

**NOT MEASUREMENT  
SENSITIVE**

**MIL-HDBK-338B**

**1 October 1998**

---

**SUPERSEDING**

**MIL-HDBK-338A**

**12 October 1988**

## **MILITARY HANDBOOK**

### **ELECTRONIC RELIABILITY DESIGN HANDBOOK**



**This handbook is for guidance only. Do not cite this document  
as a requirement**

AMSC N/A

AREA RELI

**DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.**

**FOREWORD**

1. This handbook is approved for use by all Departments and Agencies of the Department of Defense (DoD). It was developed by the DoD with the assistance of the military departments, federal agencies, and industry and replaces in its entirety MIL-HDBK-338A. The handbook is written for reliability managers and engineers and provides guidance in developing and implementing a sound reliability program for all types of products.
2. This Handbook is for guidance only. This Handbook cannot be cited as a requirement. If it is, the contractor does not have to comply.
3. Reliability is a discipline that continues to increase in importance as systems become more complex, support costs increase, and defense budgets decrease. Reliability has been a recognized performance factor for at least 50 years. During World War II, the V-1 missile team, led by Dr. Wernher von Braun, developed what was probably the first reliability model. The model was based on a theory advanced by Eric Pieruschka that if the probability of survival of an element is  $1/x$ , then the probability that a set of  $n$  identical elements will survive is  $(1/x)^n$ . The formula derived from this theory is sometimes called Lusser's law (Robert Lusser is considered a pioneer of reliability) but is more frequently known as the formula for the reliability of a series system:  $R_s = R_1 \times R_2 \times \dots \times R_n$ .
4. Despite the long gestation period for reliability, achieving the high levels needed in military systems is too often an elusive goal. System complexity, competing performance requirements, the rush to incorporate promising but immature technologies, and the pressures of acquisition budget and schedule contribute to this elusiveness. In the commercial sector, high levels of reliability are also necessary. Recently, American products once shunned in favor of foreign alternatives have made or are making a comeback. This shift in consumer preferences is directly attributable to significant improvements in the reliability and quality of the American products.
5. Noting these improvements, and facing a shrinking defense budget, the Department of Defense began the process of changing its acquisition policies to buy more commercial off-the-shelf products and to use commercial specifications and standards. The objective is to capitalize on the "best practices" that American business has developed or adopted, primarily in response to foreign competitive pressures. When combined with the knowledge and expertise of military contractors in building complex and effective military systems (soundly demonstrated during the conflict with Iraq), it is hoped that these commercial practices will allow the Department of Defense to acquire world-class systems on time and within budget.

## FOREWORD

---

6. The information in this Handbook reflects the move within the military to incorporate best commercial practices and the lessons learned over many years of acquiring weapon systems “by the book”. Military as well as commercial standards and handbooks are cited for reference because they are familiar to both military and commercial companies. Many of the military documents are being rescinded, so copies may be difficult to obtain. For those who have copies or can obtain them, the military documents provide a wealth of valuable information.
  
7. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be useful in improving this document should be addressed to: Air Force Research Laboratory/IFTB, 525 Brooks Road, Rome, NY 13441-4505. Comments should be submitted using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

## TABLE OF CONTENTS

Section	Page
1.0 SCOPE.....	1-1
1.1 Introduction.....	1-1
1.2 Application.....	1-1
1.3 Organization.....	1-1
2.0 REFERENCED DOCUMENTS.....	2-1
2.1 Government Documents .....	2-1
2.1.1 Specifications, Standards and Handbooks .....	2-1
2.2 Other Referenced Documents.....	2-3
3.0 DEFINITIONS OF TERMS AND ACRONYMS AND ABBREVIATIONS.....	3-1
3.1 Introduction .....	3-1
3.2 Definitions .....	3-1
3.3 List of Abbreviations and Acronyms.....	3-21
4.0 GENERAL STATEMENTS .....	4-1
4.1 Introduction and Background .....	4-1
4.2 The System Engineering Process .....	4-2
4.2.1 Systems Engineering and IPTs .....	4-3
4.2.2 The Four Steps of Systems Engineering .....	4-3
4.3 System Effectiveness .....	4-7
4.3.1 R/M Considerations in System Effectiveness .....	4-8
4.4 Factors Influencing System Effectiveness .....	4-8
4.4.1 Equipment of New Design .....	4-8
4.4.2 Interrelationships Among Various System Properties .....	4-9
4.5 Optimization of System Effectiveness .....	4-11
5.0 RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY .....	5-1
5.1 Introduction .....	5-1
5.2 Reliability Theory .....	5-1
5.2.1 Basic Concepts .....	5-2
5.3 Statistical Distributions Used in Reliability Models .....	5-8
5.3.1 Continuous Distributions .....	5-8
5.3.1.1 Normal (or Gaussian) Distribution .....	5-8
5.3.2 Examples of Reliability Calculations Using the Normal Distribution.....	5-14
5.3.2.1 Microwave Tube Example .....	5-14
5.3.2.2 Mechanical Equipment Example .....	5-15
5.3.3 Lognormal Distribution .....	5-16
5.3.3.1 Fatigue Failure Example .....	5-17

---

**TABLE OF CONTENTS**

Section		Page
5.3.4	Exponential Distribution .....	5-17
	5.3.4.1 Airborne Fire Control System Example .....	5-18
	5.3.4.2 Computer Example .....	5-18
5.3.5	Gamma Distribution .....	5-19
	5.3.5.1 Missile System Example .....	5-21
5.3.6	Weibull Distribution .....	5-22
	5.3.6.1 Example of Use of Weibull Distribution .....	5-23
5.3.7	Discrete Distributions .....	5-24
	5.3.7.1 Binomial Distribution .....	5-24
	5.3.7.1.1 Quality Control Example .....	5-24
	5.3.7.1.2 Reliability Example .....	5-25
5.3.8	Poisson Distribution .....	5-26
	5.3.8.1 Example With Permissible Number of Failures .....	5-27
5.4	Failure Modeling .....	5-28
5.4.1	Typical Failure Rate Curve .....	5-28
5.4.2	Reliability Modeling of Simple Structures .....	5-30
	5.4.2.1 Series Configuration .....	5-31
	5.4.2.2 Parallel Configuration .....	5-32
	5.4.2.3 K-Out-Of-N Configuration .....	5-35
5.5	Bayesian Statistics in Reliability Analysis .....	5-37
5.5.1	Bayes' Theorem .....	5-38
	5.5.1.1 Bayes' Example (Discrete Distribution) .....	5-39
	5.5.1.2 Bayes' Example (Continuous Distribution) .....	5-42
5.6	Maintainability Theory .....	5-44
5.6.1	Basic Concepts .....	5-45
5.6.2	Statistical Distributions Used in Maintainability Models .....	5-48
	5.6.2.1 Lognormal Distribution .....	5-49
	5.6.2.1.1 Ground Electronic System Maintainability Analysis Example .....	5-51
	5.6.2.2 Normal Distribution .....	5-63
	5.6.2.2.1 Equipment Example .....	5-65
	5.6.2.3 Exponential Distribution .....	5-67
	5.6.2.3.1 Computer Example .....	5-68
	5.6.2.4 Exponential Approximation .....	5-70
5.7	Availability Theory .....	5-70
5.7.1	Basic Concepts .....	5-72
5.7.2	Availability Modeling (Markov Process Approach) .....	5-73
	5.7.2.1 Single Unit Availability Analysis (Markov Process Approach) .....	5-75

---

**TABLE OF CONTENTS**

Section	Page
5.8 R&M Trade-Off Techniques .....	5-83
5.8.1 Reliability vs Maintainability.....	5-83
5.9 References For Section 5 .....	5-88
6.0 RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION .....	6-1
6.1 Introduction .....	6-1
6.2 Reliability Specification .....	6-1
6.2.1 Methods of Specifying the Reliability Requirement.....	6-1
6.2.2 Description of Environment and/or Use Conditions .....	6-3
6.2.3 Time Measure or Mission Profile .....	6-5
6.2.4 Clear Definition of Failure .....	6-6
6.2.5 Description of Method(s) for Reliability Demonstration .....	6-7
6.3 Reliability Apportionment/Allocation .....	6-7
6.3.1 Introduction .....	6-7
6.3.2 Equal Apportionment Technique .....	6-10
6.3.3 ARINC Apportionment Technique (Ref. [6]) .....	6-11
6.3.4 Feasibility-Of-Objectives Technique (Ref. [7]) .....	6-13
6.3.5 Minimization of Effort Algorithm .....	6-16
6.4 Reliability Modeling and Prediction .....	6-19
6.4.1 Introduction .....	6-19
6.4.2 General Procedure .....	6-21
6.4.2.1 Item Definition .....	6-22
6.4.2.2 Service Use Profile .....	6-22
6.4.2.3 Reliability Block Diagrams .....	6-24
6.4.2.4 Mathematical/Simulation Models .....	6-24
6.4.2.5 Part Description .....	6-24
6.4.2.6 Environmental Data .....	6-24
6.4.2.7 Stress Analysis .....	6-24
6.4.2.8 Failure Distributions .....	6-25
6.4.2.9 Failure Rates .....	6-25
6.4.2.10 Item Reliability .....	6-25
6.4.3 Tailoring Reliability Models and Predictions .....	6-25
6.4.4 Reliability Modeling .....	6-26
6.4.4.1 Reliability Block Diagrams .....	6-26
6.4.4.2 Reliability Modeling Methods .....	6-29
6.4.4.2.1 Conventional Probability Modeling Method .....	6-29
6.4.4.2.1.1 Series Model .....	6-29
6.4.4.2.1.2 Parallel Models .....	6-30
6.4.4.2.1.3 Series-Parallel Models .....	6-32
6.4.4.2.2 Boolean Truth Table Modeling Method .....	6-33

---

**TABLE OF CONTENTS**

Section		Page
	6.4.4.2.3 Logic Diagram Modeling Method .....	6-38
	6.4.4.2.4 Complex System Modeling Methods .....	6-41
	6.4.4.2.4.1 Markov Modeling (Ref. [9]) .....	6-41
	6.4.4.2.4.2 Monte Carlo Simulation Method .....	6-42
6.4.5	Reliability Prediction .....	6-44
	6.4.5.1 General .....	6-46
	6.4.5.2 Mathematical Models for Reliability Prediction .....	6-48
	6.4.5.3 Reliability Prediction Methods .....	6-50
	6.4.5.3.1 Similar Item Prediction Method .....	6-50
	6.4.5.3.2 Parts Count Prediction Method .....	6-52
	6.4.5.3.3 Parts Stress Analysis Prediction Method .....	6-54
	6.4.5.3.3.1 Stress Analysis Techniques .....	6-57
	6.4.5.3.3.2 Sample Calculation .....	6-59
	6.4.5.3.3.3 Modification for Non-Exponential Failure Densities (General Case) .....	6-63
	6.4.5.3.3.4 Nonoperating Failure Rates .....	6-66
	6.4.5.3.4 Reliability Physics Analysis (Ref. [17] and [18]) ...	6-68
	6.4.5.4 Computer Aided Reliability Prediction .....	6-71
6.5	Step-By-Step Procedure for Performing Reliability Prediction and Allocation .....	6-71
6.6	References for Section 6 .....	6-72
7.0	RELIABILITY ENGINEERING DESIGN GUIDELINES .....	7-1
7.1	Introduction .....	7-1
7.2	Parts Management .....	7-2
	7.2.1 Establishing a Preferred Parts List (PPL) .....	7-3
	7.2.2 Vendor and Device Selection .....	7-5
	7.2.2.1 Critical Devices/Technology/Vendors .....	7-8
	7.2.2.1.1 ASIC Devices .....	7-9
	7.2.2.1.2 GaAs and MMIC Devices .....	7-9
	7.2.2.2 Plastic Encapsulated Microcircuits (PEMs) .....	7-10
	7.2.2.3 Hidden Hybrids .....	7-10
	7.2.2.4 Device Specifications .....	7-11
	7.2.2.5 Screening .....	7-12
	7.2.2.6 Part Obsolescence and Diminishing Manufacturer Sources (DMS) .....	7-12
	7.2.2.7 Failure Reporting, Analysis, And Corrective Action System (FRACAS) .....	7-15
	7.2.3 Design for Reliability .....	7-15
	7.2.3.1 Electronic Part Reliability Assessment / Life Analysis .....	7-16
	7.2.4 Design for Manufacturability .....	7-19

## TABLE OF CONTENTS

Section		Page
7.2.5	Parts Management Plan Evaluation Criteria .....	7-20
	7.2.5.1 Quality Improvement Program .....	7-20
	7.2.5.2 Quality Assurance .....	7-20
	7.2.5.2.1 Part Qualification .....	7-21
	7.2.5.2.2 Production Quality Assurance .....	7-24
	7.2.5.3 Assembly Processes .....	7-26
	7.2.5.4 Design Criteria .....	7-28
7.3	Derating .....	7-30
	7.3.1 Electronic Part Derating .....	7-30
	7.3.2 Derating of Mechanical and Structural Components .....	7-32
7.4	Reliable Circuit Design .....	7-38
	7.4.1 Transient and Overstress Protection .....	7-38
	7.4.1.1 On-Chip Protection Networks .....	7-40
	7.4.1.2 Metal Oxide Varistors (MOVs) .....	7-42
	7.4.1.3 Protective Diodes .....	7-43
	7.4.1.4 Silicon Controlled Rectifier Protection .....	7-43
	7.4.1.5 Passive Component Protection .....	7-44
	7.4.1.6 Protective Devices Summary .....	7-47
	7.4.1.7 Protection Design For Parts, Assemblies and Equipment .....	7-48
	7.4.1.8 Printed Wiring Board Layout .....	7-49
	7.4.1.9 Shielding .....	7-50
	7.4.1.10 Grounding .....	7-52
	7.4.1.11 Protection With MOVs .....	7-54
	7.4.1.12 Protection With Diodes .....	7-57
	7.4.2 Parameter Degradation and Circuit Tolerance Analysis .....	7-62
	7.4.3 Computer Aided Circuit Analysis .....	7-70
	7.4.3.1 Advantages of Computer Aided Circuit Analysis/Simulation .	7-71
	7.4.3.2 Limitations of Computer-Aided Circuit Analysis/Simulation	7-71
	Programs .....	7-71
	7.4.3.3 The Personal Computer (PC) as a Circuit Analysis Tool .....	7-71
	7.4.4 Fundamental Design Limitations .....	7-74
	7.4.4.1 The Voltage Gain Limitation .....	7-75
	7.4.4.2 Current Gain Limitation Considerations .....	7-78
	7.4.4.3 Thermal Factors .....	7-79
7.5	Fault Tolerant Design .....	7-80
	7.5.1 Redundancy Techniques .....	7-81
	7.5.1.1 Impact on Testability .....	7-81
	7.5.2 Reliability Role in the Fault Tolerant Design Process .....	7-84
	7.5.2.1 Fault Tolerant Design Analysis .....	7-86



---

**TABLE OF CONTENTS**

Section		Page
7.5.3	Redundancy as a Design Technique .....	7-88
	7.5.3.1 Levels of Redundancy .....	7-92
	7.5.3.2 Probability Notation for Redundancy Computations .....	7-93
	7.5.3.3 Redundancy Combinations .....	7-94
7.5.4	Redundancy in Time Dependent Situations .....	7-96
7.5.5	Redundancy Considerations in Design .....	7-98
	7.5.5.1 Partial Redundancy .....	7-105
	7.5.5.2 Operating Standby Redundancy .....	7-109
	7.5.5.2.1 Two Parallel Elements .....	7-109
	7.5.5.2.2 Three Parallel Elements .....	7-111
	7.5.5.2.3 Voting Redundancy .....	7-112
	7.5.5.3 Inactive Standby Redundancy .....	7-113
	7.5.5.4 Dependent Failure Probabilities .....	7-117
	7.5.5.5 Optimum Allocation of Redundancy .....	7-118
7.5.6	Reliability Analysis Using Markov Modeling .....	7-119
	7.5.6.1 Introduction .....	7-119
	7.5.6.2 Markov Theory .....	7-121
	7.5.6.3 Development of the Markov Model Equation .....	7-123
	7.5.6.4 Markov Model Reduction Techniques .....	7-125
	7.5.6.5 Application of Coverage to Markov Modeling .....	7-127
	7.5.6.6 Markov Conclusions .....	7-128
7.6	Environmental Design ..... <a href="http://www.kekaoxing.com">www.kekaoxing.com</a> .....	7-128
	7.6.1 Environmental Strength .....	7-128
	7.6.2 Designing for the Environment .....	7-129
	7.6.3 Temperature Protection .....	7-140
	7.6.4 Shock and Vibration Protection .....	7-142
	7.6.5 Moisture Protection .....	7-144
	7.6.6 Sand and Dust Protection .....	7-145
	7.6.7 Explosion Proofing .....	7-146
	7.6.8 Electromagnetic Radiation Protection .....	7-147
	7.6.9 Nuclear Radiation .....	7-149
	7.6.10 Avionics Integrity Program (AVIP) .....	7-151
	7.6.10.1 MIL-STD-1670: Environmental Criteria and Guidelines for Air Launched Weapons .....	7-153
7.7	Human Performance Reliability .....	7-159
	7.7.1 Introduction .....	7-159
	7.7.2 Reliability, Maintainability, and Availability Parameters for Human - Machine Systems .....	7-161
	7.7.3 Allocating System Reliability to Human Elements .....	7-165
	7.7.3.1 Qualitative Allocation .....	7-165
	7.7.3.2 Quantitative Allocation .....	7-167

---

**TABLE OF CONTENTS**

Section		Page
7.7.4	Sources of Human Performance Reliability Data .....	7-169
7.7.5	Tools for Designing Man-Machine Systems .....	7-172
7.7.5.1	Task Analysis .....	7-173
7.7.5.2	General Design Tools .....	7-173
7.7.5.3	Computer-Based Design Tools .....	7-175
7.7.5.3.1	Parametric Design Tools .....	7-176
7.7.5.3.2	Interface Design Tools .....	7-176
7.7.5.3.3	Work Space Design Tools .....	7-176
7.7.6	Reliability Prediction for Human-Machine Systems .....	7-177
7.7.6.1	Probability Compounding .....	7-178
7.7.6.2	Stochastic Models .....	7-183
7.7.6.3	Digital Simulation .....	7-184
7.7.6.4	Expert Judgment Techniques .....	7-186
7.7.7	Verification of Human Performance Reliability .....	7-187
7.8	Failure Mode and Effects Analysis (FMEA) .....	7-187
7.8.1	Introduction .....	7-187
7.8.2	Phase 1 .....	7-190
7.8.3	Phase 2 .....	7-201
7.8.4	Example .....	7-203
7.8.5	Risk Priority Number .....	7-206
7.8.5.1	Instituting Corrective Action .....	7-209
7.8.6	Computer Aided FMEA .....	7-209
7.8.7	FMEA Summary .....	7-210
7.9	Fault Tree Analysis .....	7-210
7.9.1	Discussions of FTA Methods .....	7-221
7.10	Sneak Circuit Analysis (SCA) .....	7-222
7.10.1	Definition of Sneak Circuit .....	7-222
7.10.2	SCA: Definition and Traditional Techniques .....	7-223
7.10.3	New SCA Techniques .....	7-224
7.10.4	Examples of Categories of SNEAK Circuits .....	7-225
7.10.5	SCA Methodology .....	7-229
7.10.5.1	Network Tree Production .....	7-229
7.10.5.2	Topological Pattern Identification .....	7-229
7.10.5.3	Clue Application .....	7-231
7.10.6	Software Sneak Analysis .....	7-231
7.10.7	Integration of Hardware/Software Analysis .....	7-234
7.10.8	Summary .....	7-235
7.11	Design Reviews ..... <a href="http://www.keakaoxing.com">www.keakaoxing.com</a> .....	7-236
7.11.1	Introduction and General Information .....	7-236
7.11.2	Informal Reliability Design Review .....	7-239
7.11.3	Formal Design Reviews .....	7-240

## TABLE OF CONTENTS

## TABLE OF CONTENTS

Section	Page
7.11.4 Design Review Checklists .....	7-246
7.12 Design for Testability .....	7-250
7.12.1 Definition of Testability and Related Terms .....	7-251
7.12.2 Distinction between Testability and Diagnostics .....	7-251
7.12.3 Designing for Testability .....	7-251
7.12.4 Developing a Diagnostic Capability .....	7-255
7.12.5 Designing BIT .....	7-256
7.12.6 Testability Analysis .....	7-257
7.12.6.1 Dependency Analysis .....	7-258
7.12.6.1.1 Dependency Analysis Tools .....	7-260
7.12.6.2 Other Types of Testability Analyses .....	7-260
7.13 System Safety Program .....	7-262
7.13.1 Introduction .....	7-262
7.13.2 Definition of Safety Terms and Acronyms .....	7-267
7.13.3 Program Management and Control Elements .....	7-268
7.13.3.1 System Safety Program .....	7-268
7.13.3.2 System Safety Program Plan .....	7-268
7.13.3.3 Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms .....	7-269
7.13.3.4 System Safety Program Reviews/Audits .....	7-269
7.13.3.5 System Safety Group/System Safety Working Group Support .....	7-269
7.13.3.6 Hazard Tracking and Risk Resolution .....	7-269
7.13.3.7 System Safety Progress Summary .....	7-269
7.13.4 Design and Integration Elements .....	7-269
7.13.4.1 Preliminary Hazard List .....	7-269
7.13.4.2 Preliminary Hazard Analysis .....	7-270
7.13.4.3 Safety Requirements/Criteria Analysis .....	7-270
7.13.4.4 Subsystem Hazard Analysis .....	7-270
7.13.4.5 System Hazard Analysis .....	7-270
7.13.4.6 Operating and Support Hazard Analysis .....	7-270
7.13.4.7 Occupational Health Hazard Assessment .....	7-270
7.13.5 Design Evaluation Elements .....	7-270
7.13.5.1 Safety Assessment .....	7-270
7.13.5.2 Test and Evaluation Safety .....	7-271
7.13.5.3 Safety Review of Engineering Change Proposals and Requests for Deviation/Waiver .....	7-271

