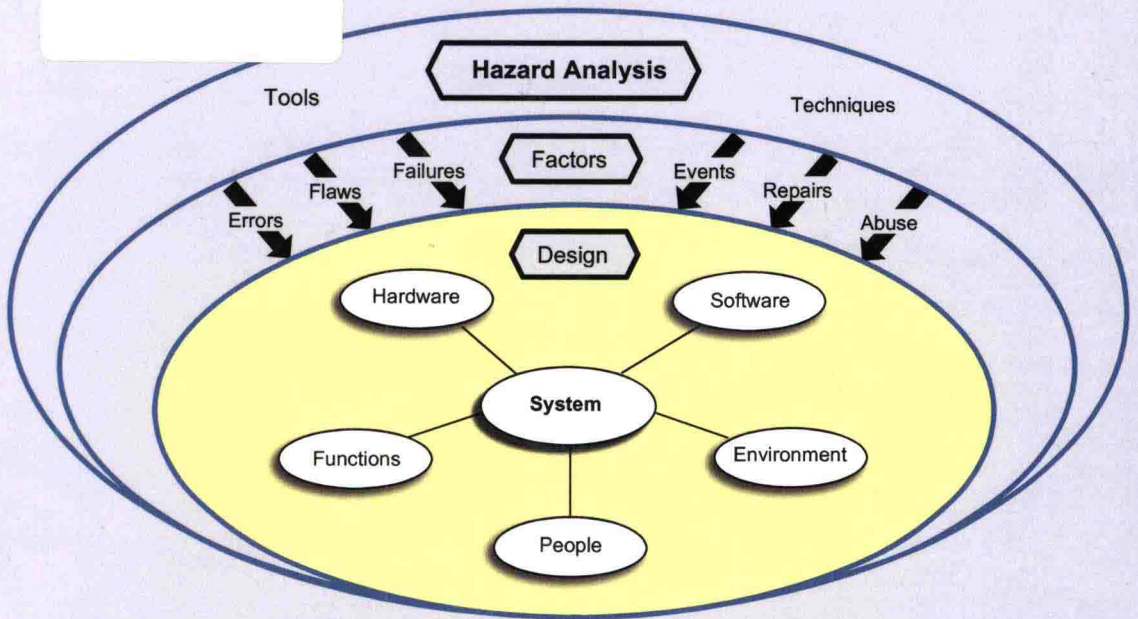


CLIFTON A. ERICSON II



# HAZARD ANALYSIS TECHNIQUES FOR SYSTEM SAFETY

SECOND EDITION

WILEY

*Hazard Analysis  
Techniques for  
System Safety*

Second Edition

**Clifton A. Ericson, II**  
Fredericksburg, Virginia



**WILEY**

Copyright © 2016 by John Wiley & Sons, Inc. All rights reserved

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

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

**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 the 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 or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States 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 may not be available in electronic formats. For more information about Wiley products, visit our web site at [www.wiley.com](http://www.wiley.com).

***Library of Congress Cataloging-in-Publication Data***

Ericson, Clifton A., II.

Hazard analysis techniques for system safety / Clifton A. Ericson, II. –

Second edition.

pages cm

Includes index.

ISBN 978-1-118-94038-9 (hardback)

1. Industrial safety—Data processing. 2. System safety. I. Title.

T55.E72 2015

363.11—dc23

2015016350

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

*Hazard Analysis  
Techniques for  
System Safety*

# *Preface*

During my 50 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. This is significant because risk cannot be determined unless the hazard is fully understood and described. Second, there is a lack of good reference material describing in detail how to perform the most relevant hazard analysis techniques or methodologies. This too is significant because hazard analysis is more complex than most people think, thus good descriptions and reference material are needed. 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 28 of the most commonly used hazard analysis methodologies in the system safety discipline. Each of the 28 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 these 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 saving 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.

This revised version of the book has added eight new chapters, six of which are additional hazard analysis techniques. Also, this updated version has added new and revised material to reflect changes made as a result of the new MIL-STD-882, version E, which was released in 2012.

