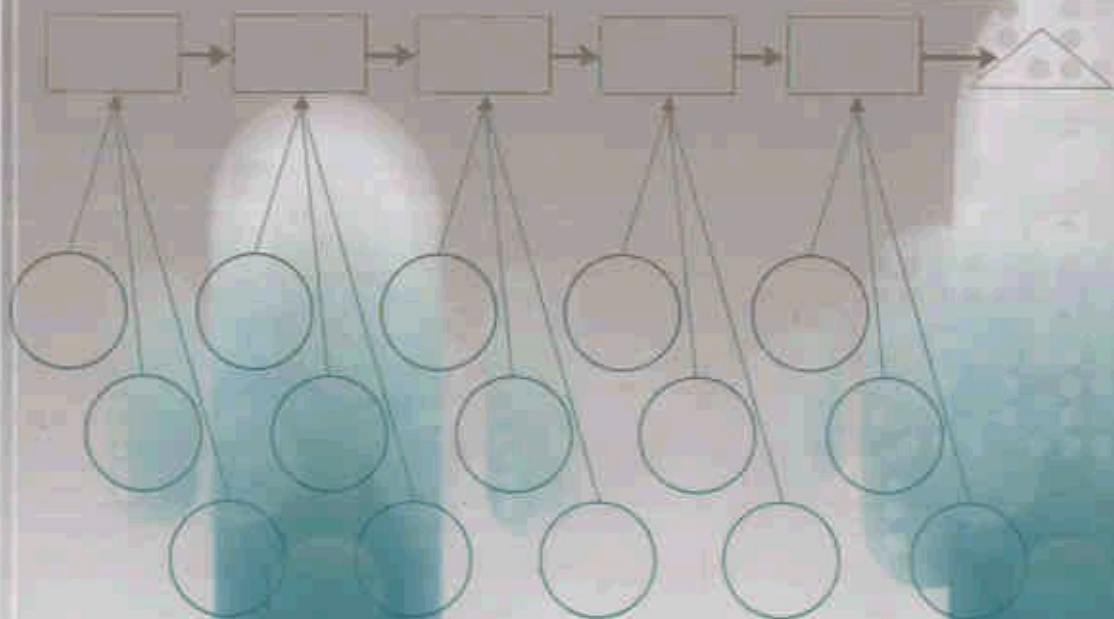


ASSURANCE TECHNOLOGIES PRINCIPLES AND PRACTICES

A Product, Process, and System Safety Perspective

Second Edition

Dev G. Raheja and Michael Allocco



CONTENTS

PREFACE

xix

CHAPTER 1 ASSURANCE TECHNOLOGIES, PROFITS, AND MANAGING SAFETY-RELATED RISKS

1

- 1.1 Introduction / 1
- 1.2 Cheaper, Better, and Faster Products / 2
- 1.3 What Is System Assurance? / 5
- 1.4 Key Management Responsibilities / 5
 - 1.4.1 Integration / 5
 - 1.4.2 Budget Consistent with Objectives / 5
 - 1.4.3 Managing Risk / 6
 - 1.4.3.1 Managing Safety-Related Risk / 6
 - 1.4.3.2 Risk Assessment / 7
 - 1.4.3.3 Risk Types / 7
 - 1.4.3.4 Risk Terms / 8
 - 1.4.3.5 Risk Knowledge / 8
- 1.5 Is System Assurance a Process? / 8
- 1.6 System Assurance Programs / 10
- References / 10
- Further Reading / 10

CHAPTER 2 INTRODUCTION TO STATISTICAL CONCEPTS

11

- 2.1 Probabilistic Designs / 11
- 2.2 Probability Computations for Reliability, Safety, and Maintainability / 12
 - 2.2.1 Construction of a Histogram and the Empirical Distribution / 12
 - 2.2.2 Computing Reliability / 14
 - 2.2.3 Failure Rate and Hazard Function / 15
- 2.3 Normal Distribution / 16
- 2.4 Log Normal Distribution / 22
- 2.5 Exponential Distribution / 25
- 2.6 Weibull Distribution / 29
- 2.7 Data Analysis with Weibull Distribution / 32
- 2.8 Discrete Distributions / 36
 - 2.8.1 Binomial Distribution / 37
 - 2.8.2 Poisson Distribution / 38
- 2.9 Topics for Student Projects and Theses / 39
- References / 39
- Further Reading / 40