---

**TABLE OF CONTENTS**

Section	Page
7.13.6	Compliance and Verification ..... 7-271
7.13.6.1	Safety Verification ..... 7-271
7.13.6.2	Safety Compliance Assessment ..... 7-271
7.13.6.3	Explosive Hazard Classification and Characteristics Data ..... 7-271
7.13.6.4	Explosive Ordinance Disposal Source Data ..... 7-271
7.13.7	Tailoring Guidelines ..... 7-272
7.14	Finite Element Analysis ..... 7-272
7.14.1	Introduction and General Information ..... 7-272
7.14.2	Finite Element Analysis Application ..... 7-272
7.14.3	Finite Element Analysis Procedure ..... 7-276
7.14.4	Applications ..... 7-278
7.14.5	Limitations ..... 7-278
7.15	References for Section 7 ..... 7-279
8.0	RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION AND GROWTH ..... 8-1
8.1	Introduction ..... 8-1
8.2	Failure Reporting, Analysis, and Corrective Action System (FRACAS) and Failure Review Board (FRB) ..... 8-2
8.2.1	Failure Reporting, Analysis and Corrective Action System (FRACAS) .. 8-2
8.2.1.1	Closed Loop Failure Reporting/Corrective Actions System .... 8-3
8.2.1.2	Failure Reporting Systems ..... 8-7
8.2.1.3	Failure Reporting Forms ..... 8-7
8.2.1.4	Data Collection and Retention ..... 8-7
8.2.2	Failure Review Board ..... 8-9
8.3	Reliability Data Analysis ..... 8-10
8.3.1	Graphical Methods ..... 8-10
8.3.1.1	Examples of Graphical Methods ..... 8-13
8.3.2	Statistical Analysis ..... 8-21
8.3.2.1	Introduction ..... 8-21
8.3.2.2	Treatment of Failure Data ..... 8-22
8.3.2.3	Reliability Function (Survival Curves) ..... 8-29
8.3.2.3.1	Computation of Theoretical Exponential Reliability Function ..... 8-31
8.3.2.3.2	Computation For Normal Reliability Function .... 8-33
8.3.2.4	Censored Data ..... 8-36
8.3.2.5	Confidence Limits and Intervals ..... 8-37
8.3.2.5.1	Confidence Limits - Normal Distribution ..... 8-39
8.3.2.5.2	Confidence Limits - Exponential Distribution ..... 8-43
8.3.2.5.3	Confidence-Interval Estimates for the Binomial Distribution ..... 8-50

## TABLE OF CONTENTS

<b>TABLE OF CONTENTS</b>		Page
Section		
	8.3.2.6 Tests for Validity of the Assumption Of A Theoretical Reliability Parameter Distribution .....	8-52
	8.3.2.6.1 Kolmogorov-Smirnov (K-S) Goodness-of-Fit Test (also called “d” test) .....	8-53
	8.3.2.6.2 Chi-Square Goodness-of-Fit Test .....	8-60
	8.3.2.6.3 Comparison of K-S and Chi-Square Goodness-of-Fit Tests .....	8-67
8.4	Reliability Demonstration .....	8-68
	8.4.1 Introduction .....	8-68
	8.4.2 Attributes and Variables .....	8-75
	8.4.3 Fixed Sample and Sequential Tests .....	8-75
	8.4.4 Determinants of Sample Size .....	8-75
	8.4.5 Tests Designed Around Sample Size .....	8-76
	8.4.6 Parameterization of Reliability .....	8-76
	8.4.7 Instructions on the Use of Reliability Demonstration Test Plans .....	8-76
	8.4.7.1 Attributes Demonstration Tests .....	8-77
	8.4.7.1.1 Attributes Plans for Small Lots .....	8-77
	8.4.7.1.2 Attributes Plans for Large Lots .....	8-81
	8.4.7.2 Attributes Demonstration Test Plans for Large Lots, Using the Poisson Approximation Method .....	8-84
	8.4.7.3 Attributes Sampling Using ANSI/ASQC Z1.4-1993 .....	8-87
	8.4.7.4 Sequential Binomial Test Plans .....	8-89
	8.4.7.5 Variables Demonstration Tests .....	8-93
	8.4.7.5.1 Time Truncated Demonstration Test Plans .....	8-93
	8.4.7.5.1.1 Exponential Distribution (H-108) .....	8-93
	8.4.7.5.1.2 Normal Distribution .....	8-95
	8.4.7.5.1.3 Weibull Distribution (TR-3, TR-4, TR-6) .....	8-100
	8.4.7.5.2 Failure Truncated Tests .....	8-103
	8.4.7.5.2.1 Exponential Distribution (MIL-HDBK-H108) .....	8-103
	8.4.7.5.2.2 Normal Distribution, $\sigma$ Known .....	8-105
	8.4.7.5.2.3 Normal Distribution, $\sigma$ Unknown (MIL-STD-414) .....	8-110
	8.4.7.5.2.4 Weibull Distribution .....	8-113
	8.4.7.5.3 Sequential Tests .....	8-116
	8.4.7.5.3.1 Exponential Distribution (MIL-HDBK-781) .....	8-116
	8.4.7.5.3.2 Normal Distribution .....	8-119
	8.4.7.6 Interference Demonstration Tests .....	8-123
	8.4.7.7 Bayes Sequential Tests .....	8-127
8.4.8	Reliability Demonstration Summary .....	8-131



## TABLE OF CONTENTS

## TABLE OF CONTENTS

Section		Page
9.3	Software Design .....	9-12
9.3.1	Preliminary Design .....	9-12
9.3.1.1	Develop the Architecture .....	9-13
9.3.1.2	Physical Solutions .....	9-13
9.3.1.3	External Characteristics .....	9-14
9.3.1.4	System Functional Decomposition .....	9-15
9.3.2	Detailed Design .....	9-15
9.3.2.1	Design Examples .....	9-15
9.3.2.2	Detailed Design Tools .....	9-16
9.3.2.3	Software Design and Coding Techniques .....	9-16
9.4	Software Design and Development Process Model .....	9-17
9.4.1	Ad Hoc Software Development .....	9-19
9.4.2	Waterfall Model .....	9-19
9.4.3	Classic Development Model .....	9-20
9.4.4	Prototyping Approach .....	9-22
9.4.5	Spiral Model .....	9-24
9.4.6	Incremental Development Model .....	9-26
9.4.7	Cleanroom Model .....	9-28
9.5	Software Reliability Prediction and Estimation Models .....	9-30
9.5.1	Prediction Models .....	9-31
9.5.1.1	In-house Historical Data Collection Model .....	9-31
9.5.1.2	Musa's Execution Time Model .....	9-32
9.5.1.3	Putnam's Model .....	9-33
9.5.1.4	Rome Laboratory Prediction Model: RL-TR-92-52 (Ref. [16]) .....	9-35
9.5.1.5	Rome Laboratory Prediction Model: RL-TR-92-15 (Ref. [17]) .....	9-38
9.5.2	Estimation Models .....	9-40
9.5.2.1	Exponential Distribution Models .....	9-40
9.5.2.2	Weibull Distribution Model (Ref. [19]) .....	9-46
9.5.2.3	Bayesian Fault Rate Estimation Model .....	9-46
9.5.2.4	Test Coverage Reliability Metrics .....	9-48
9.5.3	Estimating Total Number of Faults Using Tagging .....	9-49
9.6	Software Reliability Allocation .....	9-51
9.6.1	Equal Apportionment Applied to Sequential Software CSCIs .....	9-53
9.6.2	Equal Apportionment Applied to Concurrent Software CSCIs .....	9-54
9.6.3	Allocation Based on Operational Criticality Factors .....	9-54
9.6.4	Allocation Based on Complexity Factors .....	9-56

---

**TABLE OF CONTENTS**

Section	Page	
9.7	Software Testing .....	9-58
9.7.1	Module Testing .....	9-58
9.7.2	Integration Testing .....	9-59
9.7.3	System Testing .....	9-61
9.7.4	General Methodology for Software Failure Data Analysis .....	9-61
9.8	Software Analyses .....	9-62
9.8.1	Failure Modes .....	9-64
9.8.2	Failure Effects .....	9-64
9.8.3	Failure Criticality .....	9-65
9.8.4	Fault Tree Analysis .....	9-66
9.8.5	Failure Modes and Effects Analysis .....	9-67
9.9	References .....	9-69
10.0	SYSTEMS RELIABILITY ENGINEERING .....	10-1
10.1	Introduction .....	10-1
10.1.1	Commercial-Off-The-Shelf (COTS) and Nondevelopmental Item (NDI) Considerations .....	10-2
10.1.2	COTS/NDI as the End Product .....	10-8
10.1.3	COTS/NDI Integrated with Other Items .....	10-8
10.1.4	Related COTS/NDI Issues .....	10-9
10.2	System Effectiveness Concepts .....	10-9
10.2.1	The ARINC Concept of System Effectiveness (Ref. [1]) .....	10-9
10.2.2	The Air Force (WSEIAC) Concept (Ref. [2]) .....	10-10
10.2.3	The Navy Concept of System Effectiveness (Ref. [4]) .....	10-14
10.2.4	An Illustrative Model of a System Effectiveness Calculation .....	10-16
10.3	System R&M Parameters .....	10-20
10.3.1	Parameter Translation Models .....	10-21
10.3.1.1	Reliability Adjustment Factors .....	10-21
10.3.1.2	Reliability Prediction of Dormant Products .....	10-24
10.3.2	Operational Parameter Translation .....	10-25
10.3.2.1	Parameter Definitions .....	10-27
10.3.2.2	Equipment Operating Hour to Flight Hour Conversion .....	10-27
10.3.3	Availability, Operational Readiness, Mission Reliability, and Dependability - Similarities and Differences .....	10-28
10.4	System, R&M Modeling Techniques .....	10-30
10.4.1	Availability Models .....	10-33
10.4.1.1	Model A - Single Unit System (Point Availability) .....	10-33
10.4.1.2	Model B - Average or Interval Availability .....	10-38
10.4.1.3	Model C - Series System with Repairable/Replaceable Units .....	10-40
10.4.1.4	Model D - Redundant Systems .....	10-43

---



## TABLE OF CONTENTS

<b>TABLE OF CONTENTS</b>		Page
Section		
	10.4.1.5 Model E - R&M Parameters Not Defined in Terms of Time .....	10-55
10.4.2	Mission Reliability and Dependability Models .....	10-58
10.4.3	Operational Readiness Models .....	10-60
	10.4.3.1 Model A - Based Upon Probability of Failure During Previous Mission and Probability of Repair Before Next Mission Demand .....	10-61
	10.4.3.2 Model B - Same As Model A Except Mission Duration Time, t is Probabilistic .....	10-63
	10.4.3.3 Model C - Similar To Model A But Includes Checkout Equipment Detectability .....	10-64
	10.4.3.4 Model D - For a Population of N Systems .....	10-66
10.5	Complex Models .....	10-73
10.6	Trade-off Techniques .....	10-74
	10.6.1 General .....	10-74
	10.6.2 Reliability - Availability - Maintainability Trade-offs .....	10-75
10.7	Allocation of Availability, Failure and Repair Rates .....	10-86
	10.7.1 Availability Failure Rate and Repair Rate Allocation for Series Systems .....	10-87
	10.7.1.1 Case (1) .....	10-87
	10.7.1.2 Case (2) .....	10-88
	10.7.2 Failure and Repair Rate Allocations For Parallel Redundant Systems .....	10-93
	10.7.3 Allocation Under State-of-the-Art Constraints .....	10-99
10.8	System Reliability Specification, Prediction and Demonstration .....	10-100
	10.8.1 Availability Demonstration Plans .....	10-100
	10.8.1.1 Fixed Sample Size Plans .....	10-101
	10.8.1.2 Fixed-Time Sample Plans .....	10-104
10.9	System Design Considerations .....	10-106
10.10	Cost Considerations .....	10-109
	10.10.1 Life Cycle Cost (LCC) Concepts .....	10-109
10.11	References for Section 10 .....	10-117
11.0	PRODUCTION AND USE (DEPLOYMENT) R&M .....	11-1
11.1	Introduction .....	11-1
11.2	Production Reliability Control .....	11-3
	11.2.1 Quality Engineering (QE) and Quality Control (QC) .....	11-4
	11.2.1.1 Quality System Requirements .....	11-6
	11.2.1.1.1 ISO 9000 .....	11-6
	11.2.1.1.1.1 Comparing ISO 9000 to MIL-Q-9858 .....	11-8
	11.2.1.1.1.2 Why ISO 9000? .....	11-9
	11.2.1.2 Quality Control .....	11-10

---

**TABLE OF CONTENTS**

Section		Page
11.2.2	Production Reliability Degradation Assessment & Control .....	11-14
11.2.2.1	Factors Contributing to Reliability Degradation During Production: Infant Mortality .....	11-15
11.2.2.2	Process Reliability Analysis .....	11-19
11.2.3	Application of Environmental Stress Screening (ESS) During Production to Reduce Degradation and Promote Growth .....	11-26
11.2.3.1	Part Level Screening .....	11-28
11.2.3.2	Screening at Higher Levels of Assembly .....	11-30
11.2.3.3	Screen Test Planning and Effectiveness .....	11-32
11.2.3.3.1	Environmental Stress Screening per MIL-HDBK-344 .....	11-32
11.2.3.3.2	Tri-Service ESS Guidelines .....	11-36
11.2.3.3.2.1	Types of Flaws to be Precipitated .....	11-37
11.2.3.3.2.2	Levels of Assembly at which ESS May be Performed .....	11-37
11.2.3.3.2.3	Types and Severities of Stresses .....	11-40
11.2.3.3.2.4	Failure Detection Measurements During Thermal Cycling and Random Vibration .....	11-41
11.2.3.3.2.5	Baseline ESS Profiles .....	11-41
11.2.3.3.2.6	Optimizing/Tailoring of ESS .....	11-44
11.2.4	Production Reliability Acceptance Testing (MIL-HDBK-781) .....	11-45
11.2.5	Data Collection and Analysis (During Production) .....	11-52
11.2.6	Monitor/Control of Subcontractors and Suppliers .....	11-54
11.2.6.1	Major Subcontractor and Manufacturer Monitoring .....	11-54
11.2.6.2	Establishing Vendor Capability and Program Reviews .....	11-54
11.2.6.3	Supplier Monitoring .....	11-55
11.3	Production Maintainability Control .....	11-55
11.4	Reliability and Quality During Shipment and Storage .....	11-55
11.4.1	Factors Contributing to Reliability Degradation During Shipment & Storage .....	11-56
11.4.2	Protection Methods .....	11-58
11.4.3	Shipment and Storage Degradation Control (Storage Serviceability Standards) .....	11-62
11.4.3.1	Application of Cyclic Inspection During Storage to Assure Reliability and Material Readiness .....	11-72
11.4.4	Data Collection and Analysis (During Storage) .....	11-72
11.5	Operational R&M Assessment and Improvement .....	11-74
11.5.1	Factors Contributing to R&M Degradation During Field Operation .....	11-75
11.5.2	Maintenance Degradation Control (During Depot Storage) .....	11-76
11.5.3	Maintenance Documentation Requirements .....	11-79
11.5.4	Data Collection and Analysis (During Field Deployment) .....	11-80

## TABLE OF CONTENTS

## TABLE OF CONTENTS

Section	Page
11.5.5 System R&M Assessment .....	11-82
11.5.6 System R&M Improvement .....	11-85
11.6 References For Section 11 .....	11-87
12.0 RELIABILITY MANAGEMENT CONSIDERATIONS .....	12-1
12.1 Impacts of Acquisition Reform .....	12-1
12.1.1 Acquisition Reform History .....	12-1
12.1.1.1 Performance-based Specifications .....	12-1
12.1.1.2 Other Standardization Documents .....	12-3
12.1.1.3 Overall Acquisition Policy and Procedures .....	12-4
12.1.1.4 Impacts on Reliability Management .....	12-4
12.2 Reliability Program Management Issues .....	12-5
12.3 Reliability Specification Requirements .....	12-6
12.3.1 Template for Preparing Reliability Section of Solicitation .....	12-7
12.3.2 Guidance for Selecting Sources .....	12-15
12.4 Reliability Program Elements .....	12-17
12.5 Phasing of Reliability Program Activities .....	12-19
12.5.1 Reliability Activities by Life Cycle Phase .....	12-20
12.5.1.1 Phase 0 - Concept Exploration .....	12-22
12.5.1.2 Phase I - Program Definition and Risk Reduction .....	12-22
12.5.1.3 Phase II - Engineering and Manufacturing Development .....	12-23
12.5.1.4 Phase III - Production, Deployment, and Operational Support .....	12-24
12.6 R&M Planning and Budgeting .....	12-25
12.6.1 Conceptual Exploration Phase Planning .....	12-26
12.6.2 Program Definition and Risk Reduction .....	12-26
12.6.3 Engineering and Manufacturing Development (EMD) Phase Planning ...	12-27
12.6.4 Production, Deployment, and Operational Support Phase Planning .....	12-28
12.7 Trade-offs .....	12-28
12.7.1 Concept Exploration Phase Trade-off Studies .....	12-29
12.7.2 Program Definition and Risk Reduction Phase Trade-off Studies .....	12-30
12.7.3 Trade-offs During Engineering Manufacturing Development (EMD), Production, Deployment and Operational Support Phases .....	12-31
12.8 Other Considerations .....	12-32
12.8.1 Software Reliability .....	12-32
12.8.1.1 Requirements Definition .....	12-35
12.8.1.2 System Analysis .....	12-35
12.8.1.3 Package Design .....	12-37
12.8.1.4 Unit Design, Code and Debug .....	12-37
12.8.1.5 Module Integration and Test .....	12-37
12.8.1.6 System Integration and Test .....	12-38

## TABLE OF CONTENTS

Section		Page
	12.8.1.7 Acceptance Test .....	12-38
	12.8.1.8 Program Plan .....	12-38
	12.8.1.9 Specifications .....	12-38
	12.8.1.10 Data System .....	12-39
	12.8.1.11 Program Review .....	12-39
	12.8.1.12 Test Plan .....	12-40
	12.8.1.13 Technical Manuals .....	12-40
12.8.2	Cost Factors and Guidelines .....	12-40
	12.8.2.1 Design-To-Cost Procedures .....	12-43
	12.8.2.2 Life Cycle Cost (LCC) Concepts .....	12-45
12.8.3	Product Performance Agreements .....	12-45
	12.8.3.1 Types of Product Performance Agreements .....	12-47
	12.8.3.2 Warranty/Guarantee Plans .....	12-51
12.8.4	Reliability Program Requirements, Evaluation and Surveillance .....	12-53
	12.8.4.1 Reliability Program Requirements Based Upon the Type of Procurement .....	12-53
	12.8.4.2 Reliability Program Evaluation and Surveillance .....	12-55
12.9	References for Section 12 .....	12-56

## TABLE OF CONTENTS

## LIST OF FIGURES

	Page
FIGURE 3-1: INTERVALS OF TIME .....	3-19
FIGURE 4.2-1: SYSTEM MANAGEMENT ACTIVITIES .....	4-4
FIGURE 4.2-2: FUNDAMENTAL SYSTEM PROCESS CYCLE.....	4-6
FIGURE 4.5-1: FLOW DIAGRAM FOR A GENERAL OPTIMIZATION PROCESS .....	4-12
FIGURE 5.2-1: SUMMARY OF BASIC RELIABILITY CONCEPTS .....	5-7
FIGURE 5.3-1: SHAPES OF FAILURE DENSITY, RELIABILITY AND HAZARD RATE FUNCTIONS FOR COMMONLY USED CONTINUOUS DISTRIBUTIONS .....	5-9
FIGURE 5.3-2: SHAPES OF FAILURE DENSITY AND RELIABILITY FUNCTIONS OF COMMONLY USED DISCRETE DISTRIBUTIONS .....	5-10
FIGURE 5.3-3: FIVE CHANNEL RECEIVER WITH TWO FAILURES ALLOWED	5-25
FIGURE 5.4-1: HAZARD RATE AS A FUNCTION OF AGE.....	5-28
FIGURE 5.4-2: STABILIZATION OF FAILURE FREQUENCY .....	5-30
FIGURE 5.4-3: SERIES CONFIGURATION .....	5-31
FIGURE 5.4-4: PARALLEL CONFIGURATION .....	5-33
FIGURE 5.4-5: COMBINED CONFIGURATION NETWORK .....	5-33
FIGURE 5.5-1: SIMPLE PRIOR DISTRIBUTION .....	5-40
FIGURE 5.5-2: SIMPLE POSTERIOR DISTRIBUTION .....	5-41
FIGURE 5.5-3: TREE DIAGRAM EXAMPLE .....	5-42
FIGURE 5.6-1: BASIC METHODS OF MAINTAINABILITY MEASUREMENT .....	5-47
FIGURE 5.6-2: EXAMPLE MAINTAINABILITY FUNCTION DERIVED FROM TIME-TO-REPAIR DISTRIBUTION .....	5-47
FIGURE 5.6-3: PLOT OF THE LOGNORMAL OF THE TIMES-TO-RESTORE DATA GIVEN IN TABLE 5.6-5 IN TERMS OF THE STRAIGHT $t'$ 'S .....	5-56
FIGURE 5.6-4: PLOT OF THE LOGNORMAL PDF OF THE TIMES-TO-RESTORE DATA GIVEN IN TABLE 5.6-5 IN TERMS OF THE LOGARITHMS OF T, OR $\ln t'$ .....	5-58
FIGURE 5.6-5: PLOT OF THE MAINTAINABILITY FUNCTION FOR THE TIMES-TO-REPAIR DATA OF EXAMPLE 2 .....	5-61
FIGURE 5.6-6: EXPONENTIAL APPROXIMATION OF LOGNORMAL MAINTAINABILITY FUNCTIONS .....	5-71
FIGURE 5.7-1: THE RELATIONSHIP BETWEEN INSTANTANEOUS, MISSION, AND STEADY STATE AVAILABILITIES AS A FUNCTION OF OPERATING TIME .....	5-74
FIGURE 5.7-2: MARKOV GRAPH FOR SINGLE UNIT .....	5-75
FIGURE 5.7-3: SINGLE UNIT AVAILABILITY WITH REPAIR.....	5-81
FIGURE 5.8-1: BLOCK DIAGRAM OF A SERIES SYSTEM .....	5-84
FIGURE 5.8-2: RELIABILITY-MAINTAINABILITY TRADE-OFFS .....	5-87

