for existing facilities, line diagrams must be checked to ensure they are up to date and that modifications have not been made since the facility was constructed.

The HAZOP analyses are normally carried out by a multidisciplinary team with members being chosen for their individual knowledge and experience in design, operation, maintenance, or health and safety. A typical team would have between four and seven members, each with a detailed knowledge of the way in which the facility or system is intended to operate. The technique allows experts in the process to bring their knowledge and expertise to bear systematically so that problems are less likely to be missed. HAZOP is a technique for bringing fresh minds to work on a problem. It is essential that the team leader is an expert in the HAZOP technique. The team leader's role is to ensure the team follows the procedure. The leader must be skilled in leading a team of people who may not want to focus on meticulous attention and detail. It is recommended that the team leader should be an independent person; the team leader should not be associated with program management. The team leader must have sufficient technical knowledge to guide the study properly but should not necessarily be expected to make a technical contribution. It is beneficial if team members have had some training in the HAZOP technique.

Many HAZOP studies can be completed in 5 to 10 meetings, although for a small modification only 1 or 2 meetings may be necessary. However, for a large project it may take several months even with 2 or 3 teams working in parallel on different sections of the system. HAZOPs require major resources, which should not be underestimated. If HAZOP analyses are to be introduced to any organization for the first time, it may be appropriate to apply the technique to 1 or 2 problems to find out whether it is useful and can be applied successfully. If the technique can be successfully applied, it can grow naturally and be applied to larger projects.

It is common practice to record each step of a HAZOP analysis. Analysis recording includes a data file, which is a copy of the data (flow diagrams, original and final process and instrument diagrams, running instructions, bar sheets, models, etc.) used by the team during the examinations sessions and marked by the study leader to show that they have been examined.

Key HAZOP activities or tasks and who should perform these tasks are delineated in Table 21.2. It is important that these roles are performed by the team members.

21.5.1 Design Representations

A design representation models the system design and portrays the intention of the system designers through the features of the design. The design representation can take many forms and may be more or less detailed, depending on the stage of system

TABLE 21.2 HAZOP Roles

	Postulate	Explore	Explain	Conclude	Record
Leader	Yes	Possibly	Possibly	Yes	
Expert		Yes	Yes		
Designer		Possibly	Yes		
User		Possibly	Yes		
Recorder		Possibly			Yes

development. The design representation can be either physical or logical. A physical model shows the physical real-world layout of the system, such as through a drawing, schematic, or reliability block diagram. A logical design representation portrays the logical relationships between system elements in a form of how components should logically work and can be represented by functional flow diagrams, data flow diagrams, and the like. An extensive HAZOP analysis will likely be utilized for both physical and logical design representations.

The study leader can use the design representation as a form of analysis control. The representation acts as an agenda for the study team meetings as the team sequentially evaluates each item in the design representation.

The use of design representation aids, such as functional block diagrams, reliability block diagrams, context diagrams, data flow diagrams, timing diagrams, and so forth, greatly aids and simplifies the HAZOP analysis process. Each person on the team must understand the design representations utilized for the analysis.

21.5.2 System Parameters

A system is comprised of a set of components, and on a design representation a path between two components indicates an interaction or design feature that exists. An interaction can consist of a flow or transfer from one component to another. A flow may be tangible (such as a fluid) or intangible (such as an item of data). In either case, the flow is designed with certain properties, which can be referred to as attributes or parameters, which affect how the system operates. These parameters are the key to identifying design deviations in a HAZOP analysis.

The correct operation of a system is determined by the parameters of the interactions and components maintaining their design values (i.e., design intent). Hazards can be identified by studying what happens when the parameters deviate from the design intent. This is the principle behind HAZOP analysis.

Table 21.3 contains a list of example system parameters. The list is purely illustrative, as the words employed in an actual HAZOP review will depend upon the plant or system being studied.

Note that some parameter words may not appear to be related to any reasonable interpretation of the design intent of a process. For example, one may question the use of the word *corrode* on the assumption that no one would intend that corrosion should occur. Bear in mind, however, that most systems are designed with a certain life span in mind, and implicit in the design intent is that corrosion should not occur,

TABLE 21.3 Example System Parameters

- Flow (gas, liquid, electric current)
- Pressure
- Separate (settle, filter, centrifuge)
- Reaction
- Reduce (grind, crush, etc.)
- Corrode
- Isolate
- Vent
- Inspection, surveillance
- Viscosity
- Instruments
- Corrosion
- Vibration
- Software data flow
- Temperature
- Level
- Composition
- Mix
- Absorb
- Erode
- Drain
- Purge
- Maintain
- Shutdown
- Startup
- Erosion
- Shock
- Density

or if it is expected, it should not exceed a certain rate. An increased corrosion rate in such circumstances would be a deviation from the design intent.

21.5.3 Guide Words

Guide words help both to direct and to stimulate the creative process of identifying potential design deviations. Guide words may be interpreted differently in different industries and at different stages of the system's life cycle. The interpretation of a guide word must be in these contexts of these factors. The purpose of the interpretations is to enable the exploration of plausible deviations from the design intent.

The HAZOP analysis guide words are short words used to stimulate the imagination of a deviation of the design intent. For example, for the parameter "data flow" in a computer system, the guide word *more* can be interpreted as more data is passed than intended, or data is passed at a higher rate than intended. For the parameter "wire" in a system, the guide word *more* can be interpreted as higher voltage or current than intended. Table 21.4 contains an example list of HAZOP guide words.

21.5.4 Deviation from Design Intent

Since HAZOP analysis is based on searching for *deviations from design intent*, it is important to understand this concept. All systems are designed with an overall purpose in mind. For an industrial plant system it may be to produce a certain tonnage per year of a particular chemical, to manufacture a specified number of cars, to process and dispose of a certain volume of effluent per annum, and so forth. For a weapons system the purpose is to intentionally hit the intended target. These are the primary design intents for these systems; however, a secondary intent would be to operate the system in the safest and most efficient manner possible.

In order to achieve its goals, each subsystem of the system must consistently function in a particular manner. It is this manner of performance that could be classified as the design intent for that particular item. To illustrate, imagine that as part of

TABLE 21.4 Example HAZOP Guide Words

Guide Word	Meaning
No	The design intent does not occur (e.g., Flow/No), or the operational aspect is not achievable (Isolate/No).
Less	A quantitative decrease in the design intent occurs (e.g., Pressure/Less).
More	A quantitative increase in the design intent occurs (e.g., Temperature/More).
Reverse	The opposite of the design intent occurs (e.g., Flow/Reverse).
Also	The design intent is completely fulfilled, but in addition some other related activity occurs (e.g., Flow/Also indicating contamination in a product stream, or Level/Also meaning material in a tank or vessel that should not be there).
Other	The activity occurs, but not in the way intended (e.g., Flow/Other could indicate a leak or product flowing where it should not, or Composition/Other might suggest unexpected proportions in a feedstock).
Fluctuation	The design intention is achieved only part of the time (e.g., an air lock in a pipeline might result in Flow/Fluctuation).
Early	The timing is different from the intention. Usually used when studying sequential operations, this would indicate that a step is started at the wrong time or done out of sequence.
Late	Same as for Early.
As well as (more than)	An additional activity occurs.
Part of	Only some of the design intention is achieved.
Reverse	Logical opposite of the design intention occurs.
Where else	Applicable for flows, transfers, sources, and destinations.
Before/after	The step (or some part of it) is effected out of sequence.
Faster/slower	The step is done/not done with the right timing.
Fails	Fails to operate or perform its intended purpose.
Inadvertent	Function occurs inadvertently or prematurely (i.e., unintentionally).

the overall production requirement for a system is the need for a cooling-water facility. Meeting this requirement would involve circulating water in a pipe system that is driven by a pump. A simplified statement as to the design intent of this small section of the plant would be “to continuously circulate cooling water at an initial temperature of x°C and at a rate of n gallons per hour.” It is usually at this low level of design intent that a HAZOP analysis is directed. The use of the word *deviation* now becomes easier to understand. A deviation or departure from the design intent in the case of the cooling facility would be a failure of circulation, or the water being at too high an initial temperature. Note the difference between a deviation and its cause. In this case, failure of the pump would be a cause not a deviation.

21.6 WORKSHEET

The HAZOP analysis technique is a detailed hazard analysis utilizing structure and rigor. It is desirable to perform the HAZOP analysis using a specialized worksheet. Although the format of the analysis worksheet is not critical, typically, matrix or columnar-type worksheets are used to help maintain focus and structure in the analysis. The HAZOP analysis sessions are primarily reported in the HAZOP worksheets, in which the different items and proceedings are recorded. As a minimum, the following basic information is required from the HAZOP analysis worksheet:

1. Item under analysis
2. Guide words
3. System effect if guide word occurs
4. Resulting hazard or deviation (if any)
5. Risk assessment
6. Safety requirements for eliminating or mitigating the hazards.

The recommended HAZOP analysis worksheet is shown in Figure 21.2. This particular HAZOP analysis worksheet utilizes a columnar-type format. Other worksheet formats may exist because different organizations often tailor their HAZOP analysis worksheet to fit their particular needs. The specific worksheet to be used may be determined by the system safety program (SSP), system safety working group, or the HAZOP analysis team performing the analysis.

The following instructions describe the information required under each column entry of the HAZOP worksheet:

1. *No.* This column identifies each HAZOP line item and is used for purposes of reference to any part of the analysis.
2. *Item* This column identifies the process, component, item, or function being analyzed.
3. *Function/Purpose* This column describes the item's purpose or function in the system so that the operational intent is understood.
4. *Parameter* This column identifies the system parameter that will be evaluated against the guide words.

HAZOP Analysis										
No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments
①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪

Figure 21.2 *Recommended HAZOP worksheet.*

5. *Guide Word* This column identifies the guide words selected for the analysis.
6. *Consequence* This column identifies the most immediate and direct effect of the guide word occurring, usually in terms of a system deviation from design intent.
7. *Cause* This column identifies all of the possible factors that can cause the specific deviation. Causal factors may include many different sources, such as physical failure, wear out, temperature stress, vibration stress, and the like. All conditions that affect a component or assembly should be listed to indicate whether there are special periods of operation, stress, personnel action, or combinations of events that would increase the probabilities of failure or damage.
8. *Hazard* This column identifies the specific hazard that is created as a result of the specific consequence or deviation. (Remember: Document all hazard considerations, even if they are later proven to be nonhazardous.)
9. *Risk* This column provides a qualitative measure of mishap risk for the potential effect of the identified hazard. Risk measures are a combination of mishap severity and probability, and the recommended qualitative values from MIL-STD-882 are shown below.

Severity	Probability
1. Catastrophic	A. Frequent
2. Critical	B. Probable
3. Marginal	C. Occasional
4. Negligible	D. Remote
	E. Improbable

10. *Recommendation* This column provides for any recommendations for hazard mitigation that are evident from the HAZOP analysis, such as design or procedural safety requirements.
11. *Comments* This column provides for any pertinent comments to the analysis that need to be remembered for possible future use.

21.7 EXAMPLE 1

Figure 21.3 contains an example water pumping system for this HAZOP analysis example. In this system water is supplied from a common source to three steam generators. For successful system operation, two of the three generators must be operational. Some redundancy has been designed into the system to help achieve this operational requirement. The pumps are electrical-driven pumps that pump the water from the tank to the motor operated valves (MOVs). The MOVs are opened and closed by electric power. The pumps, MOVs, and generators are all monitored and controlled by a single common computer, and they are powered from a common electrical source.

After carefully reviewing all of the design representations for this system, the following design parameters have been selected for HAZOP analysis: fluid, pressure,

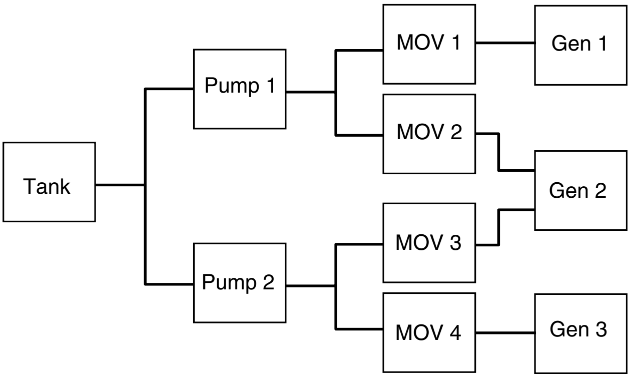


Figure 21.3 *Example 1 system diagram.*

temperature, electricity, and steam. The HAZOP analysis worksheet for this example is shown in Table 21.5. Note that the analysis worksheet was not completed for the entire set of parameters and guide words but only a few in order to demonstrate the HAZOP analysis technique.

21.8 EXAMPLE 2

Example 2 is a software-oriented HAZOP analysis. Figure 21.4 depicts the software design for a hypothetical missile system. The software segment shown is for the missile fire control system, which handles missile status data and missile command data.

The HAZOP analysis worksheet for this example is shown in Table 21.6.

21.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the HAZOP technique:

1. HAZOP analysis is easily learned and performed.
2. HAZOP analysis does not require considerable technical expertise for technique application.
3. HAZOP analysis provides rigor for focusing on system elements and hazards.
4. HAZOP analysis is a team effort with many viewpoints.
5. Commercial software is available to assist in HAZOP analysis.

The following are disadvantages of the HAZOP technique:

1. HAZOP analysis focuses on single events rather than combinations of possible events.

TABLE 21.5 HAZOP Worksheet for Example 1

HAZOP Analysis										
No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments
1	Pipes	To carry water through system	Fluid	No	Loss of fluid, system failure; equipment damage	Pipe leak; pipe rupture	Equipment damage	2D		
2				More	Pressure becomes too high, resulting in pipe rupture	No pressure relief valves in system	Equipment damage	2C	Add pressure relief valves to system	
3				Less	Insufficient water for operation of generators	Pipe leak; pipe rupture	Equipment damage	2D		
4				Reverse	Not applicable			—		
5	Electric power	To provide electricity to operate pumps, MOVs, and generators	Electricity	No	Loss of power to operate system components	Power grid loss; circuit breakers trip	Loss of system operation	2D	Provide source of emergency backup power	

(*continued*)

TABLE 21.5 *Continued*

HAZOP Analysis										
No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments
6				More	Trips circuit breakers	Power surge	Loss of system operation	2C	Provide for fault detection and isolation	
7				Less	Insufficient power to adequately operate system components	Power grid fault	Equipment damage	2D	Provide source of emergency backup power	
8				Reverse	Not applicable			—		
Analyst:				Date:					Page: 1 of 1	

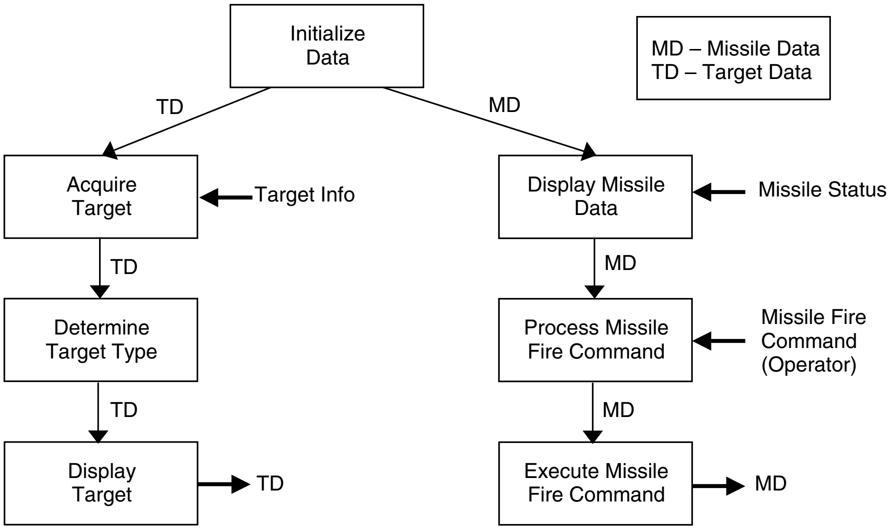


Figure 21.4 *Example 2 system diagram.*

2. The HAZOP analysis focus on guide words allows it to overlook some hazards not related to a guide word.
3. HAZOP analysis training is essential for optimum results, especially for the facilitator.
4. The HAZOP analysis can be time consuming and thus expensive.

21.10 COMMON MISTAKES TO AVOID

When first learning how to perform a HAZOP analysis, it is commonplace to commit some typical errors. The following is a list of common errors made during the conduct of a HAZOP analysis:

1. Not selecting an experienced and trained team leader
2. Not selecting the appropriate team
3. Not adequately planning, scheduling, or funding the HAZOP analysis

21.11 SUMMARY

This chapter discussed the HAZOP analysis technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of HAZOP is to identify deviations from design intent that can lead to the occurrence of an undesired event or hazard.

TABLE 21.6 HAZOP Worksheet for Example 2

HAZOP Analysis										
No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments
1	Missile fire control	Performs missile status and control	Missile data	No (None)	Loss of missile status to operator	Hardware fault; software error	Unsafe missile	2D		
2				More/Less (wrong)	Missile status to operator is incorrect	Hardware fault; software error	Equipment damage	2D		
3				Early/Late (timing)	Missile status to operator is incorrect	Hardware fault; software error	Equipment damage	2D		
4			Missile command	No (none)	Loss of missile control	Hardware fault; software error	Unable to safe missile	2D		
5				More/Less (wrong)	Operator command to missile is incorrect	Hardware fault; software error	Inadvertent launch command	1D	Add command status checks to design	
6				Early/Late (timing)	Operator command to missile is incorrect	Hardware fault; software error	Unable to safe missile	2D		
Analyst:					Date:				Page: 1 of 1	

2. HAZOP analysis requires an experienced team leader in conjunction with an appropriately selected team.
3. The use of design representation aids, such as functional block diagrams, reliability block diagrams, context diagrams, and the like, greatly aids and simplifies the HAZOP analysis process.

BIBLIOGRAPHY

Chemical Industries Association, *A Guide to Hazard and Operability Studies*, Chemical Industries Association, 1977.

Kletz, T. A., *HAZOP and Hazan*, 4th ed., Taylor & Francis, 1999.

International Electrotechnical Commission, IEC 61882, *Hazard and Operability (HAZOP) Studies Application Guide*, IEC, 2001.

Nolan, D. P., *Application of Hazop and What-If Safety Reviews to the Petroleum, Petrochemical and Chemical Industries*, Noyes, 1994.

Redmill, F., M. Chudleigh, and J. Catmur, *System Safety: HAZOP and Software HAZOP*, Wiley, New York, 1999.

Swann, C. D. and M. L. Preston, Twenty Five Years of HAZOPS, *J. Loss Prevention*, **8**(6): 349–353 (1995).

Chapter 22

Cause–Consequence Analysis

22.1 INTRODUCTION

Cause–consequence analysis (CCA) is an analysis methodology for identifying and evaluating the sequence of events resulting from the occurrence of an initiating event. CCA utilizes a visual logic tree structure known as a cause–consequence diagram (CCD). The objective of CCA is to determine whether the initiating event will develop into a serious mishap, or if the event is sufficiently controlled by the safety systems and procedures implemented in the system design. A CCA can result in many different possible outcomes from a single initiating event, and it provides the capability to obtain a probability for each outcome.

The CCA technique is a method of risk assessment that provides a means of graphically displaying interrelationships between consequences and their causes. Safety design features that are intended to arrest accident sequences are accounted for in the CCA.

22.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (SD-HAT). Refer to Chapter 3 for a discussion on hazard analysis types.

The purpose of CCA is to identify and evaluate all of the possible outcomes that can result from an initiating event (IE). An IE is an event that starts an accident sequence that may result in an undesirable consequence. Generally, there are

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

many different outcomes possible from an IE, depending upon whether design safety systems work properly or malfunction when needed. CCA provides a probabilistic risk assessment (PRA) of the risk associated with each potential outcome.

The CCA method can be used to model an entire system, with analysis coverage given to subsystems, assemblies, components, software, procedures, environment, and human error. CCA can be conducted at different abstraction levels, such as conceptual design, top-level design, and detailed component design. CCA has been successfully applied to a wide range of systems, such as nuclear power plants, spacecraft, and chemical plants. The technique can be applied to a system very early in design development and thereby identify safety issues early in the design process. Early application helps system developers to design in safety of a system during early development rather than having to take corrective action after a test failure or a mishap. CCA could be a supplement to the SD-HAT and the detailed design hazard type (DD-HAT).

The CCA technique, when applied to a given system by an experienced analyst, is thorough at identifying and evaluating all of the possible outcomes resulting from an initiating event and combining them together in a visual diagram. A basic understanding of CCA and fault tree analysis (FTA) theory is essential to developing a CCA model. In addition it is crucial for the analyst to have a detailed understanding of the system. As system complexity increases, increased knowledge and experience in CCA and FTA is also required. Overall, CCA is very easy to learn and understand. Proper application depends on the complexity of the system and the skill of the analyst.

The CCA method is a very powerful tool for identifying and evaluating all of the system consequence paths that are possible after an initiating event occurs. The CCA model will show the probability of the system design resulting in a safe operation path, a degraded operation path, and an unsafe operation path.

The use of a CCA is recommended for a PRA of the possible outcomes resulting from an initiating event. The resulting risk profiles provide management and design guidance on areas requiring additional safety countermeasures design methods. The CCD provides a means for the analyst to organize the system design into a manner showing the failure behavior of the system. CCA emphasizes the fact that an IE has many possible causes and many possible consequences, and the CCD displays these relationships.

22.3 HISTORY

The CCA methodology was developed at RISO National Laboratories, Denmark, in the 1970s, specifically to aid in the reliability and risk analysis of nuclear power plants in Scandinavian countries. The method was developed to assist in the cause–consequence accident analysis of key system components. Some analysts feel that the technique is superior to an event tree analysis (ETA), which is also capable of identifying all possible consequences of a given critical event.

22.4 DEFINITIONS

Cause–consequence analysis is based on the following definitions:

Accident scenario Series of events that ultimately result in an accident, mishap, or undesired outcome. The sequence of events begins with an initiating event and is (usually) followed by one or more intermediate events that lead to the undesired end state or outcome.

Initiating event (IE) Failure or undesired event that initiates the start of an accident sequence. The IE may result in a mishap, depending upon successful operation of the hazard countermeasure methods designed into the system. Refer to Chapter 2 on hazard theory for information on the components of a hazard.

Consequence (outcome) Outcome resulting from the occurrence of a series of incremental system successes and failures. System safety analysts are generally concerned with outcomes that result in mishaps, while reliability analysts generally are concerned with system unavailability outcomes.

Intermediate event Intermediate event in the cause–consequence sequence of events. These are the failure/success events of the design safety methods established to prevent the IE from resulting in a mishap. If an intermediate event works successfully, it stops the accident scenario and is referred to as a mitigating event. If an intermediate event fails to work, the accident scenario is then allowed to progress and is referred to as an aggravating outcome event. The intermediate event is similar to the pivotal event in ETA (refer to Chapter 12).

Probabilistic risk assessment (PRA) Comprehensive, structured, and logical analysis method for identifying and evaluating risk in a complex technological system. The detailed identification and assessment of accident scenarios, with a quantitative analysis is the PRA goal.

22.5 THEORY

When performing a CCA, identifying and developing accident scenarios is fundamental to the concept. CCA is very similar to ETA (see Chapter 12). The theory is to first identify all of the IEs that have significant safety impact or concern and then perform a CCA on each IE. Hazard analysis is a methodology for identifying IEs of concern. A CCD is constructed that models the sequence of events that can result from an IE, taking into account the success or failure of design safety features intended to prevent undesirable consequences. The CCD combines the causes and consequences of each IE, resulting in a model with many different possible outcomes from a single IE.

An accident scenario contains an IE and (usually) one or more intermediate events leading to an end state or outcome. A scenario contains an IE and (usually) one or more pivotal events leading to an end state as shown in Figure 22.1.

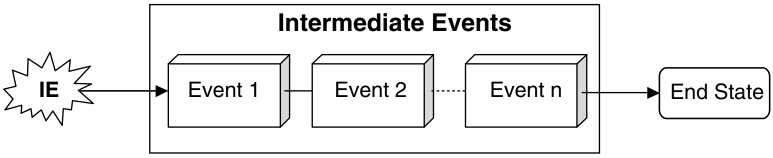


Figure 22.1 *Accident scenario concept.*

Figure 22.2 shows the CCA concept. Through the use of FT logic and CCD logic, probability values can be obtained from the CCA. Note that FTA is used to determine the event causes of failure and their failure probability. To determine the probability of an outcome, the event probabilities in the outcome path are multiplied together.

22.6 METHODOLOGY

Table 22.1 describes the basic steps of the CCA process. This process involves identifying and evaluating the sequence events that are possible after the occurrence of a given IE.

Complex systems tend to have a large number of interdependent components, redundancy, standby systems, and safety systems. Sometimes it is too difficult or cumbersome to model a system with just a FT, so PRA studies have combined

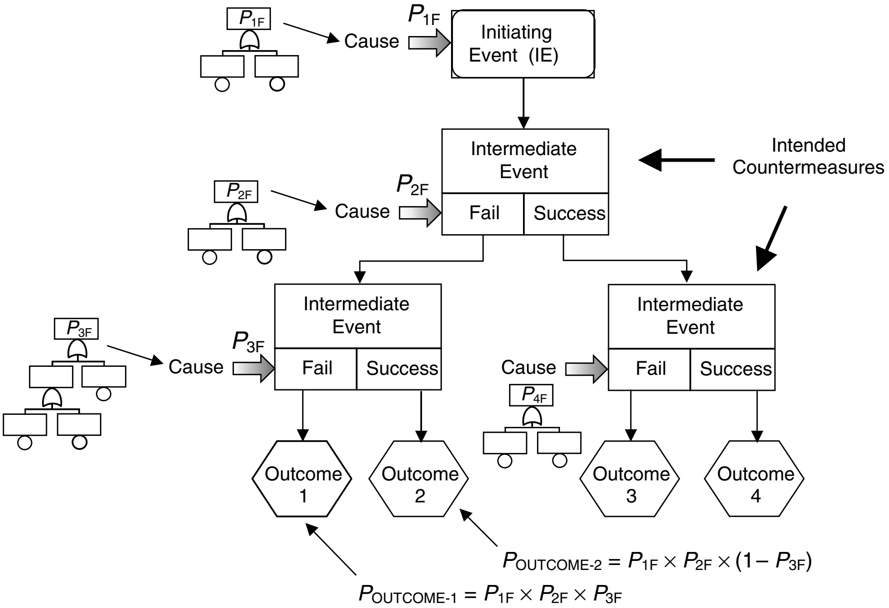


Figure 22.2 *CCA overview.*

TABLE 22.1 CCA Process

Step	Task	Description
1	Define the system.	Examine the system and define the system boundaries, subsystems, and interfaces.
2	Identify the accident scenarios.	Perform a system assessment or hazard analysis to identify the system hazards and accident scenarios existing within the system design.
3	Identify the initiating events (IEs).	Refine the hazard analysis to identify the significant IEs in the accident scenarios. IEs include events such as fire, collision, explosion, pipe break, toxic release, etc.
4	Identify the intermediate events.	Identify the safety barriers or countermeasures involved with the particular scenario that are intended to preclude a mishap. These become the intermediate events.
5	Build the CCA diagram.	Construct the logical CCD, starting with the IE, then the intermediate events and completing with the outcomes of each path.
6	Obtain the failure event probabilities.	Obtain or compute the failure probabilities for the intermediate failure events on the CCD. It may be necessary to use FTs to determine how an event can fail and to obtain the failure probability.
7	Identify the outcome risk.	Compute the risk for each outcome in the CCD. To determine the probability of an outcome, the event probabilities in the outcome path are multiplied together.
8	Evaluate the outcome risk.	Evaluate the outcome risk of each path and determine if the risk is acceptable.
9	Recommend corrective action.	If the outcome risk of a path is not acceptable, develop design strategies to change the risk.
10	Hazard tracking.	Enter identified hazards, or supporting data, into the hazard tracking system (HTS).
11	Document CCA.	Document the entire CCA process on the CCDs. Update for new information as necessary.

the use of FTs and CCDs. The CCD models accident/mishap cause–consequence scenarios, and FTs model complex subsystems to obtain the probability of these subsystems failing. An accident scenario can have many different outcomes, depending on which components fail and which function correctly. The CCD/FT combination models this complexity very well.