# *Acknowledgments*

In a book of this undertaking, there are naturally many people to acknowledge. This book reflects my life's journey through 50 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 whom 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.

First and foremost, I would like to dedicate this book to my parents, Clifton Ericson I and Margaret Ericson. They instilled in me many good qualities that I might not have found without them, particularly the values of reading, education, science, religion, morality, and a work ethic.

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 who helped in my development included Dave Haasl, Gordon Willard, Dwight Leffingwell, Kaz Kanda, Brad Wolfe, Joe Muldoon, Harvey Moon, and Bob Schroder. Another Boeing manager who 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 Champine, 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.

# *Contents*

<b>PREFACE</b>	<b>xxi</b>
<b>ACKNOWLEDGMENTS</b>	<b>xxiii</b>
<b>1. System Safety and Hazard Analysis</b>	<b>1</b>
1.1 Introduction / 1	
1.2 The Need for Hazard Analysis / 2	
1.3 System Safety Background / 3	
1.4 System Safety Overview / 4	
1.5 System Safety Process / 6	
1.6 System Safety Standards / 7	
1.7 System Safety Principles / 7	
1.8 Key Terms / 8	
1.9 Summary / 9	
<b>2. Systems</b>	<b>10</b>
2.1 System Concept / 10	
2.2 System Attributes / 12	
2.3 System Types / 13	
2.4 System Life Cycle / 13	
2.5 System Development / 15	
2.6 System Development Process / 16	
2.7 System Hierarchy / 16	
2.8 System Views / 18	

2.9	System Development Artifacts /	19
2.10	Systems Complexity and Safety /	20
2.11	System Requirements /	21
2.12	System Laws /	26
2.13	Summary /	26
<b>3.</b>	<b>Hazards, Mishap, and Risk</b>	<b>28</b>
3.1	Introduction /	28
3.2	Hazard, Mishap, and Risk Definitions /	29
3.3	Accident (Mishap) Theory /	30
3.4	The Hazard–Mishap Relationship /	31
3.5	Hazard Risk /	33
3.6	The Components of a Hazard /	33
3.7	Hazard Triangle /	35
3.8	Hazard Actuation /	35
3.9	Hazard Causal Factors /	37
3.10	Hazard–Mishap Probability Example /	39
3.11	Recognizing Hazards /	40
3.12	Hazard Description /	43
3.13	Hazard Theory Summary /	43
<b>4.</b>	<b>Hazard Analysis Features</b>	<b>45</b>
4.1	Introduction /	45
4.2	Types Versus Technique /	46
4.3	Description of Hazard Analysis Types /	48
4.3.1	Conceptual Design Hazard Analysis Type /	48
4.3.2	Preliminary Design Hazard Analysis Type /	49
4.3.3	Detailed Design Hazard Analysis Type /	51
4.3.4	System Design Hazard Analysis Type /	52
4.3.5	Operations Design Hazard Analysis Type /	53
4.3.6	Human Health Design Hazard Analysis Type (HD-HAT) /	54
4.3.7	Requirements Design Hazard Analysis Type (RD-HAT) /	55
4.4	The Timing of Hazard Analysis Types /	57
4.5	The Interrelationship of Hazard Analysis Types /	57
4.6	Hazard Analysis Techniques /	59
4.7	Hazard Analysis Technique Attributes /	59
4.8	Primary and Secondary Techniques /	59
4.9	Inductive and Deductive Techniques /	63
4.10	Qualitative and Quantitative Techniques /	65
4.11	Summary /	67