## LIST OF FIGURES

	Page
FIGURE 6.2-1: SATISFACTORY PERFORMANCE LIMITS FOR EXAMPLE RADAR .....	6-4
FIGURE 6.2-2: TEMPERATURE PROFILE .....	6-5
FIGURE 6.2-3: TYPICAL OPERATIONAL SEQUENCE FOR AIRBORNE FIRE CONTROL SYSTEM .....	6-6
FIGURE 6.2-4: EXAMPLE DEFINITION OF RELIABILITY DESIGN REQUIREMENTS IN A SYSTEM SPECIFICATION FOR (1) AVIONICS, (2) MISSILE SYSTEM AND (3) AIRCRAFT .....	6-8
FIGURE 6.4-1: SERVICE USE EVENTS IN THE LOGISTIC AND OPERATIONAL CYCLES .....	6-23
FIGURE 6.4-2: PROGRESSIVE EXPANSION OF RELIABILITY BLOCK DIAGRAM AS DESIGN DETAIL BECOMES KNOWN .....	6-27
FIGURE 6.4-3: RADAR SYSTEM HIERARCHY (PARTIAL LISTING) .....	6-45
FIGURE 6.4-4: SAMPLE RELIABILITY CALCULATION .....	6-56
FIGURE 7.2-1: VENDOR SELECTION METHODOLOGIES.....	7-6
FIGURE 7.2-2: PART OBSOLESCENCE AND DMS PROCESS FLOW .....	7-14
FIGURE 7.2-3: REDUCED SCREEN FLOW.....	7-25
FIGURE 7.3-1: STRESS-STRENGTH DISTRIBUTIONS AND UNRELIABILITY IN DESIGN.....	7-35
FIGURE 7.3-2: NORMAL (GAUSSIAN) STRESS-STRENGTH DISTRIBUTIONS AND UNRELIABILITY IN DESIGN .....	7-36
FIGURE 7.3-3: FACTORS AFFECTING UNRELIABILITY.....	7-37
FIGURE 7.4-1: ON-CHIP DIODE PROTECTION CIRCUIT.....	7-41
FIGURE 7.4-2: (A) FOUR-LAYER STRUCTURE OF AN SCR (B) CURRENT - VOLTAGE CHARACTERISTIC .....	7-44
FIGURE 7.4-3: GROUNDING PRACTICE AT A SINGLE PHASE SERVICE ENTRANCE .....	7-52
FIGURE 7.4-4: CIRCUIT SUBSYSTEMS WITH GROUND CONNECTIONS “DAISY-CHAINED” INVITES PROBLEMS.....	7-53
FIGURE 7.4-5: GROUND TRACES RETURNED TO A COMMON POINT .....	7-54
FIGURE 7.4-6: DIODE PROTECTION OF A BIPOLAR TRANSISTOR .....	7-58
FIGURE 7.4-7: DIODE PROTECTION FOR A DISCRETE MOSFET TRANSISTOR.....	7-58
FIGURE 7.4-8: DIODE PROTECTION FOR SILICON CONTROLLED RECTIFIERS .....	7-59
FIGURE 7.4-9: TRANSIENT PROTECTION FOR A TTL CIRCUIT USING DIODES.....	7-59
FIGURE 7.4-10: TRANSIENT PROTECTION FOR A CMOS CIRCUIT .....	7-60
FIGURE 7.4-11: INPUT PROTECTION FOR POWER SUPPLIES .....	7-60
FIGURE 7.4-12: PROTECTION OF DATA LINES OR POWER BUSES USING A DIODE ARRAY .....	7-61

## TABLE OF CONTENTS

## LIST OF FIGURES

	Page
FIGURE 7.4-13: FUSE PROTECTION FOR A TRANSIENT VOLTAGE SUPPRESSOR DIODE .....	7-62
FIGURE 7.4-14: RESISTOR PARAMETER VARIATION WITH TIME (TYPICAL) ...	7-64
FIGURE 7.4-15: CAPACITOR PARAMETER VARIATION WITH TIME (TYPICAL).....	7-65
FIGURE 7.4-16: RESISTOR PARAMETER CHANGE WITH STRESS AND TIME (TYPICAL).....	7-66
FIGURE 7.4-17: OUTPUT VOLTAGE VERSUS TRANSISTOR GAIN BASED ON A FIGURE APPEARING IN TAGUCHI TECHNIQUES FOR QUALITY ENGINEERING (REFERENCE [21]).....	7-69
FIGURE 7.4-18: RATIO OF $I_{CO}$ OVER TEMPERATURE T TO $I_{CO}$ AT T = 25°C ...	7-79
FIGURE 7.5-1: HARDWARE REDUNDANCY TECHNIQUES .....	7-82
FIGURE 7.5-2: EFFECT OF MAINTENANCE CONCEPT ON LEVEL OF FAULT TOLERANCE.....	7-85
FIGURE 7.5-3: PARALLEL NETWORK.....	7-88
FIGURE 7.5-4: SIMPLE PARALLEL REDUNDANCY: SUMMARY .....	7-91
FIGURE 7.5-5: SERIES-PARALLEL REDUNDANCY NETWORK .....	7-92
FIGURE 7.5-6: RELIABILITY BLOCK DIAGRAM DEPICTING REDUNDANCY AT THE SYSTEM, SUBSYSTEM, AND COMPONENT LEVELS.....	7-93
FIGURE 7.5-7: SERIES-PARALLEL CONFIGURATION .....	7-94
FIGURE 7.5-8: PARALLEL-SERIES CONFIGURATION .....	7-95
FIGURE 7.5-9: DECREASING GAIN IN RELIABILITY AS NUMBER OF ACTIVE ELEMENTS INCREASES.....	7-103
FIGURE 7.5-10: RELIABILITY GAIN FOR REPAIR OF SIMPLE PARALLEL ELEMENT AT FAILURE.....	7-104
FIGURE 7.5-11: PARTIAL REDUNDANT ARRAY.....	7-106
FIGURE 7.5-12: RELIABILITY FUNCTIONS FOR PARTIAL REDUNDANT ARRAY OF FIGURE 7.5-11.....	7-108
FIGURE 7.5-13: REDUNDANCY WITH SWITCHING.....	7-109
FIGURE 7.5-14: THREE-ELEMENT REDUNDANT CONFIGURATIONS WITH SWITCHING .....	7-111
FIGURE 7.5-15: THREE-ELEMENT VOTING REDUNDANCY .....	7-112
FIGURE 7.5-16: MAJORITY VOTING REDUNDANCY .....	7-115
FIGURE 7.5-17: SYSTEM RELIABILITY FOR N STANDBY REDUNDANT ELEMENTS.....	7-116
FIGURE 7.5-18: LOAD SHARING REDUNDANT CONFIGURATION.....	7-117
FIGURE 7.5-19: SUCCESS COMBINATIONS IN TWO-ELEMENT LOAD-SHARING CASE.....	7-118
FIGURE 7.5-20: POSSIBLE REDUNDANT CONFIGURATIONS RESULTING FROM ALLOCATION STUDY .....	7-120
FIGURE 7.5-21: MARKOV MODELING PROCESS.....	7-122

## LIST OF FIGURES

	Page
FIGURE 7.5-22: MARKOV FLOW DIAGRAM .....	7-124
FIGURE 7.5-23: TWO CHANNEL EXAMPLE .....	7-126
FIGURE 7.5-24: COVERAGE EXAMPLE.....	7-127
FIGURE 7.6-1: EFFECTS OF COMBINED ENVIRONMENTS.....	7-130
FIGURE 7.7-1: THE HUMAN IN SYSTEM RELIABILITY AND MAINTAINABILITY [44].....	7-162
FIGURE 7.7-2: THE COGNITIVE HUMAN MODEL.....	7-163
FIGURE 7.7-3: FACTORS THAT AFFECT HUMAN FUNCTION RELIABILITY.....	7-163
FIGURE 7.7-4: ZONES OF HUMAN PERFORMANCE FOR LONGITUDINAL VIBRATION (ADAPTED FROM MIL-STD-1472) .....	7-164
FIGURE 7.7-5: HIERARCHICAL STRUCTURE OF FUNCTIONAL ANALYSIS (EXAMPLE).....	7-166
FIGURE 7.7-6: SIMPLIFIED DYNAMIC PROGRAMMING.....	7-170
FIGURE 7.7-7: TOOLS FOR DESIGNING HUMAN-MACHINE SYSTEMS.....	7-172
FIGURE 7.7-8: GOAL-SUCCESS TREE.....	7-175
FIGURE 7.7-9: CATEGORIES OF HUMAN PERFORMANCE RELIABILITY PREDICTION METHODS .....	7-177
FIGURE 7.7-10: THERP PROBABILITY TREE [62].....	7-180
FIGURE 7.8-1: TYPICAL SYSTEM SYMBOLIC LOGIC BLOCK DIAGRAM .....	7-191
FIGURE 7.8-2: TYPICAL UNIT SYMBOLIC LOGIC BLOCK DIAGRAM .....	7-192
FIGURE 7.8-3: FAILURE EFFECTS ANALYSIS FORM.....	7-200
FIGURE 7.8-4: SYMBOLIC LOGIC DIAGRAM OF RADAR EXAMPLE .....	7-203
FIGURE 7.8-5: DETERMINATION OF PREAMPLIFIER CRITICALITY.....	7-205
FIGURE 7.9-1: FAULT TREE ANALYSIS SYMBOLS .....	7-213
FIGURE 7.9-2: TRANSFORMATION OF TWO-ELEMENT SERIES RELIABILITY BLOCK DIAGRAM TO “FAULT TREE” LOGIC DIAGRAMS .....	7-214
FIGURE 7.9-3: TRANSFORMATION OF SERIES/PARALLEL BLOCK DIAGRAM TO EQUIVALENT FAULT TREE LOGIC DIAGRAM .....	7-215
FIGURE 7.9-4: RELIABILITY BLOCK DIAGRAM OF HYPOTHETICAL ROCKET MOTOR FIRING CIRCUIT.....	7-216
FIGURE 7.9-5: FAULT TREE FOR SIMPLIFIED ROCKET MOTOR FIRING CIRCUIT .....	7-217
FIGURE 7.10-1: AUTOMOTIVE SNEAK CIRCUIT .....	7-223
FIGURE 7.10-2: SNEAK PATH ENABLE.....	7-226
FIGURE 7.10-3: REDUNDANT CIRCUIT SWITCHED GROUND.....	7-226
FIGURE 7.10-4: EXAMPLES OF CATEGORIES OF SNEAK CIRCUITS.....	7-228
FIGURE 7.10-5: BASIC TOPOGRAPHS .....	7-230
FIGURE 7.10-6: SOFTWARE TOPOGRAPHS.....	7-232
FIGURE 7.10-7: SOFTWARE SNEAK EXAMPLE.....	7-234
FIGURE 7.11-1: DESIGN REVIEW AS A CHECK VALVE IN THE SYSTEM ENGINEERING CYCLE .....	7-237



## TABLE OF CONTENTS

## LIST OF FIGURES

	Page
FIGURE 7.11-2: BASIC STEPS IN THE PRELIMINARY DESIGN REVIEW (PDR) CYCLE.....	7-242
FIGURE 7.11-3: DESIGN RELIABILITY TASKS FOR THE PDR.....	7-243
FIGURE 7.11-4: BASIC STEPS IN THE CDR CYCLE.....	7-244
FIGURE 7.11-5: DESIGN RELIABILITY TASKS FOR THE CRITICAL DESIGN REVIEW (CDR).....	7-245
FIGURE 7.11-6: TYPICAL AREAS TO BE COVERED IN A DESIGN REVIEW.....	7-246
FIGURE 7.11-7: TYPICAL QUESTIONS CHECKLIST FOR THE DESIGN REVIEW.....	7-249
FIGURE 7.12-1: SIMPLE SYSTEM SHOWING TEST DEPENDENCIES.....	7-258
FIGURE 7.12-2: REDUNDANCY BIT (SOURCE: RADC-TR-89-209, VOL. II).....	7-261
FIGURE 7.12-3: WRAP-AROUND BIT (SOURCE: RADC-TR-89-209, VOL II).....	7-261
FIGURE 7.14-1: NODAL ANALYSIS.....	7-276
FIGURE 7.14-2: DISPLACEMENT/STRESS INTERPRETATION.....	7-277
FIGURE 7.14-3: DETERMINISTIC ANALYSIS.....	7-277
FIGURE 7.14-4: LIFETIME ESTIMATE.....	7-278
FIGURE 8.2-1: CLOSED LOOP FAILURE REPORTING AND CORRECTIVE ACTION SYSTEM.....	8-4
FIGURE 8.2-2: EXAMPLE OF FAILURE REPORT FORM.....	8-8
FIGURE 8.2-3: CLOSED LOOP FAILURE REPORTING AND CORRECTIVE ACTION SYSTEM WITH FAILURE REVIEW BOARD.....	8-9
FIGURE 8.3-1: GRAPHICAL POINT ESTIMATION FOR THE NORMAL DISTRIBUTION.....	8-14
FIGURE 8.3-2: GRAPHICAL POINT ESTIMATION FOR THE WEIBULL DISTRIBUTION.....	8-20
FIGURE 8.3-3: DISTRIBUTION GRAPHICAL EVALUATION.....	8-21
FIGURE 8.3-4: HAZARD AND DENSITY FUNCTIONS FOR TABLE 8.3-3.....	8-25
FIGURE 8.3-5: RELIABILITY FUNCTIONS FOR THE EXAMPLE GIVEN IN TABLE 8.3-4.....	8-28
FIGURE 8.3-6: NORMAL DISTRIBUTION OF FAILURE IN TIME.....	8-30
FIGURE 8.3-7: CALCULATION AND PRESENTATION OF A NORMAL SURVIVAL CURVE.....	8-30
FIGURE 8.3-8: EXPONENTIAL DISTRIBUTION OF FAILURES IN TIME.....	8-30
FIGURE 8.3-9: CALCULATION AND PRESENTATION OF AN EXPONENTIAL CURVE.....	8-30
FIGURE 8.3-10: OBSERVED AND THEORETICAL EXPONENTIAL SURVIVAL CURVES.....	8-32
FIGURE 8.3-11: OBSERVED AND THEORETICAL NORMAL SURVIVAL CURVES.....	8-32
FIGURE 8.3-12: ACTUAL RELIABILITY FUNCTION AND THEORETICAL EXPONENTIAL RELIABILITY FUNCTION.....	8-34

## LIST OF FIGURES

	Page
FIGURE 8.3-13: NON-PARAMETRIC AND THEORETICAL NORMAL RELIABILITY FUNCTIONS .....	8-36
FIGURE 8.3-14: GEOMETRICAL INTERPRETATION OF THE CONCEPT OF A CONFIDENCE INTERVAL .....	8-39
FIGURE 8.3-15: TWO-SIDED CONFIDENCE INTERVAL AND LIMITS .....	8-41
FIGURE 8.3-16: MULTIPLICATION RATIOS FOR DETERMINING UPPER AND LOWER CONFIDENCE LIMITS VS. NUMBER OF FAILURES FOR TEST TRUNCATED AT A FIXED TIME .....	8-49
FIGURE 8.3-17: CHART FOR 95% CONFIDENCE LIMITS ON THE PROBABILITY S/N .....	8-51
FIGURE 8.3-18: EXAMPLE OF THE APPLICATION OF THE "d" TEST .....	8-57
FIGURE 8.3-19: FUEL SYSTEM FAILURE TIMES .....	8-62
FIGURE 8.3-20: COMPUTATION .....	8-63
FIGURE 8.4-1: NORMAL DISTRIBUTION .....	8-69
FIGURE 8.4-2A: HYPOTHESIS TEST A .....	8-70
FIGURE 8.4-2B: HYPOTHESIS TEST B .....	8-70
FIGURE 8.4-3A: IDEAL OPERATING CHARACTERISTIC (OC) CURVE .....	8-71
FIGURE 8.4-3B: TYPICAL OPERATING CHARACTERISTIC CURVE .....	8-71
FIGURE 8.4-4: ACTUAL OPERATING CHARACTERISTIC CURVE.....	8-72
FIGURE 8.4-5: OC CURVE CHARACTERISTICS .....	8-73
FIGURE 8.4-6: GRAPHICAL SOLUTION OF SEQUENTIAL BINOMIAL TEST .....	8-92
FIGURE 8.5-1: RELIABILITY GROWTH PROCESS.....	8-134
FIGURE 8.5-2: RELIABILITY GROWTH PLOTS.....	8-136
FIGURE 8.5-3: UP-IS-GOOD DUANE CHART WITH PLOT OF CURRENT MTBF .....	8-138
FIGURE 8.5-4: FAILURE RATE VS. DEVELOPMENT TIME FOR WEIBULL FAILURE RATE .....	8-141
FIGURE 8.5-5: FAILURE RATE VS. DEVELOPMENT TEST TIME FOR WEIBULL FAILURE RATE .....	8-144
FIGURE 8.5-6: RELIABILITY GROWTH ANALYSIS (AMSAA MODEL) .....	8-146
FIGURE 8.5-7: RELIABILITY GROWTH PLOTS.....	8-150
FIGURE 8.5-8: COMPARISON OF CUMULATIVE LIFE CYCLE COSTS WITH AND WITHOUT SPECIFIED RELIABILITY GROWTH TEST REQUIREMENTS .....	8-153
FIGURE 8.5-9: RELIABILITY GROWTH MANAGEMENT MODEL (ASSESSMENT) .....	8-155
FIGURE 8.5-10: EXAMPLE OF A RELIABILITY GROWTH CURVE .....	8-156
FIGURE 8.5-11: INFORMATION SOURCES THAT INITIATE RELIABILITY GROWTH .....	8-157
FIGURE 8.6-1: RELIABILITY TESTING OPTIONS .....	8-160
FIGURE 8.7-1: ARRHENIUS ACCELERATION MODEL .....	8-167

## TABLE OF CONTENTS

## LIST OF FIGURES

	Page
FIGURE 8.7-2: STEP STRESS PROFILE .....	8-170
FIGURE 8.7-3: PROGRESSIVE STRESS PROFILE .....	8-171
FIGURE 9.1-1: SOFTWARE ENVIRONMENT TIMELINE .....	9-2
FIGURE 9.1-2: HARDWARE/SOFTWARE SYSTEM LIFE CYCLE RELATIONSHIP (REF. [2]) .....	9-4
FIGURE 9.2-1: BATHTUB CURVE FOR HARDWARE RELIABILITY .....	9-9
FIGURE 9.2-2: REVISED BATHTUB CURVE FOR SOFTWARE RELIABILITY ....	9-11
FIGURE 9.3-1: HIGH-LEVEL SOFTWARE ARCHITECTURE EXAMPLE .....	9-14
FIGURE 9.4-1: WATERFALL MODEL (REF. [6]) .....	9-20
FIGURE 9.4-2: THE CLASSIC DEVELOPMENT MODEL (REF. [7]) .....	9-21
FIGURE 9.4-3: STEPS IN THE PROTOTYPING APPROACH .....	9-23
FIGURE 9.4-4: SPIRAL MODEL (REF. [7]) .....	9-25
FIGURE 9.4-5: INCREMENTAL DEVELOPMENT MODEL (REF. [7]) .....	9-27
FIGURE 9.4-6: THE CLEANROOM DEVELOPMENT PROCESS (REF. [10]) .....	9-29
FIGURE 9.5-1: EXPECTED PROPORTION OF THE TOTAL NUMBER OF DEFECTS .....	9-35
FIGURE 9.5-2: EXPONENTIAL MODEL BASIS .....	9-41
FIGURE 9.6-1: RELIABILITY ALLOCATION PROCESS (REF. [2]) .....	9-52
FIGURE 9.7-1: STRUCTURAL REPRESENTATION OF A SOFTWARE SYSTEM .....	9-60
FIGURE 9.7-2: FLOWCHART FOR SOFTWARE FAILURE DATA ANALYSIS AND DECISION-MAKING .....	9-63
FIGURE 9.8-1: EXAMPLE OF SOFTWARE FMECA .....	9-68
FIGURE 10.1-1: THE COMMERCIAL/NDI DECISION PROCESS .....	10-7
FIGURE 10.2-1: SYSTEM EFFECTIVENESS MODELS .....	10-15
FIGURE 10.3-1: PART DATABASE DISTRIBUTION .....	10-22
FIGURE 10.4-1: PRINCIPAL STEPS REQUIRED FOR EVALUATION OF SYSTEM EFFECTIVENESS .....	10-32
FIGURE 10.4-2: THE AVAILABILITY OF A SINGLE UNIT .....	10-35
FIGURE 10.4-3: AVERAGE AND POINTWISE AVAILABILITY .....	10-39
FIGURE 10.4-4: BLOCK DIAGRAM OF A SERIES SYSTEM .....	10-42
FIGURE 10.4-5: HYPOTHETICAL HISTORY OF MACHINE GUN USAGE .....	10-56
FIGURE 10.4-6: RENEWAL PROCESS IN TERMS OF ROUNDS FIRED .....	10-57
FIGURE 10.4-7: OPERATIONAL READINESS PROBABILITY VERSUS QUEUING FACTOR $\rho$ . FOR POPULATION SIZE $N = 15$ ; NUMBER OF REPAIR CHANNELS $k$ .....	10-72
FIGURE 10.4-8: OPERATIONAL READINESS PROBABILITY VERSUS QUEUING FACTOR $\rho$ . FOR POPULATION SIZE $N = 20$ ; NUMBER OF REPAIR CHANNELS $k$ .....	10-73
FIGURE 10.6-1: RELIABILITY - MAINTAINABILITY - AVAILABILITY RELATIONSHIPS .....	10-77