The goal of CCA is to determine the probability of all the possible outcomes resulting from the occurrence of an IE. By analyzing all possible outcomes, it is possible to determine the percentage of outcomes that lead to the desired result and the percentage of outcomes that lead to the undesired result.

The CCD is a diagram modeling all of the possible events that follow an IE. The IE can be a design failure or an operational human error. The objective is to identify the chain of events following one or more specified intermediate events in order to evaluate the consequences and determine whether the event will develop into a mishap or are sufficiently controlled by the safety systems implemented. The results can therefore be recommendations to increase the redundancy or to modifications to the safety systems.

The CCA begins with the identified IE listed at the top of the diagram. All safety design methods or countermeasures are then listed sequentially below, in the form of decision boxes. The decision box provides two possible paths: (a) operates successfully and (b) fails to operate. The resulting diagram combines all of the various success/failure event combinations and fans out in a downward tree structure. Each success/failure event can be assigned a probability of occurrence, and the final outcome probability is the product of the event probabilities along a particular path. Note that the final outcomes can range from safe to catastrophic, depending upon the chain of events.

The CCA identifies all of the causes of an undesired event, as well as all of the possible outcomes resulting from it. The CCA documents the failure logic involved in mishaps resulting from an IE. CCA also provides a mechanism for time delays and sequencing between events.

A failure dependency arises when the same fault event exists in more than one FT structure on the same path in the CCD. Repeated failures often influence more than one decision box in the CCA. As in FTA, repeated failure events must be properly accounted for in the mathematical evaluation, otherwise the final probability calculation will be incorrect. In order to resolve this problem, the failure event is extracted from the various FTs and placed on the CCD (see Example 2 later in this chapter).

An IE is an event that starts a certain operational sequence or an event that activates safety systems. The IE must be carefully selected for the CCA. Potential IEs are identified from hazard analyses and known system problems.

22.7 SYMBOLS

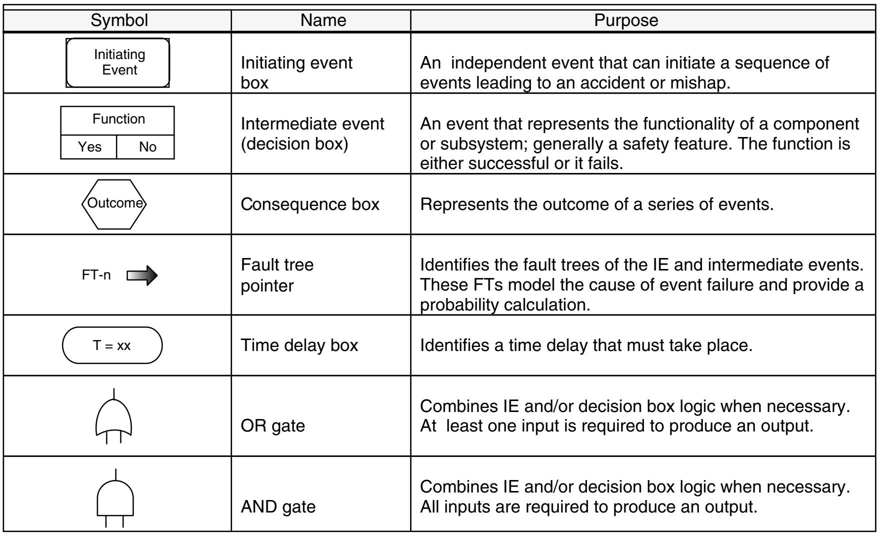
Figure 22.3 shows the CCD symbols along with their definitions.

22.8 WORKSHEET

The primary worksheet for a CCA is the CCD, which provides the following information:

1. Initiating event
2. Intermediate events (i.e., pivotal events)
3. Outcomes
4. Event and outcome probabilities
5. Timing

Figure 22.2 showed a generic CCD structure. Each intermediate event is divided into two paths, success and failure. The CCA has only one IE, which is identified at the



Symbol	Name	Purpose
Initiating Event	Initiating event box	An independent event that can initiate a sequence of events leading to an accident or mishap.
Function Yes No	Intermediate event (decision box)	An event that represents the functionality of a component or subsystem; generally a safety feature. The function is either successful or it fails.
Outcome	Consequence box	Represents the outcome of a series of events.
FT-n	Fault tree pointer	Identifies the fault trees of the IE and intermediate events. These FTs model the cause of event failure and provide a probability calculation.
T = xx	Time delay box	Identifies a time delay that must take place.
	OR gate	Combines IE and/or decision box logic when necessary. At least one input is required to produce an output.
	AND gate	Combines IE and/or decision box logic when necessary. All inputs are required to produce an output.

Figure 22.3 *CCA symbols.*

top of the diagram, and as many intermediate events as necessary to fully describe the system as traced through by the CCD. The more intermediate events involved, the larger the resulting CCA and the more branches required.

22.9 EXAMPLE 1: THREE-COMPONENT PARALLEL SYSTEM

Figure 22.4 contains a CCA for an example system comprised of three components in parallel. Successful system operation requires successful operation of any one, or more, of the three components. The IE for this example is “power applied to the system.”

22.10 EXAMPLE 2: GAS PIPELINE SYSTEM

Example 2 involves a gas pipeline system as shown in Figure 22.5. It has been determined from hazard analyses that an undesired IE is a high-pressure surge in the pipeline. The CCD shows the various outcomes that are possible from this IE.

Table 22.2 lists the components in this example system and describes their function. This portion of the system is intended to prevent a pipeline rupture if a gas pressure surge occurs in the line. Sensor S1 detects high pressure and sends a warning signal to the master computer C1. When C1 receives the pressure warning, it sends out signals to master valves MV1, MV2, and MV3 to immediately close. Should this primary pressure detection and control system fail, there is a backup pressure detection and control system that functions in a similar manner.

Figure 22.6 contains the CCD for this example gas pipeline system. Figure 22.7 contains the FTs that support the CCD shown in Figure 22.6.

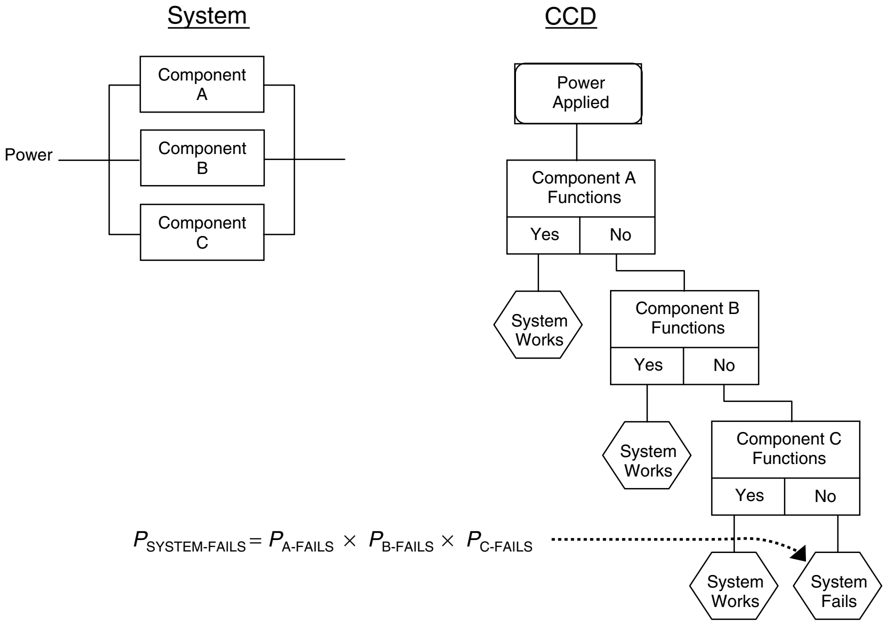


Figure 22.4 *Example 1: Three-component parallel system and CCD.*

22.10.1 Reducing Repeated Events

The CCA version 1 fault trees shown in Figure 22.7 reveal that there are some repeated failures in the CCD events. FT transfer symbol A indicates that this FT branch in FT-1 also occurs in FT-2 and FT-3, and transfer symbol B in FT-4 also occurs in FT-5. This means that if the CCD events were to be multiplied together, there would be an error in the calculation because of the repeated events being in each of the event calculations.

In order to derive a correct calculation, the repeated events must be mathematically reduced. Chapter 11 on FTA describes how to do this for FTs. In CCA the

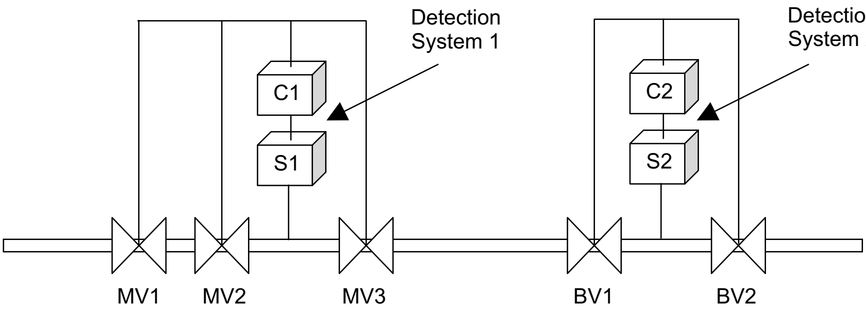


Figure 22.5 *Example 2: Gas pipeline system diagram.*

TABLE 22.2 System Components for Gas Pipeline

Label	Name	Function
S1	Sensor 1	Senses high pressure and sends warning to C1.
C1	Computer 1	Sends command to the three master valves to close.
MV1	Master valve 1	When open allows gas flow; when closed stops gas flow.
MV2	Master valve 2	When open allows gas flow; when closed stops gas flow.
MV3	Master valve 3	When open allows gas flow; when closed stops gas flow.
S2	Sensor 2	Senses high pressure and sends warning to C2.
C2	Computer 2	Sends command to the two backup valves to close.
BV1	Backup valve 1	When open allows gas flow; when closed stops gas flow.
BV2	Backup valve 2	When open allows gas flow; when closed stops gas flow.

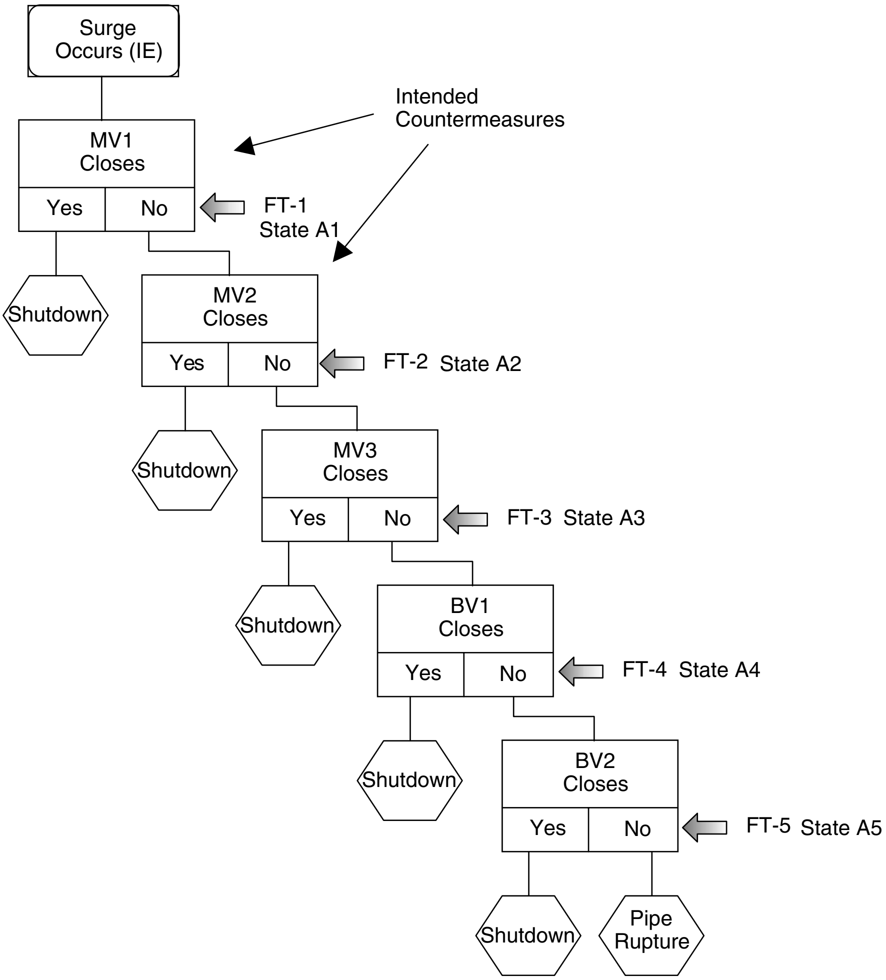


Figure 22.6 *Example 2: CCD (version 1).*

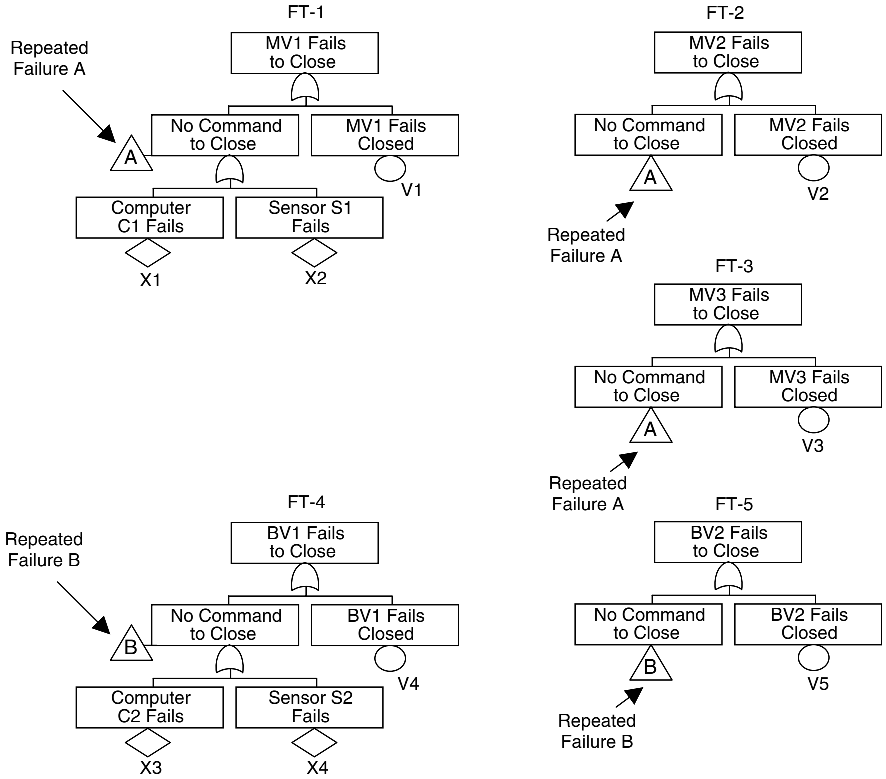


Figure 22.7 *Example 2: CCD fault trees (version 1).*

reduction can be achieved through Boolean reduction or by revising the CCD accordingly, as shown in Figures 22.8 and 22.9.

Figure 22.8 breaks the original CCD into two separate branches via the OR gate at the top of the diagram. This revised structure eliminates the repeated events in all of the paths.

Figure 22.9 contains the FTs that support the version 2 CCD shown in Figure 22.8. The mathematical equations for computing the probability of pipe rupture for the two CCD versions are as follows:

Version 1

$$\begin{aligned}P_{\mathrm{RUPTURE}} &= P_{\mathrm{IE}} \times P_{\mathrm{A1}} \times P_{\mathrm{A2}} \times P_{\mathrm{A3}} \times P_{\mathrm{A4}} \times P_{\mathrm{A5}} \\ &= (P_{\mathrm{IE}})(P_{\mathrm{X1}} + P_{\mathrm{X2}} + P_{\mathrm{V1}})(P_{\mathrm{X1}} + P_{\mathrm{X2}} + P_{\mathrm{V2}})(P_{\mathrm{X1}} + P_{\mathrm{X2}} + P_{\mathrm{V3}}) \\ &\quad \times (P_{\mathrm{X3}} + P_{\mathrm{X4}} + P_{\mathrm{V4}})(P_{\mathrm{X3}} + P_{\mathrm{X4}} + P_{\mathrm{V5}})\end{aligned}$$

Note: State A5 is from the version 1 CCD.

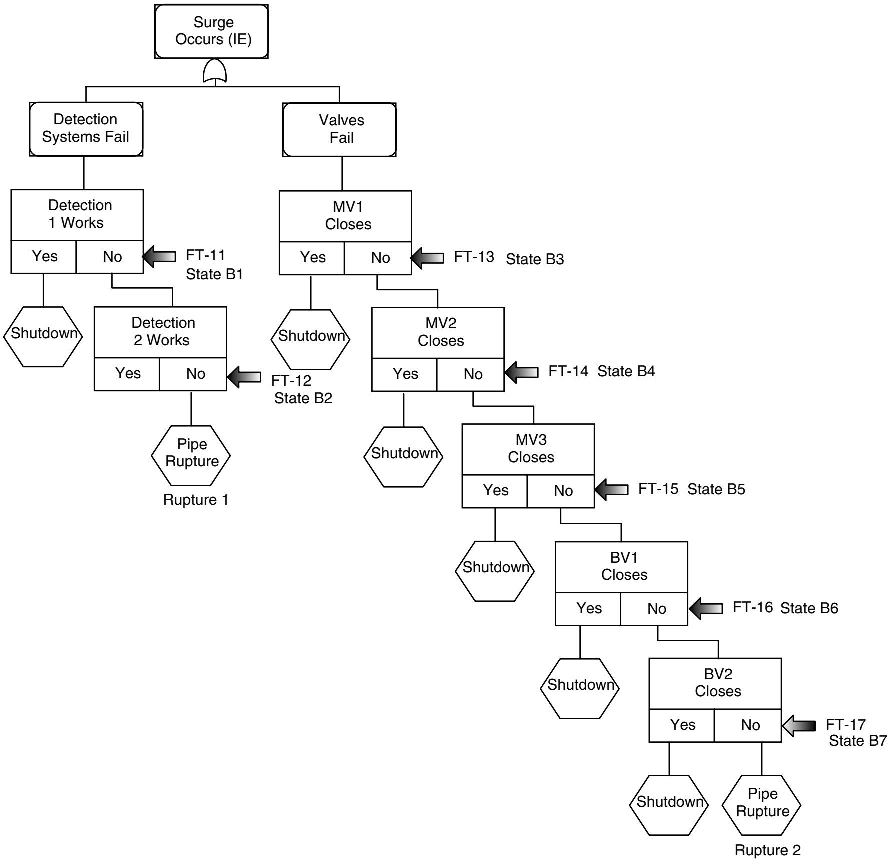


Figure 22.8 *Example 2: CCD revised (version 2).*

Version 2

$$\begin{aligned} P_{\text{RUPTURE}} &= P_{\text{RUPTURE}-1} + P_{\text{RUPTURE}-2} \\ &= (P_{\text{IE}} \times P_{\text{B1}} \times P_{\text{B2}}) + (P_{\text{IE}} \times P_{\text{B3}} \times P_{\text{B4}} \times P_{\text{B5}} \times P_{\text{B6}} \times P_{\text{B7}}) \\ &= (P_{\text{IE}})[(P_{\text{B1}} \times P_{\text{B2}}) + (P_{\text{B3}} \times P_{\text{B4}} \times P_{\text{B5}} \times P_{\text{B6}} \times P_{\text{B7}})] \\ &= (P_{\text{IE}})[(P_{\text{X1}} + P_{\text{X2}})(P_{\text{X3}} + P_{\text{X4}}) + (P_{\text{V1}} \times P_{\text{V2}} \times P_{\text{V3}} \times P_{\text{V4}} \times P_{\text{V5}})] \end{aligned}$$

Note: State B7 is from the version 2 CCD.

Note also that version 1 contains the repeated events X1, X2, X3, and X4 that will have to be reduced via Boolean algebra in order to obtain a correct solution. However, in version 2 the repeated events have been reduced via the modified CCD structure.

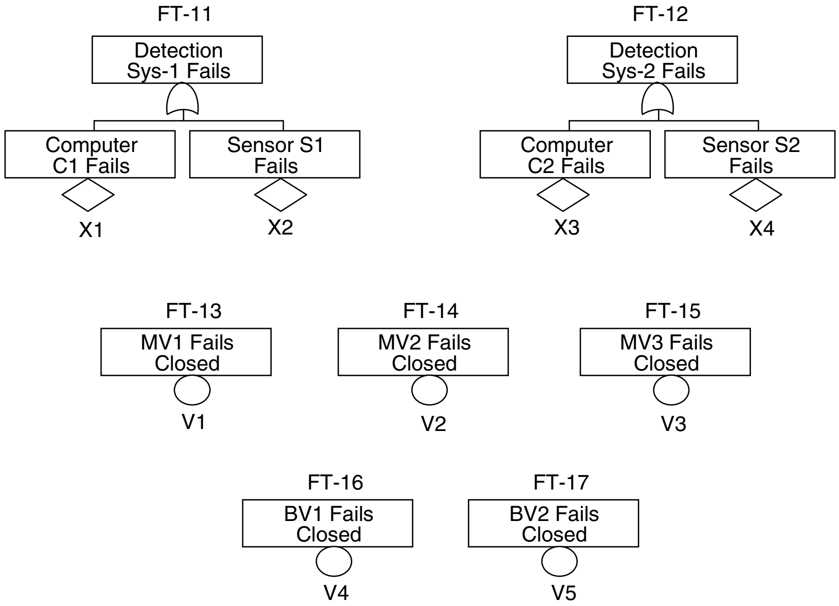


Figure 22.9 *Example 2: CCD revised fault trees (version 2).*

22.11 ADVANTAGES AND DISADVANTAGES

The following are advantages of the CCA technique:

1. Structured, rigorous, and methodical approach.
2. A large portion of the work can be computerized.
3. Visual model displaying cause–effect relationships.
4. Relatively easy to learn, do, and follow.
5. Models complex system relationships in an understandable manner.
6. Combines hardware, software, environment, and human interaction.
7. Permits probability assessment.
8. Multiple outcomes are analyzed.
9. Time sequences of events are treated.

The following are disadvantages of the CCA technique:

1. A CCA can only have one initiating event; therefore, multiple CCA will be required to evaluate the consequence of multiple initiating events.
2. Requires an analyst with some training and practical experience.

22.12 COMMON MISTAKES TO AVOID

When first learning how to perform a CCA, it is commonplace to commit some typical errors. The following are some typical errors made during the conduct of a CCA:

1. Not identifying the proper IE
2. Not identifying all of the contributing intermediate or pivotal events
3. Incorrect system CCA model developed

22.13 SUMMARY

This chapter discussed the CCA technique. The following are basic principles that help summarize the discussion in this chapter:

1. CCA is used to model accident scenarios and to evaluate the various outcome risk profiles resulting from an initiating event.
2. A quantitative CCA is used to perform a PRA of a system. A qualitative CCA is used to help recognize design weaknesses.
3. The CCD provides structure and rigor to the CCA process.
4. A CCA would make a useful supplement to the SD-HAT and the DD-HAT analyses.

BIBLIOGRAPHY

Andrews, J. D. and L. M. Ridley, Reliability of Sequential Systems Using the Cause–Consequence Diagram Method, *Proc. Instit. Mech. Eng.*, **215**(Part E):207–220 (2001).

Andrews, J. D. and L. M. Ridley, Application of the Cause–Consequence Diagram Method to Static Systems, *Reliability Eng. Syst. Safety*, **75**:47–58 (2002).

Danish Atomic Energy Commission, The Cause–Consequence Diagram Method as a Basis for Quantitative Accident Analysis, RISO-M-1374, Danish Atomic Energy Commission, 1971.

Danish Atomic Energy Commission, Interlock Design Using Fault Tree Analysis and Cause–Consequence Analysis, RISO-M-1890, Danish Atomic Energy Commission, 1977.

Kaufman, L. M., J. B. Fussell, D. P. Wagner, J. S. Arendt, J. J. Rooney, W. K. Crowley, and D. J. Campbell, Improving System Safety Through Risk Assessment, Proceedings 1979 Annual Reliability and Maintainability Symposium, 1979, pp. 160–164.

A Cause–Consequence Chart of a Redundant Protection System, IEEE *Trans. Reliability*, **24**(1): 1975.

Chapter 23

Common Cause Failure Analysis

23.1 INTRODUCTION

Common cause failure analysis (CCFA) is an analysis methodology for identifying common causes of multiple failure events. A common cause failure (CCF) is a single-point failure (SPF) that destroys independent redundant designs. The objective of CCFA is to discover common cause vulnerabilities in the system design that can result in the common failure of redundant subsystems and to develop design strategies to mitigate these types of hazards. An example of a CCF would be the compelled failure of two independent, and redundant, flight control computers due to the failure of a common circuit breaker in the system design providing electrical power.

The CCFs create the subtlest type of hazards because they are not always obvious, making them difficult to identify. The potential for this type of event exists in any system architecture that relies on redundancy or uses identical components or software in multiple subsystems. CCF vulnerability results from system failure dependencies inadvertently designed into the system.

If a CCF is overlooked, total system risk is understated because the probability of this hazard is not included in the total risk calculation. If the common cause dependency is in a critical subsystem, CCFs could contribute to a significant impact in overall system risk.

The CCFs can be caused from a variety of sources, such as:

a. Common weakness in design redundancy
b. Use of identical components in multiple subsystems

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

c. Common software design
d. Common manufacturing errors
e. Common requirements errors
f. Common production process errors
g. Common maintenance errors
h. Common installation errors
i. Common environmental factor vulnerabilities

23.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (SD-HAT). Refer to Chapter 3 for a discussion on hazard analysis types.

The purpose of CCFA is to identify CCF vulnerabilities in the system design that eliminate or bypass design redundancy, where such redundancy is necessary for safe and reliable operation. Once CCFs are identified and evaluated for risk, defense strategies mitigating critical CCFs can be established and implemented. CCFA also provides a methodology for determining the quantitative risk presented by CCFs. An alternate name for this analysis technique is common mode failure analysis.

The CCFA technique can be applied to any type of system, but it is particularly useful for safety critical systems using design redundancy. The CCFA technique, when applied to a given system by an experienced analyst, is thorough at identifying and evaluating all of the possible CCFs in a system.

A basic understanding of CCFA and FTA theory is essential to developing a CCFA model. In addition it is crucial for the analyst to have a detailed understanding of the system. As system complexity increases, increased knowledge and experience in CCFA and FTA is required. Proper application depends on the complexity of the system and the skill of the analyst.

Applying CCFA to the analysis of a system design is not a trivial process. It is more difficult than an analysis technique such as a PHA, primarily because it requires an understanding of FTA along with extensive data collection and analysis of CCFA components.

The CCFA method is a very powerful tool for identifying and evaluating potential CCFs in a system design, and it is the only tool to date that provides any rigor to the identification of CCF events. If CCFs are not included in system risk analysis, total system risk is understated because the probability of this type hazard is not included in the total risk calculation. If common cause dependencies exist in a critical subsystem, CCFs could contribute to a significant impact in overall system risk.

Use of CCFA is recommended by the system safety program (SSP) to support the goal of identifying and mitigating all CCF modes. CCFA is recommended as part of a probabilistic risk assessment (PRA), particularly in order to obtain a truer view of system risk. CCFA is especially applicable to the evaluation of redundant designs in safety critical applications. A CCFA is a recommended analysis specified in the SAE document ARP-4754 [1], commonly imposed by the FAA.

23.3 HISTORY

Since the inception of system safety, there has always been a concern with regard to CCFs and how to identify them. Many analysts attempted to identify CCFs with hit-or-miss brute force analyses without utilizing any sort of coherent methodology. It was probably not until 1988 when Mosleh and co-workers [2] published their study and 1998 when they [3] published a study for the U.S. Nuclear Regulatory Commission that CCFA became more of a formalized analysis technique with a coherent and comprehensive framework.