**5. Hazard Recognition and Management****69**

- 5.1 Introduction / 69
- 5.2 Hazard Analysis Tasks / 69
  - 5.2.1 Plan the Hazard Analysis / 70
  - 5.2.2 Understand the System Design / 71
  - 5.2.3 Acquire Hazard Analysis Tools / 71
  - 5.2.4 Identify Hazards / 72
  - 5.2.5 Validate Hazards / 72
  - 5.2.6 Assess Risk / 72
  - 5.2.7 Mitigate Risk / 72
  - 5.2.8 Verify Mitigation / 73
  - 5.2.9 Accept Risk / 73
  - 5.2.10 Track Hazards / 73
- 5.3 Hazard Recognition / 74
  - 5.3.1 Hazard Recognition Introduction / 74
  - 5.3.2 Hazard Recognition: System Perspectives / 74
  - 5.3.3 Hazard Recognition: Failure Perspectives / 75
  - 5.3.4 Key Hazard Recognition Factors / 76
  - 5.3.5 Hazard Recognition Basics / 79
  - 5.3.6 Hazard Recognition Sources / 79
- 5.4 Describing the Identified Hazard / 79
- 5.5 Hazard Types by General Circumstances / 81
- 5.6 Hazard Types by Analysis Category / 82
- 5.7 Modelling Hazard Space / 83
  - 5.7.1 System Mishap Model / 84
  - 5.7.2 System Mishap Model Examples / 87
- 5.8 Summary / 92

**6. Functional Hazard Analysis****93**

- 6.1 FHA Introduction / 93
- 6.2 FHA Background / 93
- 6.3 FHA History / 94
- 6.4 FHA Theory / 94
- 6.5 FHA Methodology / 95
- 6.6 FHA Worksheets / 96
- 6.7 FHA Example 1: Aircraft Flight Functions / 99
- 6.8 FHA Example 2: Aircraft Landing Gear Software / 99
- 6.9 FHA Example 3: Ace Missile System / 102
- 6.10 FHA Advantages and Disadvantages / 105
- 6.11 Common FHA Mistakes to Avoid / 105
- 6.12 FHA Summary / 108

<b>7. Preliminary Hazard List Analysis</b>	<b>109</b>
7.1 PHL Introduction /	109
7.2 PHL Background /	109
7.3 PHL History /	110
7.4 PHL Theory /	110
7.5 PHL Methodology /	111
7.6 PHL Worksheet /	114
7.7 Hazard Checklists /	115
7.8 PHL Guidelines /	117
7.9 PHL Example: Ace Missile System /	118
7.10 PHL Advantages and Disadvantages /	121
7.11 Common PHL Mistakes to Avoid /	122
7.12 PHL Summary /	124
<b>8. Preliminary Hazard Analysis</b>	<b>125</b>
8.1 PHA Introduction /	125
8.2 PHA Background /	125
8.3 PHA History /	126
8.4 PHA Theory /	126
8.5 PHA Methodology /	127
8.6 PHA Worksheet /	130
8.7 PHA Guidelines /	132
8.8 PHA Example: Ace Missile System /	133
8.9 PHA Advantages and Disadvantages /	136
8.10 Common PHA Mistakes to Avoid /	136
8.11 PHA Summary /	143
<b>9. Subsystem Hazard Analysis</b>	<b>145</b>
9.1 SSHA Introduction /	145
9.2 SSHA Background /	145
9.3 SSHA History /	146
9.4 SSHA Theory /	146
9.5 SSHA Methodology /	147
9.6 SSHA Worksheet /	149
9.7 SSHA Guidelines /	151
9.8 SSHA Example: Ace Missile System /	152
9.9 SSHA Advantages and Disadvantages /	156
9.10 Common SSHA Mistakes to Avoid /	156
9.11 SSHA Summary /	162