## LIST OF FIGURES

	Page
FIGURE 10.6-2: AVAILABILITY AS A FUNCTION OF $\lambda/\mu$ .....	10-78
FIGURE 10.6-3: AVAILABILITY AS A FUNCTION OF MTBF AND 1/MTTR .....	10-78
FIGURE 10.6-4: AVAILABILITY NOMOGRAPH .....	10-79
FIGURE 10.6-5: RELIABILITY-MAINTAINABILITY TRADE-OFFS .....	10-82
FIGURE 10.6-6: BLOCK DIAGRAM OF A SERIES SYSTEM .....	10-84
FIGURE 10.7-1: PERMISSIBLE EQUIPMENT FAILURE AND REPAIR RATES FOR $\lambda/\mu = .25$ .....	10-97
FIGURE 10.7-2: UNAVAILABILITY CURVES .....	10-98
FIGURE 10.10-1: LCC CATEGORIES VS. LIFE CYCLE .....	10-111
FIGURE 10.10-2: R&M AND COST METHODS .....	10-114
FIGURE 10.10-3: LIFE CYCLE COSTS VS. RELIABILITY .....	10-116
FIGURE 11.1-1: RELIABILITY LIFE CYCLE DEGRADATION & GROWTH CONTROL .....	11-2
FIGURE 11.2-1: QUALITY ENGINEERING AND CONTROL OVER TIME .....	11-5
FIGURE 11.2-2: ISO 9000 FAMILY OF STANDARDS .....	11-7
FIGURE 11.2-3: LIFE CHARACTERISTIC CURVE .....	11-16
FIGURE 11.2-4: IMPACT OF DESIGN AND PRODUCTION ACTIVITIES ON EQUIPMENT RELIABILITY .....	11-18
FIGURE 11.2-5: "STEP" MTBF APPROXIMATION .....	11-19
FIGURE 11.2-6: MTBF (OUTGOING FROM PRODUCTION) ESTIMATING PROCESS .....	11-23
FIGURE 11.2-7: SAMPLE PROCESS FLOW DIAGRAM .....	11-24
FIGURE 11.2-8: A TYPICAL PRODUCTION PROCESS, FINDING DEFECTS AT THE LOWEST LEVEL OF MANUFACTURE IS THE MOST COST- EFFECTIVE .....	11-28
FIGURE 11.2-9: APPLICATION OF SCREENING WITHIN THE MANUFACTURING PROCESS .....	11-29
FIGURE 11.2-10: EFFECTIVENESS OF ENVIRONMENTAL SCREENS .....	11-31
FIGURE 11.2-11: MIL-HDBK-344 ESS PROCESS .....	11-35
FIGURE 11.2-12: SAMPLE ENVIRONMENTAL TEST CYCLE .....	11-49
FIGURE 11.2-13: REJECT-ACCEPT CRITERIA FOR TEST PLAN XVIIIIC .....	11-50
FIGURE 11.4-1: PROTECTIVE CONTROL DURING SHIPMENT AND STORAGE .	11-60
FIGURE 11.4-2: TECHNICAL APPROACH TO STORAGE SERVICEABILITY STANDARDS (SSS) .....	11-64
FIGURE 11.4-3: STORAGE SERVICEABILITY STANDARD PREPARATION PROCESS .....	11-68
FIGURE 11.4-4: DETERIORATION CLASSIFICATION OF MATERIAL .....	11-69
FIGURE 11.4-5: INSPECTION FREQUENCY MATRIX .....	11-71
FIGURE 11.4-6: CODED QUALITY INSPECTION LEVELS .....	11-73
FIGURE 12.3-1: CHECKLIST FOR EVALUATING RELIABILITY PORTION OF A PROPOSAL .....	12-16

TABLE OF CONTENTS

---

**LIST OF FIGURES**

	Page
FIGURE 12.5-1: LIFE CYCLE PHASES OF A PRODUCT .....	12-21
FIGURE 12.8-1: CONCURRENT SYSTEM DEVELOPMENT PROCESS FOR BOTH HARDWARE AND SOFTWARE (REF. [6]) .....	12-33
FIGURE 12.8-2: SOFTWARE RELIABILITY PROGRAM ELEMENTS BY PROGRAM PHASE .....	12-36
FIGURE 12.8-3: BALANCED DESIGN APPROACH .....	12-41
FIGURE 12.8-4: EXPENDITURES DURING LIFE CYCLE .....	12-42
FIGURE 12.8-5: EFFECT OF EARLY DECISION ON LIFE CYCLE COST .....	12-42
FIGURE 12.8-6: LIFE CYCLE COST ACTIVITIES .....	12-46

## LIST OF TABLES

	Page
TABLE 4.5-1: PARTIAL LIST OF OPTIMIZATION TECHNIQUES .....	4-13
TABLE 5.3-1: VALUES OF THE STANDARD NORMAL DISTRIBUTION FUNCTION .....	5-12
TABLE 5.3-2: ORDINATES F(z) OF THE STANDARD NORMAL CURVE AT z ..	5-13
TABLE 5.3-3: GAMMA FUNCTION $\Gamma(n)$ .....	5-20
TABLE 5.6-1: COMPARISON OF BASIC RELIABILITY AND MAINTAINABILITY FUNCTIONS .....	5-46
TABLE 5.6-2: VALUES OF $\phi$ OR Z(T' <sub>(1-<math>\alpha</math>)</sub> ) MOST COMMONLY USED IN MAINTAINABILITY ANALYSIS .....	5-51
TABLE 5.6-3: TIME-TO-REPAIR DATA ON A GROUND ELECTRONIC SYSTEM .....	5-52
TABLE 5.6-4: CALCULATIONS TO DETERMINE $\bar{t}'$ AND $\sigma_T$ FOR THE DATA IN TABLE 5.6-3 .....	5-54
TABLE 5.6-5: THE PROBABILITY DENSITY OF TIME-TO-REPAIR DATA (FROM TABLE 5.6.2.1.1-1 BASED ON THE STRAIGHT TIMES TO REPAIR AND THE NATURAL LOGARITHM OF THE TIMES TO REPAIR USED TO PLOT FIGURES 5.6-3 AND 5.6-4, RESPECTIVELY.*) .....	5-57
TABLE 5.6-6: VALUES OF $\phi$ FOR SPECIFIED $\alpha$ .....	5-65
TABLE 5.6-7: VALUES OF $k_E$ FOR SPECIFIED $\alpha$ .....	5-68
TABLE 5.7-1: THE AVAILABILITY OF A SINGLE SYSTEM OR UNIT .....	5-82
TABLE 6.3-1: MECHANICAL-ELECTRICAL SYSTEM .....	6-16
TABLE 6.4-1: USES OF RELIABILITY MODELS AND PREDICTIONS .....	6-21
TABLE 6.4-2: TRUTH TABLE CALCULATION FOR THE SYSTEM RELIABILITY DIAGRAM .....	6-35
TABLE 6.4-3: REDUCTION TABULATION .....	6-37
TABLE 6.4-4: LOGIC DIAGRAM EXAMPLES .....	6-39
TABLE 6.4-5: PROS AND CONS OF PHYSICS-OF-FAILURE PREDICTION MODELS .....	6-46
TABLE 6.4-6: ENVIRONMENTAL SYMBOL IDENTIFICATION AND DESCRIPTION .....	6-47
TABLE 6.4-7: RELIABILITY ANALYSIS SIMILAR ITEM .....	6-52
TABLE 6.4-8: GENERIC FAILURE RATE - $\lambda_G$ (FAILURES PER 10 <sup>6</sup> HOURS) FOR DISCRETE SEMICONDUCTORS .....	6-55
TABLE 6.4-9: DISCRETE SEMICONDUCTOR QUALITY FACTORS - $\pi_Q$ .....	6-56
TABLE 6.4-10: MAJOR INFLUENCE FACTORS ON PART RELIABILITY .....	6-57
TABLE 6.4-11: FORMULAS FOR CALCULATING MICROCIRCUIT RELIABILITY .....	6-58
TABLE 6.4-12: BIPOLAR COMPLEXITY FAILURE RATE C1 .....	6-60
TABLE 6.4-13: ENVIRONMENTAL FACTOR - $\pi_E$ .....	6-61

## TABLE OF CONTENTS

## LIST OF TABLES

	Page
TABLE 6.4-14: QUALITY FACTORS - $\pi_Q$ .....	6-61
TABLE 6.4-15: BASIC APPROACH TO RELIABILITY PHYSICS ANALYSIS .....	6-69
TABLE 6.4-16: EXAMPLE OF A PINION RELIABILITY ANALYSIS .....	6-70
TABLE 7.2-1: QUESTIONS FOR PART SUPPLIERS.....	7-7
TABLE 7.2-2: HIDDEN HYBRID CHECKLIST.....	7-11
TABLE 7.2-3: GENERIC PART APPLICATION FACTORS.....	7-17
TABLE 7.3-1: PRINCIPLE RELIABILITY DEPENDENT STRESS FACTORS/DERATING FACTORS.....	7-31
TABLE 7.3-2: DERATING VALUES FOR TRANSISTORS.....	7-32
TABLE 7.4-1: COMPARISON OF PROTECTION DEVICES .....	7-48
TABLE 7.4-2: 0.5 $\mu$ S - 100 KHZ RING WAVE.....	7-56
TABLE 7.4-3: 8/20 $\mu$ S, 1.2/50 $\mu$ S COMBINATION WAVE.....	7-57
TABLE 7.4-4: COMPARISON OF VARIABILITY ANALYSIS METHODS .....	7-68
TABLE 7.5-1: DIAGNOSTIC IMPLICATIONS OF FAULT TOLERANT DESIGN APPROACHES .....	7-83
TABLE 7.5-2: REDUNDANCY TECHNIQUES .....	7-100
TABLE 7.5-3: RELIABILITY CALCULATIONS FOR EXAMPLE 2 .....	7-107
TABLE 7.6-1: ENVIRONMENTAL COVERAGE CHECKLIST (TYPICAL) .....	7-129
TABLE 7.6-2: VARIOUS ENVIRONMENTAL PAIRS.....	7-131
TABLE 7.6-3: ENVIRONMENTAL EFFECTS .....	7-135
TABLE 7.6-4: LOW TEMPERATURE PROTECTION METHODS.....	7-142
TABLE 7.6-5: ENVIRONMENTAL STRESSES IMPROVEMENT TECHNIQUES IN ELECTRONIC EQUIPMENT .....	7-150
TABLE 7.6-6: SYSTEM USE CONDITIONS CHECKLIST (TYPICAL).....	7-154
TABLE 7.6-7: ENVIRONMENTAL ANALYSIS (INDUCED ENVIRONMENT).....	7-156
TABLE 7.6-8: ASSOCIATION OF FACTOR IMPORTANCE WITH REGION OF ENVIRONMENT .....	7-158
TABLE 7.7-1: COMPARISON BETWEEN HARDWARE AND HUMAN RELIABILITY [39].....	7-160
TABLE 7.7-2: HUMAN-MACHINE COMPARATIVE CAPABILITIES.....	7-167
TABLE 7.7-3: DATA BANKS AND THEIR AFFILIATIONS [55] .....	7-171
TABLE 7.7-4: DATA CATEGORIES OF NATIONAL DATA BANKS [55] .....	7-172
TABLE 7.7-5: MAPPS SCOPE.....	7-185
TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS .....	7-193
TABLE 7.8-2: COLUMN DESCRIPTIONS FOR FIGURE 7.8-3 .....	7-200
TABLE 7.8-3: SEVERITY CLASSIFICATION.....	7-207
TABLE 7.8-4: OCCURRENCE RANKING .....	7-207
TABLE 7.8-5: DETECTION RANKING.....	7-209
TABLE 7.11-1: DESIGN REVIEW GROUP, RESPONSIBILITIES AND MEMBERSHIP SCHEDULE.....	7-241
TABLE 7.11-2: RELIABILITY ACTIONS CHECKLIST .....	7-247

## LIST OF TABLES

	Page
TABLE 7.12-1: RISKS AND CONSEQUENCES OF NOT MAKING BIT PART OF PRODUCT DESIGN .....	7-257
TABLE 7.12-2: FIRST ORDER DEPENDENCY MODEL FOR SIMPLE SYSTEM ....	7-258
TABLE 7.12-3: INHERENT TESTABILITY CHECKLIST .....	7-263
TABLE 7.13-1: APPLICATION MATRIX FOR SYSTEM PROGRAM DEVELOPMENT .....	7-273
TABLE 7.13-2: APPLICATION MATRIX FOR FACILITIES ACQUISITION.....	7-274
TABLE 8.3-1: DATA ON TIMES TO FAILURE OF 20 ITEMS .....	8-12
TABLE 8.3-2: MEDIAN RANKS .....	8-15
TABLE 8.3-3: FAILURE DATA FOR TEN HYPOTHETICAL ELECTRONIC COMPONENTS .....	8-23
TABLE 8.3-4: COMPUTATION OF DATA FAILURE DENSITY AND DATA HAZARD RATE .....	8-24
TABLE 8.3-5: FAILURE DATA FOR 1,000 B-52 AIRCRAFT .....	8-26
TABLE 8.3-6: TIME-TO-FAILURE DATA FOR S = 1000 MISSION HOURS .....	8-27
TABLE 8.3-7: COMPUTATION OF THEORETICAL EXPONENTIAL RELIABILITY FUNCTION FOR MTBF = 1546 HOURS .....	8-34
TABLE 8.3-8: OBSERVED FAILURE DATA .....	8-35
TABLE 8.3-9: CONFIDENCE LIMITS - NORMAL DISTRIBUTION .....	8-40
TABLE 8.3-10: CONFIDENCE INTERVAL .....	8-42
TABLE 8.3-11: DISTRIBUTION OF $\chi^2$ (CHI-SQUARE).....	8-44
TABLE 8.3-12: FACTORS FOR CALCULATION OF MEAN LIFE CONFIDENCE INTERVALS FROM TEST DATA (FACTORS = $2/\chi^2_{P,D}$ ) .....	8-48
TABLE 8.3-13: CRITICAL VALUES $d_{\alpha,n}$ OF THE MAXIMUM ABSOLUTE DIFFERENCE BETWEEN SAMPLE AND POPULATION RELIABILITY FUNCTIONS .....	8-54
TABLE 8.7-1: ACTIVATION ENERGIES ASSOCIATED WITH VARIOUS SILICON SEMICONDUCTOR FAILURE MECHANISMS .....	8-166
TABLE 9.2-1: ASSESSING THE ORGANIZATIONAL COMMUNICATIONS GAP .....	9-7
TABLE 9.2-2: SUMMARY: LIFE CYCLE DIFFERENCES .....	9-12
TABLE 9.3-1: SOFTWARE DESIGN TECHNIQUES .....	9-17
TABLE 9.3-2: SOFTWARE CODING TECHNIQUES .....	9-17
TABLE 9.4-1: SOFTWARE DEVELOPMENT PROCESS SELECTION .....	9-18
TABLE 9.4-2: CLEANROOM PERFORMANCE MEASURES (REF. [11]) .....	9-30
TABLE 9.5-1: COMPARING PREDICTION AND ESTIMATION MODELS .....	9-31
TABLE 9.5-2: SOFTWARE RELIABILITY PREDICTION TECHNIQUES .....	9-32
TABLE 9.5-3: TERMS IN MUSA'S EXECUTION TIME MODEL .....	9-33
TABLE 9.5-4: PUTNAM'S TIME AXIS MILESTONES .....	9-34
TABLE 9.5-5: RL-TR-92-52 TERMINOLOGY .....	9-36



## TABLE OF CONTENTS

## LIST OF TABLES

	Page
TABLE 9.5-6: AMOUNT OF HISTORICAL DATA INCLUDED .....	9-36
TABLE 9.5-7: SUMMARY OF THE RL-TR-92-52 MODEL .....	9-37
TABLE 9.5-8: REGRESSION EQUATION COEFFICIENTS .....	9-39
TABLE 9.5-9: NOTATIONS FOR THE EXPONENTIAL DISTRIBUTION MODEL .....	9-41
TABLE 9.5-10: VARIOUS EXPONENTIAL MODELS .....	9-42
TABLE 9.6-1: SOFTWARE RELIABILITY ALLOCATION TECHNIQUES (REF. [2]) .....	9-52
TABLE 9.6-2: SOFTWARE FUNCTIONS BY SYSTEM MODE - EXAMPLE .....	9-51
TABLE 9.6-3: COMPLEXITY PROCEDURES .....	9-56
TABLE 9.8-1: HARDWARE FAILURE SEVERITY LEVELS (REF. [26]) .....	9-65
TABLE 9.8-2: SOFTWARE FAILURE SEVERITY LEVELS (REF. [5]) .....	9-66
TABLE 9.8-3: SOFTWARE FAILURE MODES AND CRITICALITY ANALYSIS CATEGORIES .....	9-67
TABLE 10.1-1: CONCEPT OF SYSTEM EFFECTIVENESS .....	10-1
TABLE 10.1-2: ADVANTAGES AND DISADVANTAGES OF COTS/NDI .....	10-5
TABLE 10.1-3: R&M ACTIVITIES FOR NEW DEVELOPMENT ITEMS AND FOR COTS .....	10-6
TABLE 10.3-1: SYSTEM R&M PARAMETERS .....	10-20
TABLE 10.3-2: PART QUALITY FACTORS (MULTIPLY SERIES MTBF BY) .....	10-22
TABLE 10.3-3: ENVIRONMENTAL CONVERSION FACTORS (MULTIPLY SERIES MTBF BY) .....	10-23
TABLE 10.3-4: TEMPERATURE CONVERSION FACTORS (MULTIPLY SERIES MTBF BY) .....	10-24
TABLE 10.3-5: AIRCRAFT RECEIVER CONVERSION: AIRBORNE OPERATING TO GROUND DORMANT FAILURE RATE (EXAMPLE) .....	10-25
TABLE 10.3-6: RELIABILITY TRANSLATION MODELS .....	10-26
TABLE 10.3-7: DEFINITIONS OF KEY R&M SYSTEM PARAMETERS .....	10-29
TABLE 10.4-1: AVAILABILITY OF SOME REDUNDANT SYSTEMS BASED ON EXPONENTIAL FAILURE AND REPAIR DISTRIBUTIONS ....	10-48
TABLE 10.6-1: ALTERNATIVE DESIGN TRADE-OFF CONFIGURATIONS .....	10-83
TABLE 10.6-2: COST COMPARISON OF ALTERNATIVE DESIGN CONFIGURATIONS .....	10-83
TABLE 10.7-1: PRELIMINARY SYSTEM AND SUBSYSTEM RELIABILITY SPECIFICATIONS .....	10-95
TABLE 10.10-1: LIFE CYCLE COST BREAKDOWN .....	10-115
TABLE 11.2-1: MIL-Q-9858 QUALITY PROGRAM ELEMENTS .....	11-9
TABLE 11.2-2: QUALITY ENGINEERING TASKS .....	11-12
TABLE 11.2-3: FOUR TYPES OF FAILURES .....	11-15

---

**LIST OF TABLES**

	Page
TABLE 11.2-4: SCREENING ENVIRONMENTS VERSUS TYPICAL FAILURE MECHANICS .....	11-37
TABLE 11.2-5: RISKS AND RESULTS OF ESS AT VARIOUS LEVELS .....	11-39
TABLE 11.2-6: BASELINE VIBRATION PROFILE .....	11-42
TABLE 11.2-7: BASELINE THERMAL CYCLE PROFILE .....	11-43
TABLE 11.2-8: TEST CONDITIONS MATRIX (TAKEN FROM MIL-HDBK-781) ...	11-48
TABLE 11.4-1: FAILURE MODES ENCOUNTERED WITH ELECTRONIC COMPONENTS DURING STORAGE .....	11-59
TABLE 11.4-2: STORAGE-INDUCED QUALITY DEFECTS .....	11-65
TABLE 11.5-1: DEPOT MAINTENANCE REQUIREMENT AREAS .....	11-79
TABLE 12.4-1: COMMON RELIABILITY PROGRAM ELEMENTS .....	12-18
TABLE 12.5-1: RELIABILITY PROGRAM ACTIVITIES TO BE CONSIDERED IN THE CONCEPT EXPLORATION PHASE.....	12-22
TABLE 12.5-2: RELIABILITY PROGRAM ACTIVITIES TO BE CONSIDERED IN THE PROGRAM DEFINITION AND RISK REDUCTION PHASE .....	12-23
TABLE 12.5-3: RELIABILITY PROGRAM ACTIVITIES TO BE CONSIDERED IN THE ENGINEERING AND MANUFACTURING DEVELOPMENT PHASE .....	12-24
TABLE 12.5-4: RELIABILITY PROGRAM ACTIVITIES TO BE CONSIDERED IN THE PRODUCTION, DEPLOYMENT, AND OPERATIONAL SUPPORT PHASE .....	12-25
TABLE 12.8-1: TYPES OF DESIGN-TO-COST PROGRAMS .....	12-44
TABLE 12.8-2: FEATURES OF CURRENT WARRANTY-GUARANTEES PLANS ...	12-52

TABLE OF CONTENTS

---

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

## 1.0 SCOPE

### 1.1 Introduction

This Handbook provides procuring activities and development contractors with an understanding of the concepts, principles, and methodologies covering all aspects of electronic systems reliability engineering and cost analysis as they relate to the design, acquisition, and deployment of DoD equipment/systems.

### 1.2 Application

This Handbook is intended for use by both contractor and government personnel during the conceptual, validation, full scale development, production phases of an equipment/system life cycle.

### 1.3 Organization

The Handbook is organized as follows:

SECTION 2	Referenced Documents
SECTION 3	Definitions
SECTION 4	General Statements
SECTION 5	Reliability/Maintainability/Availability Theory
SECTION 6	Reliability Specification, Allocation and Prediction
SECTION 7	Reliability Engineering Design Guidelines
SECTION 8	Reliability Data Collection and Analysis, Demonstration and Growth
SECTION 9	Software Reliability
SECTION 10	Systems Reliability Engineering
SECTION 11	Production and Use (Deployment) R&M
SECTION 12	R&M Management Considerations

SECTION 1: INTRODUCTION

---

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

---

**SECTION 2: REFERENCED DOCUMENTS**

---

**2.0 REFERENCED DOCUMENTS**

The documents cited in this section are for guidance and information.