23.4 DEFINITIONS

In order to understand CCFA, it is necessary to define some common terms, which will help to provide a better grasp of the complications involved in CCF theory. The relevant terms include:

Independent event Events are independent when the outcome of one event does not influence the outcome of a second event (probability theory). To find the probability of two independent events both occurring, multiply the probability of the first event by the probability of the second event; for example, $P(\text{A and B}) = P(\text{A}) \bullet P(\text{B})$. For example, find the probability of tossing two number cubes (dice) and getting a 3 on each one. These events are independent; $P(3) \bullet P(3) = \left(\frac{1}{6}\right) \bullet \left(\frac{1}{6}\right) = \frac{1}{36}$. The probability is $\frac{1}{36}$.

Dependent event Events are dependent when the outcome of one event directly affects or influences the outcome of a second event (probability theory). To find the probability of two dependent events both occurring, multiply the probability of A and the probability of B after A occurs; $P(\text{A and B}) = P(\text{A}) \bullet P(\text{B given A})$ or $P(\text{A and B}) = P(\text{A}) \bullet P(\text{B}|\text{A})$. This is known as conditional probability. For example, a box contains a nickel, a penny, and a dime. Find the probability of choosing first a dime and then, without replacing the dime, choosing a penny. These events are dependent. The first probability of choosing a dime is $P(\text{A}) = \frac{1}{3}$. The probability of choosing a penny is $P(\text{B}|\text{A}) = \frac{1}{2}$ since there are now only 2 coins left. The probability of both is $\frac{1}{3} \bullet \frac{1}{2} = \frac{1}{6}$. Keywords such as "not put back" and "not replace" suggest that events are dependent.

Independence (in design) Design concept that ensures the failure of one item does not cause the failure of another item [4]. This concept is very important in many safety and reliability analysis techniques due to the impact on logic and mathematics. Many models, such as FTA, assume event independence.

Dependence (in design) Design whereby the failure of one item directly causes, or leads to, the failure of another item. This refers to when the functional status of one component is affected by the functional status of another component. CCF dependencies normally stem from the way the system is designed to perform its intended function. Dependent failures are those failures that defeat redundancy or diversity, which are intentionally employed to improve reliability and/or safety.

In some system designs, dependency relationships can be very subtle, such as in the following cases [5]:

a. Standby redundancy When an operating component fails, a standby component is put into operation, and the system continues to function. Failure of an operating component causes a standby component to be more susceptible to failure because it is now under load.
b. Common loads When failure of one component increases the load carried by other components. Since the other components are now more likely to fail, we cannot assume statistical independence.
c. Mutually exclusive events When the occurrence of one event precludes the occurrence of another event.

Two failure events A and B are said to be dependent if $P(\text{A and B}) \neq P(\text{A})P(\text{B})$. In the presence of dependencies, often, but not always, $P(\text{A and B}) > P(\text{A})P(\text{B})$. This increased probability of two (or more) events is why CCFs are of concern.

Common cause failure (CCF) The failure (or unavailable state) of more than one component due to a shared cause during the system operation. Viewed in this fashion, CCFs are inseparable from the class of dependent failures [4]. An event or failure, which bypasses or invalidates redundancy or independence (ARP-4761).

A CCF is the simultaneous failure of multiple components due to a common or shared cause. For example, when two electrical motors become inoperable simultaneously due to a common circuit breaker failure that provides power to both motors. CCFs include common mode failures (CMFs), but CCF is much larger in scope and coverage. Components that fail due to a shared cause normally fail in the same functional mode. CCFs deal with causes other than just design dependencies, such as environmental factors, human error, and the like. Ignoring the effects of dependency and CCFs can result in overestimation of the level of reliability and/or safety.

For system safety, a CCF event consists of item/component failures that meet the following criteria:

1. Two or more individual components fail or are degraded such that they cannot be used when needed, or used safely if still operational.
2. The component failures result from a single shared cause and coupling mechanism.

Common mode failure (CMF) Failure of multiple components in the same mode [4]. An event, which simultaneously affects a number of elements otherwise, considered to be independent [1]. For example, a set of identical resistors from the same manufacturer may all fail in the same mode (and exposure time) due to a common manufacturing flaw.

The term CMF, which was used in the early literature and is still used by some practitioners, is more indicative of the most common symptom of the CCF, but it is not a precise term for describing all of the different dependency situations that can result in a CCF event. A CMF is a special case of a CCF, or a subset of a CCF.

Cascading failure Failure event for which the probability of occurrence is substantially increased by the existence of a previous failure [1]. Cascading failures are dependent events, where the failure of one component causes the failure of the next component in line, similar to the falling domino effect.

Mutually exclusive events Two events are mutually exclusive if the occurrence of one event precludes the occurrence of the other. For example, if the event “switch A fails closed” occurs, then the event “switch A fails open” cannot possibly occur.

CCF root cause Most basic reason(s) for the component failure, which if corrected, would prevent recurrence. Example CCF root causes include events such as heat, vibration, moisture, and the like. The identification of a root cause enables the analyst to implement design defenses against CCFs.

CCF coupling factor Qualitative characteristic of a group of components or piece parts that identifies them as susceptible to the same causal mechanisms of failure. Such factors include similarity in design, location, environment, mission, and operational, maintenance, and test procedures. The coupling factor(s) is part of the root cause for a CCF. The identification of coupling factors enables the analyst to implement defenses against common root cause failure vulnerabilities.

Common cause component group (CCCG) Group of components that share a common coupling factor.

23.5 THEORY

Many systems utilize subsystem design redundancy to ensure that a specific function occurs upon demand. The idea is that two separate and independent subsystems are much less likely to fail from independent failures than a single independent subsystem. System designs have become so complex, however, that occasionally a dependency is inadvertently built into the redundancy design. One form of dependency is the CCF event that can cause failure of both redundant subsystems. A CCF is effectively an SPF that nullifies independent redundant subsystem designs.

For example, a DC-10 crash occurred when an engine exploded and a fan blade from the engine cut two independent and separated hydraulic lines. Aircraft control depended upon system hydraulics, and the design, therefore, intentionally had two independent and redundant hydraulic systems. Though the redundant hydraulic lines were physically separated by a large distance, the engine exploding was the common cause SPF resulting in the loss of both critical hydraulic subsystems.

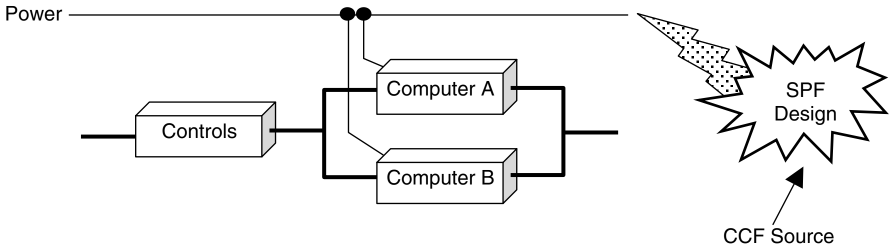


Figure 23.1 *Example redundant system.*

Figure 23.1 demonstrates the CCF concept where the root cause is an SPF, and the coupling factor is the design vulnerability to an SPF. In this simplified example, two computers are used in parallel to ensure that safety critical output is provided when necessary. Only one computer is necessary for system success, but should one computer fail (independently), the second computer takes over operation.

Note that in this example system a common electrical power source is utilized for both computers. The electrical power is a CCF source. Both computers are dependent on the same electrical power source. If power fails, then both computers will instantly fail with a probability of $P = 1.0$. The conditional probability of the dependent event, *computer fails given failure of power*, is $P = 1.0$.

Figure 23.2 demonstrates a slightly different CCF concept. In this example, the two computers are supplied by different and independent power sources to eliminate the power dependency. However, there is the possibility of both computers being exposed to a strong RF energy field, which can cause computer upset or failure. Since both computers are identical and manufactured under the same specifications, they are both susceptible to failing in the same mode from the common energy source. In this example, the root cause is the presence of RF energy, and the coupling factor is the design vulnerability of the safety critical components to RF energy.

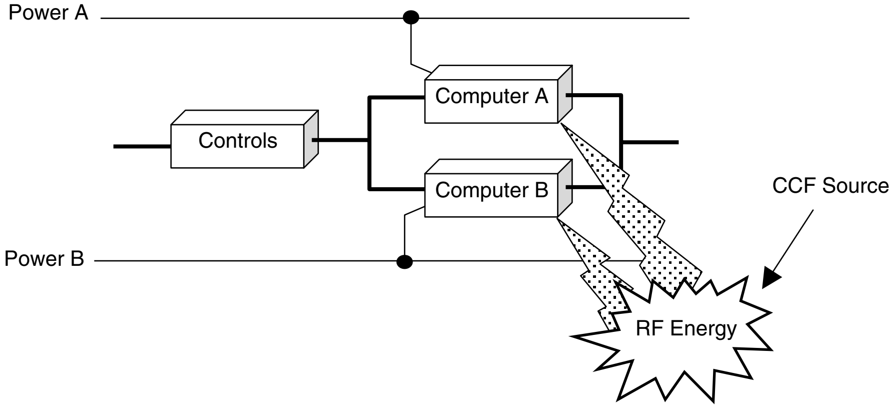


Figure 23.2 *Improved redundant system.*

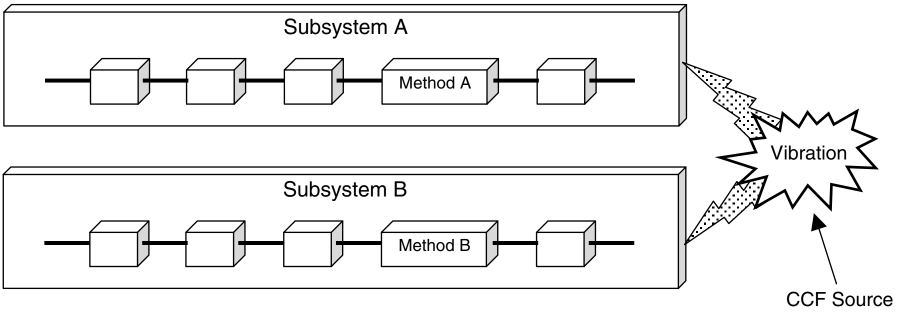


Figure 23.3 *Diverse redundant system.*

Figure 23.3 demonstrates another CCF concept. In this example, two redundant subsystems perform the same system function. One component in each subsystem uses a different (diverse) operational method (e.g., a mechanical fuze and an electrical fuze) to ensure that they do not fail simultaneously in the same mode due to a CCF. However, even with diversity in design, both items are vulnerable to an external CCF source, such as vibration, which can cause both items to fail. In this example, the root cause is the presence of external vibration, and the coupling factor is the design vulnerability of the safety critical components to external vibration.

Figure 23.4 demonstrates the cascading CCF concept. In this example, several items are connected in series, having an interdependency between items. If item A should partially fail, it places a heavier load on item B, possibly exceeding item B's design load limits. As a result, item B either fails or passes a heavier load onto item C, and so on. For example, a steel beam plate may have seven rivets holding two beams together. If two rivets fail, the load weakens the plate–beam connection. Or, several electrical components may be connected in series. If one component partially fails, it may pass a higher than designed for current to the next component, resulting in a cascading effect on the circuit. In this example, the root cause is the failure of component A, and the coupling factor is the design

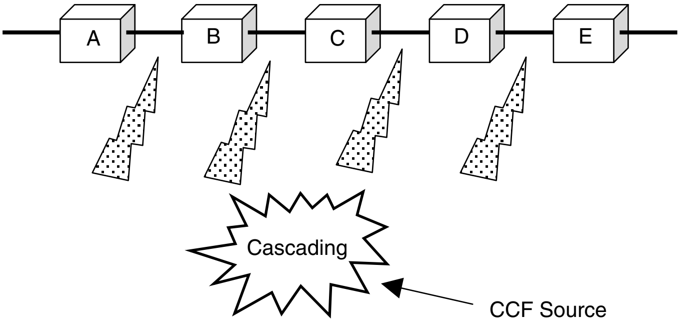


Figure 23.4 *Cascading CCF.*

vulnerability of the safety critical components to a stress level higher than the design limit.

As demonstrated in the above figures, the definition of CCF is closely related to the general definition of a dependent failure. Two events, A and B, are said to be dependent if

$$P(\text{A and B}) \neq P(\text{A})P(\text{B})$$

In the presence of dependencies, often, but not always, $P(\text{AB}) > P(\text{A})P(\text{B})$. Therefore, if A and B represent failure of a safety function, the actual probability of failure of both may be higher than the expected probability calculated based on the assumption of independence. In cases where a system provides multiple layers of defense against total system or functional failure, presence of dependence may translate into a reduced level of safety and reliability, if the dependence is ignored.

Dependencies can be classified in many different ways. Dependencies are categorized based on whether they stem from intended intrinsic functional physical characteristics of the system or are due to external factors and unintended characteristics. Therefore, CCF dependence is either intrinsic or extrinsic to the system.

Intrinsic dependency refers to dependencies where the functional status of one component is affected by the functional status of another. These dependencies normally stem from the way the system is designed to perform its intended function. This type of dependency is based on the type of influence that components have on each other.

Extrinsic dependency refers to dependencies where the couplings are not inherent and not intended in the designed functional characteristics of the system. Such dependencies are often physically external to the system, such as vibration, heat, RF, environment, mission changes beyond original design limits, and so forth.

23.6 METHODOLOGY

The CCFs result from the presence of two key factors in a system design:

1. A root cause of component failure [i.e., the particular reason(s) for failure of each component that failed in the CCF event]
2. A coupling factor (or factors) that creates the conditions for multiple components to be involved in the CCF event and be affected by the same root cause

For example, using two switches in a system that are both susceptible to failure from vibration creates a common cause failure situation. Failure from vibration is the root cause. The vibration, and both components designed for exposure to the same vibration, are the coupling factors. However, if a switch can be used that is not susceptible to vibration or the vibration is eliminated, the CCF situation is avoided.

As another example, consider the failure of two identical redundant electronic devices due to exposure to excessively high temperatures. This CCF event is the result of susceptibility of each of the devices to heat (considered to be the root cause in this case) and a result of both units being identical and also being exposed to the same harsh environment (coupling factors).

Since the use of identical components in redundancy formation is a common strategy to improve system safety and reliability, coupling factors stemming from similarities of the redundant components are often present in system designs, leading to vulnerability to CCF events. CCF events of identical redundant components, therefore, merit special attention in risk and reliability analysis of such systems.

Characterization of CCF events in terms of susceptibilities and coupling factors provides an effective means of assessing the CCF phenomenon and evaluating the need for and effectiveness of defenses against them.

There are several different CCFA models that can be applied to the evaluation of CCFs, however, the fault tree analysis (FTA) model seems to be the best and most used methodology. The FTA model methodology is presented herein. Table 23.1 lists and describes the basic steps of the CCFA process using the FTA approach.

Step 1 is input to the process and steps 5, 6, 7, and 8 are outputs of the CCFA process. Steps 2, 3, and 4 comprise the analysis portion of the CCFA process. These steps are described next.

CCFA Process Step 2—Initial System Fault Tree Model The development of a system-level FTA is a key step in the CCFA process. The initial system fault tree (FT) logic model is developed as a basic system model that identifies the primary contributing components fault events leading to the undesired top-level event.

TABLE 23.1 CCFA Process Methodology

Step	Task	Description
1	Define the system.	Examine the system and define the system boundaries, subsystems, and interfaces. Identify analysis boundaries.
2	Develop initial system logic model.	Development of an initial component-level system logic model (e.g., fault tree) that identifies major contributing components.
3	Screening analysis.	Screen system design and data for identification of CCF vulnerabilities and CCF events.
4	Detailed CCF analysis.	Place CCF components in FT and perform a qualitative and quantitative analysis to assess CCF risk.
5	Evaluate the outcome risk.	Evaluate the outcome risk of each CCF event and determine if the risk is acceptable.
6	Recommend corrective action.	If the outcome risk not acceptable, develop design strategies to countermeasure CCF effect and change system risk.
7	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
8	Document CCFA.	Document the entire CCFA process, including the system-level FTs. Update for new information as necessary.

The initial FT is developed around basic independent failure events, which provides a first approximation of cut sets and probability.

Many component failure dependencies among the components are not accounted for explicitly in the first approximation FT model, resulting in an underestimation of the risk of the FTs top-level event. As CCF events are identified in step 3, the analyst expands the FT model in step 4 to include identified CCFs.

The FT model is much more complete and accurate with CCF events included. The FT is recomputed to reevaluate the criticality, sensitivity, and probability of the CCF within the FT. The revised FT probability risk estimate that includes CCFs provides a correct risk estimate over the first-approximation FT. Refer to Chapter 11 for a full discussion on FTA and guidance on developing a FT model and performing quantitative calculations.

CCFA Process Step 3—Common Cause Screening The purpose of screening is to identify CCF vulnerabilities in the system design and to identify the specific CCF events and components that are required in the FT model. An analysis is performed to identify a list of potential susceptibilities of the system and the CCF components involved. During the screening analysis, it is important not to discount any potential CCF susceptibilities. An effective CCF screening analysis should involve the following activities:

- Review of system design and operating practices
- Review of operating historical experience (if available)
- Review of other similar systems
- Evaluation of root cause–defense and coupling factor–defense methods

A group of components or piece parts with a common susceptibility to CCF is called a common cause component group (CCCG) and the following guidelines help identify CCCGs:

1. When identical, functionally nondiverse, and active components are used to provide redundancy, these components should always be assigned to a CCCG, one for each group of identical redundant components (e.g., resistor groups, pump groups, thermostat groups, etc.).
2. The initial assumption of independent failure modes among diverse components is a good one if it is supported by operating experience. However, when diverse redundant components have piece parts that are identically redundant, the components should not be assumed fully independent. One approach in this case is to break down the component boundaries and identify the common piece parts as a CCCG (e.g., pumps can be identical except for their power supply).
3. In system reliability analysis, it is frequently assumed that certain passive components can be omitted, based on the argument that active components dominate. In applying these screening criteria to common cause analysis, it is important to include events such as debris blockage of redundant or even diverse pump strainers.

The most efficient approach to identifying CCF system susceptibilities is to focus on identifying coupling factors, regardless of defenses that might be in place. The resulting list will be a conservative assessment of the system susceptibilities to CCFs. A coupling mechanism is what distinguishes CCFs from multiple independent failures. Coupling mechanisms are suspected to exist when two or more component failures exhibit similar characteristics, both in the cause and in the actual failure mechanism. The analyst, therefore, should focus on identifying those components of the system that share common characteristics.

When identifying CCF coupling factors, remember that a:

1. CCF root cause is the most basic reason or reasons for the component failure, which if corrected, would prevent recurrence.
2. CCF coupling factor is a characteristic of a group of components or piece parts that identifies them as susceptible to the same causal mechanisms of failure. Such factors include similarity in design, location, environment, mission, and operational, maintenance, and test procedures.

A list of common factors is provided in Table 23.2. This list is a tool to help identify the presence of identical components in the system and most commonly observed coupling factors. Any group of components that share similarities in one or more of these characteristics is a potential point of vulnerability to CCF.

Coupling factors can be divided into four major classes:

- Hardware based
- Operation based
- Environment based
- Software based

Hardware-based coupling factors propagate a failure mechanism among several components due to identical physical characteristics. An example of hardware-based coupling factors is failure of several residual heat removal (RHR) pumps because of the failure of identical pump air deflectors. There are two subcategories of hardware-based coupling factors: (1) hardware design and (2) hardware quality (manufacturing and installation).

Hardware design coupling factors result from common characteristics among components determined at the design level. There are two groups of design-related hardware couplings: system level and component level. System-level coupling factors include features of the system or groups of components external to the components that can cause propagation of failures to multiple components. Features within the boundaries of each component cause component-level coupling factors. Table 23.3 lists some example coupling factors in the hardware design category.

The operational-based coupling factors propagate a failure mechanism due to identical operational characteristics among several components. Table 23.4 lists some example coupling factors in the operational category.

TABLE 23.2 Key Common Cause Attributes

Characteristic	Description
Same design	The use of the same design in multiple subsystems can be the source of a CCF coupling factor vulnerabilities. This is particularly true of software design.
Same hardware	The use of identical components in multiple subsystems resulting in a vulnerability of multiple subsystems.
Same function	When the same function is used in multiple places, it may require identical or similar hardware that provides CCF vulnerabilities.
Same staff	Items are vulnerable to the same installation, maintenance, test, or operations staff that can make common errors.
Same procedures	Items are vulnerable to the same installation, maintenance, test, or operations procedures, which may have common errors.
Redundancy	When redundant items are identical, they are vulnerable to the same failure modes, failure rates, and CCF coupling factors.
Same location	Items are located in the same physical location, making them vulnerable to the same undesired conditions (fire, water, shock, etc.).
Same environment	Items are vulnerable to the same undesired environmental conditions (fire, water, shock, electromagnetic radiation, dust, salt, etc.).
Same manufacturer	Components have the same manufacturer, making all components vulnerable to the same failure modes and failure rates.
Common requirements	Common requirements for items or functions may contain common errors that generate CCF vulnerabilities.
Common energy sources	Items with common energy sources (e.g., electrical, chemical, hydraulic, etc.) generate CCF vulnerabilities.
Common data sources	Items with common data sources generate CCF vulnerabilities, particularly in software design.
Common boundaries	Items that share a common boundary (physical, functional, logical, etc.) may have CCF vulnerabilities.

The environmental-based coupling factors propagate a failure mechanism via identical external or internal environmental characteristics. Table 23.5 lists some example coupling factors in the environmental category.

Software-based coupling factors propagate a failure mechanism among several components due to a common software module. For example, three separate aircraft flight control displays may be controlled by a common software module, with common data inputs. Table 23.6 lists some example coupling factors in the software category.

Additional methods and/or tools that can be used to identify CCFs include:

1. Network tree diagrams used in sneak circuit analysis (see Chapter 16).
2. Zonal analysis analyzes the major zones of a system [1, 6].
3. Connector bent pin analysis and water shorts (see Chapter 20).

It should be noted, however, that these techniques are oriented for particular types of CCF types and, therefore, are not all inclusive of all CCF types.

TABLE 23.3 Hardware-Based Component Coupling Factors

Characteristic	Description
Same physical appearance	This refers to cases where several components have the same identifiers (e.g., same color, distinguishing number, letter coding, and/or same size/shape). These conditions could lead to misidentification by the operating or maintenance staff.
System layout/ configuration	This refers to the arrangement of components to form a system. Component arrangement may result in independent systems being dependent upon a common source.
Same component internal parts	This refers to cases where several components could fail because they each use similar or identical internal subcomponents. A manufacturing flaw in a subcomponent could affect the entire lot.
Same maintenance, test, and/or calibration characteristics	This refers to cases where several components are maintained, tested, and/or calibrated by the same set of procedures. A flaw in the procedures could affect an entire lot of components.
Manufacturing attributes	This refers to the same manufacturing staff, quality control procedure, manufacturing method, and material being used for an entire lot of components. The same flaw applies to all components equally, thus they could all be expected to fail equally.
Construction and installation attributes	This refers to the same construction/installation staff, procedures, and testing being applied to an entire lot of components. The same flaw applies to all components equally; thus, they could all be expected to fail equally.

TABLE 23.4 Operational-Based Component Coupling Factors

Characteristic	Description
Same operating staff	This refers to cases where the same operator or operators are assigned to operate all trains of a system, increasing the probability that operator errors will affect multiple components simultaneously.
Same operating procedure	This refers to cases where the same operating procedures governs operation of all physically or functionally identical components. Any deficiency in the procedures could affect all of the components.
Same maintenance, test, and/or calibration schedule	This refers to cases where the same maintenance/test/ calibration schedule is applied at the same time for identical components. Any deficiency could affect all of the components.
Same maintenance, test, and/or calibration staff	This refers to cases where the same maintenance/test/ calibration staff being responsible for identical components. Any deficiency could affect all of the components.
Same maintenance, test, and/or calibration procedures	This refers to cases where the same maintenance/test/ calibration procedure is applied on identical components. Any deficiency could affect all of the components.

TABLE 23.5 Environmental-Based Component Coupling Factors

Characteristic	Description
Same system location	This refers to all redundant systems/components being exposed to the same environmental stresses because of the same system (e.g., flood, fire, high humidity, earthquake, etc.).
Same component location	This refers to all redundant systems/components being exposed to the same environmental stresses because of the component location within the system (e.g., vibration, heat, human error, etc.).
Internal environment/ working medium	This refers to the common exposure of components in terms of the medium of their operation, such as internal fluids, oils, gases, etc.

CCFA Process Step 4—Detailed CCF Analysis This step is a qualitative and/or quantitative evaluation of the revised FT model that has had all credible CCF causal factor events incorporated into the model. This step utilizes the results of steps 2 and 3. The intent of this step is to perform a system risk evaluation of the identified CCFs after they have been placed in the FT model. This involves identifying the appropriate CCF events, placing them in the FT, and obtaining the failure frequency or probability for these events.

A common cause basic event (CCBE) involves failure of a specific set of CCF components due to a common cause. For instance, in a system of three redundant components A, B, and C, the CCBEs are C_{AB}, C_{AC}, C_{BC}, and C_{ABC}, and are defined as follows:

$$
\begin{aligned}
&\mathrm{A} = \text{single independent failure of component A (a basic event)}\\
&\mathrm{B} = \text{single independent failure of component B (a basic event)}\\
&C = \text{single independent failure of component C (a basic event)}\\
&C_{\mathrm{AB}} = \text{failure of components A and B (and not C) from common causes (a CCBE)}\\
&C_{\mathrm{AC}} = \text{failure of components A and C (and not B) from common causes (a CCBE)}\\
&C_{\mathrm{BC}} = \text{failure of components B and C (and not A) from common causes (a CCBE)}\\
&C_{\mathrm{ABC}} = \text{failure of components A, B, and C from common causes (a CCBE)}
\end{aligned}
$$

TABLE 23.6 Software-Based Coupling Factors

Characteristic	Description
Common algorithms	This refers to multiple hardware items that are driven by a single or common software module containing the control algorithm.
Common data	This refers to multiple hardware items that are provided data by a single or common software module.
Common requirements	This refers to multiple software modules that are developed using common software design requirements.

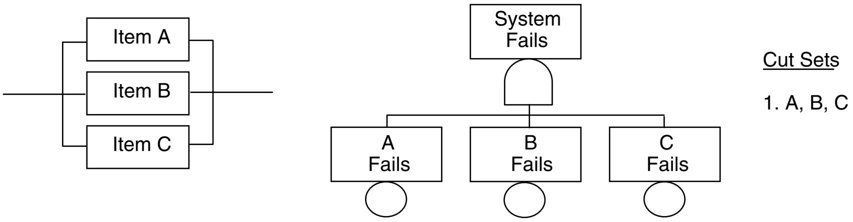


Figure 23.5 *Redundant system and initial FT model.*

Figure 23.5 shows a system design where three components operate in parallel redundancy, and only successful operation of one component is necessary for system success. This figure also shows the initial system FT model of the independent failure events.

The CCBEs for this three-component system are C_{AB}, C_{AC}, C_{BC}, and C_{ABC}. However, since failure of all three components is necessary for system failure, C_{AB}, C_{AC}, C_{BC} have no system impact, but C_{ABC} does have an impact since this is the CCBE that causes failure of all three components. Figure 23.6 shows the revised FT model that incorporates the CCBE "C_{ABC}."

Note that in Figure 23.5 the FT produces only one cut set, which is a 3-order cut set, indicating that the probability of system failure should be small. In Figure 23.6, the FT produces two cut sets, the original 3-order cut set and an SPF cut set. Depending upon the probability of the SPF CCF event, the probability could be much higher than the initial FT probability.

Figure 23.7 shows a system design where three components operate in parallel redundancy, and two of three components must operate for system success. This figure also shows the initial system FT model of the independent failure events.