CHAPTER 3 RELIABILITY ENGINEERING AND SAFETY-RELATED APPLICATIONS

41

- 3.1 Reliability Principles / 41
- 3.2 Reliability in the Design Phase / 44
 - 3.2.1 Writing Reliability Specifications / 45
 - 3.2.2 Conducting Design Reviews / 45
 - 3.2.2.1 Preliminary Design Review / 46
 - 3.2.2.2 Lessons Learned and Checklists / 47
 - 3.2.3 Reliability Allocation / 48
 - 3.2.4 Reliability Modeling / 49
 - 3.2.4.1 Series Model / 49
 - 3.2.4.2 Parallel Model / 50
 - 3.2.5 Reliability Prediction / 51
 - 3.2.6 Failure-Mode, Effects, and Criticality Analysis / 54
 - 3.2.7 Worst-Case Analysis / 61
 - 3.2.8 Other Analysis Techniques / 61
 - 3.2.9 Design Improvement Approaches / 62
 - 3.2.9.1 Derating / 62
 - 3.2.9.2 Fault Tolerance / 62

3.3	Reliability in the Manufacturing Phase /	65
3.4	Reliability in the Test Phase /	66
3.4.1	Reliability Growth Testing /	67
3.4.2	Tests for Durability /	70
3.4.3	Testing for Low Failure Rates /	75
3.4.4	Burn-in and Screening /	82
3.5	Reliability in the Use Phase /	86
3.6	Reliability and Safety Commonalities /	87
3.6.1	Common System Objective /	87
3.6.2	Unreliability and Hazards /	87
3.6.3	Complex Risks /	88
3.6.4	Potential System Accidents /	88
3.6.5	Software Reliability and Safety /	89
3.6.6	Reliability and Safety Trade-offs /	89
3.6.7	Reliability and Safety Misconceptions /	89
3.6.7.1	Redundancy /	90
3.6.7.2	Monitoring /	91
3.6.7.3	Concepts of Probability /	91
3.6.7.4	Familiarization to Automation /	92
3.6.7.5	Reliable Software and Safety Considerations /	93
3.6.7.6	Reliable Analyses and Safety Applications /	95
3.7	Topics for Student Projects and Theses /	100
	References /	101
	Further Reading /	102

CHAPTER 4 MAINTAINABILITY ENGINEERING AND SAFETY-RELATED APPLICATIONS

103

4.1	Maintainability Engineering Principles /	103
4.2	Maintainability during the Design Phase /	106
4.2.1	Developing Maintainability Specifications /	106
4.2.2	Design Review for Maintainability /	107
4.2.3	Maintainability Analysis /	109
4.2.4	FMECA for Maintainability /	109
4.2.5	Maintainability Prediction /	110
4.2.6	Life-Cycle Cost Analysis /	111
4.2.7	Design for Accessibility /	114
4.2.8	Design for Ease of Maintenance /	114
4.2.9	Design for MM of Testing /	118

4.3	Maintainability in the Manufacturing Stage /	122
4.3.1	Maintainability for Existing Equipment /	122
4.3.2	Maintainability for New Equipment /	124
4.4	Maintainability in the Test Stage /	126
4.4.1	Prerequisites for Maintainability Tests /	127
4.4.2	Tests for Inherent Equipment Downtime /	127
4.4.3	Tests for Human Variations /	127
4.4.4	Maintenance Level Tests /	127
4.5	Maintainability in the Use Stage /	128
4.5.1	Prediction and Reduction of Limited-Life Items /	128
4.5.2	Monitoring and Predicting Operational Availability /	129
4.5.3	Minimizing Support Costs /	132
4.6	Maintainability and System Safety /	132
4.6.1	Remote Maintenance Safety and Security /	132
4.6.2	System Health Monitoring and Maintenance /	134
4.6.3	Using Models to Develop Maintenance Diagnostics and Monitoring /	134
4.6.3.1	Stress–Strength Analysis /	134
4.6.3.2	Safety Factor and Safety Margin Variability /	135
4.6.3.3	Safety Margin and a Hazard Control /	135
4.6.3.4	Integration Considerations Between Safety-Related Models and Hazard Analysis /	136
4.6.3.5	Real World Verification /	137
4.6.4	Hazard Analysis in Support of Maintenance /	137
4.7	Topics for Student Projects and Theses /	144
	References /	145
	Further Reading /	145