**2.1 Government Documents****2.1.1 Specifications, Standards and Handbooks**

The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DODISS) and applicable supplement thereto.

**SPECIFICATIONS****Military**

MIL-E-4158	General Specification For Ground Electronic Equipment
MIL-E-5400	General Specifications For Aerospace Electronic Equipment
MIL-E-16400	General Specification For Naval Ship and Shore: Electronic, Interior Communication and Navigation Equipment
MIL-E-17555	Packaging of Electronic and Electrical Equipment, Accessories, and Provisioned Items (Repair Parts)
MIL-M-28787	General Specification For Standard Electronic Modules
MIL-H-38534	General Specification For Hybrid Microcircuits
MIL-I-38535	General Specification For Manufacturing Integrated Circuits
MIL-H-46855	Human Engineering Requirements For Military Systems, Equipment and Facilities
MIL-PRF-19500K	General Specification For Semiconductor Devices
MIL-PRF-3853C	General Specification For Microcircuits
MIL-S-52779	Software Quality Assurance Program Requirements

**SECTION 2: REFERENCED DOCUMENTS**

---

**STANDARDS**Military

MIL-STD-210	Climatic Extremes For Military Equipment
MIL-STD-414	Sampling Procedures and Tables For Inspection by Variables For Percent
MIL-STD-701	Lists of Standard Semiconductor Devices
MIL-STD-721	Definitions of Terms For Reliability, and Maintainability
MIL-STD-750	Tests Methods For Semiconductor Devices
MIL-STD-756	Reliability Modeling and Prediction
MIL-STD-790	Reliability Assurance Program For Electronic Part Specifications
MIL-STD-810	Environmental Test Methods and Engineering Guidelines
MIL-STD-882	System Safety Program Requirements
MIL-STD-883	Test Methods and Procedures For Microelectronics
MIL-STD-975	Standard Parts Derating Guidelines
MIL-STD-1472	Human Engineering Design Criteria For Military Systems, Equipment and Facilities
MIL-STD-1562	Lists of Standard Microcircuits
MIL-STD-1670	Environmental Criteria and Guidelines for Air Launched Weapons
MIL-STD-1686	Electrostatic Discharge Control Program For Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)
MIL-STD-1772	Certification Requirements For Hybrid Microcircuit Facility and Lines
MIL-STD-2155	Failure Reporting, Analysis and Corrective Action System
MIL-STD-2167	Defense System Software Development

## SECTION 2: REFERENCED DOCUMENTS

**HANDBOOKS**Military

MIL-HDBK-454	Standard General Requirements For Electronic Equipment
MIL-HDBK-470	Maintainability Program Requirements For Systems and Equipment
MIL-HDBK-471	Maintainability Verification/Demonstration/Evaluation
MIL-HDBK-781	Reliability Testing For Engineering Development, Qualification and Production
MIL-HDBK-965	Parts Control Program
MIL-HDBK-1547	Technical Requirements For Parts, Materials, and Processes for Space and Launch Vehicles
MIL-HDBK-2084	General Requirements For Maintainability
MIL-HDBK-2164	Environmental Stress Screening Process For Electronic Equipment
MIL-HDBK-2165	Testability Program For Electronic Systems and Equipment

Unless otherwise indicated, copies of federal and military specification, standards, handbooks and bulletins are available from:

Standardization Documents Order Desk  
 Bldg. 4D  
 700 Robbins Avenue  
 Philadelphia, PA 19110-5094  
 For Assistance: (215) 697-2667 or 2179  
 Telephone Order Entry System (Touch-Tone Access Only): (215) 697-1187  
 FAX: (215) 697-2978

Copies of the DODISS's are also available on a yearly subscription basis from the Standardization Documents Order Desk.

## 2.2 Other Referenced Documents

Other referenced documents, government and non-government are listed in other sections of this handbook under "REFERENCES."



SECTION 2: REFERENCED DOCUMENTS

---

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

3.0 DEFINITIONS OF TERMS AND ACRONYMS AND ABBREVIATIONS

3.1 Introduction

The information contained herein is intended for reference only. Many definitions, acronyms, and abbreviations are used in the field of reliability, and no attempt has been made to list them all here. Instead, a compilation of terms from historical documents (such as MIL-STD-721) and key terms from this handbook is provided. In addition, a list of acronyms and abbreviations used in this handbook or commonly associated with reliability and related disciplines, together with their meanings, is provided for the convenience of the reader.

For additional terms and definitions, the reader is referred to the Product Assurance Dictionary by Richard R. Landers, 1996 and those references listed in RL-TR-97-27, "A Primer of US and Non-US Commercial and Government Documents," March 1997.

3.2 Definitions

**-A-**

**ACCESSIBILITY:** A measure of the relative ease of admission to the various areas of an item for the purpose of operation or maintenance.

**ACCEPTANCE TEST:** A test conducted under specified conditions by or on behalf of the customer, using delivered or deliverable items, to determine whether or not the item satisfies specified requirements. Includes acceptance of first production units.

**ACHIEVED:** Obtained as verified by measurement, as in "achieved reliability performance."

**ACTIVE TIME:** That time during which an item is in an operational inventory.

**ADMINISTRATIVE TIME:** That element of delay time, not included in the supply delay time.

**AFFORDABILITY:** Affordability is a measure of how well customers can afford to purchase, operate, and maintain a product over its planned service life. Affordability is a function of product value and product costs. It is the result of a balanced design in which long-term support costs are considered equally with near-term development and manufacturing costs.

**ALERT TIME:** That time during which a product is immediately ready to perform its function or mission if required. No maintenance or other activities that would impede or slow the start of the function or mission is permitted.

**ALIGNMENT:** Performing the adjustments necessary to return an item to specified operation.

### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**AMBIGUITY:** The inability to distinguish which of two or more subunits of a product or item has failed.

**AMBIGUITY GROUP:** The number of possible subunits of a product or item identified by BIT, ETE, or manual test procedures, which might contain the failed hardware or software component.

**ANTHROPOMETRICS:** Quantitative descriptions and measurements of the physical body variations in people. These are useful in human factors design.

**AUTOMATIC TEST EQUIPMENT (ATE):** Equipment that is designed to automatically conduct analysis of functional or static parameters and to evaluate the degree of UUT (Unit Under Test) performance degradation; and may be used to perform fault isolation of UUT malfunctions. The decision making, control, or evaluative functions are conducted with minimum reliance on human intervention and usually done under computer control.

**AVAILABILITY:** A measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time. (Item state at start of a mission includes the combined effects of the readiness-related system R & M parameters, but excludes mission time.)

#### **-B-**

**BUILT-IN-TEST (BIT):** An integral capability of the mission equipment which provides an on-board, automated test capability, consisting of software or hardware (or both) components, to detect, diagnose, or isolate product (system) failures. The fault detection and, possibly, isolation capability is used for periodic or continuous monitoring of a system's operational health, and for observation and, possibly, diagnosis as a prelude to maintenance action.

**BUILT-IN TEST EQUIPMENT (BITE):** Any device permanently mounted in the prime product or item and used for the express purpose of testing the product or item, either independently or in association with external test equipment.

**BURN-IN:** Also known as preconditioning, burn-in is the operation of an item under stress to stabilize its characteristics. Not to be confused with debugging.

#### **-C-**

**CALIBRATION:** A comparison of a measuring device with a known standard and a subsequent adjustment to eliminate any differences. Not to be confused with alignment.

**CHARGEABLE:** Within the responsibility of a given organizational entity. Used with terms such as failures, maintenance time, etc.

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**CHECKOUT TIME:** That element of maintenance time during which performance of an item is verified to be a specified condition.

**CHECKOUT:** Tests or observations of an item to determine its condition or status.

**COMMERCIAL ITEM:** Any item, other than real property, that is of a type customarily used for nongovernmental purposes and that has been sold, leased, or licensed to the general public, or has been offered for sale, lease, or license to the general public; items evolved from these items that are not yet available in the commercial market but will be in time to meet the delivery requirements of a solicitation. (See “Buying Commercial and Non-Developmental Items: A Handbook [SD-2, Apr 1996, OUSD/A&T]” or the Federal Acquisition Regulation, Parts 6, 10, 11, 12 and 14, for a complete definition and criteria.)

**COMMERCIAL-OFF-THE-SHELF (COTS):** Items available in a domestic or foreign commercial marketplace and usually ordered by part number.

**COMPONENT:** Within a product, system, subsystem, or equipment, a component is a constituent module, part, or item.

**COMPUTER-AIDED DESIGN (CAD):** A process which uses a computer system to assist in the creation, modification, verification, and display of a design.

**CONFIGURATION ITEM (CI):** A collection of hardware and software which satisfies a defined end-use function. The CI is designated for separate as-designed, as-built and as-shipped content makeup management control.

**CONTRACT DELIVERABLES REQUIREMENTS LIST (CDRL):** A listing of all technical data and information which the contractor must deliver to the Customer.

**CORRECTIVE ACTION:** A documented design, process, procedure, or materials change implemented and validated to correct the cause of failure or design deficiency.

**CORRECTIVE MAINTENANCE (CM):** All actions performed as a result of failure, to restore an item to a specified condition. Corrective maintenance can include any or all of the following steps: Localization, Isolation, Disassembly, Interchange, Reassembly, Alignment and Checkout.

**CRITICAL DESIGN REVIEW (CDR):** The comparative evaluation of an item and program parameters. It is usually held just prior to production release after the item has reached a degree of completion permitting a comprehensive examination and analysis.

**CRITICALITY:** A relative measure of the consequence and frequency of occurrence of a failure mode.

### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

#### **-D-**

**DATA ITEM DESCRIPTION (DID):** A Government form used to define and describe the written outputs required from a contractor.

**DEBUGGING:** A process to detect and remedy inadequacies in an item. Not to be confused with burn-in, fault-isolation, or screening.

**DEGRADATION:** A gradual decrease in an item's characteristic or ability to perform.

**DELAY TIME:** That element of downtime during which no maintenance is being accomplished on the item because of either supply or administrative delay.

**DEMONSTRATED:** That which has been measured using objective evidence gathered under specified and predetermined conditions.

**DEMONSTRATION TEST:** A test conducted under specified conditions, by or on behalf of the customer, using items representative of the production configuration, in order to determine compliance with item design requirements as a basis for production approval (also known as a Qualification Test).

**DEPENDABILITY:** A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given that the item is available at mission start. (Item state during a mission includes the combined effects of the mission-related system R&M parameters but excludes non-mission time; see availability.)

**DERATING:** (a) Using an item in such a way that applied stresses are below rated values. (b) The lowering of the rating of an item in one stress field to allow an increase in another stress field.

**DETECTABLE FAILURE:** Failures at the component, equipment, subsystem, or system (product) level that can be identified through periodic testing or revealed by an alarm or an indication of an anomaly.

**DEVELOPMENT TEST:** Testing performed during development and integration to ensure critical design parameters are met, verify the performance of an item's design, and produce data supporting design improvements. Development test, sometimes called engineering test, also discloses deficiencies and verifies that corrective action effectively prevents recurrence of these deficiencies. Properly done, development test reduces the risk of redesign being necessary following demonstration testing or delivery to the customer.

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**DEVELOPMENT TEST AND EVALUATION (DT&E):** Test and evaluation focused on the technological and engineering aspects of the product (system, subsystem, or equipment).

**DIAGNOSTICS:** The hardware, software, or other documented means used to determine that a malfunction has occurred and to isolate the cause of the malfunction. Also refers to "the action of detecting and isolating failures or faults."

**DIRECT MAINTENANCE MANHOURS PER MAINTENANCE ACTION (DMMH/MA):** A measure of the maintainability parameter related to item demand for maintenance labor. The sum of direct maintenance labor hours divided by the total number of preventive and corrective maintenance actions during a stated period of time.

**DIRECT MAINTENANCE MANHOURS PER MAINTENANCE EVENT (DMMH/ME):** A measure of the maintainability parameter related to item demand for maintenance labor. The sum of direct maintenance labor hours, divided by the total number of preventive and corrective maintenance events during a stated period of time.

**DISASSEMBLE:** Opening an item and removing a number of parts or subassemblies to make the item that is to be replaced accessible for removal. This does not include the actual removal of the item to be replaced.

**DORMANT:** A state in which an item is able to but is not required to function. Most often associated with long-term storage and "wooden" rounds. Not to be confused with downtime.

**DOWNING EVENT:** An event which causes an item to become unavailable to begin a mission (i.e., the transition from up-time to down-time).

**DOWNTIME:** That element of time during which an item is in an operational inventory but is not in condition to perform its required function.

**DURABILITY:** A measure of an item's useful life (a special case of reliability). Often referred to as ruggedness.

**-E-**

**ENVIRONMENT:** The aggregate of all external and internal conditions (such as temperature, humidity, radiation, magnetic and electrical fields, shock, vibration, etc.), whether natural, man-made, or self-induced, that influences the form, fit, or function of an item.

**ENVIRONMENTAL STRESS SCREENING (ESS):** A series of tests conducted under environmental stresses to disclose weak parts and workmanship defects so that corrective action can be taken.

### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**EQUIPMENT:** A general term designating an item or group of items capable of performing a complete function.

#### **-F-**

**FAILURE:** The event, or inoperable state, in which any item or part of an item does not, or would not, perform as previously specified.

**FAILURE ANALYSIS:** Subsequent to a failure, the logical systematic examination of an item, its construction, application, and documentation to identify the failure mode and determine the failure mechanism and its basic course.

**FAILURE, CATASTROPHIC:** A failure that causes loss of the item, human life, or serious collateral damage to property.

**FAILURE, CRITICAL:** A failure or combination of failures that prevents an item from performing a specified mission.

**FAILURE, DEPENDENT:** A failure of one item caused by the failure of an associated item(s). A failure that is not independent.

**FAILURE EFFECT:** The consequence(s) a failure mode has on the operation, function, or status of an item. Failure effects are typically classified as local, next higher level, and end.

**FAILURE, INDEPENDENT:** A failure of an item that is not caused by the failure of any other item. A failure that is not dependent.

**FAILURE, INTERMITTENT:** Failure for a limited period of time, followed by the item's recovery of its ability to perform within specified limits without any remedial action.

**FAILURE MECHANISM:** The physical, chemical, electrical, thermal or other process which results in failure.

**FAILURE MODE:** The consequence of the mechanism through which the failure occurs, i.e., short, open, fracture, excessive wear.

**FAILURE MODE AND EFFECTS ANALYSIS (FMEA):** A procedure for analyzing each potential failure mode in a product to determine the results or effects thereof on the product. When the analysis is extended to classify each potential failure mode according to its severity and probability of occurrence, it is called a Failure Mode, Effects, and Criticality Analysis (FMECA).

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**FAILURE, NON-CHARGEABLE:** (a) A non-relevant failure. (b) A relevant failure caused by a condition previously not specified as being the responsibility of a given organizational entity. All relevant failures are chargeable to one organizational entity or another.

**FAILURE, NON-RELEVANT:** (a) A failure verified as having been caused by a condition not present in the operational environment. (b) A failure verified as peculiar to an item design that will not enter the operational, or active, inventory.

**FAILURE, RANDOM:** A failure, the occurrence of which cannot be predicted except in a probabilistic or statistical sense.

**FAILURE RATE:** The total number of failures within an item population, divided by the total number of life units expended by that population, during a particular measurement period under stated conditions.

**FALSE ALARM RATE (FAR):** The frequency of occurrence of false alarms over a defined period of measure (e.g., time, cycles, etc.).

**FALSE ALARM:** A fault indicated by BIT or other monitoring circuitry where no fault can be found or confirmed.

**FAULT:** Immediate cause of failure (e.g., maladjustment, misalignment, defect, etc.).

**FAULT DETECTION (FD):** A process which discovers the existence of faults.

**FAULT ISOLATION (FI):** The process of determining the location of a fault to the extent necessary to effect repair.

**FAULT ISOLATION TIME:** The time spent arriving at a decision as to which items caused the system to malfunction. This includes time spent working on (replacing, attempting to repair, and adjusting) portions of the system shown by subsequent interim tests not to have been the cause of the malfunction.

**FAULT LOCALIZATION:** The process of determining the approximate location of a fault.

**FRACTION OF FAULTS DETECTABLE (FFD):** That fraction of all failures that occur over operating time,  $t$ , that can be correctly identified through direct observation or other specified means by an operator or by maintenance personnel under stated conditions.

**FRACTION OF FAULTS ISOLATABLE (FFI):** That fraction of all failures that occur over operating time,  $t$ , that can be correctly isolated to  $n$  or fewer units at a given maintenance level through the use of specified means by maintenance personnel under stated conditions.



### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**FUNCTIONAL TEST:** An evaluation of a product or item while it is being operated and checked under limited conditions without the aid of its associated equipment in order to determine its fitness for use.

#### **-G-**

**GOVERNMENT-FURNISHED EQUIPMENT (GFE):** An item provided for inclusion in or use with a product or service being procured by the Government.

**GUIDE SPECIFICATION:** This is a type of performance specification prepared by the Government. It identifies standard, recurring requirements that must be addressed when developing new systems, subsystems, equipments, and assemblies. Its structure forces appropriate tailoring to meet user needs.

#### **-H-**

**HUMAN ENGINEERING (HE):** The application of scientific knowledge to the design of items to achieve effective user-system integration (man-machine interface).

**HUMAN FACTORS:** A 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, work loads, and human performance evaluation.

#### **-I-**

**INACTIVE TIME:** That time during which an item is in reserve. (In an inactive inventory).

**INHERENT AVAILABILITY(A<sub>i</sub>):** A measure of availability that includes only the effects of an item design and its application, and does not account for effects of the operational and support environment. Sometimes referred to as "intrinsic" availability.

**INHERENT R&M VALUE:** A measure of reliability or maintainability that includes only the effects of an item's design and application, and assumes an ideal operating and support environment.

**INITIAL ISOLATION LEVEL OF AMBIGUITY:** The initial number of possible product subunits, identified by the built-in-test, built-in-test equipment, external test equipment, or manual test procedure, which might contain the failed component.

**INITIAL ISOLATION:** Isolation to the product subunit which must be replaced on line to return the product to operation. A subunit can be a modular assembly, or a component such as a crystal

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

or antenna subsection. In the event that the maintenance concept requires a subunit to be removed, repaired and then replaced in the product, initial isolation includes both isolation to the failed subunit and isolation to the failed and removable portion of the subunit.

**INTEGRATED DIAGNOSTICS:** A structured process which maximizes the effectiveness of diagnostics by integrating pertinent elements, such as testability, automatic and manual testing, training, maintenance aiding, and technical information as a means for providing a cost effective capability to unambiguously detect and isolate all faults known or expected in items and to satisfy system mission requirements. Products of this process are hardware, software, documentation, and trained personnel.

**INTEGRATED PRODUCT TEAM:** A concurrent engineering team made up of individuals representing all relevant disciplines associated with a product's design, manufacturing, and marketing. All members work together using shared knowledge and capabilities to develop and manufacture a product in which requirements are balanced. The individuals must be committed to a common purpose, work to a unified set of requirements, and hold themselves accountable for decisions made and actions taken.

**INTERCHANGE:** Removing the item that is to be replaced, and installing the replacement item.

**INTERCHANGEABILITY:** The ability to interchange, without restriction, like equipments or portions thereof in manufacture, maintenance, or operation. Like products are two or more items that possess such functional and physical characteristics as to be equivalent in performance and durability, and are capable of being exchanged one for the other without alteration of the items themselves or of adjoining items, except for adjustment, and without selection for fit and performance.

**INTERFACE DEVICE:** An item which provides mechanical and electrical connections and any signal conditioning required between the automatic test equipment (ATE) and the unit under test (UUT); also known as an interface test adapter or interface adapter unit.

**INVENTORY, ACTIVE:** The group of items assigned to an operational status.

**INVENTORY, INACTIVE:** The group of items being held in reserve for possible future assignment to an operational status.

**ISOLATION:** Determining the location of a failure to the extent possible.

**ITEM:** A general term used to denote any product, system, material, part, subassembly, set, accessory, shop replaceable assembly (SRA), Shop Replaceable Unit (SRU), Weapon Replaceable Assembly (WRA), Line Replaceable Unit (LRU), etc.

### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

#### **-L-**

**LEVELS OF MAINTENANCE:** The division of maintenance, based on different and requisite technical skill, which jobs are allocated to organizations in accordance with the availability of personnel, tools, supplies, and the time within the organization. Within the DoD, typical maintenance levels are organizational, intermediate and depot.

**LIFE CYCLE COST (LCC):** The sum of acquisition, logistics support, operating, and retirement and phase-out expenses.

**LIFE CYCLE PHASES:** Identifiable stages in the life of a product from the development of the first concept to removing the product from service and disposing of it. Within the Department of Defense, four phases are formally defined: Concept Exploration; Program Definition and Risk Reduction; Engineering and Manufacturing Development; and Production, Deployment, and Operational Support. Although not defined as a phase, demilitarization and disposal is defined as those activities conducted at the end of a product's useful life. Within the commercial sector, various ways of dividing the life cycle into phases are used. One way is: Customer Need Analysis, Design and Development, Production and Construction, Operation and Maintenance, and Retirement and Phase-out.

**LIFE PROFILE:** A time-phased description of the events and environments experienced by an item throughout its life. Life begins with manufacture, continues during operational use (during which the item has one or more mission profiles), and ends with final expenditure or removal from the operational inventory.

**LINE REPLACEABLE UNIT (LRU):** A unit designed to be removed upon failure from a larger entity (product or item) in the operational environment, normally at the organizational level.

**LIFE UNITS:** A measure of use duration applicable to the item. Measures include time, cycles, distance, rounds fired, attempts to operate, etc.

**LOCALIZATION:** Determining the location of a failure to the extent possible, without using accessory test equipment.

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**-M-**

**MAINTAINABILITY:** The relative ease and economy of time and resources with which an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. Also, the probability that an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

**MAINTAINABILITY, MISSION:** Maintainability as measured when maintenance is performed during the course of a specified mission profile. A mission-related system maintainability parameter.