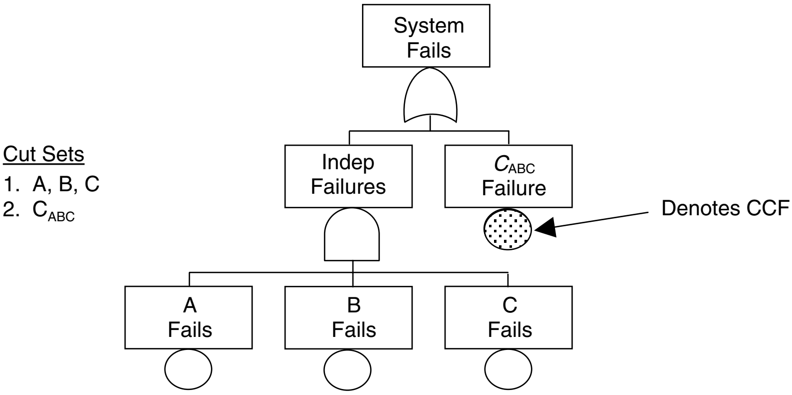


Figure 23.6 *CCBEs added to FT model.*

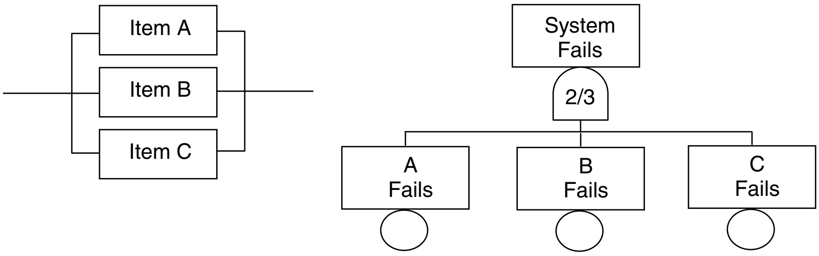


Figure 23.7 *Redundant 2 of 3 system and initial FT model.*

The FT model in Figure 23.7 uses a *k*-of-*n* gate to show the required failure combinations. Figure 23.8 shows a modified FT where all of the combination events are modeled explicitly.

Figure 23.9 shows the revised FT model that incorporates the CCBEs for the particular system design parameters. Table 23.7 provides the results for the FT model of

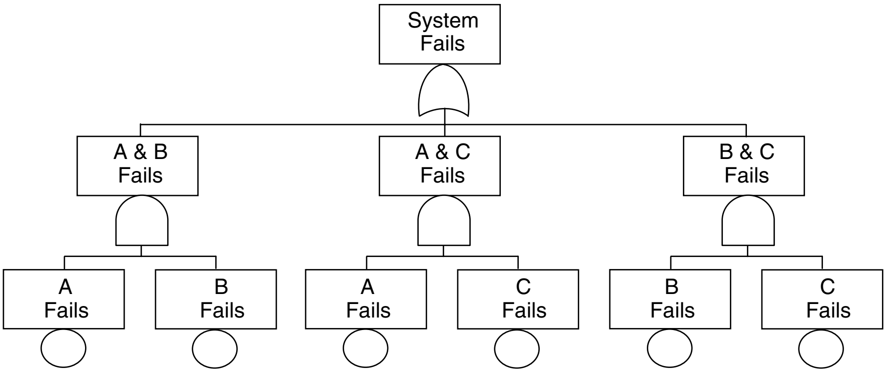


Figure 23.8 *Modified FT model.*

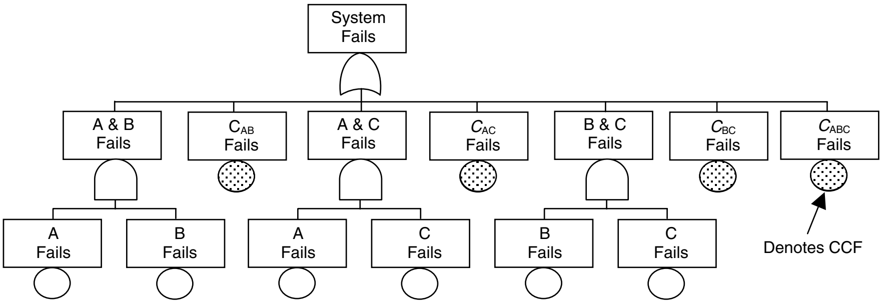


Figure 23.9 *CCBEs added to FT model.*

TABLE 23.7 FT Results for 2 of 3 Redundant System Designs

Cut Sets and First-Order Probability Approximation Equation	
Initial FT Model	FT Model with CCBEs Added
{A, B}; {A, C}; {B, C)	{A, B}; {A, C}; {B, C) $\{C_{AB}\}$; $\{C_{AC}\}$; $\{C_{BC}\}$ $\{C_{ABC}\}$
$P = P(A)P(B) + P(A)P(C) + P(B)P(C)$	$P = P(A)P(B) + P(A)P(C) + P(B)P(C)$ $+P(C_{AC}) + P(C_{AC}) + P(C_{BC}) + P(C_{ABC})$

the 2 of 3 redundant system design. Note from these results that when the CCBEs are added to the FT that the number of cut sets increases, which in turn increase the probability of occurrence.

Note that the CCBEs are only identified and used according to the impact they have on the specific sets of components within the CCCGs and system function. In the first example (Fig. 23.4) the CCF events C_{AB}, C_{AC}, and C_{BC} were not used because they would not cause system failure. However, they were used in the second example (Fig. 23.6) because they could cause system failure. The analysts must watch out for subtleties such as this when conducting CCFA.

It can be seen that the CCF expansion of a FT results in a proliferation of the number of cut sets (CSs), which may create practical difficulties when dealing with complex systems. However, in most cases standard fault tree computer codes for cut set determination and probabilistic quantification can be applied without concern about dependencies or size due to CCFs. If, after careful screening, the number of CSs is still unmanageable, a practical solution is to prune the FT of low-probability events.

23.7 DEFENSE MECHANISMS

To understand a defense strategy against a CCF event, it is necessary to understand that defending against a CCF event is no different than defending against an independent failure that has a single root cause of failure (i.e., SPF). In the case of a CCF event, more than one failure occurs, and the failures are related through a coupling mechanism.

There are three methods of defense against a CCF:

1. Defend against the CCF root cause
2. Defend against the CCF coupling factor
3. Defend against both items 1 and 2

A defense strategy against root causes is usually somewhat difficult because components generally have an inherent set of failure modes that cannot be eliminated. However, the failure modes can be protected via redundancy, diversity, and barriers.

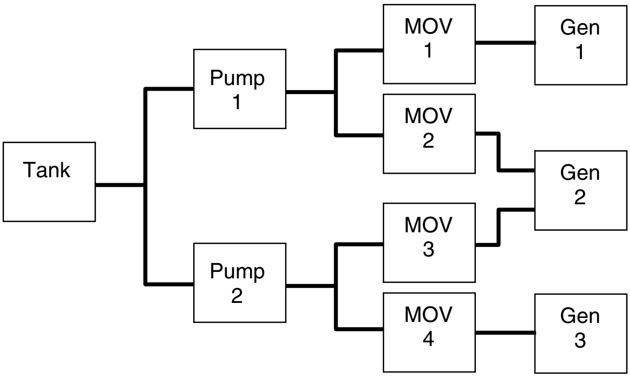


Figure 23.10 *Example system diagram.*

A defense strategy for coupling factors typically includes diversity (functional, staff, and equipment), barriers, personnel training, and staggered testing and maintenance.

23.8 EXAMPLE

Figure 23.10 contains an example water pumping system for this CCFA example. In this system water is supplied from a common source to three steam generators. For successful system operation, two of the three generators must be operational. Some redundancy has been designed into the system to help achieve this operational requirement. The pumps are electrical-driven pumps that pump the water from the tank to the motor-operated valves (MOVs). The MOVs are opened and closed by electric power. The pumps, MOVs, and generators are all monitored and controlled by a single common computer, and they are powered from a common electrical source.

Figure 23.11 is the top-level FT for the undesired event *loss of 2 out of 3 generators*. This top-level FT applies to both the preliminary (without CCFs) and final (with CCFs) subtrees.

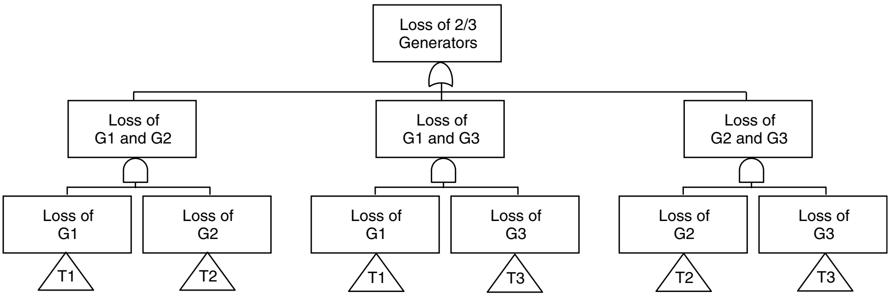


Figure 23.11 *Example system—top-level FT.*

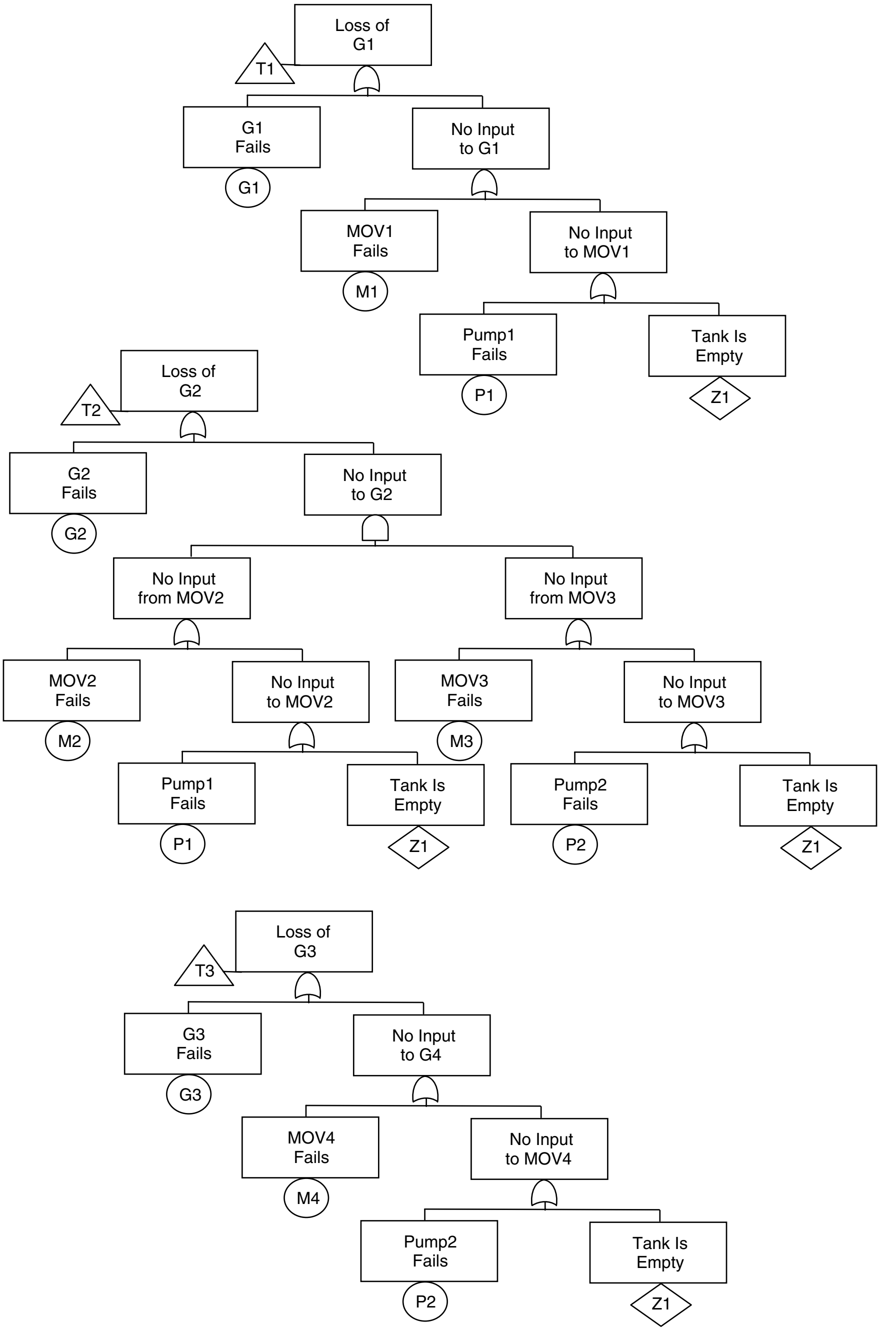


Figure 23.12 *Example system—sub-FTs without CCFs (version 1).*

Figure 23.12 contains three preliminary version subtrees for system analysis without consideration given to CCFs, and Figure 23.13 contains the three final version subtrees for system analysis with consideration given to CCFs.

This example problem has been simplified in order to demonstrate the CCF concept. The FTs in Figure 23.13 contain CCF events for the pumps, MOVs, and generators. These CCFs are denoted by the double diamond symbol in the FTs.

Through screening of the system design and the preliminary FT, it has been determined that the factors shown in Table 23.8 contribute to CCF events. In a real-world situation, each of these factors (power, computer, software, etc.) would create an

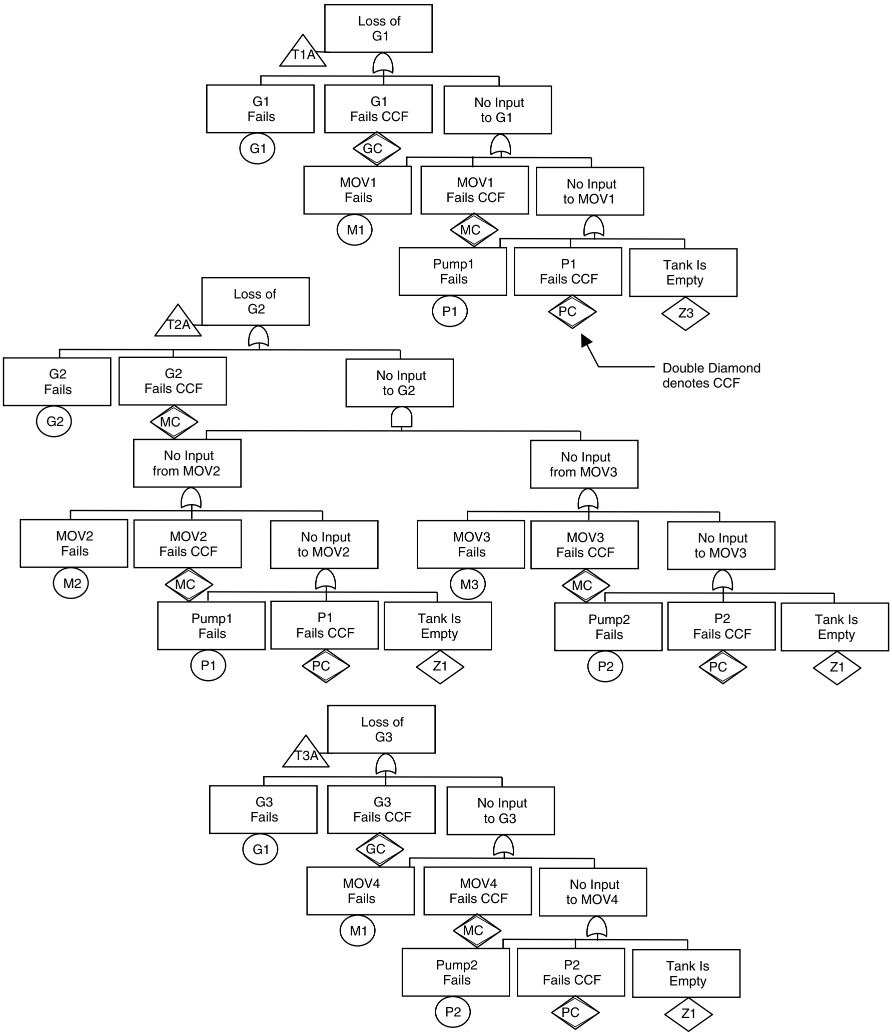


Figure 23.13 *Example system—revised sub-FTs with CCFs (version 2).*

TABLE 23.8 Component Coupling Factors

Coupling Factor	Effect	Impact On
Electrical power	Common power to pumps; common power to MOVs; common power to generators. Pumps, MOVs, and generator power is separate	Pumps, MOVs, generators
Computer control	Common computer sensing and control to pumps, MOVs, and generators	Pumps, MOVs, generators
Software	Common computer software for pumps, MOVs, and generators	Pumps, MOVs, generators
Manufacturing	Common manufacturing of pumps; common manufacturing of MOVs; manufacturing of generators	Pumps, MOVs, generators
Maintenance	Common maintenance procedures for pumps; common maintenance procedures for MOVs; common maintenance procedures for generators	Pumps, MOVs, generators
Installation	Common installation procedures for pumps; common installation procedures for MOVs; common installation procedures for generators	Pumps, MOVs, generators

individual CCF event. However, for purposes of simplification, each of these factors has been combined into a single CCF event for the pumps, MOVs, and generators.

Table 23.9 contains the basic failure rate data for the basic fault events in the three preliminary FT branches shown in Figure 23.12. The component basic failure rate and exposure (operating) times are provided, along with the computed probability of failure for the events. A 1-hour operating time was used to keep the calculations simple.

Table 23.10 contains the qualitative and quantitative results of the preliminary version 1 FT. This FT yielded 22 cut sets (CSs), with the lowest CS probability being 1.00×10^{-10} for failure of generator 1 and generator 2 (also G1 and G3, G2 and G3).

Table 23.11 contains the basic failure rate data for the basic fault events in the three preliminary FT branches shown in Figure 23.13. The values are identical to

TABLE 23.9 Basic Event Data for Version 1 FT

Event	Failure Rate	Exposure Time (hr)	Probability
P1	1.00×10^{-6}	1	1.00×10^{-6}
P2	1.00×10^{-6}	1	1.00×10^{-6}
M1	4.00×10^{-6}	1	4.00×10^{-6}
M2	4.00×10^{-6}	1	4.00×10^{-6}
M3	4.00×10^{-6}	1	4.00×10^{-6}
M4	4.00×10^{-6}	1	4.00×10^{-6}
G1	1.00×10^{-5}	1	1.00×10^{-5}
G2	1.00×10^{-5}	1	1.00×10^{-5}
G3	1.00×10^{-5}	1	1.00×10^{-5}
Z1	2.50×10^{-10}	1	2.50×10^{-10}

TABLE 23.10 Results of Version 1 FT

CS No	CS			Probability
1	G1	G2		1.00×10^{-10}
2	G1	G3		1.00×10^{-10}
3	G2	G3		1.00×10^{-10}
4	Z1			2.50×10^{-10}
5	G1	P2		1.00×10^{-11}
6	G2	P1		1.00×10^{-11}
7	G2	P2		1.00×10^{-11}
8	G3	P1		1.00×10^{-11}
9	M1	M4		1.60×10^{-11}
10	G1	M4		4.00×10^{-11}
11	G2	M1		4.00×10^{-11}
12	G2	M4		4.00×10^{-11}
13	G3	M1		4.00×10^{-11}
14	P1	P2		1.00×10^{-12}
15	M1	P2		4.00×10^{-12}
16	M2	P2		4.00×10^{-12}
17	M3	P1		4.00×10^{-12}
18	M4	P1		4.00×10^{-12}
19	G1	M2	M3	1.60×10^{-16}
20	G3	M2	M3	1.60×10^{-16}
21	M1	M2	M3	6.40×10^{-17}
22	M2	M3	M4	6.40×10^{-17}

Table 23.9, except additional events and rates have been added for the three identified CCFBEs.

Table 23.12 contains the qualitative and quantitative results of the final version 2 FT containing the CCF events. This FT yielded 25 CSs, with the lowest CS probability for the CCF events. Note that all the CSs in this table are the same as in Table 23.10, except the CCF CSs are now included. Note that even though the

TABLE 23.11 Basic Event Data for Version 2 FT

Event	Failure Rate	Exposure Time (hr)	Probability
P1	1.00×10^{-6}	1	1.00×10^{-6}
P2	1.00×10^{-6}	1	1.00×10^{-6}
M1	4.00×10^{-6}	1	4.00×10^{-6}
M2	4.00×10^{-6}	1	4.00×10^{-6}
M3	4.00×10^{-6}	1	4.00×10^{-6}
M4	4.00×10^{-6}	1	4.00×10^{-6}
G1	1.00×10^{-5}	1	1.00×10^{-5}
G2	1.00×10^{-5}	1	1.00×10^{-5}
G3	1.00×10^{-5}	1	1.00×10^{-5}
Z1	2.50×10^{-10}	1	2.50×10^{-10}
PC	3.00×10^{-9}	1	3.00×10^{-9}
MC	2.00×10^{-9}	1	2.00×10^{-9}
GC	1.00×10^{-9}	1	1.00×10^{-9}

TABLE 23.12 Results of Version 2 FT

CS No.	CS			Probability
1	GC			1.00×10^{-9}
2	MC			2.00×10^{-9}
3	PC			3.00×10^{-9}
4	G1	G2		1.00×10^{-10}
5	G1	G3		1.00×10^{-10}
6	G2	G3		1.00×10^{-10}
7	Z1			2.50×10^{-10}
8	G1	P2		1.00×10^{-11}
9	G2	P1		1.00×10^{-11}
10	G2	P2		1.00×10^{-11}
11	G3	P1		1.00×10^{-11}
12	M1	M4		1.60×10^{-11}
13	G1	M4		4.00×10^{-11}
14	G2	M1		4.00×10^{-11}
15	G2	M4		4.00×10^{-11}
16	G3	M1		4.00×10^{-11}
17	P1	P2		1.00×10^{-12}
18	M1	P2		4.00×10^{-12}
19	M2	P2		4.00×10^{-12}
20	M3	P1		4.00×10^{-12}
21	M4	P1		4.00×10^{-12}
22	G1	M2	M3	1.60×10^{-16}
23	G3	M2	M3	1.60×10^{-16}
24	M1	M2	M3	6.40×10^{-17}
25	M2	M3	M4	6.40×10^{-17}

CCF events failure rates were much smaller than the basic event failure rates, the CCF events are more likely to occur because they are SPFs (i.e., all of the other CS are 2 and 3 order, except for tank failure).

The system failure probability calculations can be summarized as follows:

- $P(\text{failure without CCFs}) = 7.83 \times 10^{-10}$
- $P(\text{failure with CCFs}) = 6.78 \times 10^{-9}$

These probability numbers indicate how CCFs can have a significant impact on the total system failure frequency. When CCFs are ignored in an analysis, the total failure frequency can be understated, making a risk assessment incorrect.

23.9 MODELS

Several different models have developed that can be used for CCF evaluation. These models include the following:

1. Beta factor (BF) model [7].
2. Basic parameter (BP) model [8].

3. Multiple Greek letter (MGL) model [9].
4. Binomial failure rate (BFR) model [10].
5. System fault tree model [1, 4]. This is the approach presented in this chapter.

23.10 ADVANTAGES AND DISADVANTAGES

The following are advantages of the CCFA technique:

1. Structured, rigorous, and methodical approach.
2. Identifies fault events that can bypass safety critical redundant designs.
3. Permits probability assessment of CCF.
4. Probability assessment of CCF provides a truer view of system risk.

The following are disadvantages of the CCFA technique:

1. Requires an analyst with some training and practical experience.
2. Sometimes avoided because of the complexity and cost.
3. Does not identify all system hazards, only those associated with CCFs.

23.11 COMMON MISTAKES TO AVOID

When first learning how to perform a CCFA, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of a CCFA:

1. Not conducting a thorough investigation of CCF factors, events, or groups
2. Not evaluating all redundant subsystems for CCF vulnerability
3. Not using an FTA for visualization of CCF events

23.12 SUMMARY

This chapter discussed the CCFA technique. The following are basic principles that help summarize the discussion in this chapter:

1. The primary purpose of the CCFA is to identify single failure events that defeat design redundancy, where the redundancy is primarily intended to assure operation in safety critical applications.
2. If a CCF is overlooked, total system risk is understated because the probability of the CCF hazard is not included in the total risk calculation.

3. CCFA should be a supplement to the SD-HAT.
4. Some CCFA-identified hazards may require more detailed analysis by other techniques (e.g., FTA) to ensure that all causal factors are identified.

REFERENCES

1. ARP-4754, SAE Aerospace Recommended Practice, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, 1996.
2. A. Mosleh, et al., *Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples*, Volume 1, NUREG/CR-4780, U.S. NRC, Washington, DC, 1988.
3. A. Mosleh, D. M. Rasmuson, and F. M. Marshall, *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, INEEL/EXT-97-01327, U.S. NRC, Washington, DC, 1998.
4. NASA, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, NASA, August, 2002.
5. H. Kumanoto and E. J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed., IEEE Press, 1996.
6. ARP-4761, SAE Aerospace Recommended Practice, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996.
7. K. N. Fleming, A Reliability Model for Common Mode Failure in Redundant Safety Systems, Proceedings of the 6th Annual Pittsburgh Conference on Modeling and Simulation, General Atomic Report GA-A13284, April, 1975, pp. 23–25.
8. K. N. Fleming, et al., Classification and Analysis of Reactor Operating Experience Involving Dependent Events, Pickard, Lowe and Garrick, Inc., PLG-0400, prepared for EPRI, Feb., 1985.
9. Pickard, Lowe and Garrick, Inc., Seabrook Station Probabilistic Safety Assessment, prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG-0300, Dec., 1983.
10. PRA Procedures Guide: A Guide to the Performance of Probabilistic Assessments for Nuclear Power Plants, USNRC, NUREG/CR-2300, Appendix B, 1983.

BIBLIOGRAPHY

Groen, F. J., A. Mosleh, and C. Smidts, Automated Modeling and Analysis of Common Cause Failure with QRAS, Proceedings of the 20th International System Safety Conference, 2002, pp. 38–44.

Kaufman, L. M., S. Bhide, and B. W. Johnson, Modeling of Common-Mode Failures in Digital Embedded Systems, Proceedings 2000 Annual Reliability and Maintainability Symposium, 2000, pp. 350–357.

Mosleh, A., et al., *Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Analytical Background and Techniques*, Volume 2, NUREG/CR-4780, US NRC, Washington, DC, 1989.

Chapter 24

Management Oversight Risk Tree Analysis

24.1 INTRODUCTION

Management oversight and risk tree (MORT) is an analysis technique for identifying safety-related oversights, errors, and/or omissions that lead to the occurrence of a mishap. MORT is primarily a reactive analysis tool for accident/mishap investigation, but it can also be used for the proactive evaluation and control of hazards. MORT analysis is used to trace out and identify all of the causal factors leading to a mishap or undesired event.

The MORT analysis utilizes the logic tree structure and rules of fault tree analysis (FTA), with the incorporation of some new symbols. This means that MORT can be used to generate risk probability calculations such as FTA. MORT analysis provides decision points in a safety program evaluation where design or program change is needed. MORT attempts to combine design safety with management safety.

24.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (SD-HAT). Refer to Chapter 3 for a description of the analysis types. A smaller and less complex form of MORT has been developed that is referred to as mini-MORT.

The MORT technique is a root cause analysis tool that provides a systematic methodology for planning, organizing, and conducting a detailed and comprehensive mishap investigation. It is used to identify those specific design control

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

measures and management system factors that are less than adequate (LTA) and need to be corrected to prevent the reoccurrence of the mishap or prevent the undesired event. The primary focus of MORT is on oversights, errors, and/or omissions and to determine what failed in the management system.

The MORT analysis is applicable to all types of systems and equipment, with analysis coverage given to systems, subsystems, procedures, environment, and human error. The primary application of MORT is in mishap investigation to identify all of the root causal factors and to ensure that corrective action is adequate.

The MORT analysis is capable of producing detailed analyses of root causes leading to an undesired event or mishap. By meticulously and logically tracking energy flows within and out of a system, MORT analysis compels a thorough analysis for each specific energy type. The degree of thoroughness depends on the self-discipline and ability of the analyst to track logically the flows and barriers in the system.