CHAPTER 5 SYSTEM SAFETY ENGINEERING

147

5.1	System Safety Principles /	147
5.1.1	System Safety Process /	150
5.1.2	Risk Assessment /	150
5.1.3	Technical Risk Analysis /	150
5.1.4	Residual Risk /	153
5.1.5	Emergency Preparedness /	153
5.2	System Safety in Design /	153
5.2.1	Criteria for a Safe Design /	154
5.2.2	Safety Engineering Tasks /	156
5.2.3	Preliminary Hazard Analysis /	156
5.2.4	Subsystem Hazard Analysis /	161

- 5.2.5 Fault-Tree Analysis / 163
- 5.2.6 Cut Set Analysis / 167
- 5.2.7 Failure-Mode, Effects, and Criticality Analysis / 169
- 5.2.8 Maintenance Engineering Safety Analysis / 169
- 5.2.9 Event Trees / 170
- 5.2.10 Operating and Support Hazard Analysis / 172
- 5.2.11 Occupational Health Hazard Assessment / 174
- 5.2.12 Sneak Circuit Analysis / 174
- 5.2.13 System Hazard Analysis / 176
- 5.3 System Safety in Manufacturing / 176
 - 5.3.1 Determining Safety-Critical Items / 176
 - 5.3.2 Manufacturing Controls for Safety / 176
- 5.4 System Safety in the Test Stage / 178
 - 5.4.1 Testing Principles / 178
 - 5.4.2 Prerequisites for Developing Appropriate Tests / 179
 - 5.4.3 Product Qualification Tests / 180
 - 5.4.4 Production Tests / 180
 - 5.4.5 Tests for Human-Related Errors / 181
 - 5.4.6 Testing the Safety of Design Modifications / 182
 - 5.4.7 Testing Procedures / 182
 - 5.4.8 Analyzing Test Data—The Right Way / 182
 - 5.4.9 How Much Testing Is Enough? / 183
- 5.5 System Safety in the Use Stage / 183
 - 5.5.1 Closed-Loop Hazard Management (Hazard Tracking and Risk Resolution) / 183
 - 5.5.2 Integrity of the Procedures / 183
 - 5.5.3 Control of Changes / 184
 - 5.5.3.1 Changes in Product Design / 184
 - 5.5.3.2 Changes in Manufacturing Process / 184
 - 5.5.4 Accident/Incident Investigation / 184
- 5.6 Analyzing System Hazards and Risks / 185
 - 5.6.1 SDHA Process Development / 186
 - 5.6.2 Designing Accidents / 187
 - 5.6.2.1 SDHA-Related Concept / 187
 - 5.6.2.2 Adverse Event Model / 187
 - 5.6.2.3 Life Cycle of a System Accident / 188
 - 5.6.2.4 Potential Pitfalls in Logic Development / 189
 - 5.6.2.5 Determining Hazards (Unsafe Acts are Unsafe Conditions) / 190

5.6.2.6	Tabular Worksheet /	190
5.6.2.7	Deductive and Inductive Approaches Toward Scenario Development /	190
5.7	Hazard Identification /	191
5.7.1	Scenario Themes /	191
5.7.2	Primary Hazards /	192
5.7.3	Initiators /	193
5.7.4	Contributors /	194
5.7.5	Overlapping Hazards /	195
5.8	Topics for Student Projects and Theses /	195
	References /	196
	Further Reading /	197

CHAPTER 6 QUALITY ASSURANCE ENGINEERING AND PREVENTING LATENT SAFETY DEFECTS

199

6.1	Quality Assurance Principles /	199
6.2	Quality Assurance in the Design Phase /	201
6.2.1	Product Design Review for Quality /	202
6.2.1.1	Quality Function Deployment /	203
6.2.1.2	Benchmarking /	204
6.2.1.3	Quality Loss Function /	204
6.2.2	Process Design Review for Quality and Yield /	206
6.2.2.1	Capital Equipment Analysis /	207
6.2.3	Design Optimization for Robustness /	209
6.2.3.1	Shainin Approach /	210
6.2.3.2	Taguchi Approach /	211
6.2.4	Process FMECA /	214
6.2.5	Quality Assurance Plans for Procurement and Process Control in the Design Phase /	217
6.2.5.1	Equipment Procurement Plans /	217
6.2.5.2	Process Control Plans /	217
6.2.5.3	Component Procurement Quality Plans /	218
6.3	Quality Assurance in the Manufacturing Phase /	220
6.3.1	Evaluation of Pilot Run /	220
6.3.2	Process Control /	221
6.3.2.1	Identifying Causes of Variation /	222
6.3.2.2	Verifying the Influence of Causes /	224
6.3.2.3	Statistical Process Control /	226
6.3.2.4	Control Charts for Variables /	228
6.3.3	PPM Control for World-Class Quality /	228