**MAINTENANCE:** All actions necessary for retaining an item in or restoring it to a specified condition.

**MAINTENANCE ACTION:** An element of a maintenance event. One or more tasks (i.e., fault localization, fault isolation, servicing and inspection) necessary to retain an item in or restore it to a specified condition.

**MAINTENANCE, CORRECTIVE:** See Corrective Maintenance.

**MAINTENANCE EVENT:** One or more maintenance actions required to effect corrective and preventive maintenance due to any type of failure or malfunction, false alarm or scheduled maintenance plan.

**MAINTENANCE, MANNING LEVEL:** The total number of authorized or assigned personnel to support a given system at specified levels of maintenance.

**MAINTENANCE, PREVENTIVE:** See Preventive Maintenance.

**MAINTENANCE RATIO:** A measure of the total maintenance manpower burden required to maintain an item. It is expressed as the cumulative number of labor hours of maintenance expended in direct labor during a given period of the life units divided by the cumulative number of end item life units during the same period.

**MAINTENANCE, SCHEDULED:** See Scheduled Maintenance

**MAINTENANCE, UNSCHEDULED:** See Unscheduled Maintenance

### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**MAINTENANCE TASK:** The maintenance effort necessary for retaining an item in, or changing/restoring it to a specified condition.

**MAINTENANCE TIME:** An element of downtime which excludes modification and delay time.

**MEAN DOWNTIME (MDT):** The average time a system is unavailable for use due to a failure. Time includes the actual repair time plus all delay time associated with a repair person arriving with the appropriate replacement parts.

**MEAN MAINTENANCE TIME:** A basic measure of maintainability taking into account maintenance policy. The sum of preventive and corrective maintenance times, divided by the sum of scheduled and unscheduled maintenance events, during a stated period of time.

**MEAN TIME BETWEEN DEMAND (MTBD):** A measure of system reliability related to demand for logistic support. The total number of system life units divided by the total number of system demands on the supply system during a stated period of time.

**MEAN TIME BETWEEN DOWNING EVENTS:** A measure of system reliability related to readiness and availability. The total number of system life units divided by the total number of events which cause the system to be unavailable to initiate its mission(s), over a stated period of time.

**MEAN TIME BETWEEN CRITICAL FAILURE (MTBCF):** A measure of mission or functional reliability. The mean number of life units during which the item performs its mission or function within specified limits, during a particular measurement interval under stated conditions.

**MEAN TIME BETWEEN FAILURE (MTBF):** A basic measure of reliability for repairable items. The mean number of life units during which all parts of the item perform within their specified limits, during a particular measurement interval under stated conditions.

**MEAN TIME BETWEEN MAINTENANCE (MTBM):** A measure of the reliability taking into account maintenance policy. The total number of life units expended by a given time, divided by the total number of maintenance events (scheduled and unscheduled) due to that item.

**MEAN TIME BETWEEN MAINTENANCE ACTIONS (MTBMA):** A measure of the product reliability parameter related to demand for maintenance labor. The total number of product life units, divided by the total number of maintenance actions (preventive and corrective) during a stated period of time.

**MEAN TIME BETWEEN REMOVALS (MTBR):** A measure of the product reliability parameter related to demand for logistic support: The total number of system life units divided by the total number of items removed from that product during a stated period of time. This term

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

is defined to exclude removals performed to facilitate other maintenance and removals for product improvement.

**MEAN TIME TO FAILURE (MTTF):** A basic measure of reliability for non-repairable items. The total number of life units of an item population divided by the number of failures within that population, during a particular measurement interval under stated conditions.

**MEAN TIME TO REPAIR (MTTR):** A basic measure of maintainability. The sum of corrective maintenance times at any specific level of repair, divided by the total number of failures within an item repaired at that level, during a particular interval under stated conditions.

**MEAN TIME TO RESTORE SYSTEM (MTTRS):** A measure of the product maintainability parameter, related to availability and readiness: The total corrective maintenance time, associated with downing events, divided by the total number of downing events, during a stated period of time. (Excludes time for off-product maintenance and repair of detached components.)

**MEAN TIME TO SERVICE (MTTS):** A measure of an on-product maintainability characteristic related to servicing that is calculated by dividing the total scheduled crew/operator/driver servicing time by the number of times the item was serviced.

**MISSION RELIABILITY:** The measure of the ability of an item to perform its required function for the duration of a specified mission profile. Mission reliability defines the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation.

**MISSION PROFILE:** A time-phased description of the events and environments experienced by an item during a given mission. The description includes the criteria for mission success and critical failures.

**MISSION TIME:** That element of up time required to perform a stated mission profile.

**MISSION-TIME-TO-RESTORE-FUNCTIONS (MTTRF):** A measure of mission maintainability: The total corrective critical failure maintenance time, divided by the total number of critical failures, during the course of a specified mission profile.

**MODIFICATION TIME:** That time during which a product is being modified to enhance or expand functionality, correct a design deficiency, improve safety or reliability through design changes, or to bring the product up to the latest configuration.

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**-N-**

**NON-DEVELOPMENTAL ITEM (NDI):** Any previously developed item used exclusively for governmental purposes by a Federal agency, a State or local government, or a foreign government with which the U.S. has a mutual defense cooperation agreement; any such item with minor modifications; and any item fully developed and in production but not yet in use. (See “Buying Commercial and Non-Developmental Items: A Handbook [SD-2, Apr 1996, OUSD/A&T]” or the Federal Acquisition Regulation Parts 6, 10, 11, 12 and 14, for a complete definition and criteria.)

**NON-DESTRUCTIVE INSPECTION (NDI):** Any method used for inspecting an item without physically, chemically, or otherwise destroying or changing the design characteristics of the item. However, it may be necessary to remove paint or other external coatings to use the NDI method. A wide range of technology is usually described as nondestructive inspection, evaluation, or testing (collectively referred to as non-destructive evaluation or NDE). The core of NDE is commonly thought to contain ultrasonic, visual, radiographic, eddy current, liquid penetrant, and magnetic particle inspection methods. Other methodologies, include acoustic emission, use of laser interference, microwaves, magnetic resonance imaging, thermal imaging, and so forth.

**NON-DETECTABLE FAILURE:** Failures at the component, equipment, subsystem, or system (product) level that are identifiable by analysis but cannot be identified through periodic testing or revealed by an alarm or an indication of an anomaly.

**NOT-OPERATING TIME:** That time during which the product is operable according to all indications or the last functional test, but is not being operated.

**-O-**

**OPERABLE:** The state in which an item is able to perform its intended function(s).

**OPERATIONAL ENVIRONMENT:** The aggregate of all external and internal conditions (such as temperature, humidity, radiation, magnetic and electric fields, shock vibration, etc.) either natural or man made, or self-induced, that influences the form, operational performance, reliability or survival of an item.

**OPERATIONAL R&M:** A measure of reliability and maintainability that includes the combined effects of design, installation, quality, environment, operation, maintenance, etc. on an item.

**OPERATIONAL READINESS:** The ability of a military unit to respond to its operation plan(s) upon receipt of an operations order. (A function of assigned strength, item availability, status, or supply, training, etc.).

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

OPERATIONAL TEST AND EVALUATION (OT&E): Test and evaluation which focuses on the development of optimum tactics, techniques, procedures, and concepts for products and items, evaluation of reliability, maintainability and operational effectiveness, and suitability of products and items under realistic operational conditions.

**-P-**

PERCENT ISOLATION TO A GROUP OF RIs: The percent of time that detected failures can be fault isolated to a specified ambiguity group of size n or less, where n is the number of replaceable items (RIs).

PERCENT ISOLATION TO A SINGLE RI: The percent of time that detected failures can be fault isolated to exactly one replaceable item (RI).

PERFORMANCE SPECIFICATION (PS): A design document stating the functional requirements for an item.

PERFORMANCE-BASED REQUIREMENTS (SPECIFICATION): Requirements that describe what the product should do, how it should perform, the environment in which it should operate, and interface and interchangeability characteristics. They should not specify how the product should be designed or manufactured.

PREDICTED: That which is expected at some future time, postulated on analysis of past experience and tests.

PROCESS ACTION TEAM (PAT): A group of individuals with complementary skills, committed to a common purpose, set of performance goals, and approach for which they hold themselves accountable, who work together using shared knowledge and capabilities to improve business processes.

PROGRAM-UNIQUE SPECIFICATION. This type of Government specification, also called a system specification, establishes requirements for items used for a particular weapon system or program. Little potential exists for the use of the document in other programs or applications. It is written as a performance specification, but it may include a blend of performance and detail design type requirements.

PREPARATION TIME: The time spent obtaining, setting up, and calibrating maintenance aids; warming up equipment; etc.

PREVENTIVE MAINTENANCE (PM): All actions performed to retain an item in specified condition by providing systematic inspection, detection, and prevention of incipient failures.



### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

#### **-Q-**

**QUALIFICATION TEST:** A test conducted under specified conditions, by or on behalf of the customer, using items representative of the production configuration, to determine if item design requirements have been satisfied. Serves as a basis for production approval. Also known as a Demonstration Test.

#### **-R-**

**REACTION TIME:** The time between the instant a product is required to perform a function or mission and the time it is ready to perform that function or mission. It is the time needed for a product to be transitioned from a non-operating state to an operating state.

**REASSEMBLY:** Assembling the items that were removed during disassembly and closing the reassembled items.

**RECONDITIONING:** See Burn-In.

**REDUNDANCY:** The existence of more than one means for accomplishing a given function. Each means of accomplishing the function need not necessarily be identical. The two basic types of redundancy are active and standby.

Active Redundancy - Redundancy in which all redundant items operate simultaneously.

Standby Redundancy - Redundancy in which some or all of the redundant items are not operating continuously but are activated only upon failure of the primary item performing the function(s).

**RELEVANT:** That which can occur or recur during the life of an item.

**RELIABILITY:** (1) The duration or probability of failure-free performance under stated conditions. (2) The probability that an item can perform its intended function for a specified interval under stated conditions. (For non-redundant items this is equivalent to definition (1). For redundant items this is equivalent to definition of mission reliability.)

**RELIABILITY-CENTERED MAINTENANCE (RCM):** A disciplined logic or methodology used to identify preventive and corrective maintenance tasks to realize the inherent reliability of equipment at a minimum expenditure of resources.

**RELIABILITY GROWTH:** The improvement in reliability that results when design, material, or part deficiencies are revealed by testing and eliminated or mitigated through corrective action.

---

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**REPAIR TIME:** The time spent replacing, repairing, or adjusting all items suspected to have been the cause of the malfunction, except those subsequently shown by interim test of the system not to have been the cause.

**REPAIRABILITY:** The probability that a failed item will be restored to operable condition within a specified time of active repair.

**REPAIRABLE ITEM:** An item which, when failed, can be restored by corrective maintenance to an operable state in which it can perform all required functions

**REPLACEABLE ITEM (RI) or REPLACEABLE UNIT (RU):** An item, unit, subassembly, or part which is normally intended to be replaced during corrective maintenance after its failure.

**REQUEST FOR PROPOSAL (RFP):** A letter or document sent to suppliers asking to show how a problem or situation can be addressed. Normally the supplier's response proposes a solution and quotes a price. Similar to a Request for Quote (RFQ), although the RFQ is usually used for products already developed.

**-S-**

**SCHEDULED MAINTENANCE:** Periodic prescribed inspection and servicing of products or items accomplished on the basis of calendar, mileage or hours of operation. Included in Preventive Maintenance.

**SCREENING:** A process for inspecting items to remove those that are unsatisfactory or likely to exhibit early failure. Inspection methods includes visual examination, physical dimension measurement, and functional performance measurement under specified environmental conditions.

**SERVICEABILITY:** The relative ease with which an item can be serviced (i.e., kept in operating condition).

**SERVICING:** The performance of any act needed to keep an item in operating condition, (i.e. lubricating, fueling, oiling, cleaning, etc.), but not including preventive maintenance of parts or corrective maintenance tasks.

**SINGLE-POINT FAILURE:** A failure of an item that causes the system to fail and for which no redundancy or alternative operational procedure exists.

**SNEAK CIRCUIT ANALYSIS:** An analytical procedure for identifying latent paths that cause occurrence of unwanted functions or inhibit desired functions, assuming all components are operating properly.

### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**STANDARD PERFORMANCE SPECIFICATION (SPS):** A type of specification that establishes requirements for military-unique items used in multiple programs or applications.

**STORAGE LIFE:** The length of time an item can be stored under specified conditions and still meet specified operating requirements. Also called shelf life.

**SUBSYSTEM:** A combination of sets, groups, etc. which performs an operational function within a product (system) and is a major subdivision of the product. (Example: Data processing subsystem, guidance subsystem).

**SUPPLY DELAY TIME:** The time between the demand on the supply system for a part or item to repair a product, or for a new product to replace a failed product, and the time when it is available.

**SYSTEM:** A composite of equipment and skills, and techniques capable of performing or supporting an operational role, or both. A complete system includes all equipment, related facilities, material, software, services, and personnel required for its operation and support to the degree that it can be considered self-sufficient in its intended operational environment.

**SYSTEM DOWNTIME:** The time interval between the commencement of work on a system (product) malfunction and the time when the system has been repaired and/or checked by the maintenance person, and no further maintenance activity is executed.

**SYSTEM EFFECTIVENESS:** (a) For repairable systems and items: the probability that a system can successfully meet an operational demand within a given time when operated under specified conditions. (b) For "one-shot" devices and non-repairable items: the probability that the system will operate successfully when called upon to do so under specified conditions.

**SYSTEM FINAL TEST TIME:** The time spent confirming that a system is in satisfactory operating condition (as determined by the maintenance person) following maintenance. It is possible for a system final test to be performed after each correction of a malfunction.

**SYSTEM R&M PARAMETER:** A measure of reliability or maintainability in which the units of measurement are directly related to operational readiness, mission success, maintenance labor costs, or logistics support costs.

#### **-T-**

**TESTABILITY:** A design characteristic which allows an item's status (operable, inoperable, or degraded) be determined and faults within the item to be isolated in a timely manner.

## SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

**TEST, ANALYZE, AND FIX (TAAF):** A synonym for reliability growth in which the three main elements (test, analyze deficiencies, and take corrective action) for achieving reliability growth are identified.

**TEST, MEASUREMENT, AND DIAGNOSTIC EQUIPMENT (TMDE):** Any product or item used to evaluate the condition of another product or item to identify or isolate any actual or potential failures.

**TEST POINT:** A jack or similar fitting to which a test probe is attached for measuring a circuit parameter or wave form.

**TIME:** Time is a fundamental element used in developing the concept of reliability and is used in many of the measures of reliability. Determining the applicable interval of time for a specific measurement is a prerequisite to accurate measurement.. In general, the interval of interest is calendar time, but this can be broken down into other intervals as shown in Figure 3-1.

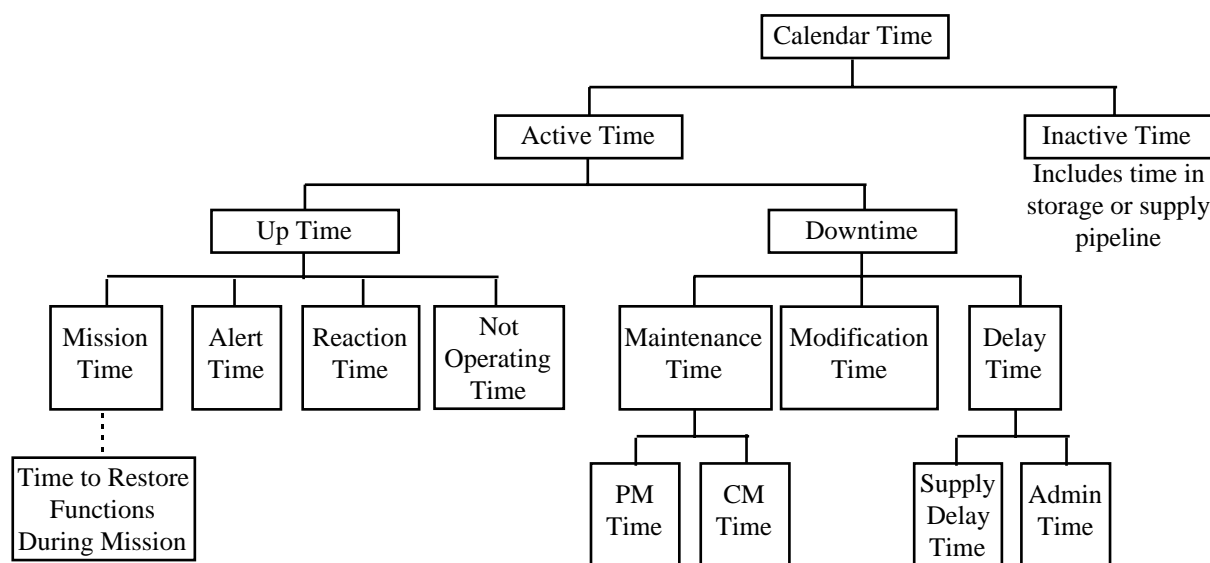


FIGURE 3-1: INTERVALS OF TIME

**TIME, TURN AROUND:** That element of maintenance time needed to replenish consumables and check out an item for recommitment.

**TOTAL SYSTEM DOWNTIME:** The time interval between the reporting of a system (product) malfunction and the time when the system has been repaired and/or checked by the maintenance person, and no further maintenance activity is executed.

### SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

#### **-U-**

**UNIT UNDER TEST (UUT):** A UUT is any product or item (system, set, subsystem, assembly or subassembly, etc.) undergoing testing or otherwise being evaluated by technical means.

**UNSCHEDULED MAINTENANCE:** Corrective maintenance performed in response to a suspected failure.

**UPTIME:** That element of ACTIVE TIME during which an item is in condition to perform its required functions. (Increases availability and dependability).

**UPTIME RATIO:** A composite measure of operational availability and dependability that includes the combined effects of item design, installation, quality, environment, operation, maintenance, repair and logistic support: The quotient of uptime divided by the sum of uptime and downtime.)

**USEFUL LIFE:** The number of life units from manufacture to when the item has an unreparable failure or unacceptable failure rate. Also, the period of time before the failure rate increases due to wearout.

**UTILIZATION RATE:** The planned or actual number of life units expended, or missions attempted during a stated interval of calendar time.

#### **-V-**

**VERIFICATION:** The contractor effort to: (1) determine the accuracy of and update the analytical (predicted) data; (2) identify design deficiencies; and (3) gain progressive assurance that the required performance of the item can be achieved and demonstrated in subsequent phases. This effort is monitored by the procuring activity from date of award of the contract, through hardware development from components to the configuration item (CI).

#### **-W-**

**WEAROUT:** The process that results in an increase of the failure rate or probability of failure as the of number of life units increases.

---

**SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS**

---

**3.3 List of Abbreviations and Acronyms****-A-**

Ai	-	Availability, Inherent (or intrinsic)
Ao	-	Availability, Operational
ACAT	-	Acquisition Category
AGREE	-	Advisory Group on Reliability of Electronic Equipment
ANSI	-	American National Standards Institute
ARINC	-	Aeronautical Radio Incorporated
ASIC	-	Application Specific Integrated Circuit
ATE	-	Automatic Test Equipment
AVIP	-	Avionics Integrity Program

**-B-**

BIT	-	Built-In Test
BITE	-	Built-In Test Equipment
BOL	-	Beginning of Life

**-C-**

CAD	-	Computer Aided Design
CAM	-	Computer Aided Manufacturing
CDR	-	Critical Design Review
CDRL	-	Contract Data Requirements List
CI	-	Configuration Item
CID	-	Commercial Item Description
CM	-	Corrective Maintenance
CND	-	Cannot Duplicate
COTS	-	Commercial-Off-The-Shelf
CUT	-	Circuit Under Test

**-D-**

DAR	-	Defense Acquisition Reform
DARPA	-	Defense Advanced Research Project Agency
DESC	-	Defense Electronic Supply Center
DLA	-	Defense Logistics Agency
DoD	-	Department of Defense
DoDISS	-	Department of Defense Index of Standards and Specifications
DOE	-	Design of Experiments

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

DT	-	Development Test
DTIC	-	Defense Technical Information Center
DMH/MA	-	Direct Manhours per Maintenance Action
DT&E	-	Development Test and Evaluation

**-E-**

ECP	-	Engineering Change Proposal
EDIF	-	Electronic Data Interchange Format
EHC	-	Explosive Hazard Classification
EMC	-	Electromagnetic Compatibility
EMD	-	Engineering and Manufacturing Development
EMI	-	Electromagnetic Interference
EMP	-	Electromagnetic Pulse
EOL	-	End of Life
ESD	-	Electrostatic Discharge
ESS	-	Environmental Stress Screening
ETE	-	External Test Equipment

**-F-**

FA	-	False Alarm
FAR	-	False Alarm Rate
FEA	-	Finite Element Analysis
FMEA	-	Failure Modes and Effects Analysis
FMECA	-	Failure Modes, Effects, and Criticality Analysis
FD	-	Fault Detection
FD&I	-	Fault Detection and Isolation
FEA	-	Finite Element Analysis
FFD	-	Fraction of Faults Detectable
FFI	-	Fraction of Faults Isolatable
FI	-	Fault Isolation
FL	-	Fault Localization
FFD	-	Fraction of Faults Detected
FFI	-	Fraction of Faults Isolated
FH	-	Flying Hours
F3I	-	Form, Fit, Function, and Interface
FPGA	-	Field Programmable Gate Arrays
FRACAS	-	Failure Reporting and Corrective Action System
FTA	-	Fault Tree Analysis

---

**SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS**

---

**-G-**

GaAs	-	Gallium Arsenide
GEM	-	Generalized Emulation of Microcircuits
GIDEP	-	Government-Industry Data Exchange Program
GPTE	-	General Purpose Test Equipment
GS	-	Guide Specification

**-H-**

HALT	-	Highly Accelerated Life Test
HAST	-	Highly Accelerated Stress Test
HCR	-	Human Cognitive Reliability
HE	-	Human Engineering

**-I-**

IC	-	Integrated Circuit
IEC	-	International Electrotechnical Commission
IEEE	-	Institute of Electrical and Electronic Engineers
ILS	-	Integrated Logistics Support
IOT&E	-	Initial Operational Test and Evaluation
IPD	-	Integrated Product Team
IPDT	-	Integrated Product Development Team