The analyst can master MORT analysis with appropriate training. The analyst must have the ability to understand energy flow concepts, for which at least a rudimentary knowledge of the behaviors of each of the basic energy types is necessary. Ability to logically identify energy sources and track flows in systems is an essential skill. Ability to visualize energy releases or energy exchange or transformation effects is another helpful skill. Since MORT analysis is based on an extended form of FTA, the FTA technique itself could be used as a replacement for MORT analysis. A condensed version of MORT, called mini-MORT, could also be used.

Use of MORT is not recommended for the general system safety program since it is complex, time consuming, unwieldy in size, and difficult to understand. Other hazard analysis techniques are available that provide results more effectively. MORT could be used for mishap investigation, but FTA is more easily understood and just as effective.

24.3 HISTORY

The MORT analysis technique was developed circa 1970 by W. G. Johnson of the Aerojet Nuclear Company. The development work was sponsored by the Energy Research and Development Administration (Department of Energy, formerly the Atomic Energy Commission) at the Idaho National Engineering Laboratory (INEL). MORT analysis is predicated upon hazardous energy flows and safety barriers mitigating these flows.

24.4 THEORY

The theory behind MORT analysis is fairly simple and straightforward. The analyst starts with a predefined MORT graphical tree that was developed by the original MORT developers. The analyst works through this predefined tree, comparing the management and operations structure of his or her program to the ideal MORT structure, and develops a MORT diagram modeling the program or project. MORT and FTA logic and symbols are used to build the program MORT diagram. The predefined tree consists of 1500 basic events, 100 generic problem areas, and a large number of judging criteria. This diagram can be obtained from *The MORT User's Manual* [1].

The concept emphasizes energy-related hazards in the system design and the management structure. MORT analysis is based on energy transfer and barriers to prevent or mitigate mishaps. Consideration is given to management structure, system design, potential human error, and environmental factors.

Common terminology used in MORT analysis charts includes the following acronyms:

- LTA: less than adequate
- DN: did not
- FT: failed to
- HAP: hazard analysis process
- JSA: job safety analysis
- CS&R: codes standards and regulations

The generic MORT diagram has many redundancies in it due to the philosophy that it is better to ask a question twice rather than fail to ask it at all.

The MORT analysis is based on the following definitions:

Accepted or assumed risk Very specific risk that has been identified, analyzed, quantified to the maximum practical degree, and accepted by the appropriate level of management after proper thought and evaluation. Losses from assumed risks are normally those associated with earthquakes, tornadoes, hurricanes, and other acts of nature.

Amelioration Postaccident actions such as medical services, fire fighting, rescue efforts, and public relations.

24.5 METHODOLOGY

Table 24.1 shows an overview of the basic MORT analysis process and summarizes the important steps and relationships involved. This process consists of utilizing design information and known hazardous energy source information to verify complete safety coverage and control of hazards.

24.6 WORKSHEET

The MORT analysis worksheet is essentially a slightly modified fault tree with some added symbols and color coding. All of the symbols, rules, and logic of FTA

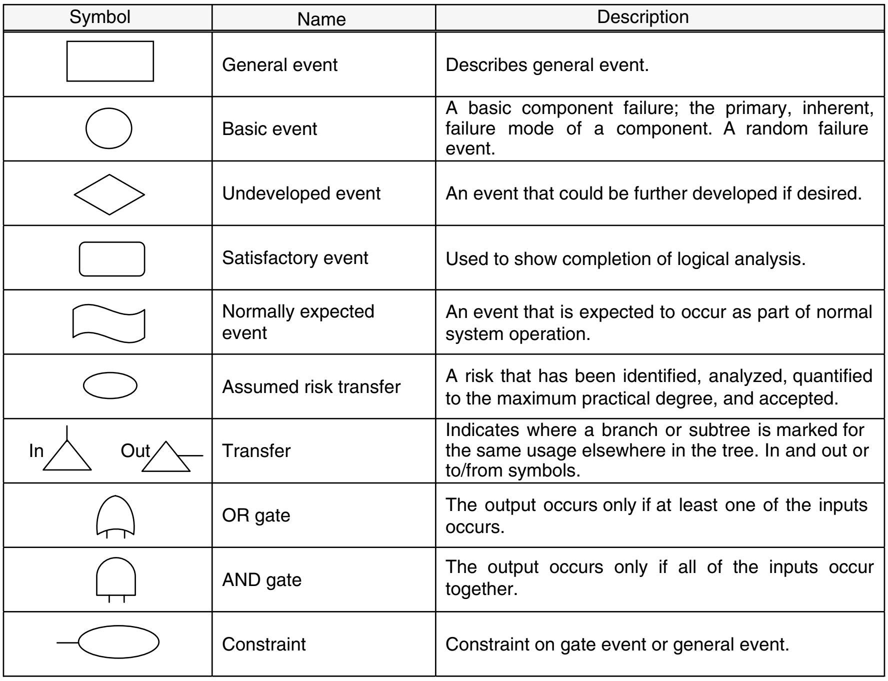
TABLE 24.1 MORT Analysis Process

Step	Task	Description
1	Define system.	Define, scope, and bound the system. Define the mission, mission phases, and mission environments. Understand the system design and operation.
2	Plan MORT analysis.	Establish MORT analysis goals, definitions, worksheets, schedule, and process. Divide the system under analysis into the smallest segments desired for the analysis. Identify items to be analyzed and establish indenture levels for items/functions to be analyzed.
4	Acquire data.	Acquire all of the necessary design and process data needed (e.g., functional diagrams, code, schematics, and drawings) for the system, subsystems, and functions. Refine the system information and design representation for MORT analysis.
5	Conduct MORT analysis.	a. Using the predefined tree, draw a new diagram for the system under review. b. Color code events on tree diagram. c. Continue analysis until all events are sufficiently analyzed with supporting data.
6	Recommend corrective action.	Recommend corrective action for hazards with unacceptable risk. Assign responsibility and schedule for implementing corrective action.
7	Monitor corrective action.	Review the MORT diagram at scheduled intervals to ensure that corrective action is being implemented.
8	Track hazards.	Transfer identified hazards into the hazard tracking system (HTS).
9	Document MORT analysis.	Document the entire MORT process on the worksheets. Update for new information and closure of assigned corrective actions.

(see Chapter 11 on FTA) apply to MORT analysis. New symbols added specifically for MORT are shown in Figure 24.1. Events on the MORT diagram are color coded according to the criteria in Table 24.2.

The MORT analysis is essentially an FTA that asks *what* oversights and omissions could have occurred to cause the undesired event or mishap and *why* in terms of the management system. In some ways, MORT analysis is like using the basic MORT diagram as a checklist to ensure everything pertinent is considered.

Figure 24.2 shows the top level of the ideal MORT analysis from the *MORT User's Manual*. Figure 24.3 expands the S branch of the MORT shown in Figure 24.2. Figure 24.4 expands the M branch of the MORT shown in Figure 24.2. Figure 24.5 expands the 1 branch of the MORT shown in Figure 24.3. Figure 24.6 expands the 2 branch of the MORT shown in Figure 24.5.



Symbol	Name	Description
	General event	Describes general event.
	Basic event	A basic component failure; the primary, inherent, failure mode of a component. A random failure event.
	Undeveloped event	An event that could be further developed if desired.
	Satisfactory event	Used to show completion of logical analysis.
	Normally expected event	An event that is expected to occur as part of normal system operation.
	Assumed risk transfer	A risk that has been identified, analyzed, quantified to the maximum practical degree, and accepted.
In Out	Transfer	Indicates where a branch or subtree is marked for the same usage elsewhere in the tree. In and out or to/from symbols.
	OR gate	The output occurs only if at least one of the inputs occurs.
	AND gate	The output occurs only if all of the inputs occur together.
	Constraint	Constraint on gate event or general event.

Figure 24.1 *MORT symbols.*

24.7 ADVANTAGES AND DISADVANTAGES

The following are advantages of the MORT analysis technique:

1. Has a pictorial benefit that aids analysts in visualizing hazards.
2. Can be quantified (but usually is not).

TABLE 24.2 MORT Color Coding

Color	Meaning
Red	Any factor or event found to be LTA is colored red on the chart. Should be addressed in the final report with appropriate recommendations to correct the deficiency. Use judiciously; must be supported by facts.
Green	Any factor or event found to be adequate is colored green on the chart. Use judiciously; must be supported by facts.
Black	Any factor or event found to be not applicable is color-coded black (or simply crossed out) on the chart.
Blue	Indicates that the block has been examined, but insufficient evidence or information is available to evaluate the block. All blue blocks should be replaced with another color by the time the investigation is complete.

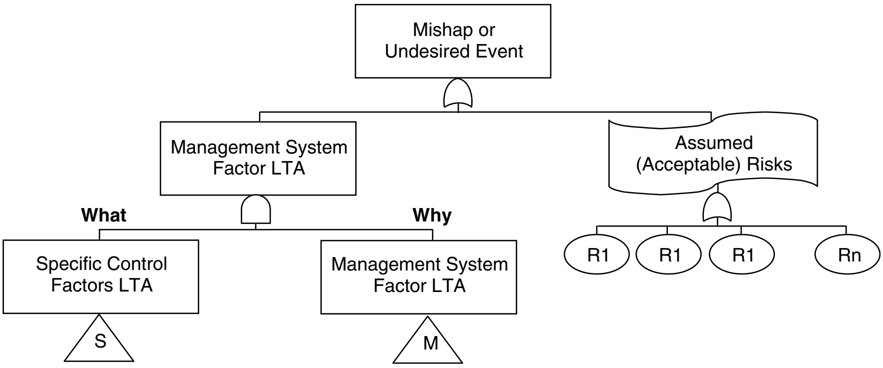


Figure 24.2 *MORT top tiers.*

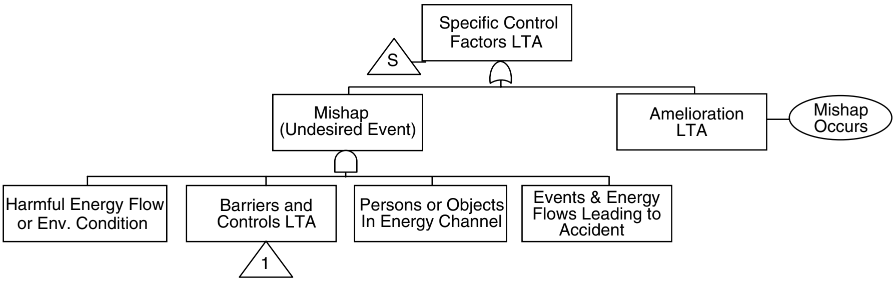


Figure 24.3 *MORT specific control factors.*

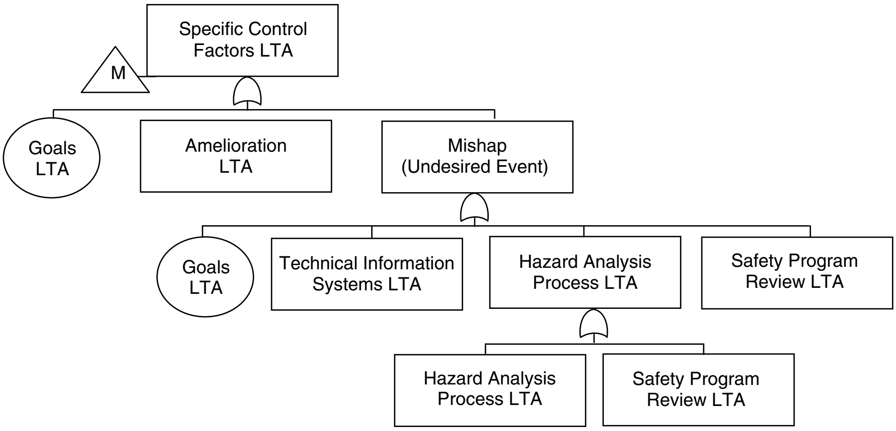


Figure 24.4 *MORT management system factors.*

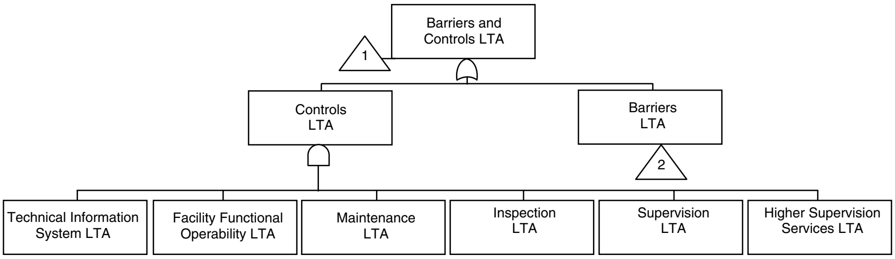

Barriers and Controls LTA
1
Controls LTA
Barriers LTA
2
Technical Information System LTA
Facility Functional Operability LTA
Maintenance LTA
Inspection LTA
Supervision LTA
Higher Supervision Services LTA

Figure 24.5 *MORT barriers and controls diagram.*

3. Is simple to perform (once understood).
4. Commercial software is available to assist the analyst.

The following are disadvantages of the MORT analysis technique:

1. Though simple in concept, the process is labor intensive and requires significant training.
2. Is limited by the ability of the analyst to identify all the hazardous energy sources.
3. Tree size can become too large for effective comprehension by the novice.

24.8 COMMON MISTAKES TO AVOID

When first learning how to perform a MORT analysis, it is commonplace to commit some traditional errors. The following is a list of typical errors made during the conduct of a MORT analysis:

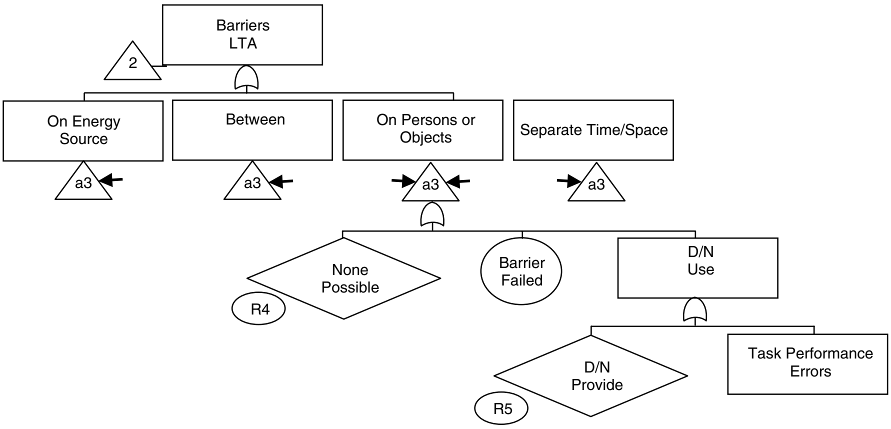


Figure 24.6 *MORT barriers diagram.*

1. Not obtaining the necessary training
2. Not thoroughly investigating all causal factor paths

24.9 SUMMARY

This chapter discussed the MORT hazard analysis technique. The following are basic principles that help summarize the discussion in this chapter:

1. MORT analysis is a root cause analysis tool similar to FTA.
2. The primary purpose of MORT analysis is for mishap investigation analysis.
3. MORT analysis should be a supplement to the SHA.
4. MORT analysis involves a focus on hazardous energy sources and barriers.
5. MORT analysis is based on an existing predefined tree diagram.
6. MORT provides analysis of the management system for a project.

REFERENCE

1. N. W. Knox, and R. W. Eicher, *MORT User's Manual*, SSDC-4 (Revision 2), U.S. Dept. of Energy, Idaho Falls, ID, 1983.

BIBLIOGRAPHY

Clark, J. L. The Management Oversight and Risk Tree (MORT)—A New System Safety Program, Proceedings of the 2nd International System Safety Conference, 1975, pp. 334–350.

Johnson, W. G., *MORT, the Management Oversight and Risk Tree*, U.S. Atomic Energy Commission, SAN-821-2, U.S. Government Printing Office, Washington DC, 1973.

Johnson, W. G., *MORT Safety Assurance Systems*, Marcel Dekker, New York, 1980.

Stephenson, J., *System Safety 2000: A Practical Guide for Planning, Managing, and Conducting System Safety Programs*, Wiley, New York, 1991, pp. 218–255.

Chapter 25

Software Safety Assessment

25.1 INTRODUCTION

Software safety assessment (SWSA) is an analysis methodology for evaluating and assessing the potential safety hazards software may present to a system. It is used to determine if a system contains software and, if so, to identify what safety considerations are necessary to ensure safe software. If software safety implications are found in the system software, then a software system safety program (SWSSP) should be implemented. The SWSA provides enough information to size and scope an SWSSP or to document that a SWSSP is not warranted. The SWSA helps the system development program determine if software presents a safety risk and the scope of an SWSSP.

It should be noted that SWSA is not strictly a hazard analysis but an assessment of the potential safety criticality of software in the system design. If the SWSA indicates that an SWSSP is warranted, then hazard analysis and other safety tasks will be performed on the system software.

25.2 BACKGROUND

This analysis technique falls under the system design hazard analysis type (the basic analysis types are described in Chapter 3). There are no alternate names for this technique.

The purpose of the SWSA is to evaluate a system and determine if an SWSSP is required and, if so, determine what and how much safety effort is required. The SWSA is a high-level review of the system and software performed to establish the necessity, scope, and funding of a more detailed SWSSP.

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

The SWSA technique can be used on any type or size of system. It is a high-level assessment to determine if a system contains software and, if so, the level of safety criticality. The SWSA technique, when applied to a given system by experienced safety personnel, should provide a thorough and comprehensive identification of the software safety tasks required by an SWSSP.

The technique is uncomplicated and easily learned. Standard, easily followed SWSA worksheets and instructions are provided in this chapter. An SWSA performed early in the system development cycle will help ensure that software safety is adequately addressed or document that the program does not need an SWSSP.

It is recommended that an SWSA be performed on every new or modified system in order to determine if the system contains software, the size of the software, and the safety criticality of the software. Sometimes system developers overlook the fact that a system may contain firmware, which is considered software, and requires an SWSSP.

25.3 HISTORY

The SWSA was developed by C. A. Ericson at the Boeing Company circa 1977 to evaluate software involvement in a system design and scope the level of effort required for an effective SWSSP.

25.4 THEORY

Figure 25.1 shows an overview of the basic SWSA concept and summarizes the important relationships involved. The SWSA process consists of identifying software modules in the system design and evaluating the level of safety risk presented by the software. The amount of safety risk that is presented by the software will drive the size and scope of the SWSSP.

The information resulting from the SWSA provides the safety analyst with data to determine if an SWSSP is warranted and the potential amount of effort required. The SWSA is conducted to assess system software early in the design process. The intent

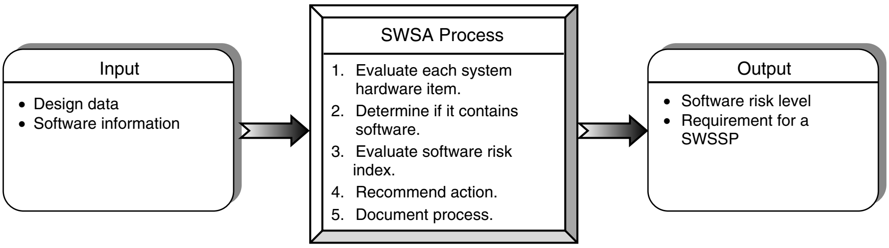

Input
• Design data
• Software information
SWSA Process
1. Evaluate each system hardware item.
2. Determine if it contains software.
3. Evaluate software risk index.
4. Recommend action.
5. Document process.
Output
• Software risk level
• Requirement for a SWSSP

Figure 25.1 *SWSA concept.*

of the SWSA is not to immediately identify software-related hazards and risks but to recognize the safety implications of software in the system design.

The SWSA method is based on the following definitions:

Software Combination of associated computer instructions and computer data that enable a computer to perform computational or control functions. Embedded software is software developed to control a hardware device. It may be executed on a processor contained within a device or an external computer connected to the hardware to be controlled. Software includes computer programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system [1].

Firmware Software that resides in a nonvolatile medium that is read-only in nature, which cannot be dynamically modified by the computer during processing (write protected during operation) [1]. Provisions that apply to software as defined above also apply to firmware.

25.5 METHODOLOGY

Figure 25.2 contains a functional diagram of the SWSA methodology. This process begins by acquiring design information in the form of the design concept, the operational concept, major components planned for use in the system, and major system functions. Sources for this information could include: statement of work (SOW), statement of objectives (SOO), design specifications, sketches, drawings, or schematics. From this information, the next step is to identify and understand software planned within the system design.

The SWSA is generally performed very early in the design life cycle, usually before software requirements or design have been initiated; therefore, the analysis starts by looking at the hardware and then gradually moving into software associated with the hardware. The SWSA process begins by listing all of the major system

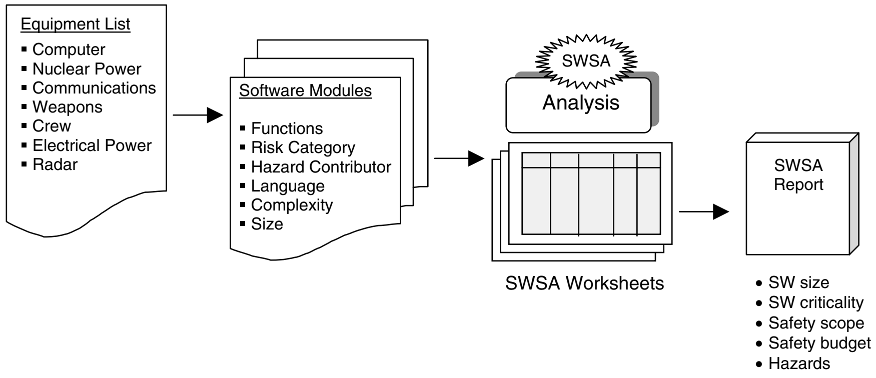


Figure 25.2 *SWSA methodology.*

hardware elements or components. Each component is then evaluated for software function, whether embedded or stored. Basic data is then collected on the software, such as purpose, size, language, and the like. The software is then classified into risk levels in order to determine the safety significance of the software. These risk levels determine the amount of future effort that must be applied to ensure the development of safe software.

Table 25.1 lists and describes the basic steps of the SWSA process.

25.6 WORKSHEET

The SWSA technique utilizes a worksheet to provide structure and rigor. Although the exact format of the assessment worksheet is not critical, typically, matrix or columnar-type worksheets are used to help maintain focus and composition in the analysis. As a minimum, the following basic information is required from the SWSA worksheet:

1. Item under assessment
2. Purpose or function of item
3. Does the item contain software or firmware
4. Data on software
5. Safety criticality index of software
6. Software safety effort required

TABLE 25.1 SWSA Process

Step	Task	Description
1	Define the system.	Examine the system and define the system boundaries, subsystems, functions, and interfaces.
2	Identify the hardware/ functions.	Identify and list all of the major system elements or components. Understand their function and purpose.
3	Identify software or firmware.	Identify if the hardware components will contain embedded or resident software.
4	Identify the software modules.	Identify the software modules that will be used by the hardware components to achieve the system functions. This may require some analysis and predictions if not already done by the project.
5	Identify software module data.	Identify pertinent data on the software modules, such as language, size, complexity, interfaces, etc.
6	Identify the software risk index.	Apply the software risk index to each software module to determine its safety criticality level.
7	Identify software related hazards.	If there is visibility, identify hazards to which the software modules may contribute.
8	Recommend corrective action.	Provide recommendations resulting from the assessment.
9	Document SWSA.	Document the entire SSA process on the worksheets. Update for new information as necessary.

The recommended SWSA worksheet is shown in Figures 25.3. This particular SWSA worksheet utilizes a columnar-type format. Other worksheet formats may exist because different organizations often tailor their SWSA worksheet to fit their particular needs. The specific worksheet to be used may be determined by the system safety working group, the safety integrated product team (IPT), or the safety analyst performing the SWSA.

The steps for this SWSA worksheet are as follows:

1. *Item* This column identifies the major hardware subsystem, component, function, or item for analysis. Examples include radar subsystem, avionics computer subsystem, flight control system subsystem, and the like.
2. *Function/Purpose* This column describes the item's purpose or function of the item in column 1. It is possible to identify software modules when the operational intent of the item is understood.
3. *S/F* This column identifies whether or not the hardware item contains software or firmware. If neither software nor firmware is involved, then this column should contain the word *None*.
4. *Software Module Data* This column identifies the software module(s) that are expected to be associated with the identified item. Other pertinent information should be recorded here, such as the programming language of the module, the number of source lines of code (SLOC), complexity, and the like.
5. *Risk Category* This column provides a qualitative index measure for the relative safety risk level of the software module. This category indicates the relative safety significance expected for the software module and the level of safety rigor that will be required of the software. The *DoD Joint Software System Safety Handbook* [2] provides an index referred to as the software hazard risk index (SHRI) that classifies the relative risk level of software modules. The process is described in Section 25.7 of Ref. 2.

Software Safety Assessment

Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
①	②	③	④	⑤	⑥	⑦	⑧	⑨

Figure 25.3 *Recommended SWSA worksheet.*

6. *SR–SC* This column identifies if the software is considered as being safety related (SR) or safety critical (SC). A blank in this column would automatically mean that the software is nonsafety related.
7. *Software-Related Hazards/Mishaps* This column identifies hazards or top-level mishaps to which the identified software module may be a contributing factor. If there is no hazard/mishap visibility when the SWSA is performed, this column may be blank.
8. *Recommendation* This column provides for any recommendations that are immediately evident from the SWSA, such as the need and scope for an SWSSP. Recommendations may also include preliminary design or procedural safety requirements.
9. *Comments* This column provides for any pertinent comments to the analysis that need to be documented for possible future use. For example, this column can be used to record that a software module is a COTS item.

25.7 SOFTWARE RISK LEVEL

The initial assessment of risk for software and, consequently, software-controlled or software-intensive systems, cannot rely solely on hazard severity and probability. Determination of the probability of failure of a single software function is difficult at best and cannot be based on historical data. Software is generally application specific and reliability parameters associated with it cannot be estimated in the same manner as hardware is. Therefore, the SHRI approach is recommended for the initial software risk assessment that considers the potential hazard severity and the degree of control that software exercises over the hardware.

The first step in the code review is to determine the software control code (CC) category and the SHRI level for each software code module. The modules with a higher SHRI are automatically subject to greater analysis and testing scrutiny.

The criterion for these tables is from the *DoD Joint System Software Safety Handbook* [1], MIL-STD-882C, and STANAG 4404. The software risk assessment process is shown in the four steps below.

Step 1 Identify the control category for software module using the criteria in Table 25.2.

Step 2 Identify the severity of the mishap to which the software would pertain, using the criteria in Table 25.3.

Step 3 Using the classifications from steps 1 and 2, determine the SHRI for the software using the criteria in Table 25.4.

Step 4 Based on the SHRI determine the risk level for the software using the criteria in Table 25.5.

Unlike the hardware-related hazard risk index (HRI), a low software HRI number does not mean that a design is unacceptable. Rather, it indicates that greater resources need to be applied to the analysis and testing of the software and its interaction with the system.

TABLE 25.2 Software Control Code (CC) Categories

Control Category	Definition
I	Software exercises autonomous control over potentially hazardous hardware systems, subsystems, or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard's occurrence.
IIa	Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.
IIb	Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow or fail to prevent the hazard's occurrence.
IIIa	Software item issues commands over potentially hazardous hardware systems, subsystems, or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.
IIIb	Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.
IV	Software does not control safety critical hardware systems, subsystems, or components and does not provide safety critical information.

25.8 EXAMPLE

In order to demonstrate the SWSA methodology, the hypothetical Ace Missile System will be used (example from Chapter 5). This system is comprised of the missile and the weapon control system (WCS).

TABLE 25.3 Hazard Severity Categories

Description	Categories	Mishap Definition
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1 million, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200,000 but less than $1 million, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10,000 but less than $200,000, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2000 but less than $10,000, or minimal environmental damage not violating law or regulation.