<b>10. System Hazard Analysis</b>	<b>164</b>
10.1 SHA Introduction /	164
10.2 SHA Background /	165
10.3 SHA History /	166
10.4 SHA Theory /	166
10.5 SHA Methodology /	167
10.6 SHA Worksheet /	167
10.7 SHA Guidelines /	170
10.8 SHA Example /	172
10.9 SHA Advantages and Disadvantages /	175
10.10 Common SHA Mistakes to Avoid /	175
10.11 SHA Summary /	176
<b>11. Operating and Support Hazard Analysis</b>	<b>177</b>
11.1 O&SHA Introduction /	177
11.2 O&SHA Background /	177
11.3 O&SHA History /	178
11.4 O&SHA Definitions /	179
11.4.1 Operation /	179
11.4.2 Procedure /	179
11.4.3 Task /	179
11.5 O&SHA Theory /	180
11.6 O&SHA Methodology /	181
11.7 O&SHA Worksheet /	183
11.8 O&SHA Hazard Checklists /	185
11.9 O&SHA Support Tools /	186
11.10 O&SHA Guidelines /	187
11.11 O&SHA Examples /	188
11.11.1 Example 1 /	188
11.11.2 O&SHA Example 2 /	188
11.12 O&SHA Advantages and Disadvantages /	198
11.13 Common O&SHA Mistakes to Avoid /	198
11.14 Summary /	198
<b>12. Health Hazard Analysis</b>	<b>199</b>
12.1 HHA Introduction /	199
12.2 HHA Background /	199
12.3 HHA History /	200
12.4 HHA Theory /	200

- 12.5 HHA Methodology / 201
- 12.6 HHA Worksheet / 204
- 12.7 Human Health Hazard Checklist / 206
- 12.8 HHA Example / 207
- 12.9 HHA Advantages and Disadvantages / 207
- 12.10 Common HHA Mistakes to Avoid / 207
- 12.11 Summary / 211

**13. Requirements Hazard Analysis**

**212**

- 13.1 RHA Introduction / 212
- 13.2 RHA Background / 212
- 13.3 RHA History / 213
- 13.4 RHA Theory / 213
- 13.5 RHA Methodology / 214
- 13.6 RHA Worksheets / 214
- 13.7 RHA Example / 217
- 13.8 RHA Advantages and Disadvantages / 222
- 13.9 Common RHA Mistakes to Avoid / 222
- 13.10 Summary / 222

**14. Environmental Hazard Analysis (EHA)**

**224**

- 14.1 EHA Introduction / 224
- 14.2 EHA Background / 225
- 14.3 EHA History / 226
- 14.4 EHA Theory / 226
- 14.5 EHA Methodology / 227
- 14.6 EHA Worksheet / 230
- 14.7 Example Checklists / 232
- 14.8 EHA Example / 233
- 14.9 EHA Advantages and Disadvantages / 233
- 14.10 Common EHA Mistakes to Avoid / 237
- 14.11 Summary / 237
- 14.12 References / 237
- 14.13 National Environmental Policy Act / 237
- 14.14 Environmental Protection Agency / 238

**15. Fault Tree Analysis**

**240**

- 15.1 FTA Introduction / 240
- 15.2 FTA Background / 242
- 15.3 FTA History / 243
- 15.4 FTA Theory / 243
- 15.5 FTA Methodology / 244

15.5.1	FT Building Blocks /	245
15.5.2	FT Definitions /	247
15.5.3	FT Construction: Basics /	248
15.5.4	FT Construction: Advanced /	251
15.5.5	FT Construction Rules /	252
15.6	Functional Block Diagrams /	253
15.7	FT Cut Sets /	254
15.8	MOCUS Algorithm /	254
15.9	Bottom-Up Algorithm /	256
15.10	FT Mathematics /	256
15.10.1	Probability of Success /	256
15.10.2	Probability of Failure /	256
15.10.3	Boolean Rules for FTA /	256
15.10.4	AND Gate Probability Expansion /	257
15.10.5	OR Gate Probability Expansion /	257
15.10.6	FT Probability Expansion /	257
15.10.7	Inclusion–Exclusion Approximation /	257
15.11	Probability /	258
15.12	Importance Measures /	259
15.12.1	Cut Set Importance /	260
15.12.2	Fussell–Vesely Importance /	260
15.12.3	Risk Reduction Worth /	261
15.12.4	Risk Achievement Worth /	261
15.12.5	Birnbaum’s Importance Measure /	261
15.13	FT Example 1 /	262
15.14	FT Example 2 /	262
15.15	FT Example 3 /	271
15.16	Phase- and Time-Dependent FTA /	271
15.17	Dynamic FTA /	274
15.18	FTA Advantages and Disadvantages /	275
15.19	Common FTA Mistakes to Avoid /	276
15.20	Summary /	276