**-L-**

LCC	-	Life Cycle Cost
LRM	-	Line Replaceable Module
LRU	-	Line Replaceable Unit
LSA	-	Logistics Support Analysis

**-M-**

MA	-	Maintenance Action
MCM	-	Multichip Module
MDT	-	Mean Downtime
MIMIC	-	Monolithic Microwave Millimeter Wave Integrated Circuit
MOS	-	Metal Oxide Semiconductor
MOV	-	Metal Oxide Varistor
MPCAG	-	Military Parts Control Advisory Group
MR	-	Mission Reliability or Maintenance Rate



SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

MTBF	-	Mean Time Between Failure
MTBCF	-	Mean Time Between Critical Failure
MTBD	-	Mean Time Between Demand
MTBDE	-	Mean Time Between Downing Events
MTBF	-	Mean Time Between Failure
MTBM	-	Mean Time Between Maintenance
MTTF	-	Mean Time To Failure
MTTR	-	Mean Time To Repair
MTTRS	-	Mean Time To Restore System
MTTS	-	Mean Time To Service
MVT	-	Majority Vote Comparator

**-N-**

NDI	-	Non-Developmental Item or Non-Destructive Inspection
-----	---	--

**-O-**

O&M	-	Operation and Maintenance
O&SHA	-	Operating and Support Hazard Analysis
OHHA	-	Occupational Health Hazard Assessment
OT&E	-	Operational Test and Evaluation

**-P-**

PAT	-	Process Action Team
PCB	-	Printed Circuit Board
PDR	-	Preliminary Design Review
PEM	-	Plastic Encapsulated Microcircuit
PHA	-	Preliminary Hazard Analysis
PHL	-	Preliminary Hazard List
PLD	-	Programmable Logic Device
PM	-	Preventive Maintenance
PMP	-	Parts Management Program
PPL	-	Preferred Parts List
PPSL	-	Program Parts Selection List
PRDR	-	Preproduction Reliability Design Review
PSP	-	Performance Shaping Factor
P&V	-	Power and Voltage

---

**SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS**

---

**-Q-**

QFD	-	Quality Function Deployment
QML	-	Qualified Manufacturers List

**-R-**

RAM	-	Reliability, Availability, Maintainability
R&D	-	Research and Development
R/R	-	Remove and Replace
RAC	-	Reliability Analysis Center
RADC	-	Rome Air Development Center
RCM	-	Reliability Centered Maintenance
RF	-	Radio Frequency
RFP	-	Request for Proposal
RGA	-	Residual Gas Analysis
RGT	-	Reliability Growth Test
RISC	-	Reduced Instruction Set Computer
RIW	-	Reliability Improvement Warranty
RL	-	Rome Laboratory
RMS	-	Reliability, Maintainability, Supportability
RPN	-	Risk Priority Number
RTOK	-	Retest OK
R&M	-	Reliability and Maintainability

**-S-**

SAE	-	Society of Automotive Engineers
SCA	-	Sneak Circuit Analysis
SCR	-	Silicon Controlled Rectifier
SHA	-	System Hazard Analysis
SLI	-	Success Likelihood Index
SMD	-	Surface Mount Device
SOO	-	Statement of Objectives
SOW	-	Statement of Work
SPC	-	Statistical Process Control
SPS	-	Standard Performance Specification
SRA	-	Shop Replaceable Assembly
SRU	-	Shop Replaceable Unit
SSHA	-	Subsystem Hazard Analysis
SSG	-	System Safety Group
SSWG	-	System Safety Working Group

SECTION 3: DEFINITIONS OF TERMS, ACRONYMS AND ABBREVIATIONS

---

**-T-**

TAAF	-	Test, Analyze, and Fix
TMDE	-	Test, Measurement, and Diagnostic Equipment
TQM	-	Total Quality Management
TRB	-	Technology Review Board
TTF	-	Time to Failure

**-U-**

UR	-	Uptime Ratio or Utilization Rate
UUT	-	Unit Under Test

**-V-**

VHDL	-	VHSIC Hardware Description Language
VHSIC	-	Very High Speed Integrated Circuit

**-W-**

WSEIAC	-	Weapon System Effectiveness Industry Advisory Committee
WCA	-	Worst Case Analysis
WCCA	-	Worst Case Circuit Analysis
WRA	-	Weapon Replaceable Assembly
WUC	-	Work Unit Code

---

**SECTION 4: GENERAL STATEMENTS**

---

**4.0 GENERAL STATEMENTS****4.1 Introduction and Background**

For all but the most recent years of human history, the performance expected from man's implements was quite low and the life realized was long, both because it just happened to be so in terms of man's lifetime and because he had no reason to expect otherwise. The great technological advances, beginning in the latter half of the twentieth century, have been inextricably tied to more and more complex implements or devices. In general, these have been synthesized from simpler devices having a satisfactory life. It is a well known fact that any device which requires all its parts to function will always be less stable than any of its parts. Although significant improvements have been made in increasing the lives of basic components - for example, microelectronics - these have not usually been accompanied by corresponding increases in the lives of equipment and systems. In some cases, equipment and system complexity has progressed at so rapid a pace as to negate, in part, the increased life expected from use of the longer-lived basic components. In other cases, the basic components have been misapplied or overstressed so that their potentially long lives were cut short. In still other cases, management has been reluctant to devote the time and attention necessary to ensure that the potentially long lives of the basic components were achieved.

The military services, because they tended to have the most complex systems and hence the most acute problems, provided the impetus to the orderly development of the discipline of reliability engineering. It was they who were instrumental in developing mathematical models for reliability, as well as design techniques to permit the quantitative specification, prediction and measurement of reliability.

Reliability engineering is the doing of those things which insure that an item will perform its mission successfully. The discipline of reliability engineering consists of two fundamental aspects:

- (1) paying attention to detail
- (2) handling uncertainties

The traditional, narrow definition of reliability is "the probability that an item can perform its intended function for a specified interval under stated conditions."

This narrow definition is applicable largely to items which have simple missions, e.g., equipment, simple vehicles, or components of systems. For large complex systems (e.g., command and control systems, aircraft weapon systems, a squadron of tanks, naval vessels), it is more appropriate to use more sophisticated concepts such as "system effectiveness" to describe the worth of a system. A more precise definition of system effectiveness and the factors contributing to it are presented in Section 4.3. For the present, it is sufficient to observe that

## SECTION 4: GENERAL STATEMENTS

---

system effectiveness relates to that property of a system output which was the real reason for buying the system in the first place - namely, the carrying out of some intended function. If the system is effective, it carries out this function well. If it is not effective, attention must be focused on those system attributes which are deficient.

### 4.2 The System Engineering Process

In recent years, the word “system” has come to include:

- (1) The prime mission equipment
- (2) The facilities required for operation and maintenance
- (3) The selection and training of personnel
- (4) Operational and maintenance procedures
- (5) Instrumentation and data reduction for test and evaluation
- (6) Special activation and acceptance programs
- (7) Logistic support programs

System engineering is the application of scientific, engineering, and management effort to:

- (1) Transform an operational need into a description of system performance parameters and a system configuration through the use of an iterative process of definition, synthesis, analysis, design, test, and evaluation.
- (2) Integrate related technical parameters and assure compatibility of all physical, functional, and program interfaces in a manner that optimizes the total system design.
- (3) Integrate reliability, maintainability, safety, survivability (including electronic warfare considerations), human factors, and other factors into the total engineering effort.

From the system management viewpoint, system engineering is but one of five major activities required to develop a system from Conceptual Exploration through the subsequent phases of Program Definition and Risk Reduction; Engineering and Manufacturing Development (EMD); and Production, Fielding/Deployment, and Operational Support. (These are the major phases defined in DoD 5000.2-R). These five activities (procurement and production, program control, configuration management, system engineering, and test and deployment management), must

---

## SECTION 4: GENERAL STATEMENTS

---

perform their general functions within each of the system evolutionary phases, and their relationships to one another are summarized in Figure 4.2-1.

### 4.2.1 Systems Engineering and IPTs

Integrated Product Teams (IPTs) are a pragmatic means of implementing a true systems engineering approach. As part of Defense Acquisition Reform (see Section 12), then Secretary of Defense William Perry instituted the Integrated Product/Process Development (IPPD) approach to system acquisition. It is a systematic approach to the integrated, concurrent design of products and their related processes, including manufacturing and life cycle support. Essential to the IPPD approach is the use of IPTs. These teams are multi-functional groups of individuals who manage and integrate critical processes.

All too often in the past, each phase of system acquisition was dominated by one functional group. For example, during design, the design engineers were the primary “players.” Although some interaction between the designers and other functional groups occurred, it did so in an iterative, serial fashion. Sometime prior to the beginning of production, the design was handed off to the manufacturing organization which was supposed to design the processes needed to produce the system. Also, after the design was “frozen,” the support community was given the task of planning for the support of the system. This essentially sequential approach led to problems of poor producibility, high manufacturing costs, slipped schedules, high support requirements, and so forth.

Efforts were made to solve this “stovepiping” of functions. In the late 1970’s, Integrated Logistics Support Offices (ILSOs) were co-located with and as part of major system program offices. One objective of these co-located ILSOs was to influence the design to enhance inherent supportability. In the 1970’s and 1980’s, computer-aided design (CAD) and computer-aided manufacturing (CAM) were introduced as tools for linking the various functional disciplines together. With the advent of IPTs, however, came a multi-disciplined approach to *decision-making*. By empowering these IPTs to make decisions in a collaborative manner, many of the problems of stovepiping are being overcome. Together with tools such as CAD/CAM, IPTs are proving to be an effective way of implementing the systems engineering concept and finding the optimal balance among competing requirements under the constraints of cost and schedule.

### 4.2.2 The Four Steps of Systems Engineering

System engineering consists of four steps in an interacting cycle (Figure 4.2-2). Step 1 considers threat forecast studies, doctrinal studies, probable military service tasks, and similar sources of desired materiel and system objectives; then it translates them into basic functional requirements or statements of operation. The usual result of Step 1 is a set of block diagrams showing basic functional operations and their relative sequences and relationships. Even though hardware may

SECTION 4: GENERAL STATEMENTS

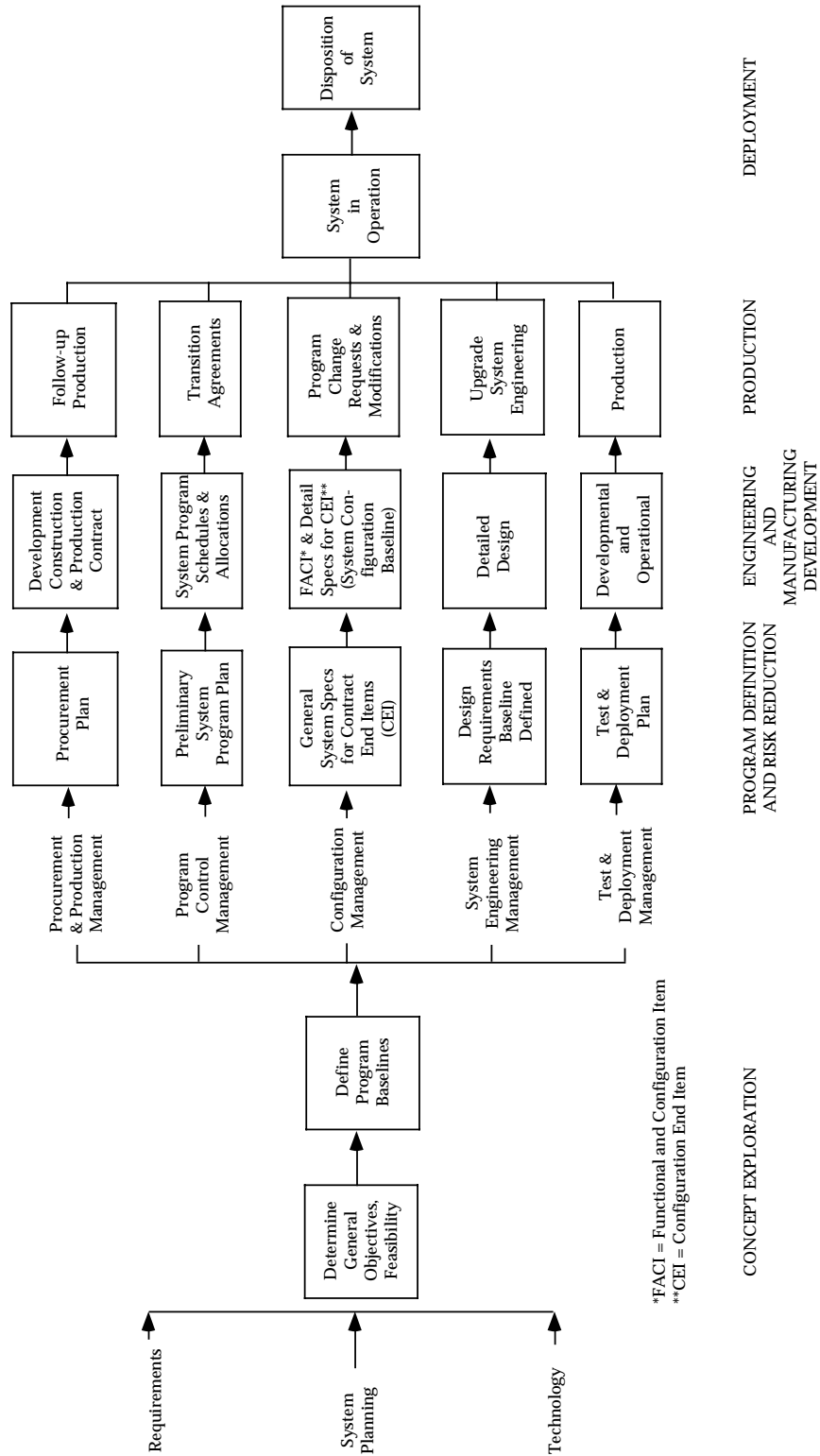


FIGURE 4.2-1: SYSTEM MANAGEMENT ACTIVITIES

---

**SECTION 4: GENERAL STATEMENTS**

---

help shape the basic system design, it is not specifically included in Step 1. Step 1 is intended to form a first hypothesis as a start toward the eventual solution.

In Step 2, the first hypothesis is evaluated against constraints such as design, cost, and time and against specific mission objectives to create criteria for designing equipment, defining intersystem interfaces, defining facilities, and determining requirements for personnel, training, training equipment and procedures.

Step 3 consists of system design studies that are performed concurrently with Steps 2 and 4 to:

- (1) Determine alternate functions and functional sequences
- (2) Establish design personnel, training and procedural data requirements imposed by the functions
- (3) Find the best way to satisfy the mission requirements
- (4) Select the best design approach for integrating mission requirements into the actual hardware and related support activities

Normally, the studies in Step 3 involve tradeoffs where data are in the form of schematic block diagrams, outline drawings, intersystem and intrasystem interface requirements, comparative matrices, and data supporting the selection of each approach. Some of the scientific tools used in the system design studies in Step 3 are: probability theory, statistical inference, simulation, computer analysis, information theory, queuing theory, servomechanism theory, cybernetics, mathematics, chemistry, and physics.

Step 4 uses the design approach selected in Step 3 to integrate the design requirements from Step 2 into the Contract End Items (CEI's). The result of Step 4 provides the criteria for detailed design, development, and test of the CEI based upon defined engineering information and associated tolerances. Outputs from Step 4 are used to:

- (1) Determine intersystem interfaces
- (2) Formulate additional requirements and functions that evolve from the selected devices or techniques
- (3) Provide feedback to modify or verify the system requirements and functional flow diagrams prepared in Step 1



## SECTION 4: GENERAL STATEMENTS

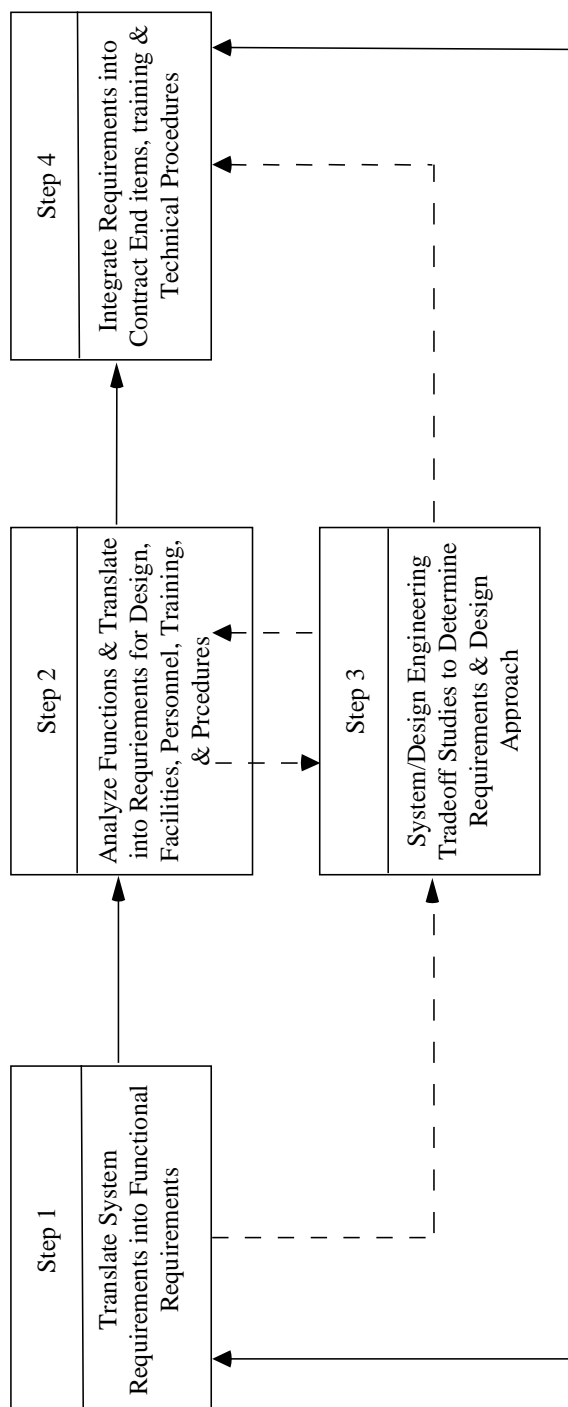


FIGURE 4.2-2: FUNDAMENTAL SYSTEM PROCESS CYCLE

---

## SECTION 4: GENERAL STATEMENTS

---

When the first cycle of the system engineering process is completed, the modifications, alternatives, imposed constraints, additional requirements, and technological problems that have been identified are recycled through the process with the original hypothesis (initial design) to make the design more practical. This cycling is continued until a satisfactory design is produced, or until available resources (time, money, etc.) are expended and the existing design is accepted, or until the objectives are found to be unattainable.

Other factors that are part of the system engineering process - such as reliability, maintainability, safety, and human factors - exist as separate but interacting engineering disciplines and provide specific inputs to each other and to the overall system program. Pertinent questions at this point might be: “How do we know when the design is adequate?” or “How is the effectiveness of a system measured?” The answers to these questions lead to the concept of system effectiveness.

### 4.3 System Effectiveness

System effectiveness is a measure of the ability of a system to achieve a set of specific mission requirements. It is a function of readiness (or availability), and mission success (or dependability).

Cost and time are also critical in the evaluation of the merits of a system or its components, and must eventually be included in making administrative decisions regarding the purchase, use, maintenance, or discard of any equipment or system.

The operational effectiveness of a system obviously is influenced by the way the equipment was designed and built. It is, however, just as influenced by the way the equipment is used and maintained; i.e., system effectiveness is influenced by the designer, production engineer, maintenance man, and user/operator. The concepts of availability and dependability illustrate these influences and their relationships to system operational effectiveness. The following are the definitions of these concepts:

- (1) **Availability** - A measure of the degree to which an item is in an operable and committable state at the start of a mission, when the mission is called for at an unknown (random) time.
- (2) **Dependability** - A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission. (This definition is significantly different than the definition of dependability used by most other US and international organizations dealing with reliability e.g., the International Electrotechnical Commission (IEC) and the Society of Automotive Engineers (SAE). The IEC defines Dependability in publication IEC 50 Chapter 191 as: “The collective term used to describe the availability performance and its influencing factors: reliability

## SECTION 4: GENERAL STATEMENTS

---

performance, maintainability performance and maintenance support performance.” As such, its use is restricted to general descriptions in non-quantitative terms).

Dependability is related to reliability; the intention was that dependability would be a more general concept than reliability.

### 4.3.1 R/M Considerations in System Effectiveness

From a system effectiveness viewpoint, reliability and maintainability jointly provide system availability and dependability. Increased reliability directly contributes to system uptime, while improved maintainability reduces downtime. If reliability and maintainability are not jointly considered and continually reviewed, serious consequences may result. With military equipment, failures or excessive downtime can jeopardize a mission and possibly cause a loss of lives. Excessive repair time and failures also impose burdens on logistic support and maintenance activities, causing high costs for repair parts and personnel training, expenditure of many man-hours for actual repair and service, obligation of facilities and equipment to test and service, and to movement and storage of repair parts.

From the cost viewpoint, reliability and maintainability must be evaluated over the system life cycle, rather than merely from the standpoint of initial acquisition. An effective design approach to reliability and maintainability can reduce the cost of upkeep.

Both reliability and maintainability are important considerations for the user of the system, although maintainability is probably more important from the point of view of most users. Although frequent system failures may be an annoyance, if each failure can be repaired in a very short time so that the system has a high availability, and the maintenance costs are reasonable, then the poor reliability may be acceptable. For example, if failures occur on the average of every fifteen minutes but can be repaired in a microsecond, at acceptable cost, the user will not be too concerned. On the other hand, if repair of a failure takes hours or days, the user has a non-available weapon system which may have a significant effect on the operational commander's readiness posture.