TABLE 25.4 Software Hazard Risk Index (SHRI)

Hazard Category / Control Category	I Catastrophic	II Critical	III Marginal	IV Negligible
I	1	1	3	5
II	1	2	4	5
III	2	3	5	5
IV	3	4	5	5

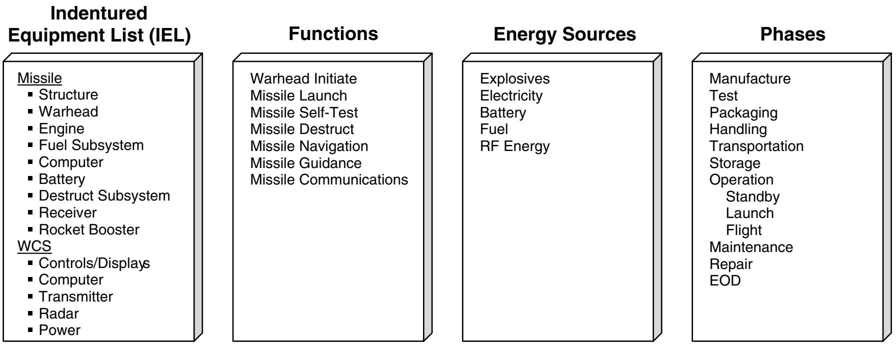
TABLE 25.5 SHRI Risk Levels

RAC	Risk	Action
1	High	Significant analysis and testing resources.
2	Medium	Requirements and design analysis and in-depth testing required.
3–4	Moderate	High-level analysis and testing, acceptable with MA approval.
5	Low	Acceptable as is.

The basic equipment and functions for this system are identified in Figure 25.4. During the conceptual design stage, this is the typical level of information that is available. From this basic design information a very credible SWSA can be performed.

Note that since the SWSA is performed early in the planned project there is usually very little information available on software. This means that the SWSA analyst must work primarily from the information available on planned hardware components and system functions. Some of the derived data may be based on estimates or engineering judgment, but it provides a starting point for system software evaluation. Note also that this is not a hazard analysis, but hazard, mishap, and safety critical information can usually be gleaned from this assessment.

Tables 25.6 through 25.10 contain SWSA worksheets for the Ace Missile System.



Indentured Equipment List (IEL)

Missile
- Structure
- Warhead
- Engine
- Fuel Subsystem
- Computer
- Battery
- Destruct Subsystem
- Receiver
- Rocket Booster

WCS
- Controls/Displays
- Computer
- Transmitter
- Radar
- Power

Functions

Warhead Initiate
Missile Launch
Missile Self-Test
Missile Destruct
Missile Navigation
Missile Guidance
Missile Communications

Energy Sources

Explosives
Electricity
Battery
Fuel
RF Energy

Phases

Manufacture
Test
Packaging
Handling
Transportation
Storage
Operation
  Standby
  Launch
  Flight
Maintenance
Repair
EOD

Figure 25.4 Ace Missile System information.

TABLE 25.6 SWSA for the Ace Missile System—Worksheet 1

Software Safety Assessment								
Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
Missile structure	Integral missile structure containing all missile components	None	None					
Missile warhead (W/H)	High explosives and initiating system containing:							
	a. Missile S&A device to interrupt power to interrupt power to W/H during PHS&T[a]	Non	None					
	b. Arm-1 switch (mechanical; environment sensing)	None	None (mechanical system)					
	c. Arm-2 switch (electronic; environment sensing)	F	W/H arming function Arm-2	2a-I	SC	Inadvertent detonation	SSRs needed	
			C++ language				Safety analysis needed	

(*continued*)

TABLE 25.6 *Continued*

Software Safety Assessment								
Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
			500 SLOC				No COTS software allowed	
Missile engine subsystem	Missile engine and control electronics	F	Engine speed control function C++ language 300 SLOC	2b-I	SR	Incorrect target	SSRs needed Safety analysis needed	
		F	Engine fuel control function C++ language 250SLOC	2b-I	SC	Incorrect target	SSRs needed Safety analysis needed	
Missile fuel subsystem	Store and transfer fuel to missile engine	None	None (mechanical system)					
Analyst:							Page: 1 of 5	

[a]PHS&T, packaging, handling, storage, and transportation.

TABLE 25.7 SWSA for the Ace Missile System—Worksheet 2

Software Safety Assessment								
Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
Missile computer	Control missile functions, including:							
	a. Missile W/H power	S	Apply W/H power function C++ language 300 SLOC	2a-I	SC	Inadvertent detonation	SSRs needed Safety analysis needed	
	b. Missile guidance	S	Missile control surface commands C++ language 300 SLOC	2b-I	SC	Incorrect target	SSRs needed Safety analysis needed	
	c. Missile navigation	S	Missile navigation calculations C++ language 300 SLOC	2b-I	SC	Incorrect target	COTS safety analysis needed	COTS software (Kahlman filter)
	d. Missile self-test	S	Missile self-test function	2b-II	SR	Unsafe missile state	SSRs needed	

(*continued*)

TABLE 25.7 *Continued*

Software Safety Assessment								
Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
			C ++ language 300 SLOC				Safety analysis needed	
	e. Missile destruct	S	Missile destruct function	2a-I	SC	Inadvertent destruct; inability to destruct	SSRs needed	
			C ++ language 300 SLOC				Safety analysis needed	
Analyst:							Page: 2 of 5	

TABLE 25.8 SWSA for the Ace Missile System—Worksheet 3

Software Safety Assessment								
Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
Missile battery subsystem	Provide power to missile electronics	None	None (electromechanical system)					
Missile destruct subsystem	Explosives and initiator for missile self-destruct function	S	Same as missile computer—destruct function (refer to missile computer)					
Analyst:						Page: 3 of 5		

TABLE 25.9 SWSA for the Ace Missile System—Worksheet 4

Software Safety Assessment								
Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
WCS controls & displays (C&D)	Operator controls and displays; interface with WCS computer	None [controlled by WCS computer]						
WCS computer	Control overall system functions, including:	S	Missile launch functions C++ language 300 SLOC	2a-1	SC	Inadvertent missile launch	SSRs needed Safety analysis needed	
	a. Missile launch	S	Missile status functions C++ language 300 SLOC	2b-1	SC	Unsafe missile state	SSRs needed Safety analysis needed	
	b. Missile self-test	S	Dispaly target data function C++ language	2b-1	SC	Incorrect target; inadvertent missile launch	SSRs needed Safety analysis needed	

(*continued*)

TABLE 25.9 *Continued*

Software Safety Assessment								
Item	Function/ Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
			300 SLOC					
	c. C&D commands		Process operator target selection C++ language 300 SLOC	2b-1	SC	Incorrect target	SSRs needed Safety analysis needed	
			Display system status C++ language 300 SLOC	2b-2	SR	Unsafe missile	SSRs needed Safety analysis needed	
			Process operator missile launch C++ language 300 SLOC	2a-1	SC	Inadvertent missile launch	SSRs needed Safety analysis needed	
Analyst:						Page: 4 of 5		

TABLE 25.10 SWSA Worksheet for the Ace Missile System—Worksheet 5

Software Safety Assessment								
Item	Function/Purpose	S/F	Software Module Data	Risk Cat	SR SC	Software Related Hazards/Mishaps	Recommendation	Comments
WCS communications with missile	WCS communications with missile; interface between WCS and missile computers:							
	a. Target data	S	Send new or modified missile target coordinates function C++ language 300 SLOC	2b-1	SC	Incorrect target	SSRs needed Safety analysis needed	
	b. Missile self-destruct	S	Send target self-destruct command function C++ language 300 SLOC	2a-1	SC	Inadvertent missile launch	SSRs needed Safety analysis needed	
WCS Radar	Target detection and coordinates	None	None [Detect target and send data to WCS computer functions]					
WCS Power	Electrical power and distribution for WCS	None	None					
Analyst:							Page: 5 of 5	

Results and conclusions from the SWSA for the Ace Missile System are summarized as follows:

1. The system contains both software and firmware.
2. The system software involves both safety critical and safety-related software.
3. Some potential top-level mishaps have been identified.
4. Some software modules have been identified that are potential casual factors for the identified top-level mishaps.
5. The high-risk categories for some software modules indicates that an SWSSP is warranted and necessary.
6. The high-risk categories for some software modules indicates that system safety requirements (SSRs) are needed for safe software design.
7. Further more detailed hazard analysis will be required to ensure safe system software.
8. Some of the software modules will have a high level of complexity due to the functions being performed, such as Kahlman filtering for navigation equations, missile launch functions, missile warhead initiation functions, and the like.

TABLE 25.11 SWSSP Calculations

Task	Pricing Rationale	Cost
Write software safety plan		
Perform hazard analyses		
PHL		
PHA		
SSHA		
SHA		
Other		
Identify SC functions and software		
Perform risk assessment		
Establish SIL for software modules		
Establish SSRs for software		
Develop coding standards for safety		
Perform SRCA traceability		
Perform hazard tracking/closure		
STR/SPR review/evaluation		
Design change review/evaluation		
Tag SC SSRs		
Tag SC software modules		
Code analysis		
Test support		
Tools validation		
OS validation		
Compiler validation		
COTS safety		
Prepare SAR (safety case)		
Prepare Review presentations		

9. Some COTS software has been identified in the system, meaning that special safety analyses will have to be performed to ensure that the COTS software does not degrade safety critical and safety-related software.
10. An SWSSP is recommended and Table 25.3 can be used to estimate the SWSSP tasks and cost. Information from the SWSA worksheet can be used to complete the items in Table 25.11. Note that the items in Table 25.3 provide a costing example and should be expanded and tailored to the specific project needs and requirements.

25.9 ADVANTAGES AND DISADVANTAGES

The following are advantages of the SWSA technique:

1. Structured, rigorous, and methodical approach.
2. Can be effectively performed on varying levels of design detail.
3. Relatively easy to learn, perform, and follow.
4. Provides a cursory software risk assessment.

The only significant disadvantage of the SWSA technique is that it requires an analyst with some knowledge and experience in software safety.

25.10 COMMON MISTAKES TO AVOID

When first learning how to perform an SWSA, it is commonplace to commit some typical errors. The following is a list of typical errors made during the conduct of an SWSA:

1. Not including subsystems and software provided by vendors and subcontractors
2. Not adequately addressing all of the system software, particularly firmware
3. Not including COTS software in the assessment
4. Not understanding or underestimating the safety critical nature of the planned software modules

25.11 SUMMARY

This chapter discussed the SWSA technique. The following are basic principles that help summarize the discussion in this chapter:

1. SWSA is used to obtain a cursory evaluation of the safety significance of the software and the potential need for an SWSSP.

2. The SWSA worksheet provides structure and rigor to the SWSA process.
3. SWSA should be performed early in the program life cycle to assist in planning and funding of the SWSSP.

REFERENCES

1. Reference EIA SEB6-A.
2. *DoD Joint Software System Safety Handbook*, December 1999.

BIBLIOGRAPHY

Ericson, C. A., Software and System Safety, Proceeding on the 5th International System Safety Conference, 1981.

Chapter 26

Summary

This book has focused on two main objectives. The first objective was to provide an understanding of hazard theory so that hazards can be better understood and therefore more easily identified and described. The second objective was to explain in detail how to perform the 22 most used hazard analysis techniques in system safety. In order to be truly professional, the system safety analyst must be able to correctly apply the appropriate techniques in order to identify and mitigate hazards. Overall, the concepts presented in this book can be briefly summarized by the following key principles:

Principle 1: Hazards, mishaps, and risk are not chance events.

Principle 2: Hazards are created during design.

Principle 3: Hazards are comprised of three components.

Principle 4: Hazard and mishap risk management is the core safety process.

Principle 5: Hazard analysis is a key element of hazard and mishap risk management.

Principle 6: Hazard management involves seven key hazard analysis types.

Principle 7: Hazard analysis primarily encompasses seven hazard analysis techniques.

26.1 PRINCIPLE 1: HAZARDS, MISHAPS, AND RISK ARE NOT CHANCE EVENTS

A mishap is not a random chance event, but instead it is a deterministic event. Mishaps and accidents do not just happen; they are the result of a unique set of

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

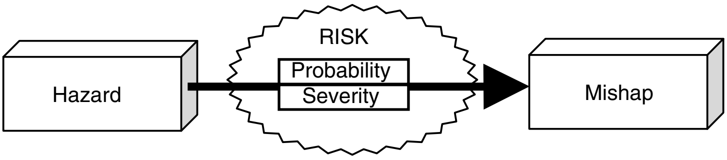


Figure 26.1 *Hazard–mishap relationship.*

conditions (i.e., hazards). A hazard is a potential condition that can result in a mishap or accident. This means that mishaps can be predicted via hazard identification. And, mishaps can be prevented or controlled via hazard elimination, control, or mitigation.

A hazard is the precursor to a mishap; a hazard is a condition that defines a potential event (i.e., mishap), while a mishap is the occurred event. This results in a direct relationship between a hazard and a mishap, whereby a hazard and a mishap are two separate states of the same phenomenon, linked by a state transition that must occur. A hazard is a "potential event" at one end of the spectrum that may be transformed into an "actual event" (the mishap) at the other end of the spectrum. The transition from the hazard state to the risk state is based upon the risk involved. This concept is shown in Figure 26.1.

There are two key points to remember about the hazard–mishap transition process. One, there is generally some sort of energy buildup in the transition phase, which ultimately causes the mishap damage. Two, there is usually a point of no return for the mishap, where there is no possibility of it being reversed. Each individual hazard is unique, and therefore this time period is unique to every hazard.

26.2 PRINCIPLE 2: HAZARDS ARE CREATED DURING DESIGN

How do hazards come into existence? Are they acts of nature or manmade? Mishaps do not just happen; they are the result of hazards. And, hazards do not just randomly happen either; they are the result of circumstance and/or design flaws inadvertently built into the system design.

The basic reasons why hazards exist are (1) they are unavoidable because hazardous elements must be used in the system, and/or (2) they are the result of inadequate design safety consideration. Inadequate design safety consideration results from poor or insufficient design or the incorrect implementation of a good design. This includes inadequate consideration given to the potential effect of hardware failures, sneak paths, software glitches, human error, and the like.

By circumstance, systems with hazardous elements will always have hazards that cannot be eliminated. In these situations the hazards are usually well known, and the objective is to reduce the system mishap risk to an acceptable level. In order to reduce the risk, the hazard causal factors must first be identified, which is accomplished via hazard analysis.

Quite often hazards are inadvertently injected into a system design through design "blunders," design errors, or lack of foresight. For example, two subsystems may have been independently designed and when combined in a system have unforeseen interface problems that result in a hazard. Or, an electrical system may have been designed with unforeseen sneak paths that create hazards. System safety practitioners must expend hazard analysis effort to identify these types of hazards, along with their causal factors.

Fortunately, since hazards are created through the design and development process, this makes them deterministic, predictable, and identifiable. This generates the need for hazard analysis and the hazard analysis techniques described in this book.

26.3 PRINCIPLE 3: HAZARDS ARE COMPRISED OF THREE COMPONENTS

A hazard is a unique and discrete entity comprised of a unique set of causal factors and outcomes. Each and every hazard is unique, with a unique level of risk attached to it. A hazard is like a minisystem; it has a dormant life until a state transition transforms it into a mishap. A hazard defines the terms and conditions of a potential mishap; it is the wrapper containing the entire potential mishap description. The mishap that results is the product of the hazard components.

A hazard is comprised of the following three basic components, each of which must be present in order for the hazard to exist:

1. *Hazardous Element (HE)* This is the basic hazardous resource creating the impetus for the hazard; for example, a hazardous energy source such as explosives being used in the system.
2. *Initiating Mechanism (IM)* This is the trigger or initiator event(s) causing the hazard to occur. This is the mechanism(s) that causes actualization of the hazard from a dormant state to an active mishap.
3. *Target and Threat (T/T)* This is the person or thing that is vulnerable to injury and/or damage, and it describes the severity of the mishap event. This is the mishap outcome and the expected consequential damage and loss.

The HE is always present in a hazard; it provides the basic source for the hazard. A hazard transforms to a mishap only when the IMs force the transition. The probability of a mishap occurring is a function that can include all three hazard components: HE, IM, and T/T. The probability of the IMs occurring is the dominant probability factor, yet the probability of T/T exposure and HE quantity and presence are considerations. Mishap severity is a function of the T/T component proximity and vulnerability and the quantity and potential damaging capacity of the HE component.

The three components form the hazard triangle, as shown in Figure 26.2. The hazard triangle illustrates that a hazard consists of three necessary and coupled

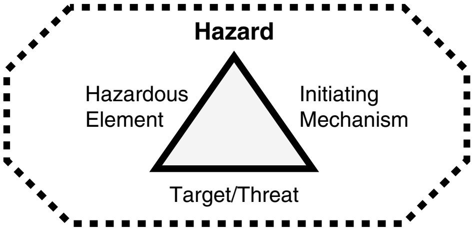


Figure 26.2 Hazard triangle.

components, each of which forms the side of a triangle. All three sides of the triangle are necessary and essential in order for a hazard to exist. Remove any one of the triangle sides and the hazard is eliminated because it is no longer able to produce a mishap (i.e., the triangle is incomplete). Reduce the probability of the IM triangle side and the mishap probability is reduced. Reduce an element in the HE or the T/T side of the triangle and the mishap severity is reduced.

It should be noted that sometimes the three hazard components are referred to as: (1) source, (2) mechanism, and (3) outcome. These terms are just as acceptable and provide the same definitions as their HE, IM, and T/T counterparts. Using the term outcome for the T/T component helps to show even more clearly the direct relationship between a hazard and a mishap.

26.4 PRINCIPLE 4: HAZARD AND MISHAP RISK MANAGEMENT IS THE CORE SAFETY PROCESS

The purpose of a system safety program is to design in safety and reduce mishap risk. From an historical perspective it has been learned that a proactive preventive approach to safety during design is much more cost effective than trying to implement safety into a system after the occurrence of an accident or mishap. This is accomplished via many different system safety tasks; however, the core system safety process revolves around hazards—hazard identification, mishap risk assessment from hazards, and then hazard elimination or mitigation. The core system safety process can be reduced to the closed-loop process shown in Figure 26.3.

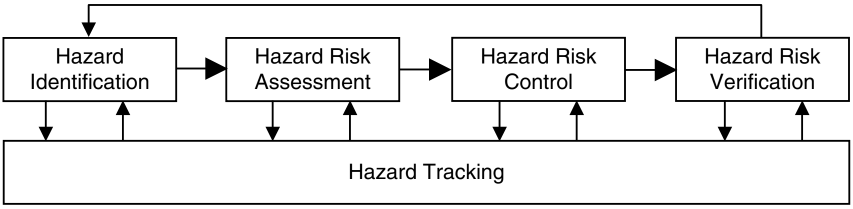


Figure 26.3 System safety focuses on hazards.

This is a hazard and mishap risk management process whereby safety is achieved through the identification of hazards, the assessment of hazard mishap risk, and the control of hazards presenting unacceptable risk. It is a closed-loop process because hazards are identified and continuously tracked and updated until acceptable closure action is implemented and verified. An automated hazard tracking system is generally used for collecting and storing hazard information.

26.5 PRINCIPLE 5: HAZARD ANALYSIS IS A KEY ELEMENT OF HAZARD AND MISHAP RISK MANAGEMENT

To reduce mishap risk, the system safety program must focus on hazards because hazards create the risk. The identification of hazards and hazard causal factors is largely achieved through hazard analysis. Hazard analysis requires methodologies that are designed specifically for the purpose of identifying and evaluating hazards and mishap risk. Hazard analysis tools are a necessary ingredient in the system safety process. The system safety analyst/engineer should be familiar with each of the hazard analysis tools presented in this book. They form the basic building blocks for performing hazard and safety analysis on any type of system.

26.6 PRINCIPLE 6: HAZARD MANAGEMENT INVOLVES SEVEN KEY HAZARD ANALYSIS TYPES

Since the advent of system safety and MIL-STD-882, there have been seven hazard analysis *types* that have been established. There is a specific rationale for each hazard analysis type. A hazard analysis type defines the analysis purpose, timing, scope, level of detail, and system coverage; it does not specify how to perform the analysis. One particular hazard analysis type does not necessarily identify all the hazards within a system; it may take more than one type. When used together, their combined effect provides an optimum process for identifying hazards, mitigating hazards, and reducing system residual risk. A best practice system safety program includes all seven hazard analysis types to ensure complete hazard coverage and provide optimum safety assurance.

The hazard analysis type establishes a category of hazard investigation and evaluation that can be optimally applied by the system safety program. Each category establishes the amount of system safety effort that should be performed and the type of information that is required. A hazard analysis type can only be fulfilled by a specific hazard analysis *technique*, of which there are many.

Figure 26.4 shows the relative relationship of each of the seven hazard analysis types and their interdependencies. This figure shows how the output of one analysis type can provide input data for another analysis type and for other system safety program tasks. There is a prime hazard analysis technique (see principle 7) just for each hazard analysis type. The associated technique is denoted above the type box in Figure 26.4.

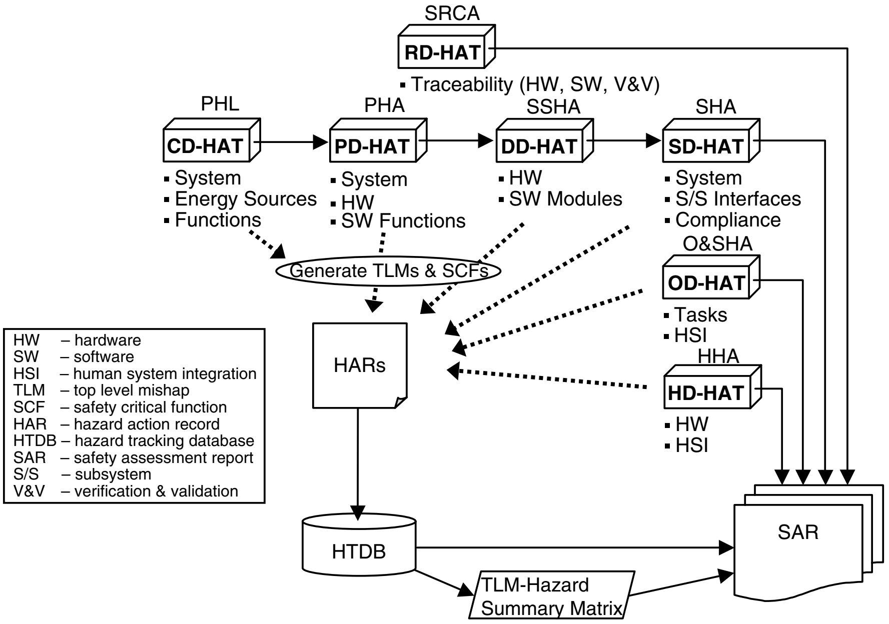


Figure 26.4 *Hazard analysis type relationships.*

26.7 PRINCIPLE 7: HAZARD ANALYSIS PRIMARILY ENCOMPASSES SEVEN HAZARD ANALYSIS TECHNIQUES

A hazard analysis technique is a unique analysis methodology with an overall objective of identifying hazards, mitigating hazards, and assessing system residual risk. Each methodology uses specific guidelines and rules for performing the analysis, has a specific purpose, has predefined inputs and outputs, and has a known utility. Over 100 different hazard analysis techniques have been identified that are available to the system safety practitioner (refer to the *System Safety Analysis Handbook* published by the System Safety Society, available at www.systemsafety.org).

It is not necessary to be knowledgeable in all the identified techniques because many of the techniques are not practical for various reasons. Some techniques are slightly modified versions of other techniques and, therefore, are essentially duplicates. Others have a very limited and narrow scope and are, therefore, only useful in very rare applications.

Of the many different hazard analysis techniques that have been developed, there are seven specific prime techniques that have established themselves as providing the core for complete hazard identification and evaluation. These seven prime techniques probably account for 90 percent of the hazard analysis that is required by a system safety program, and each of the prime techniques correlates directly with one of the analysis types.

TABLE 26.1 Analysis Techniques Applicable to the Analysis Types

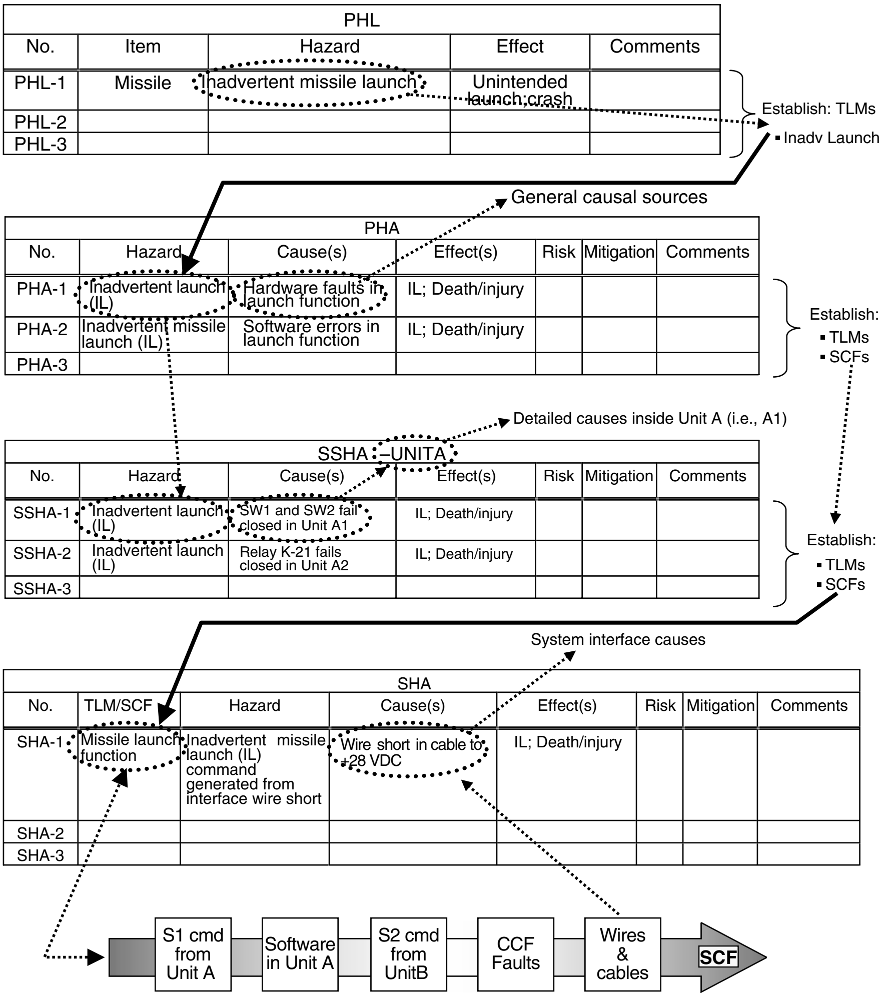
Analysis Type	Primary Analysis Technique	Major Supporting Techniques	
CD-HAT	PHL	None	
PD-HAT	PHA	FuHA	BA
		SWHA	HAZOP
DD-HAT	SSHA	FMEA	BPA
		FaHA	BA
		FuHA	MA
		FTA	PNA
		SCA	SWSA
SD-HAT	SHA	FTA	MA
		ETA	PNA
		SCA	SWSA
		BPA	MORT
		BA	CCA
		FuHA	CCFA
OD-HAT	O&SHA	None	
HD-HAT	HHA	O&SHA	
RD-HAT	SRCA	None	

Table 26.1 correlates alternative analysis techniques that can be used to accomplish each analysis type. The primary analysis technique column identifies those techniques that will meet the analysis type requirement completely. The supporting techniques column identifies those analysis techniques that can be used to support the primary analysis type, but alone they are not sufficient to satisfy the analysis type requirements. Of the many techniques in existence, the ones listed here are the most commonly used in the system safety discipline and they form the safety practitioners' toolbox.

There is a unique relationship between four of the prime hazard analysis techniques, as shown in Figure 26.5. Each of these techniques is a building block for the previous one, beginning with the PHL. Top-level mishap (TLM) information from the PHL is used to identify hazards in the PHA. Hazards identified in the PHA are carried into the SSHA for identification of detailed root causal factors. TLM and SCF identified in the PHL, PHA, and SSHA are used to help identify system interface hazards in the SHA.