- 6.3.4 Working with Suppliers / 230
- 6.3.5 PPM Assessment / 231
- 6.4 Quality Assurance in the Test Phase / 232
 - 6.4.1 Qualification Versus Production Testing / 233
 - 6.4.2 Industry Standards / 233
- 6.5 Quality Assurance in the Use Phase / 233
- 6.6 Topics for Student Projects and Theses / 234
- References / 234
- Further Reading / 235

CHAPTER 7 LOGISTICS SUPPORT ENGINEERING AND SYSTEM SAFETY CONSIDERATIONS

237

- 7.1 Logistics Support Principles / 237
- 7.2 Logistics Engineering During the Design Phase / 238
 - 7.2.1 Logistics Specifications for Existing Products / 238
 - 7.2.2 Logistics Specifications for New Products / 240
 - 7.2.3 Design Reviews / 241
 - 7.2.4 Logistics Support Analysis / 241
 - 7.2.5 FMECA for Logistics Support Analysis / 242
 - 7.2.6 Time-Line Analysis / 244
 - 7.2.7 Level-of-Repair Analysis / 245
 - 7.2.8 Logistics Support Analysis Documentation / 245
- 7.3 Logistics Engineering During the Manufacturing Phase / 245
- 7.4 Logistics Engineering During the Test Phase / 246
 - 7.4.1 Tests for R&M Characteristics / 246
 - 7.4.2 Tests of Operating Procedures / 246
 - 7.4.3 Tests for Emergency Preparedness / 246
- 7.5 Logistics Engineering in the Use Phase / 246
 - 7.5.1 Reliability-Centered Maintenance / 247
 - 7.5.1.1 RCM Analysis Planning / 247
 - 7.5.1.2 RCM Process / 247
 - 7.5.1.3 RCM Strategies / 247
 - 7.5.2 Measuring the Effectiveness of Logistics Engineering / 250
- 7.6 Logistics Support Engineering and System Safety / 251
 - 7.6.1 Product, General, and Professional Liability / 251
 - 7.6.2 Analysis of Changing Risks / 251
 - 7.6.3 Life-Cycle Logistics and System Safety / 252
 - 7.6.3.1 Production and Deployment Considerations / 252
 - 7.6.3.2 Process Runs / 253
 - 7.6.3.3 Production Inspection / 253

7.6.3.4	Quality Control and Data Analysis /	254
7.6.3.5	Storage, Transportation, and Handling /	255
7.6.3.6	Construction, Installation, Assembly, Testing, and Initial Operation /	256
7.6.3.7	Operations, Maintenance, and Upkeep /	256
7.6.3.8	Retirement and Disposal /	258
7.7	Topics for Student Projects and Theses /	259
	References /	259
	Further Reading /	260

CHAPTER 8 HUMAN FACTORS ENGINEERING AND SYSTEM SAFETY CONSIDERATIONS

261

8.1	Human Engineering Principles /	261
8.2	Human Factors in the Design Phase /	262
8.2.1	Use of Checklists and Standards in Specifications /	262
8.2.2	Design Reviews for Human Interfaces /	265
8.2.3	Using Lessons Learned /	265
8.2.4	Review of Hazard Analyses /	266
8.3	Human Factors in the Manufacturing Phase /	268
8.3.1	Types of Manufacturing Errors and Controls /	268
8.3.1.1	Errors of Illusion /	268
8.3.1.2	Errors of Vision /	269
8.3.1.3	Errors of Insufficient Knowledge /	269
8.3.1.4	Errors of Engineering Oversight /	269
8.3.2	Preventing Inspection Errors /	269
8.4	Human Factors in the Test Phase /	270
8.4.1	Tests for Stereotype Behavior /	270
8.4.2	Tests for Emergency Preparedness /	271
8.4.3	Tests for Amelioration /	273
8.4.4	Tests for the Human–Machine Interface /	273
8.5	Human Factors in the Use Phase /	274
8.6	Additional Considerations Involving Human Factors and System Safety /	274
8.6.1	Human Variability /	274
8.6.2	Human Engineering Complexities /	275
8.6.3	The Human Machine /	275
8.6.4	Human Behavior /	275
8.6.5	Human Motivation /	275
8.6.6	Motivation and Safety Culture /	276
8.6.7	Human Error /	276