## **16. Failure Mode and Effects Analysis**

**278**

16.1	FMEA Introduction /	278
16.2	FMEA Background /	278
16.3	FMEA History /	279
16.4	FMEA Definitions /	280
16.5	FMEA Theory /	281
16.5.1	FMEA Structural and Functional Models /	283
16.5.2	FMEA Product and Process FMEA /	283

- 16.5.3 FMEA Functional Failure Modes / 283
- 16.5.4 FMEA Hardware Failure Modes / 284
- 16.5.5 FMEA Software Failure Modes / 285
- 16.5.6 Quantitative Data Sources / 286
- 16.6 Methodology / 286
- 16.7 FMEA Worksheet / 289
- 16.8 FMEA Example 1: Hardware Product FMEA / 292
- 16.9 FMEA Example 3: Functional FMEA / 292
- 16.10 FMEA Level of Detail / 295
- 16.11 FMEA Advantages and Disadvantages / 298
- 16.12 Common FMEA Mistakes to Avoid / 298
- 16.13 FMEA Summary / 298

**17. Hazard and Operability (HAZOP) Analysis**

**300**

- 17.1 Introduction / 300
- 17.2 HAZOP Analysis Background / 301
- 17.3 HAZOP History / 301
- 17.4 HAZOP Theory / 302
- 17.5 HAZOP Methodology / 303
  - 17.5.1 Design Representations / 305
  - 17.5.2 System Parameters / 305
  - 17.5.3 Guide Words / 306
  - 17.5.4 Deviation from Design Intent / 307
- 17.6 HAZOP Worksheet / 309
- 17.7 HAZOP Example 1 / 310
- 17.8 HAZOP Example 2 / 311
- 17.9 HAZOP Advantages and Disadvantages / 311
- 17.10 Common HAZOP Analysis Mistakes to Avoid / 313
- 17.11 HAZOP Summary / 313

**18. Event Tree Analysis (ETA)**

**316**

- 18.1 ETA Introduction / 316
- 18.2 ETA Background / 316
- 18.3 ETA History / 317
- 18.4 ETA Definitions / 317
- 18.5 ETA Theory / 318
- 18.6 ETA Methodology / 320
- 18.7 ETA Worksheet / 323
- 18.8 ETA Example 1 / 323
- 18.9 ETA Example 2 / 323
- 18.10 ETA Example 3 / 324

- 18.11 ETA Example 4 / 324
- 18.12 ETA Advantages and Disadvantages / 324
- 18.13 Common ETA Mistakes to Avoid / 325
- 18.14 Summary / 326

## **19. Cause—Consequence Analysis 327**

- 19.1 Introduction / 327
- 19.2 CCA Background / 327
- 19.3 CCA History / 328
- 19.4 CCA Definitions / 328
- 19.5 CCA Theory / 329
- 19.6 CCA Methodology / 330
- 19.7 CCD Symbols / 331
- 19.8 CCA Worksheet / 332
- 19.9 CCA Example 1: Three-Component Parallel System / 332
- 19.10 CCA Example 2: Gas Pipeline System / 333
  - 19.10.1 Reducing Repeated Events / 335
- 19.11 CCA Advantages and Disadvantages / 337
- 19.12 Common CCA Mistakes to Avoid / 338
- 19.13 Summary / 338

## **20. Common Cause Failure Analysis 339**

- 20.1 Introduction / 339
- 20.2 CCFA Background / 340
- 20.3 CCFA History / 340
- 20.4 CCFA Definitions / 341
  - 20.4.1 Independent Event / 341
  - 20.4.2 Dependent Event / 341
  - 20.4.3 Independence (in Design) / 341
  - 20.4.4 Dependence (in Design) / 341
  - 20.4.5 Common Cause Failure / 342
  - 20.4.6 Common Mode Failure / 342
  - 20.4.7 Cascading Failure / 343
  - 20.4.8 Mutually Exclusive Events / 343
  - 20.4.9 CCF Root Cause / 343
  - 20.4.10 CCF Coupling Factor / 343
  - 20.4.11 Common Cause Component Group / 343
- 20.5 CCFA Theory / 344
- 20.6 CCFA Methodology / 346
  - 20.6.1 CCFA Process Step 2: Initial System Fault Tree Model / 347