26.8 FINIS

Remember, absolute safety is not possible because complete freedom from all hazardous conditions is not possible, particularly when dealing with inherently hazardous systems. Hazards will exist, but their risk can and must be made acceptable. Safety is an optimized level of mishap risk that is managed and constrained by cost, time, and operational effectiveness (performance). System safety requires that risk be



PHL				
No.	Item	Hazard	Effect	Comments
PHL-1	Missile	Inadvertent missile launch	Unintended launch;crash	
PHL-2				
PHL-3				

PHA						
No.	Hazard	Cause(s)	Effect(s)	Risk	Mitigation	Comments
PHA-1	Inadvertent launch (IL)	Hardware faults in launch function	IL; Death/injury			
PHA-2	Inadvertent missile launch (IL)	Software errors in launch function	IL; Death/injury			
PHA-3						

SSHA –UNITA						
No.	Hazard	Cause(s)	Effect(s)	Risk	Mitigation	Comments
SSHA-1	Inadvertent launch (IL)	SW1 and SW2 fail closed in Unit A1	IL; Death/injury			
SSHA-2	Inadvertent launch (IL)	Relay K-21 fails closed in Unit A2	IL; Death/injury			
SSHA-3						

SHA							
No.	TLM/SCF	Hazard	Cause(s)	Effect(s)	Risk	Mitigation	Comments
SHA-1	Missile launch function	Inadvertent missile launch (IL) command generated from interface wire short	Wire short in cable to +28 VDC	IL; Death/injury			
SHA-2							
SHA-3							

Figure 26.5 *Prime hazard analysis relationships.*

evaluated and the level of risk accepted or rejected by an appropriate authority within the organization. Mishap risk management is the basic origin of system safety's requirement for both engineering and management functions. System safety is a process of disciplines and controls employed from the initial design steps through system disposal or demilitarization.

System safety is an investment rather than an expense of doing business. By proactively applying system safety during system development, future potential mishaps are eliminated and reduced. The overall cost of a system safety program is significantly less than the cost of one or more mishaps that could be experienced during the life of a system. Mishap costs are calculated in terms of money, time, lives, environmental damage, publicity, and public relations.

Hazard analysis is the core of system safety, and understanding when and which hazard analysis techniques to apply, and how to correctly apply the technique, is crucial in the system safety discipline. The 7 prime techniques described in this book are used a majority of the time, while the remaining 15 techniques described herein are used for supporting analyses and special-purpose situations.

Appendix A

List of Acronyms

AIAG	Automotive Industry Action Group
ALARP	as low as reasonably practical
ASME	American Society of Mechanical Engineers
ASQC	American Society for Quality Control
BA	barrier analysis
BB	Birnbaum
BE	basic events
BF	beta factor
BFR	binomial failure rate
BP	basic parameter
BPA	bent pin analysis
CAD	computer-aided design
CC	control code
CCA	cause–consequence analysis
CCBE	common cause basic event
CCD	cause–consequence diagram
CCF	common cause failure
CCFA	common cause failure analysis
CD-HAT	conceptual design hazard analysis type
CDR	critical design review
CE	condition events

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

CFMA	cable failure matrix analysis
CIL	critical item list
CM	configuration management
CMF	common mode failure
COTS	commercial off the shelf
CPU	central processing unit
CS	cut set
CSCI	computer software configuration item
CS&R	codes, standards, and regulations
CSU	computer software unit
DC	direct current
DD-HAT	detailed design hazard analysis type
DFT	dynamic fault tree
DN	did not
DoD	Department of Defense
EEG	evidence event gate
EMI	electromagnetic interference
EMR	electromagnetic radiation
EOD	explosives ordnance disposal
ET	event tree; exposure time
ETA	event tree analysis
ETBA	energy trace and barrier analysis
ETD	event tree diagram
FaHA	fault hazard analysis
FBD	functional block diagram
FDEP	functional dependency
FFD	functional flow diagram
FMEA	failure mode and effects analysis
FMECA	failure mode and effects and criticality analysis
FMRI	final mishap risk index
FT	fault tree; failed to (MORT)
FTA	fault tree analysis
FuHA	functional hazard analysis
FV	Fussell–Vesely
GHA	gross hazard analysis
HAP	hazard analysis process
HAR	hazard action record
HAZOP	hazard and operability

HAZOPS	hazard and operability study
HCF	hazard causal factor
HCM	hazard control method
HCR	hazard control record
HD-HAT	health design hazard analysis type
HE	hazardous element
HF	human factors
HHA	health hazard assessment
HMI	human machine interface
HSI	human system integration
HTS	hazard tracking system
HWCI	hardware configuration item
ICI	Institute of Chemical Industry
IE	initiating event
IEL	indentured equipment list
IM	initiating mechanism
IMRI	inital mishap risk index
INEL	Idaho National Engineering Laboratory
IPT	integrated product team
ITL	indentured task list
JSA	job safety analysis
LRU	line replaceable units
LTA	less than adequate
MA	Markov analysis
MCS	minimal cut set
MGL	multiple Greek letter
MOB	multiple occurring branch
MOCUS	method of obtaining cut sets
MOE	multiple occurring event
MORT	management and oversight risk tree
MOV	motor-operated valves
MRI	mishap risk index
MSDS	material safety data sheets
MTBF	mean time between failures
NDI	nondevelopmental item
O&SHA	operating & support hazard analysis
OD-HAT	operations design hazard analysis type
OHA	operating hazard analysis

OS	operating system
OSD	operational sequence diagrams
OSHA	Occupational Safety and Health Administration
PD-HAT	preliminary design hazard analysis type
PDR	preliminary design review
PE	pivotal events
PFS	principal for safety
PHA	preliminary hazard analysis
PHL	preliminary hazard list
PHS&T	packaging, handling, storage, and transportation
PM	program manager
PNA	Petri net analysis
PRA	probabilistic risk assessment
RAW	risk achievement worth
RBD	reliability block diagrams
RCA	root cause analysis
RF	radio frequency
RFI	radio frequency interference
RG	reachability graphs
RHA	requirements hazard analysis
RHR	residual heat removal
RPN	risk priority number
RRW	risk reduction worth
SAE	Society of Automotive Engineers
SAR	safety assessment report
SBP	software build plan
SC	safety critical
SCA	sneak circuit analysis
SCF	safety critical function
SDF	software development file
SD-HAT	system design hazard analysis type
SDP	software development plan
SDR	system design review
SHA	system hazard analysis
SHRI	software hazard risk index
SLOC	source lines of code
SOO	statement of objective
SOW	statement of work

SPF	single-point failure
SPR	software problem report
SRCA	safety requirement/criteria analysis
SSCA	software sneak circuit analysis
SSHA	subsystem hazard analysis
SSMP	system safety management plan
SSP	system safety program
SSPP	system safety program plan
SSR	system safety requirements
STP	software test plan
STR	software trouble report
SUM	software user manual
SWHA	software hazard analysis
SWSA	software safety assessment
SWSSP	software system safety program
TE	transfer events
T/T	transfer of threat
TLM	top-level mishap
UE	undesired event
VVD	version description document
WBS	work breakdown structure
WCS	weapon control system

Appendix B

Glossary

Acceptable risk That part of identified mishap risk that is allowed to persist without taking further engineering or management action to eliminate or reduce the risk, based on knowledge and decision making. The system user is consciously exposed to this risk.

Accepted risk Accepted risk has two parts: (1) risk that is knowingly understood and accepted by the system developer or user and (2) risk that in not known or understood and is accepted by default.

Accident Unexpected event that culminates in the death or injury of personnel, system loss, or damage to property, equipment, or the environment.

Accident scenario Series of events that ultimately result in an accident. The sequence of events begins with an initiating event and is (usually) followed by one or more pivotal events that lead to the undesired end state.

As low as reasonably practical (ALARP) Level of mishap risk that has been established and is considered as low as reasonably possible and still acceptable. It is based on a set of predefined ALARP conditions and is considered acceptable.

Barrier analysis (BA) Analysis technique for identifying hazards specifically associated with hazardous energy sources. BA provides a tool to evaluate the unwanted flow of (hazardous) energy to targets (personnel or equipment) through the evaluation of barriers preventing the hazardous energy flow. BA is based on the theory that when hazardous energy sources exist within a system they pose a hazardous threat to certain targets. Placing barriers between the energy source

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

and the target can mitigate the threat to targets. BA is performed according to an established set of guidelines and rules.

Bent pin analysis (BPA) Specialized analysis of pins within a connector to determine the safety impact of potential bent pins within the connector. A bent pin is a pin inside a connector that is bent sideways while two connectors are otherwise normally mated. The concern with a bent pin is that it makes electrical contact with another pin or the connector casing during system operation. If this should occur, it is possible to cause open circuits and/or short circuits to +/− voltages, which may be hazardous in certain system designs.

Cascading failure Failure event for which the probability of occurrence is substantially increased by the existence of a previous failure. Cascading failures are dependent events, where the failure of one component causes the failure of the next component in line, similar to the falling domino effect.

Combinatorial model Graphical representation of a system that logically combines system components together according to the rules of the particular model. Various types of combinatorial models that are available include reliability block diagrams (RBDs), fault trees (FTs), and success trees.

Commercial off the shelf (COTS) Item that can be purchased commercially from a vendor's catalog. No development or manufacturing is required.

Common cause component group (CCCG) Group of components that share a common coupling factor.

Common cause failure (CCF) Failure (or unavailable state) of more than one component due to a shared cause during system operation. Viewed in this fashion, CCFs are inseparable from the class of dependent failures. An event or failure, which bypasses or invalidates redundancy or independence (ARP-4761).

A CCF is the simultaneous failure of multiple components due to a common or shared cause. For example, when two electrical motors become inoperable simultaneously due to a common circuit breaker failure that provides power to both motors. CCFs include CMFs, but CCF is much larger in scope and coverage. Components that fail due to a shared cause normally fail in the same functional mode. CCFs deal with causes other than just design dependencies, such as environmental factors, human error, etc. Ignoring the effects of dependency and CCFs can result in overestimation of the level of reliability and/or safety. For system safety, a CCF event consists of item/component failures that meet the following criteria: (1) Two or more individual components fail or are degraded such that they cannot be used when needed, or used safely if still operational. (2) The component failures result from a single shared cause and coupling mechanism.

Common cause failure coupling factor Qualitative characteristic of a group of components or piece parts that identifies them as susceptible to the same causal mechanisms of failure. Such factors include similarity in design, location, environment, mission and operational, maintenance, and test procedures. The coupling factor(s) is part of the root cause for a CCF. The identification of coupling factors enables the analyst to implement defenses against common root cause failure vulnerabilities.

Common cause failure root cause Most basic reason(s) for the component failure, which if corrected, would prevent recurrence. Example CCF root causes include events such as heat, vibration, moisture, etc. The identification of a root cause enables the analyst to implement design defenses against CCFs.

Common mode failure (CMF) Failure of multiple components in the same mode. An event that simultaneously affects a number of elements otherwise considered as being independent. For example, a set of identical resistors from the same manufacturer may all fail in the same mode (and exposure time) due to a common manufacturing flaw. The term CMF, which was used in the early literature and is still used by some practitioners, is more indicative of the most common symptom of the CCF, but it is not a precise term for describing all of the different dependency situations that can result in a CCF event. A CMF is a special case or a subset of a common cause failure.

Computer program Combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions. A computer program is also known as software.

Computer software configuration item (CSCI) Aggregation of software that satisfies and end-use function and is designated for separate configuration management by the developer or acquirer.

Computer software unit (CSU) Element in the design of a CSCI; for example, a major subdivision of a CSCI, a component of that subdivision, a class, object, module, function, routine, or database. Software units may occur at different levels of a hierarchy and may consist of other software units.

Concurrent engineering This method performs several of the development tasks concurrently in an attempt to save development time. This method has a higher probability for technical risk problems since some items are in preproduction before full development and testing.

Critical item list (CIL) List of items that are considered critical for reliable and/or safe operation of the system. The list is usually generated from the failure mode and effects analysis (FMEA).

Deductive analysis Analysis that reasons from the general to the specific to determine the causal factors for how an event actually occurred or how a suspected potential event might occur (example: fault tree analysis). Deduction tends to fill in the holes and gaps in a premise to validate the premise.

Dependence (in design) Design whereby the failure of one item directly causes, or leads to, the failure of another item. This refers to when the functional status of one component is affected by the functional status of another component. CCF dependencies normally stem from the way the system is designed to perform its intended function. Dependent failures are those failures that defeat redundancy or diversity, which are intentionally employed to improve reliability and/or safety.

In some system designs, dependency relationships can be very subtle, such as in the following cases:

a. Standby redundancy—When an operating component fails, a standby component is put into operation, and the system continues to function. Failure of an operating component causes a standby component to be more susceptible to failure because it is now under load.
b. Common loads—When failure of one component increases the load carried by other components. Since the other components are now more likely to fail, we cannot assume statistical independence.
c. Mutually exclusive events—When the occurrence of one event precludes the occurrence of another event.

Dependent event Events are dependent when the outcome of one event directly affects or influences the outcome of a second event (probability theory). To find the probability of two dependent events both occurring, multiply the probability of A and the probability of B after A occurs: $P(\text{A and B}) = P(\text{A}) \bullet P(\text{B}$ given A) or $P(\text{A and B}) = P(\text{A}) \bullet P(\text{B}|\text{A})$. This is known as conditional probability. For example, a box contains a nickel, a penny, and a dime. Find the probability of choosing first a dime and then, without replacing the dime, choosing a penny. These events are dependent. The first probability of choosing a dime is $P(\text{A}) = \frac{1}{3}$. The probability of choosing a penny is $P(\text{B}|\text{A}) = \frac{1}{2}$ since there are now only two coins left. The probability of both is $\frac{1}{3} \bullet \frac{1}{2} = \frac{1}{6}$. Keywords such as "not put back" and "not replace" suggest that events are dependent. Two failure events A and B are said to be dependent if $P(\text{A and B}) \neq P(\text{A})P(\text{B})$. In the presence of dependencies, often, but not always, $P(\text{A and B}) > P(\text{A})P(\text{B})$. This increased probability of two (or more) events is why CCFs are of concern.

Deterministic process Deterministic process or model predicts a single outcome from a given set of circumstances. A deterministic process results in a sure or certain outcome and is repeatable with the same data. A deterministic model is sure or certain and is the antonym of random.

Embedded software Embedded systems are electronic devices that incorporate microprocessors within their implementations. Use of a microprocessor simplifies system design and provides flexibility. Embedded software is usually stored in a read-only memory (ROM) chip, meaning that modification requires replacing or reprogramming the chip.

Energy barrier Any design or administrative method that prevents a hazardous energy source from reaching a potential target in sufficient magnitude to cause damage or injury. Barriers separate the target from the source by various means involving time or space. Barriers can take many forms, such as physical barriers, distance barriers, timing barriers, procedural barriers, etc.

Energy path Path of energy flow from source to target.

Energy source Any material, mechanism, or process that contains potential energy that can be released. The safety concern is that the released energy may cause harm to a potential target. Energy sources generally provide the hazardous element leg of the hazard triangle.

Engineering development model Standard traditional system development lifecycle approach that has been in use for many years. The development and test phase is subdivided into preliminary design, final design, and test for more refinement. Under this model, each phase must be complete and successful before the next phase is entered. This method normally takes the longest length of time because the system is developed in sequential stages. Three major design reviews are conducted for exit from one phase and entry into the next. These are the system design review (SDR), preliminary design review (PDR), and critical design review (CDR). These design reviews are an important aspect of the hazard analysis types.

Error (1) Occurrence arising as a result of an incorrect action or decision by personnel operating or maintaining a system, and (2) a mistake in specification, design or implementation.

Event tree (ET) Graphical model of an accident scenario that yields multiple outcomes and outcome probabilities. ETs are one of the most used tools in a probabilistic risk assessment (PRA).

Fail safe Design feature that ensures the system remains safe, or in the event of a failure, causes the system to revert to a state that will not cause a mishap (MIL-STD-882D).

Failure Departure of an item from its required or intended operation, function, or behavior; problems that users encounter. The inability of a system, subsystem, or component to perform its required function. The inability of an item to perform within previously prescribed limits.

Failure cause Process or mechanism responsible for initiating the failure mode. The possible processes that can cause component failure include physical failure, design defects, manufacturing defects, environmental forces, etc.

Failure effect Consequence(s) a failure mode has on the operation, function, or status of an item and on the system.

Failure mode Failure mode is the manner by which an item fails; the mode or state the item is in after it fails. The way in which the failure of an item occurs.

Failure mode and effects analysis (FMEA) Tool for evaluating the effect(s) of potential failure modes of subsystems, assemblies, components, or functions. It is primarily a reliability tool to identify failure modes that would adversely affect overall system reliability. FMEA has the capability to include failure rates for each failure mode in order to achieve a quantitative probabilistic analysis. Additionally, the FMEA can be extended to evaluate failure modes that may result in an undesired system state, such as a system hazard, and thereby also be used for hazard analysis. FMEA is performed according to an established set of guidelines and rules.

Fault Undesired anomaly in the functional operation of an equipment or system. The occurrence of an undesired state, which may be the result of a failure.

Fault tree analysis (FTA) Systems analysis technique used to determine the root causes and probability of occurrence of a specified undesired event. A fault tree (FT) is a model that logically and graphically represents the various combinations of possible events, faulty and normal, occurring in a system that leads to a previously identified hazard or undesired event. It is performed according to an established set of guidelines, rules, and logic gates to model cause–effect relationships.

Functional hazard analysis (FuHA) Analysis technique used to identify system hazards by the analysis of functions. Functions are the means by which a system operates to accomplish its mission or goals. System hazards are identified by evaluating the safety impact of a function failing to operate, operating incorrectly, or operating at the wrong time. When a function's failure can be determined hazardous, the casual factors of the malfunction should be investigated in greater detail via another root cause analysis. FuHA is performed according to an established set of guidelines and rules.

Guide word Special word used in a hazard and operability (HAZOP) analysis to help guide or focus the analysis. HAZOP uses a set of guide words, such as *more, less, early, late*, etc.

Hardware Object that has physical being. Generally refers to line replaceable units (LRUs), circuit cards, power supplies, etc (SAE ARP-4761).

Hardware configuration item (HWCI) Aggregation of hardware that satisfies an end-use function and is designated for separate configuration control by the acquirer.

Hazard Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment, or property; or damage to the environment (MIL-STD-882D). A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof (SAE ARP-4761).

Hazard causal factor (HCF) Specific items responsible for the existence of a hazard. At a high level the causal factors are the hazardous elements and initiating mechanisms of the hazard. At a more refined level the causal factors are the result of poor or insufficient design, incorrect implementation of a good design, or potential or actual failures that would have to occur in order to result in the condition defined as a hazard.

Hazard control record (HCR) Hazard record employed for hazard tracking; contains all information relevant to the identification, assessment, control, and closing of a hazard.

Hazard triangle A triangle formed by the three components of a hazard, indicating that all three sides are necessary. The triangle is composed of the following three components: (1) Hazardous element (HE)—This is the basic hazardous resource creating the impetus for the hazard, such as a hazardous energy source such as explosives being used in the system. (2) Initiating mechanism (IM)—This is the trigger or initiator event(s) causing the hazard to occur. The IMs cause actualization or transformation of the hazard from a dormant state to an active mishap state. (3) Target and threat (T/T)—This is the person or thing that is vulnerable to injury and/or damage, and it describes the severity of the mishap event. This is the mishap outcome and the expected consequential damage and loss.

Hazard and operability (HAZOP) Technique for identifying and analyzing hazards and operational concerns of a system. It is used primarily in the chemical process industry. HAZOP analysis looks for hazards resulting from identified potential deviations in design operational intent.

Health hazard assessment (HHA) Evaluates the system design and operational procedures to identify hazards strictly involving human health. For example, it would consider the system effect of noise, vibration, toxicity, heat, hazardous materials, etc. on humans. It is performed according to an established set of guidelines and rules.

Human engineering Application of knowledge about human capabilities and limitations to system or equipment design and development to achieve efficient, effective, and safe system performance at minimum cost and manpower, skill, and training demands. Human engineering assures that the system or equipment design, required human tasks, and work environment are compatible with the sensory, perceptual, mental, and physical attributes of the personnel who will operate, maintain, control, and support it (MIL-HDBK-1908A).

Human error Unwanted actions or inactions that arise from problems in sequencing, timing, knowledge, interfaces, and/or procedures that result in deviations from expected standards or norms that places people, equipment, and systems at risk.

Human factors (HF) Body of scientific facts about human characteristics. The term covers all biomedical and psychosocial considerations; it includes, but is not limited to, principles and applications in the areas of human engineering, personnel selection, training, life support, job performance aids, and human performance evaluation (MIL-HDBK-1908A).

Human system integration (HSI) Application of human factors and human engineering to system design to ensure the safe and reliable operation of the system throughout its life cycle. Since personnel are a major component of any system, special design consideration must be given to human performance. The human–machine interface, as well as the human influence on the system must be part of all system design considerations.

Identified risk Known risk that has been determined through the identification and evaluation of hazards.

Incremental development Development process in which a desired capability is identified, an end-state requirement is known, and that requirement is met over time by developing several increments, each dependent on available mature technology. This method breaks the development process into incremental stages in order to reduce development risk. Basic designs, technologies, and methods are developed and proven before more detailed designs are developed.

Indenture level Item levels that identify or describe relative complexity of an assembly or function. The levels progress from the more complex (system) to the simpler (part) divisions (MIL-STD-1629A). Equipment indenture levels are used, for example, to develop equipment hierarchy lists that aid in system understanding.

Independence (in design) Design concept that ensures the failure of one item does not cause the failure of another item. This concept is very important in many safety and reliability analysis techniques due to the impact on logic and mathematics. Many models, such as FTA, assume event independence.

Independent event When the outcome of one event does not influence the outcome of a second event (probability theory). To find the probability of two independent events both occurring, multiply the probability of the first event by the probability of the second event; e.g., $P(\text{A and B}) = P(\text{A}) \bullet P(\text{B})$. For example, find the probability of tossing two number cubes (dice) and getting a 3 on each one. These events are independent; $P(3) \bullet P(3) = \left(\frac{1}{6}\right) \bullet \left(\frac{1}{6}\right) = \frac{1}{36}$. The probability is $\frac{1}{36}$.

Inductive analysis Method that reasons from the specific to the general to determine what overall system effect could result from a component failure (e.g., failure mode and effects analysis). Induction tends to establish a premise from data where the data is not complete enough to entirely validate the premise (more data is necessary).

Initiating event (IE) Failure or undesired event that initiates the start of an accident sequence. The IE may result in a mishap, depending upon successful operation of the hazard countermeasure methods designed into the system.

Interlock Safety interlock is a single device and/or functionality that is part of a larger system function. Its purpose is to prevent the overall system function from being performed until a specified set of safety parameters are satisfied. If a known hazardous state is about to be entered, the interlock interrupts the system function, thereby preventing a mishap. For example, if a hazardous laser is being operated in a locked room with no personnel in the room, a sensor on the door would be a safety interlock that automatically removes power from the laser system when the door is opened by someone inadvertently entering the room.

A safety interlock is also used to prevent a function from performing unintentionally due to possible system failure modes. For example, power to launch a missile would not reach the missile until three separate and independent switches are closed. These switches are considered three independent interlocks that significantly reduce the probability of preventing inadvertent launch due to random failures. An interlock is like a temporary barrier that prevents a functional path from being completed until desired.

Latent failure Failure that is not detected and/or annunciated when it occurs. A latent failure of a backup system means the user is not aware that the backup has failed.

Markov analysis (MA) Analysis and evaluation of systems using Markov chains and Markov processes. MA provides a combinatorial-type analysis of components that is useful for dependability and reliability studies.

Markov chain Sequence of random variables in which the future variable is determined by the present variable, but is independent of the way in which the present state arose from its predecessors (the future is independent of the past given the present). The Markov chain assumes discrete states and a discrete time parameter, such as a global clock.

Markov process Assumes states are continuous. The Markov process evaluates the probability of jumping from one known state into the next logical state until the system has reached the final state. For example, the first state is everything in the system working, the next state is the first item failed, and this continues until the final system failed state is reached. The behavior of this process is that every state is memoryless, meaning that the future state of the system depends only on its present state. In a stationary system the probabilities that govern the transitions from state to state remain constant, regardless of the point in time when the transition occurs.

Mishap Unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (MIL-STD-882D).

Mishap risk Expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence (MIL-STD-882D).

Mitigation Action taken to reduce the risk presented by a hazard, by modifying the hazard in order to decrease the mishap probability and/or the mishap severity. Mitigation is generally accomplished through design measures, use of safety devices, warning devices, training, or procedures. It is also referred to as hazard mitigation and risk mitigation.

Multitasking software Task is a job to be done by the software. Multitasking is the process of performing multiple tasks (or threads) concurrently and switching back and forth between them. Since most computers utilize a single central processing unit (CPU), they can only perform a single task at a time. Multitasking only gives the appearance of concurrent operation of tasks (or threads).

Mutually exclusive events Two events are mutually exclusive if the occurrence of one event precludes the occurrence of the other. For example, if the event “switch A fails closed” occurs, then the event “switch A fails open” cannot possibly occur. The switch cannot be in both states simultaneously.

Network trees Diagram that represents a simplified version of the system circuitry, created by selective deletion of extraneous circuitry detail to reduce system complexity, while retaining all circuit elements pertinent. Used in sneak circuit analysis.

Nondevelopmental item (NDI) Already developed item that is provided from another system or development program. No development or manufacturing is required for the current program using the NDI item.

Operating & support hazard analysis (O&SHA) Performed to identify and evaluate operational-type hazards. It is based upon detailed design information and is an evaluation of operational tasks and procedures. It considers human system integration (HSI) factors such as human error, human task overload, cognitive misperception, the effect on humans of hardware failure, etc. The O&SHA establishes the necessary cautions and warnings, which are included in the operational procedures. Occasionally, the O&SHA necessitates design changes or workarounds. It is performed according to an established set of guidelines and rules.

Operating system (OS) Overarching program that guides and controls the operation of a computer. The OS manages processor time, memory utilization, application programs, concurrent threads, etc.

Operation Performance of procedures to meet an overall objective. For example, a missile maintenance operation may be "replacing missile battery." The objective is to perform all the necessary procedures and tasks to replace the battery.

Pivotal events Intermediary events between an initiating event (IE) and the final mishap. These are the failure/success events of the design safety methods established to prevent the IE from resulting in a mishap. If a pivotal event works successfully, it stops the accident scenario and is referred to as a mitigating event. If a pivotal event fails to work, then the accident scenario is allowed to progress and is referred to as an aggravating event.

Preliminary hazard analysis (PHA) Generally the first rigorous analysis that is performed to identify hazards, hazard causal factors, mishaps, and system risk. It is usually performed during the preliminary design phase and is therefore considered preliminary in nature. It is performed according to an established set of guidelines and rules. The PHA begins with hazards identified from the PHL and expands upon them. The PHA is system oriented and generally identifies system-level hazards.

Preliminary hazard list (PHL) Analysis that results in the generation of a list of hazards. This list is considered preliminary because it is the first hazard analysis performed, and it is generally performed early in the system development process when only conceptual information is available. The PHL analysis is more of a brainstorming type of analysis intended to quickly focus on hazards that can be expected by the conceptual design.

Probabilistic risk assessment (PRA) Comprehensive, structured, and logical analysis method for identifying and evaluating risk in a complex technological system. The detailed identification and assessment of accident scenarios with a quantitative analysis providing an assessment of mishap risk.

Procedure Set of tasks that must be performed to accomplish an operation. Tasks within a procedure are designed to be followed sequentially to properly and safely accomplish the operation. For example, a battery replacement operation may be comprised of two primary procedures: (1) battery removal and (2) battery replacement. Each of these procedures contains a specific set of tasks that must be performed.