8.7	Real Time and Latent Errors /	276
8.8	Analyses in Support of Human Factors and System Safety /	277
8.8.1	Human Interface Analysis /	277
8.8.2	Link Analysis /	277
8.8.3	Critical Incident Technique (CIT) /	279
8.8.4	Behavior Sampling /	279
8.8.5	Procedure Analysis /	281
8.8.6	Life Support/Life Safety Analysis /	281
8.8.7	Job Safety Analysis /	282
8.8.8	Human Reliability /	282
8.8.9	Technique for Error Rate Prediction (THERP) /	283
8.8.10	A Technique for Human Event Analysis (ATHEANA) /	284
8.8.11	Human Error Criticality Analysis (HECA) /	285
8.8.12	Workload Assessment /	286
8.9	Topics for Student Projects and Theses /	286
	References /	287
	Further Reading /	288

CHAPTER 9 SOFTWARE PERFORMANCE ASSURANCE

289

9.1	Software Performance Principles /	289
9.1.1	Software Quality /	290
9.1.2	Software Reliability /	291
9.1.3	Software System Safety /	293
9.1.4	Software Maintainability /	294
9.1.5	Software Logistics Engineering /	294
9.1.6	Some Important Definitions /	295
9.2	Software Performance in the Design Phase /	297
9.2.1	Software Quality Assurance in Design /	297
9.2.2	Software Reliability in Design /	298
9.2.2.1	Software Design Techniques for Reliability /	299
9.2.2.2	Preventing Specification and Design Errors /	300
9.2.3	Software Maintainability in Design /	300
9.2.4	Software System Safety in Design /	301
9.2.4.1	Software Safety Risk Assessment /	302
9.2.4.2	Software Safety Tools /	303
9.2.5	Software Logistics Engineering /	305
9.2.6	Software System Failure-Modes and Effects Analysis /	306
9.2.6.1	The Objective /	306
9.2.6.2	The Methodology /	306

9.2.6.3	Demonstration of Methodology /	307
9.2.6.4	Software–Hardware Interface Control /	309
9.2.6.5	Other Uses of SSFMEA /	309
9.2.6.6	Implementing a SSFMEA Program /	310
9.2.7	Software Performance Specification /	310
9.2.8	Software Design Review Checklist /	310
9.3	Software Requirements During Coding and Integration /	323
9.3.1	Coding Errors /	323
9.3.2	Quantifying Software Errors /	324
9.3.3	Coding Error Prevention /	326
9.4	Software Testing /	328
9.4.1	Testing for Quality /	328
9.4.2	Testing for Reliability /	329
9.4.3	Testing for Maintainability /	329
9.4.4	Testing for Software Safety /	329
9.4.5	Testing for Overall Qualification /	330
9.5	Software Performance in the Use Stage /	331
9.6	Topics for Student Projects and Theses /	332
	References /	332

CHAPTER 10 SYSTEM EFFECTIVENESS

335

10.1	Introduction /	335
10.2	System Effectiveness Principles /	336
10.3	Implementing the Programs /	339
10.4	Managing by Life-Cycle Costs /	341
10.5	System Effectiveness Model /	343
10.6	Authors' Recommendations /	343
10.7	System Risk and Effects on System Effectiveness /	344
10.7.1	System Accidents /	345
10.7.2	Complex System Risks /	345
10.7.3	Synergistic Risks /	345
10.7.4	Controlling Risks with Effective System Safety Requirements and Standards /	346
10.7.5	Effective System Safety Requirements and Standards /	347
10.7.5.1	Standards and Federal Codes /	348
10.7.5.2	General System Safety Requirements /	348
10.7.5.3	Derived Requirements /	349
10.7.5.4	Requirements Testing /	349
10.7.5.5	Requirements Development /	350

10.7.5.6	Requirements Compliance /	350
10.7.5.7	Requirements Revision /	350
10.7.5.8	Requirements Traceability /	351
10.7.5.9	Requirements Documentation /	351
10.7.5.10	Requirements Language /	351
10.7.5.11	Redundant Requirements /	351
10.7.6	Additional System Effectiveness Models /	352
10.7.7	Other Indicators of System Effectiveness or Success /	352
10.8	Topics for Student Projects and Theses /	353
	References /	353
	Further Reading /	354