20.6.2	CCFA Process Step 3: Common Cause Screening /	348
20.6.3	CCFA Process Step 4: Detailed CCF Analysis /	351
20.7	CCF Defense Mechanisms /	354
20.8	CCFA Example /	354
20.9	CCFA Models /	358
20.10	CCFA Advantages and Disadvantages /	359
20.11	Common CCFA Mistakes to Avoid /	360
20.12	Summary /	361
<b>21.</b>	<b>Software Hazard Analysis</b>	<b>363</b>
21.1	SwHA Introduction /	363
21.2	SwHA Background /	364
21.3	SwHA History /	365
21.4	SwHA Theory /	365
21.5	SwHA Methodology /	366
21.6	SwHA Worksheet /	367
21.7	Software Criticality Level /	368
21.8	SwHA Example /	369
21.9	Software Fault Tree Analysis /	376
21.10	SwHA Advantages and Disadvantages /	377
21.11	SwHA Mistakes to Avoid /	379
21.12	SwHA Summary /	379
<b>22.</b>	<b>Process Hazard Analysis</b>	<b>381</b>
22.1	PHA Introduction /	381
22.2	PHA Background /	381
22.3	PHA History /	382
22.4	Processing Mishaps /	382
22.5	Process Safety Management /	383
22.6	PHA Theory /	384
22.7	PHA Methodology /	385
22.8	PHA Worksheet /	386
22.9	Supporting Notes /	387
22.10	PHA Advantages and Disadvantages /	388
22.11	Common PHA Mistakes to Avoid /	389
22.12	Summary /	389
<b>23.</b>	<b>Test Hazard Analysis</b>	<b>390</b>
23.1	THA Introduction /	390
23.2	THA Background /	390



- 23.3 THA History / 391
- 23.4 THA Theory / 391
- 23.5 THA Methodology / 393
- 23.6 THA Worksheet / 394
- 23.7 THA Considerations / 395
  - 23.7.1 Verification / 395
  - 23.7.2 Validation / 395
- 23.8 Testing in the System Development Life Cycle / 396
- 23.9 Types of Testing / 397
  - 23.9.1 Standard Development Test Types / 397
  - 23.9.2 Performance Tests / 397
  - 23.9.3 Software Performance Tests / 397
  - 23.9.4 Special Safety-Related Testing / 398
- 23.10 THA Safety Goals / 398
- 23.11 THA Advantages and Disadvantages / 404
- 23.12 Common THA Mistakes to Avoid / 404
- 23.13 Summary / 404

## **24. Fault Hazard Analysis**

**406**

- 24.1 FHA Introduction / 406
- 24.2 FHA Background / 406
- 24.3 FHA History / 407
- 24.4 FHA Theory / 407
- 24.5 FHA Methodology / 408
- 24.6 FHA Worksheet / 410
- 24.7 FHA Example / 411
- 24.8 FHA Advantages and Disadvantages / 414
- 24.9 Common FHA Mistakes to Avoid / 414
- 24.10 Summary / 414

## **25. Sneak Circuit Analysis**

**416**

- 25.1 SCA Introduction / 416
- 25.2 SCA Background / 417
- 25.3 SCA History / 418
- 25.4 SCA Definitions / 418
- 25.5 SCA Theory / 419
- 25.6 SCA Methodology / 419
  - 25.6.1 Step 1: Acquire Data / 420
  - 25.6.2 Step 2: Code Data / 421
  - 25.6.3 Step 3: Process Data / 421
  - 25.6.4 Step 4: Produce Network Trees / 422