Qualitative analysis Analysis or evaluation based on qualitative values. Mathematical calculations are generally not involved; however, qualitative indices may be combined. A qualitative result is produced, which is considered subjective and/or fuzzy.

Quantitative analysis Analysis or evaluation based on numerical values and/or mathematical calculations. A quantitative result is produced, which is considered objective and concrete.

Reachability System can have many different possible states; reachability refers to the systems capability to reach any or all of those states during operation. As designed, the system may not be able to reach some states.

Real-time kernel Many embedded systems use a real-time kernel, which is a small segment of code that manages processor time and memory utilization among a number of concurrent threads.

Real-time software Real-time system is one that controls an environment by receiving data, processing them, and returning results sufficiently fast to affect the environment at that time. In a real-time system, response time is a critical element and performance deadlines are dependent on many factors.

Redundancy Design methodology using multiple identical components, such that if one component fails the next one will perform the function. This methodology creates a higher functional reliability. Multiple independent means are incorporated to accomplish a given function.

Reliability Probability that an item will perform a required function under specified conditions, without failure, for a specified period of time. A built-in system characteristic.

Repair Capability to physically repair a failed component, item, subsystem, or system and restore it to an operational state.

Requirement Identifiable element of a specification that can be validated and against which an implementation can be verified (SAE ARP-4761).

Residual risk Overall risk remaining after system safety mitigation efforts have been fully implemented. It is, according to MIL-STD-882D, "the remaining mishap risk that exists after all mitigation techniques have been implemented or exhausted, in accordance with the system safety design order of precedence." Residual risk is the sum of all risk after mishap risk management has been applied. This is the total risk passed on to the user.

Reusable software Software that has been separately developed but is considered usable for the present application, usually as-is without modification.

Risk Exposure to possible loss or injury; danger (dictionary). Risk refers to the measure of expected loss presented by a potential event, such as a financial failure event, a schedule failure event, or a mishap event. In system safety it refers to mishap risk, where risk $=$ probability $\times$ severity.

Risk analysis Risk analysis is the process of identifying safety risk. This involves identifying hazards that present mishap risk with an assessment of the risk.

Risk assessment Process of determining the risk presented by the identified hazards. This involves evaluating the identified hazard causal factors and then characterizing the risk as the product of the hazard severity times the hazard probability.

Risk communication Interactive process of exchanging risk information and opinions among stakeholders.

Risk management Process by which assessed risks are mitigated, minimized, or controlled through engineering, management, or operational means. This involves the optimal allocation of available resources in support of safety, performance, cost, and schedule.

Risk priority number (RPN) Risk ranking index for reliability, where RPN = (probability of occurrence) × (severity ranking) × (detection ranking).

Root cause analysis (RCA) Process of identifying the basic lowest level causal factors for an event. Usually the event is an undesired event, such as a hazard or mishap. There are different analysis techniques available for RCA.

Safety Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (MIL-STD-882). The ability of a system to exclude certain undesired events (i.e., mishaps) during stated operation under stated conditions for a stated time. The ability of a system or product to operate with a known and accepted level of mishap risk. A built-in system characteristic.

Safety case System developer's defense that a system is safe for service. Shows how all of the stages of the safety engineering and management process have resulted in the assurance of a safe system, with evidence (artifacts) provided to support the conclusions.

Safety critical (SC) Term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (e.g., safety critical function, safety critical path, or safety critical component) (MIL-STD-882D).

Safety critical function (SCF) Function comprised of hardware, software, and/or HSI, whose correct operation is necessary and essential for safe system operation. The definition of safe system operation may be program or system dependent, but generally it means operation precluding the occurrence of mishaps that will result in death/injury and/or system loss. Therefore, an SCF is any function whose failure or misbehavior could result in death/injury and/or system loss.

Safety related Term applied to any condition, event, operation, process, or item that does not meet the definition of safety critical but causes an increase in risk.

Safety requirements/criteria analysis (SRCA) Used for evaluating system safety requirements (SSRs) and the criteria behind them. SRCA has a twofold purpose: (1) to ensure that every identified hazard has at least one corresponding safety requirement, and (2) to verify that all safety requirements are implemented and are validated successfully. The SRCA is essentially a traceability analysis to ensure that there are no holes or gaps in the safety requirements and that all identified hazards have adequate and proven design mitigation coverage. The SRCA applies to hardware, software, firmware, and test requirements.

SCF thread Refers to the items (functions, components, etc.) comprising the SCF that are necessary for the successful performance of the SCF. Quite often, but not always, a SCF thread is the inverse of a significant top-level mishap. For example, the TLM "inadvertent missile launch" indirectly establishes the SCF "missile launch function." It becomes an SCF because everything in that SCF thread must work correctly for safe system operation. This thread contains all of the elements whose failure might contribute to the TLM.

Semi-Markov process Similar to that of a pure Markov model, except the transition times and probabilities depend upon the time at which the system reached the present state. The semi-Markov model is useful in analyzing complex dynamical systems and is frequently used in reliability calculations.

Sneak circuit Latent path or condition in an electrical system that inhibits a desired condition or initiates an unintended or unwanted action through normal system operation, without failures involved.

Sneak clues Checklist of items or clues that helps the analyst identify a sneak. The analyst compares the clues to the network tree and topograph to recognize sneaks. The clue list has been developed from past experience and research.

Software Computer programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system (ARP 4761).

Software build Version of software that meets a specified set of the requirements. A final system may be developed in several incremental builds. Builds are often necessary to correct anomalies and/or deficiencies or to incorporate new enhancements.

Software build plan (SBP) Document describing the overall plan for building software in incremental builds. This plan includes a schedule and the build naming convention that will be used. It is useful in software safety analysis.

Software configuration management (CM) plan Document that defines the software configuration management process. It is critical that rigorous control be maintained over the various software builds and versions and that software cannot be modified without following the appropriate authority and control measures. It is useful in software safety analysis.

Software development file (SDF) Repository for material pertinent to the development of a particular body of software. Contents typically include (either directly or by reference) considerations, rationale, and constraints related to requirements analysis, design, and implementation; developer–internal test information; and schedule and status information. It is useful in software safety analysis.

Software development plan (SDP) Document that describes the software engineering tasks that must be performed in developing the software. It includes tools, definitions, constraints, etc. It is useful in software safety analysis.

Software engineering standard Standard delineating the software development method, practices, coding rules, etc. for the development of software within that organization. It is useful in software safety analysis.

Software problem report (SPR) Documents software problems or anomalies identified during formal testing. Also known as a software trouble report. It is useful in software safety analysis.

Software test plan (STP) Document contains the plan for software testing, particularly CSCI qualification testing. The STP includes test objectives, qualification methods, and provides traceability from requirements to specific tests. It is useful in software safety analysis.

Software threads Sequence of instructions designed to perform a single task. A single task may be partitioned into one or more threads running concurrently, but a single thread may also contribute to the objective of one or more tasks. Separating the code into threads simplifies software development and maintenance by allowing the programmer to concentrate on one task at a time.

Software trouble report (STR) Documents software problems or anomalies identified during formal testing. Also known as a software problem report. It is useful in software safety analysis.

Software user manual (SUM) Document that records information needed by hands-on users of the software (persons who will both operate the software and make use of its results). It is useful in software safety analysis.

Specification Collection of requirements that, when taken together, constitute the criteria that define the functions and attributes of a system or an item (SAE ARP-4761).

Spiral development Process in which a desired capability is identified, but the end-state requirements are not known at program initiation. Requirements are refined through demonstration, risk management, and continuous user feedback. Each increment provides the best possible capability, but the requirements for future increments depend on user feedback and technology maturation.

State Condition of a component or system at a particular point in time (i.e., operational state, failed state, degraded state, etc.).

State transition diagram Directed graph representation of system states, transitions between states, and transition rates. These diagrams contain sufficient information for developing the state equations, which are used for probability calculations in Markov analysis.

Stochastic process Process or model that predicts a set of possible outcomes weighted by their likelihoods or probabilities. A stochastic process is a random or chance outcome.

Subsystem Grouping of items satisfying a logical group of functions within a particular system (MIL-STD-882D).

Subsystem hazard analysis (SSHA) Generally the second rigorous analysis that is performed to identify hazards, hazard causal factors, mishaps, and system risk. It is usually performed during the detailed design phase and is performed according to an established set of guidelines and rules. The SSHA begins with hazards identified by the PHA and expands upon their casual factors. The SSHA is limited to hazards within the subsystem under analysis.

System Composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement (MIL-STD-882C).

System hazard analysis (SHA) Performed to identify and evaluate system-level hazards that are generally the result of subsystem interface issues. It is based upon detailed design information and is performed according to an established set of guidelines and rules. Often a special-purpose analysis is performed to support the SHA. For example, a fault tree analysis might be performed to quantitatively evaluate a system hazard of inadvertent missile launch. The SHA is system focused and does not look into hazards that are strictly within a subsystem.

System life cycle Typically defined as the stages of conceptual design, preliminary design, detailed design, test, manufacture, operation, and disposal (demilitarization). The operational stage is usually the longest and can be 30 to 50 years or longer.

System safety Application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle (MIL-STD-882). The application of engineering and management processes during system development to intentionally design-in safety in order to prevent mishaps or reduce the risk of a mishap to an acceptable level.

System safety program (SSP) Combined tasks and activities of system safety management and system safety engineering implemented during system development to develop a safe system.

System safety program plan (SSPP) Description of the planned tasks and activities to be used by a contractor to implement a system safety program. This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

Task Element of work, which together with other elements of work comprises a procedure. For example, battery removal may consist of a series of sequential elements of work, such as power shutdown, compartment cover removal, removal of electrical terminals, unbolting of battery hold-down bolts, and battery removal.

Top-level mishap (TLM) Generic mishap category for collecting various hazards that share the same general outcome or type of mishap. A TLM is a significant mishap that can be caused by multiple different hazards. Its purpose is to serve as a collection point for all the potential hazards that can result in the same outcome but have different causal factors.

Topograph Patterns that appear in a network tree. Used in sneak circuit analysis.

Total risk Sum of individual identified risks (what is known) and unidentified risks (what is unknown).

Unacceptable risk That risk that cannot be tolerated.

Unidentified risk Unknown risk that has not been detected. It is real, and it is important, but it has not been recognized. Some unidentified risks are only subsequently identified when a mishap occurs. Some risks are never known (i.e., the probability is so small they never happen).

Validation Determination that the requirements for a product are sufficiently correct and complete.

Verification Evaluation of an implementation to determine that the applicable requirements are met.

Version description document (VDD) Description of a unique release or build of the software. This document is basically a “packing list” of what is included in the release. It is useful in software safety analysis.

Appendix C

Hazard Checklists

This chapter contains system safety hazard checklists from many different sources. Hazard checklists are an invaluable aid for assisting the system safety analyst in identifying hazards. For this reason, more the checklists are available greater will be the likelihood of identifying all hazards.

In performing a hazard analysis, the analyst compares design knowledge and information to hazard checklists. This allows the analyst to visualize or postulate possible hazards. For example, if the analyst discovers that the system design will be using jet fuel, he then compares jet fuel to a hazard checklist. From the hazard checklist it will be obvious that jet fuel is a hazardous element and that a jet fuel fire/explosion is a potential mishap with many different ignition sources presenting many different hazards.

The hazard checklist should not be considered a complete, final, or all-inclusive list. Hazard checklists help trigger the analyst's recognition of potential hazardous sources, from past lessons learned. Hazard checklists are not a replacement for good engineering analysis and judgment. A checklist is merely a mechanism or catalyst for stimulating hazard recognition.

When using multiple hazard checklists redundant entries may occur. However, this nuisance factor should be overlooked for the overall value provided by many different clues.

Table C.1 lists the checklists included in Appendix C.

C.1 GENERAL HAZARDS CHECKLIST

This checklist is a general list of possible hazards sources. When performing a hazard analysis, each of these items should be considered for hazardous impact

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

TABLE C.1 Hazard Checklist in Appendix C

Section	Title
C.1	General Hazards Checklist
C.2	Hazard Checklist for Energy Sources
C.3	Hazard Checklist for General Sources
C.4	Hazard Checklist for Space Functions
C.5	Hazard Checklist for General Operations
C.6	Operational Hazard Checklist
C.7	Hazard Checklist for Failure States

within the system. The source for this checklist is NASA Reference Publication 1358, *System Engineering "Toolbox" for Design Oriented Engineers*, 1994.

Acceleration/Deceleration/Gravity

□ Inadvertent motion
□ Loose object translation
□ Impacts
□ Falling objects
□ Fragments/missiles
□ Sloshing liquids
□ Slip/trip
□ Falls

Chemical/Water Contamination

□ System–cross connection
□ Leaks/spills
□ Vessel/pipe/conduit rupture
□ Backflow/siphon effect

Common Causes

□ Utility outages
□ Moisture/humidity
□ Temperature extremes
□ Seismic disturbance/impact
□ Vibration
□ Flooding
□ Dust/dirt
□ Faulty calibration
□ Fire

□ Single-operator coupling
□ Location
□ Radiation
□ Wear-out
□ Maintenance error
□ Vermin/varmints/mud daubers

Contingencies (Emergency Responses by System/Operators to “Unusual” Events)

□ “Hard” shutdowns/failures
□ Freezing
□ Fire
□ Windstorm
□ Hailstorm
□ Utility outrages
□ Flooding
□ Earthquake
□ Snow/ice load

Control Systems

□ Power outage
□ Interferences (EMI/RFI)
□ Moisture
□ Sneak circuit
□ Sneak software
□ Lightning strike
□ Grounding failure
□ Inadvertent activation

Electrical

□ Shock
□ Burns
□ Overheating
□ Ignition of combustibles
□ Inadvertent activation
□ Power outage
□ Distribution backfeed
□ Unsafe failure to operate

□ Explosion/electrical (electrostatic)
□ Explosion/electrical (arc)

Mechanical

□ Sharp edges/points
□ Rotating equipment
□ Reciprocating equipment
□ Pinch points
□ Lifting weights
□ Stability/topping potential
□ Ejected parts/fragments
□ Crushing surfaces

Pneumatic/Hydraulic Pressure

□ Overpressurization
□ Pipe/vessel/duct rupture
□ Implosion
□ Mislocated relief device
□ Dynamic pressure loading
□ Relief pressure improperly set
□ Backflow
□ Crossflow
□ Hydraulic ram
□ Inadvertent release
□ Miscalibrated relief device
□ Blown objects
□ Pipe/hose whip
□ Blast

Temperature Extremes

□ Heat source/sink
□ Hot/cold surface burns
□ Pressure evaluation
□ Confined gas/liquid
□ Elevated flammability
□ Elevated volatility
□ Elevated reactivity
□ Freezing

□ Humidity/moisture
□ Reduced reliability
□ Altered structural properties (e.g., embrittlement)

Radiation (Ionizing)

□ Alpha
□ Beta
□ Neutron
□ Gamma
□ X-Ray

Radiation (Nonionizing)

□ Laser
□ Infrared
□ Microwave
□ Ultraviolet

Fire/Flammability—Presence of

□ Fuel
□ Ignition source
□ Oxidizer
□ Propellant

Explosives (Initiators)

□ Heat
□ Friction
□ Impact/shock
□ Vibration
□ Electrostatic discharge
□ Chemical contamination
□ Lightning
□ Welding (stray current/sparks)

Explosives (Effects)

□ Mass fire
□ Blast overpressure
□ Thrown fragments
□ Seismic ground wave
□ Meteorological reinforcement

Explosives (Sensitizes)

□ Heat/cold
□ Vibration
□ Impact/shock
□ Low humidity
□ Chemical contamination

Explosives (Conditions)

□ Explosive propellant present
□ Explosive gas present
□ Explosive liquid present
□ Explosive vapor present
□ Explosive dust present

Leaks/Spills (Material Conditions)

□ Liquid/cryogens
□ Gases/vapors
□ Dusts—irritating
□ Radiation sources
□ Flammable
□ Toxic
□ Reactive
□ Corrosive
□ Slippery
□ Odorous
□ Pathogenic
□ Asphyxiating
□ Flooding
□ Runoff
□ Vapor propagation

Physiological (*See* Ergonomic)

□ Temperature extremes
□ Nuisance dusts/odors
□ Baropressure extremes
□ Fatigue
□ Lifted weights
□ Noise

□ Vibration (Raynaud's syndrome)
□ Mutagens
□ Asphyxiants
□ Allergens
□ Pathogens
□ Radiation (*See* Radiation)
□ Cryogens
□ Carcinogens
□ Teratogens
□ Toxins
□ Irritants

Human Factors (*See* Ergonomic)

□ Operator error
□ Inadvertent operation
□ Failure to operate
□ Operation early/late
□ Operation out of sequence
□ Right operation/wrong control
□ Operated too long
□ Operate too briefly

Ergonomic (*See* Human Factors)

□ Fatigue
□ Inaccessibility
□ Nonexistent/inadequate "kill" switches
□ Glare
□ Inadequate control/readout differentiation
□ Inappropriate control/readout location
□ Faulty/inadequate control/readout labeling
□ Faulty work station design
□ Inadequate/improper illumination

Unannunciated Utility Outages

□ Electricity
□ Steam
□ Heating/cooling
□ Ventilation

□ Air conditioning
□ Compressed air/gas
□ Lubrication drains/slumps
□ Fuel
□ Exhaust

Mission Phasing

□ Transport
□ Delivery
□ Installation
□ Calibration
□ Checkout
□ Shake down
□ Activation
□ Standard start
□ Emergency start
□ Normal operation
□ Load change
□ Coupling/uncoupling
□ Stressed operation
□ Standard shutdown
□ Shutdown emergency
□ Diagnosis/troubleshooting
□ Maintenance

C.2 HAZARD CHECKLIST FOR ENERGY SOURCES

This checklist is a general list of potentially hazardous energy sources. A system that uses any of these energy sources will very likely have various associated hazards. This checklist was collected by C. Ericson.

1. Fuels
2. Propellants
3. Initiators
4. Explosive charges
5. Charged electrical capacitors
6. Storage batteries
7. Static electrical charges
8. Pressure containers

9. Spring-loaded devices
10. Suspension systems
11. Gas generators
12. Electrical generators
13. Radio frequency energy sources
14. Radioactive energy sources
15. Falling objects
16. Catapulted objects
17. Heating devices
18. Pumps, blowers, fans
19. Rotating machinery
20. Actuating devices
21. Nuclear

C.3 HAZARD CHECKLIST FOR GENERAL SOURCES

This is another checklist of general items that often generates hazards within a system. When performing a hazard analysis, each of these items should be considered for hazardous impact within the system. This checklist was collected by C. Ericson.

1. Acceleration
2. Contamination
3. Corrosion
4. Chemical dissociation
5. Electrical
   Shock
   Thermal
   Inadvertent activation
   Power source failure
   Electromagnetic radiation
6. Explosion
7. Fire
8. Heat and temperature
   High temperature
   Low temperature
   Temperature variations
9. Leakage
10. Moisture
    High humidity
    Low humidity

11. Oxidation
12. Pressure
    High
    Low
    Rapid change
13. Radiation
    Thermal
    Electromagnetic
    Ionizing
    Ultraviolet
14. Chemical replacement
15. Shock (mechanical)
16. Stress concentrations
17. Stress reversals
18. Structural damage or failure
19. Toxicity
20. Vibration and noise
21. Weather and environment

C.4 HAZARD CHECKLIST FOR SPACE FUNCTIONS

This is checklist of general space-related functions that generally generates hazards within a system. When performing a hazard analysis each of these items should be considered for hazardous impact within the system. This checklist was collected by C. Ericson.

1. Crew egress/ingress
2. Ground-to-stage power transfer
3. Launch escape
4. Stage firing and separation
5. Ground control communication transfer
6. Rendezvous and docking
7. Ground control of crew
8. Ground data communication to crew
9. Extra vehicular activity
10. In-flight tests by crew
11. In-flight emergencies
    Loss of communications
    Loss of power/control

Fire toxicity
Explosion
Life support

12. Reentry
13. Parachute deployment and descent
14. Crew recovery
15. Vehicle safing and recovery
16. Vehicle inerting and decontamination
17. Payload mating
18. Fairing separation
19. Orbital injection
20. Solar panel deployment
21. Orbit positioning
22. Orbit correction
23. Data acquisition
24. Midcourse correction
25. Star acquisition (navigation)
26. On-orbit performance
27. Retrothrust

C.5 HAZARD CHECKLIST FOR GENERAL OPERATIONS

This is checklist of general operations that often generates hazards within a system. When performing a hazard analysis, each of these items should be considered for hazardous impact within the system. This checklist was collected by C. Ericson.

1. Welding
2. Cleaning
3. Extreme temperature operations
4. Extreme weight operations
5. Hoisting, handling, and assembly operations
6. Test chamber operations
7. Proof test of major components/subsystems/systems
8. Propellant loading/transfer/handling
9. High-energy pressurization/hydrostatic-pneumostatic testing
10. Nuclear component handling/checkout
11. Ordnance installation/checkout/test
12. Tank entry/confined space entry
13. Transport and handling of end item

14. Manned vehicle tests
15. Static firing
16. Systems operational validations

C.6 OPERATIONAL HAZARD CHECKLIST

This is checklist of general operational considerations that often generates hazards within a system. When performing a hazard analysis, each of these items should be considered for hazardous impact within the system. This checklist was collected by C. Ericson.

1. Work area
   Tripping, slipping, corners
   Illumination
   Floor load, piling
   Ventilation
   Moving objects
   Exposed surfaces—hot, electric
   Cramped quarters
   Emergency exits
2. Materials handling
   Heavy, rough, sharp
   Explosives
   Flammable
   Awkward, fragile
3. Clothing
   Loose, ragged, soiled
   Necktie, jewelry
   Shoes, high heels
   Protective
4. Machines
   Cutting, punching, forming
   Rotating shafts
   Pinch points
   Flying pieces
   Projections
   Protective equipment
5. Tools
   No tools

Incorrect tools
Damaged tools
Out-of-tolerance tools

6. Emergency
   Plans, procedures, numbers
   Equipment
   Personnel
   Training
7. Safety Devices
   Fails to function
   Inadequate

C.7 HAZARD CHECKLIST FOR FAILURE STATES

This is checklist of failure modes or failure states that can generate hazards within a system. When performing a hazard analysis, each of these items should be considered for hazardous impact within the system. This checklist was collected by C. Ericson.

1. Fails to operate
2. Operates incorrectly/erroneously
3. Operates inadvertently
4. Operates at incorrect time (early, late)
5. Unable to stop operation
6. Receives erroneous data
7. Sends erroneous data

Index

Accident scenario, 225
ALARP, 467
Amelioration, 425
Analysis Techniques
  Barrier analysis, 335–351
  Bent pin analysis, 353–364
  Cause consequence analysis, 383–395
  Common cause failure analysis, 397–422
  Definition of, 31
  Event tree analysis, 223–234
  Failure mode and effects analysis, 235–259
  Fault hazard analysis, 261–269
  Fault tree analysis, 183–221
  Functional hazard analysis, 271–289
  HAZOP analysis, 365–381
  Health hazard assessment, 155–168
  Markov analysis, 317–333
  MORT analysis, 423–430
  Operating & support hazard analysis, 131–153
  Petri net analysis, 307–316
  Preliminary hazard analysis, 73–93
  Preliminary hazard list, 55–72
  Safety requirements/criteria analysis, 169–181
  Sneak circuit analysis, 291–306
  Software safety assessment, 431–449
  Subsystem hazard analysis, 95–114
  System hazard analysis, 115–129
Analysis Types
  Conceptual design hazard analysis type, 34
  Definition of, 31
  Detailed design hazard analysis type, 37
  Health design hazard analysis type, 41
  Operations design hazard analysis type, 40
  Preliminary design hazard analysis type, 35
  Requirements design hazard analysis type, 42
  System design hazard analysis type, 38
AND gate, 190
Approximation formulas (fault tree), 201, 202
As low as reasonably practical, 467

Barrier, 337, 343
Barrier analysis, 335–351
Bent pin, 354, 355
Bent pin analysis, 353–364
Bottom-up analysis, 49

Cable failure matrix analysis, 353
Cascading failure, 401
Cause consequence analysis, 383–395
Combinatorial model, 319
Commercial off the shelf, 468
Common cause failure, 397, 400
Common cause failure analysis, 397–422
Common mode failure, 400
Common mode failure analysis, 398

Hazard Analysis Techniques for System Safety, by Clifton A. Ericson, II

Conceptual design hazard analysis type, 34
COTS, 468
Critical item list, 238
Cut set, 191

Deductive, 48
Dependent event, 399
Detailed design hazard analysis type, 37
Deterministic process, 319
Development lifecycle, 11
Dynamic fault tree analysis, 218

Energy trace and barrier analysis, 335
Engineering development lifecycle model, 11
Event tree, 223
Event tree analysis, 223–234

Failure, 237
Failure cause, 238
Failure effect, 238
Failure mode, 237
Failure mode and effects analysis, 235–259
Failure mode effects and criticality analysis, 235
Fault, 238
Fault hazard analysis, 261–269
Fault tree, 183
Fault tree analysis, 183–221
Fault tree approximation formulas, 201, 202
Firmware, 433
FMEA, 235–259
FMECA, 235
FTA, 183–221
Function, 6
Functional dependency gate, 218
Functional flow diagram, 83
Functional hazard analysis, 271–289
Functional model, 241

Guide word, 372

Hazard, 15
Hazard actuation, 19, 20
Hazard barrier, 337, 343
Hazard causal factor, 14, 18, 21
Hazard checklist, 25, 62, 483
Hazard components, 17
Hazard example, 18
Hazard mitigation, 475
Hazard theory, 15
Hazard triangle, 17
Hazardous element, 17
HAZOP analysis, 365–381
Health design hazard analysis type, 41
Health hazard assessment, 155–168
HHA, 155–168

Indenture level, 238
Indentured equipment list, 83
Indentured task list, 135, 136
Independent event, 399
Inductive, 48
Initiating event, 225
Initiating mechanism, 17
Inhibit gate, 190
Interlock, 474
Intermittent failure, 243

Less than adequate, 425

Markov analysis, 317–333
Minimal cut set, 191
Mishap, 14
Mishap risk, 16
Mitigation, 475
MORT analysis, 423–430
Mutually exclusive event, 401

NDI, 475
Non developmental item, 475

O&SHA, 131–153
Operating & support hazard analysis, 131–153
Operational sequence diagram, 141, 142
Operations design hazard analysis type, 40
OR gate, 190

Petri net analysis, 307–316
PHA, 73–93
PHA worksheet, 79
PHL, 55–72
PHL worksheet, 61
Pivotal event, 225
Preliminary design hazard analysis type, 35
Preliminary hazard analysis, 73–93
Preliminary hazard list, 55–72
Probabilistic risk assessment, 52, 385, 476
Process FMEA, 242
Product FMEA, 242

Qualitative analysis, 51
Quantitative analysis, 51

Reachability, 309, 312
Requirements design hazard analysis type, 42

Residual risk, 477
Risk, 15, 17
Risk assessment, 478
Risk mitigation, 475
Risk priority number, 238

Safety critical, 478
Safety critical function, 478
Safety critical function thread, 123,124
Safety requirements/criteria analysis, 169–181
SCA, 291–306
SHA, 115–129
SHRI, 435, 438
Sneak, 293
Sneak circuit, 291
Sneak circuit analysis, 291–306
Sneak label, 299, 300
Sneak indicator, 300, 301
Sneak path, 299, 300
Sneak timing, 299, 300
Software, 433
Software FMEA, 243
Software hazard risk index, 435, 438
Software safety assessment, 431–449
SRCA, 169–181
SSHA, 95–114
SSP, 481
SSPP, 481
State, 319
State transition diagram, 319
Stochastic process, 319
Structural model, 241
Subsystem, 480
Subsystem hazard analysis, 95–114
System, 6, 481
System attributes, 7
System design hazard analysis type, 38
System function, 6
System hazard analysis, 115–129
System lifecycle, 9
System safety, 3, 481
System safety process, 4
System safety program, 481
System safety program plan, 481
System safety requirement, 73

Target/threat, 17
Top-down analysis, 49
Top level mishap
Total risk, 482

Validation, 482
Verification, 482