CHAPTER 11 MANAGING SAFETY-RELATED RISKS 355

11.1	Establish the Appropriate Safety Program to Manage Risk /	355
11.1.1	Specific Safety Programs /	355
11.2	Programs to Address Product, Process, and System Safety /	356
11.2.1	Product Safety Management /	356
11.2.2	Process Safety Management /	358
11.2.3	System Safety Management /	362
11.3	Resource Allocation and Cost Analysis in Safety Management /	368
11.3.1	Cost of Losses Versus Cost of Control /	369
11.4	Topics for Student Projects and Theses /	369
	References /	370
	Further Reading /	370

CHAPTER 12 STATISTICAL CONCEPTS, LOSS ANALYSES, AND SAFETY-RELATED APPLICATIONS 373

12.1	Use of Distributions and Statistical Applications Associated with Safety /	373
12.2	Statistical Analysis Techniques Used Within Safety Analysis /	373
12.3	Using Statistical Control in Decision-Making for Safety /	376
12.4	Behavior Sampling /	379
12.5	Calculating Hazardous Exposures to the Human System /	380
12.6	Topics for Student Projects and Theses /	383
	References /	384
	Further Reading /	384

**CHAPTER 13 MODELS, CONCEPTS, AND EXAMPLES:
APPLYING SCENARIO-DRIVEN
HAZARD ANALYSIS**

385

- 13.1 Adverse Sequences / 385
 - 13.1.1 Scenarios Within Safety Analysis / 385
 - 13.1.2 Modeling Within Safety Analysis / 385
 - 13.1.2.1 Overviews and Models / 386
 - 13.1.2.2 Visualization / 387
 - 13.1.2.3 Scenarios, Reality, and Benefits / 387
 - 13.1.3 Integration and Presentation of Analysis Information / 390
 - 13.1.4 Narrative Reports Versus Tabular Formats / 390
- 13.2 Designing Formats for Conducting Analysis and Reporting Results / 391
- 13.3 Documentation Reports / 393
 - 13.3.1 Reporting Analysis Results / 394
- 13.4 Conceptual Models / 394
 - 13.4.1 Hammer Model / 394
 - 13.4.2 Complex Scenario Models / 395
 - 13.4.3 Fishbone Diagrams / 396
- 13.5 Life Cycle of a System Accident / 397
 - 13.5.1 Complex Interactions / 397
- 13.6 Operating and Support Hazard Analysis Example / 398
- 13.7 Topics for Student Projects and Theses / 408
- Reference / 408
- Further Reading / 408

**CHAPTER 14 AUTOMATION, COMPUTER, AND
SOFTWARE COMPLEXITIES**

411

- 14.1 Complex System Analysis / 411
- 14.2 System Context / 412
- 14.3 Understanding the Adverse Sequence / 413
 - 14.3.1 Malfunction and Failure Modes / 413
 - 14.3.2 Understanding System Functions / 413
 - 14.3.3 Understanding Conceptual Processes / 414
- 14.4 Additional Software Safety Analysis Techniques / 414
 - 14.4.1 Software Malfunction / 414
 - 14.4.2 Manifestation of Software-Related Risks / 417
 - 14.4.3 Understanding Anomalies / 417
 - 14.4.4 Complexity, Understanding Risks, and System States / 417

14.4.5	System States /	418
14.4.6	Complexity of Initiators, Contributors, and System Accidents /	418
14.4.7	Functional Abstractions and Domains /	418
14.4.8	Latent Hazards Throughout the Life Cycle /	418
14.4.9	Errors in Model Use and Development /	419
14.4.10	Understanding Safety Criticality /	419
14.4.11	Understanding Transfer and Switching Complications /	419
14.5	True Redundancy /	420
14.5.1	System Redundancy /	420
14.6	Complexities and Hazards Within Computer Hardware /	420
14.6.1	Controls, Mitigations, and Added Complexities /	420
14.7	Initiators and Contributors: The Errors Associated with Software /	421
14.8	Other Specialized Techniques, Analysis Methods, and Tools for Evaluating Software and Computer Systems /	426
14.8.1	Software Reliability /	426
14.8.2	Static Complexity Analysis /	426
14.8.3	Dynamic Analysis /	426
14.8.4	Test Coverage Monitoring /	426
14.9	Existing Legacy Systems, Reusable Software, Commercial Off-the-Shelf (COTS) Software, and Nondevelopment Items (NDIs) /	427
14.10	Topics for Student Projects and Theses /	428
	References /	429
	Further Reading /	429

APPENDIX A: REFERENCE TABLES	431
APPENDIX B: AN OUTSTANDING APPLICATION OF ASSURANCE TECHNOLOGIES	441
INDEX	449