## 4.4 Factors Influencing System Effectiveness

### 4.4.1 Equipment of New Design

A typical history of the development of a new equipment would reveal a number of interesting steps in the progression from original concept to acceptable production model. These steps are particularly marked if the equipment represents a technical innovation, i.e., if it “pushes the state of the art” by introducing entirely new functions or by performing established functions in an entirely new way. Starting with a well-defined operational need, the research scientist, designer, reliability engineer, statistician, and production engineer all combine their talents to execute a multitude of operations leading to one ultimate objective: the production of an equipment that

---

**SECTION 4: GENERAL STATEMENTS**

---

will perform as intended, with minimum breakdowns and maximum speed of repair. All this must be done at minimum cost and usually within an accelerated time schedule.

These program requirements are severe, to say the least. In order to meet them, many compromises are required. One of the first of these compromises is often a sharp curtailment in the basic research time allotted to the job of proving the feasibility of the new design. After only brief preliminary study, a pilot model of the equipment is built. With luck, it will work; but it is likely to be somewhat crude in appearance, too big and too heavy, not well-designed for mass production, subject to frequent failure, and difficult to repair. Indeed, at this early stage in the program, it is quite possible that the first model might be incapable of working if it were taken out of the laboratory and subjected to the more severe stresses of field operation, whether this be military or civilian. By the time this situation is corrected, the development program will have included many design changes, part substitutions, reliability tests, and field trials, eventually culminating in a successful operational acceptance test.

Usually, it is not until the equipment appears to have some chance of reaching this ultimate goal of acceptance that attention is focused on reduction of the frequency of failure, thus providing the impetus for a serious reliability effort. Experience has shown that this is unfortunate. Ideally, such an effort should begin immediately after the feasibility study, because some problems can be eliminated before they arise, and others can be solved at an early development stage, when design modifications can be effected most easily and economically. Even with this early start, reliability will continue to be a primary problem in new equipment, especially when it is of novel design. Early neglect of reliability must be compensated for by extraordinary efforts at a later period, because an equipment simply is not usable if it fails too frequently to permit suitable reliance on the likelihood of its operation when needed. Since such early neglect has been common in the past, reliability has received strong emphasis in the research designed to bring equipment performance characteristics up to satisfactory levels.

The description just given is generally applicable to the development of radically new equipment. However, when attention is directed to equipment in everyday use or to new equipment built predominantly on standard design principles and from well-tested parts, it becomes evident that effectiveness is dependent not only on performance capabilities and reliability but also on a number of other factors, including operational readiness, availability, maintainability, and repairability. Definitions for these concepts are given in Section 3. From the definitions it can be seen that they are all so interrelated that they must be viewed together and discussed, not as separate concepts but within the framework of the overall system to which they contribute.

#### 4.4.2 Interrelationships Among Various System Properties

The discussion above implies that it is probably not practicable to maximize all of the desirable properties of a system simultaneously. Clearly, there are "tradeoff" relationships between reliability and system cost, between maintainability and system cost, between reliability and maintainability, and between many other properties. It would be most helpful to have a

## SECTION 4: GENERAL STATEMENTS

---

numerical scale of values for each of the several properties, and to have a multi-dimensional plot or chart showing the interrelationship among those values. Before such relationships can be obtained, it is first necessary to define in a precise and quantitative manner the properties with which we are concerned. The following outline is intended to show some of the factors which must be considered:

### A. SYSTEM PERFORMANCE (DESIGN ADEQUACY)

- (1) Technical Capabilities
  - (a) Accuracy
  - (b) Range
  - (c) Invulnerability to countermeasures
  - (d) Operational simplicity
- (2) Possible Limitations on Performance
  - (a) Space and weight requirements
  - (b) Input power requirements
  - (c) Input information requirements
  - (d) Requirements for special protection against shock, vibration, low pressure, and other environmental influences

### B. OPERATIONAL READINESS

- (1) Reliability
  - (a) Failure-free operation
  - (b) Redundancy or provision for alternative modes of operation
- (2) Maintainability
  - (a) Time to restore failed system to satisfactory operating status
  - (b) Technical manpower requirements for maintenance
  - (c) Effects of use-cycle on maintenance. (Can some maintenance be performed when operational use of the system is not required?)
- (3) Logistic Supportability
- (4) Availability

### C. SYSTEM COST

- (1) Development cost, and particularly development time, from inception to operational capability
- (2) Production cost
- (3) Operating and operational support costs

---

**SECTION 4: GENERAL STATEMENTS**

---

**4.5 Optimization of System Effectiveness**

The optimization of system effectiveness is important throughout the system life cycle, from concept through the operation. Optimization is the balancing of available resources (time, money, personnel, etc.) against resulting effectiveness parameters (performance, operational readiness, etc.), until a combination is found that provides the most effectiveness for the desired expenditure of resources. Thus, the optimum system might be one that:

- (1) Meets or exceeds a particular level of effectiveness for minimum cost, and/or
- (2) Provides a maximum effectiveness for a given total cost

Optimization is illustrated by the flow diagram of Figure 4.5-1 which shows the optimization process as a feedback loop consisting of the following three steps:

- (1) Designing many systems that satisfy the operational requirements and constraints
- (2) Computing resultant values for effectiveness and resources used
- (3) Evaluating these results and making generalizations concerning appropriate combinations of design and support factors, which are then fed back into the model through the feedback loops

Optimization also can be illustrated by the purchase of a new car or, more specifically, by putting into precise, quantifiable terms the rule, or criteria, that will be followed in the automobile selection process. Although automobiles do have quantifiable characteristics, such as horsepower, cost, and seating capacity, they are basically similar in most cars of a particular class (low-price sedans, sports models, etc.). Thus the selection criteria essentially reduces to esthetic appeal, prior experience with particular models, and similar intangibles. In the same sense, the choice of best design for the weapon system is greatly influenced by experience with good engineering practices, knowledge assimilated from similar systems, and economics. Despite this fuzziness, the selection criteria must be adjusted so that:

- (1) The problem size can be reduced to ease the choice of approaches
- (2) All possible alternatives can be examined more readily and objectively for adaptation to mathematical representation and analysis
- (3) Ideas and experiences from other disciplines can be more easily incorporated into the solution
- (4) The final choice of design approaches can be based on more precise, quantifiable terms, permitting more effective review and revision, and better inputs for future optimization problems

SECTION 4: GENERAL STATEMENTS

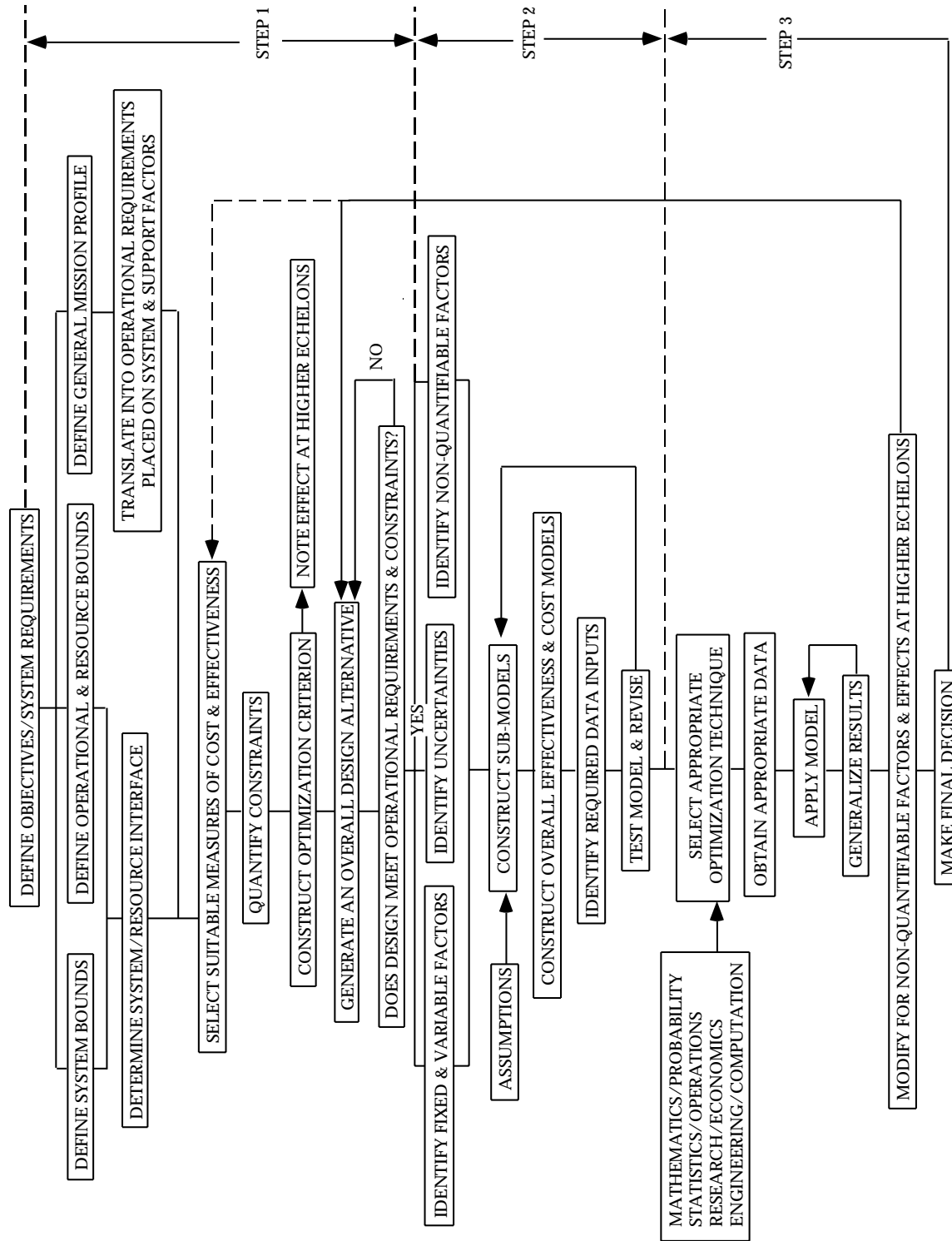


FIGURE 4.5-1: FLOW DIAGRAM FOR A GENERAL OPTIMIZATION PROCESS

## SECTION 4: GENERAL STATEMENTS

The choice of parameters in the optimization model also is influenced by system definition. The automobile purchaser, for example, may not consider the manufacturer's and dealer's service policies. If these policies are considered, the system becomes the automobile plus the service policies. If service policies are not considered, the system consists only of the automobile.

The optimization of system effectiveness is a highly complex problem; there is a degree of interaction among the factors which enter into consideration of this problem. The actual techniques used to optimize system effectiveness will be described in greater detail in Section 10 of this handbook. Table 4.5-1, for example, lists only some of the more commonly-used techniques. These techniques are not peculiar to system effectiveness optimization, nor are they limited to system engineering.

This section is an introduction to the Handbook from a top level, or system, viewpoint. The remaining sections of this Handbook will expand upon the concepts introduced in this chapter. They will cover: (1) the basic reliability/maintainability/ availability theory, (2) practical application of the theory in terms of the design methodology and procedures of reliability engineering at the equipment and system level, (3) procedures for insuring that inherent reliability is not degraded during production and field deployment of systems, and (4) steps that management must take to insure the acquisition and deployment of reliable systems at minimum life cycle cost.

TABLE 4.5-1: PARTIAL LIST OF OPTIMIZATION TECHNIQUES

<p><b>I. Mathematical Techniques</b>            Birth and death processes            Calculus of finite differences            Calculus of variations            Gradient theory            Numerical approximation            Symbolic logic            Theory of linear integrals            Theory of maxima and minima</p>	<p><b>II. Statistical Techniques</b>            Bayesian analysis            Decision theory            Experimental design            Information theory            Method of steepest ascent            Stochastic processes</p>
<p><b>III. Programming Techniques</b>            Dynamic programming            Linear programming            Nonlinear programming</p>	<p><b>IV. Other</b>            Gaming theory            Monte Carlo techniques            Queuing theory            Renewal theory            Search theory            Signal flow graphs            Value theory</p>



SECTION 4: GENERAL STATEMENTS

---

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**

---

**5.0 RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY****5.1 Introduction**

The language of engineering is mathematics. The theories behind each engineering specialty are concisely stated in a set of mathematical procedures. For the engineering specialties of reliability, availability and maintainability (RAM), the theories are stated in the mathematics of probability and statistics.

The underlying reason for the use of these concepts is the inherent uncertainty in predicting a failure. Even given a failure model based on physical or chemical reactions, the results will not be the time a part will fail, but rather the time a given percentage of the parts will fail or the probability that a given part will fail in a specified time. Individual parts will fail according to their individual strengths, which will vary from part to part and are practically unknowable. Similarly, the time to repair a failure will also vary dependent on many factors whose values in individual cases are practically unknowable.

Since RAM parameters must be defined in probabilistic terms, probabilistic parameters such as random variables, density functions, and distribution functions are utilized in the development of RAM theory.

This section describes some of the basic concepts, formulas, and simple examples of application of RAM theory which are required for better understanding of the underlying principles and design techniques presented in later sections. Practicality rather than rigorous theoretical exposition is emphasized. Many excellent texts are available (see references) for the reader who is interested in delving into the rigorous theoretical foundations of these disciplines.

**5.2 Reliability Theory**

Because, as was mentioned previously, reliability is defined in terms of probability, probabilistic parameters such as random variables, density functions, and distribution functions are utilized in the development of reliability theory. Reliability studies are concerned with both discrete and continuous random variables. An example of a discrete variable is the number of failures in a given interval of time. Examples of continuous random variables are the time from part installation to failure and the time between successive equipment failures.

The distinction between discrete and continuous variables (or functions) depends upon how the problem is treated and not necessarily on the basic physical or chemical processes involved. For example, in analyzing "one shot" systems such as missiles, one usually utilizes discrete functions such as the number of successes in "n" launches. However, whether or not a missile is successfully launched could be a function of its age, including time in storage, and could, therefore, be treated as a continuous function.

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

**5.2.1 Basic Concepts**

The cumulative distribution function  $F(t)$  is defined as the probability in a random trial that the random variable is not greater than  $t$  (see note), or

$$F(t) = \int_{-\infty}^t f(t) dt \quad (5.1)$$

where  $f(t)$  is the probability density function of the random variable, time to failure.  $F(t)$  is termed the “unreliability function” when speaking of failure. It can be thought of as representing the probability of failure prior to some time  $t$ . If the random variable is discrete, the integral is replaced by a summation. Since  $F(t)$  is zero until  $t=0$ , the integration in Equation 5.1 can be from zero to  $t$ .

**NOTE: Pure mathematicians object to the use of the same letter in the integral and also in the limits of the integral. This is done here, and in the rest of this section in spite of the objection in order to simplify the reference to time as the variable in such functions as  $F(t)$ ,  $R(t)$ ,  $M(t)$ ,  $f(t)$ , etc.**

The reliability function,  $R(t)$ , or the probability of a device not failing prior to some time  $t$ , is given by

$$R(t) = 1 - F(t) = \int_t^{\infty} f(t) dt \quad (5.2)$$

By differentiating Equation (5.2) it can be shown that

$$\frac{-dR(t)}{dt} = f(t) \quad (5.3)$$

The probability of failure in a given time interval between  $t_1$  and  $t_2$  can be expressed by the reliability function

$$\int_{t_1}^{\infty} f(t) dt - \int_{t_2}^{\infty} f(t) dt = R(t_1) - R(t_2) \quad (5.4)$$

The rate at which failures occur in the interval  $t_1$  to  $t_2$ , the failure rate,  $\lambda(t)$ , is defined as the ratio of probability that failure occurs in the interval, given that it has not occurred prior to  $t_1$ , the start of the interval, divided by the interval length. Thus,

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

$$\lambda(t) = \frac{R(t_1) - R(t_2)}{(t_2 - t_1) R(t_1)} \quad (5.5)$$

or the alternative form

$$\lambda(t) = \frac{R(t) - R(t + \Delta t)}{\Delta t R(t)} \quad (5.6)$$

where  $t = t_1$  and  $t_2 = t + \Delta t$ . The hazard rate,  $h(t)$ , or instantaneous failure rate, is defined as the limit of the failure rate as the interval length approaches zero, or

$$\begin{aligned} h(t) &= \lim_{\Delta t \rightarrow 0} \left[ \frac{R(t) - R(t + \Delta t)}{\Delta t R(t)} \right] \\ &= \frac{-1}{R(t)} \left[ \frac{dR(t)}{dt} \right] = \frac{1}{R(t)} \left[ \frac{-dR(t)}{dt} \right] \end{aligned} \quad (5.7)$$

But it was previously shown, Eq. (5.3), that

$$f(t) = \frac{-dR(t)}{dt}$$

Substituting this into Eq. (5.7) we get 
$$h(t) = \frac{f(t)}{R(t)} \quad (5.8)$$

This is one of the fundamental relationships in reliability analysis. For example, if one knows the density function of the time to failure,  $f(t)$ , and the reliability function,  $R(t)$ , the hazard rate function for any time,  $t$ , can be found. The relationship is fundamental and important because it is independent of the statistical distribution under consideration.

The differential equation of Eq. (5.7) tells us, then, that the hazard rate is nothing more than a measure of the change in survivor rate per unit change in time.

Perhaps some of these concepts can be seen more clearly by use of a more concrete example. Suppose that we start a test at time,  $t_0$ , with  $N_0$  devices. After some time  $t$ ,  $N_f$  of the original devices will have failed, and  $N_s$  will have survived ( $N_0 = N_f + N_s$ ). The reliability,  $R(t)$ , is given at any time  $t$ , by:

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

$$R(t) = \frac{N_S}{N_O} \quad (5.9)$$

$$= \frac{N_O - N_f}{N_O} = 1 - \frac{N_f}{N_O} \quad (5.10)$$

From Eq. (5.3)

$$f(t) = -\frac{dR(t)}{dt} = \frac{1}{N_O} \frac{dN_f}{dt} \quad (5.11)$$

Thus, the failure density function represents the proportion of the original population, ( $N_O$ ), which fails in the interval ( $t, t + \Delta t$ ).

On the other hand, from Eqs. (5.8), (5.9) and (5.11)

$$h(t) = \frac{f(t)}{R(t)} = \frac{\frac{1}{N_O} \frac{dN_f}{dt}}{N_S/N_O} = \frac{1}{N_S} \frac{dN_f}{dt} \quad (5.12)$$

Thus,  $h(t)$  is inversely proportional to the number of devices that survive to time  $t$ , ( $N_S$ ), which fail in the interval ( $t, t + \Delta t$ ).

Although, as can be seen by comparing Eqs. (5.6) and (5.7), failure rate,  $\lambda(t)$ , and hazard rate,  $h(t)$ , are mathematically somewhat different, they are usually used synonymously in conventional reliability engineering practice. It is not likely that this handbook will change firmly entrenched conventional practice, so the reader should be aware of this common deviation from exact mathematical accuracy.

Perhaps the simplest explanation of hazard and failure rate is made by analogy. Suppose a family takes an automobile trip of 200 miles and completes the trip in 4 hours. Their average rate was 50 mph, although they drove faster at some times and slower at other times. The rate at any given instant could have been determined by reading the speed indicated on the speedometer at that instant. The 50 mph is analogous to the failure rate and the speed at any point is analogous to the hazard rate.

In Eq. (5.8), a general expression was derived for hazard (failure) rate. This can also be done for the reliability function,  $R(t)$ . From Eq. (5.7)

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

$$h(t) = -\frac{1}{R(t)} \left[ \frac{dR(t)}{dt} \right] \quad (5.13)$$

$$\frac{dR(t)}{R(t)} = -h(t) dt$$

Integrating both sides of Eq. (5.13)

$$\int_0^t \frac{dR(t)}{R(t)} = -\int_0^t h(t) dt$$

$$\ln R(t) - \ln R(0) = -\int_0^t h(t) dt$$

but  $R(0) = 1$ ,  $\ln R(0) = 0$ , and

$$R(t) = \exp \left[ -\int_0^t h(t) dt \right] \quad (5.14)$$

Eq. (5.14) is the general expression for the reliability function. If  $h(t)$  can be considered a constant failure rate ( $\lambda$ ), which is true for many cases for electronic equipment, Eq. (5.14) becomes

$$R(t) = e^{-\lambda t} \quad (5.15)$$

Eq. (5.15) is used quite frequently in reliability analysis, particularly for electronic equipment. However, the reliability analyst should assure himself that the constant failure rate assumption is valid for the item being analyzed by performing goodness of fit tests on the data. These are discussed in Section 8.

In addition to the concepts of  $f(t)$ ,  $h(t)$ ,  $\lambda(t)$ , and  $R(t)$ , previously developed, several other basic, commonly-used reliability concepts require development. They are: mean-time-to-failure (MTTF), mean life ( $\theta$ ), and mean-time-between-failure (MTBF).

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

Mean-Time-To-Failure (MTTF)

MTTF is nothing more than the expected value of time to failure and is derived from basic statistical theory as follows:

$$\begin{aligned} \text{MTTF} &= \int_0^{\infty} t f(t) dt \\ &= \int_0^{\infty} t \left[ -\frac{dR(t)}{dt} \right] dt \end{aligned} \quad (5.16)$$

Integrating by parts and applying “Hopital's rule,” we arrive at the expression

$$\text{MTTF} = \int_0^{\infty} R(t) dt \quad (5.17)$$

Eq. (5.17), in many cases, permits the simplification of MTTF calculations. If one knows (or can model from the data) the reliability function,  $R(t)$ , the MTTF can be obtained by direct integration of  $R(t)$  (if mathematically tractable), by graphical approximation, or by Monte Carlo simulation. For repairable equipment MTTF is defined as the mean time to first failure.

Mean Life ( $\theta$ )

The mean life ( $\theta$ ) refers to the total population of items being considered. For example, given an initial population of  $n$  items, if all are operated until they fail, the mean life ( $\theta$ ) is merely the arithmetic mean time to failure of the total population given by:

$$\theta = \frac{\sum_{i=1}^n t_i}{n} \quad (5.18)$$

where:

- $t_i$  = time to failure of the  $i^{\text{th}}$  item in the population
- $n$  = total number of items in the population

Mean-Time-Between-Failure (MTBF)

This concept appears quite frequently in reliability literature; it applies to repairable items in which failed elements are replaced upon failure. The expression for MTBF is:

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

$$MTBF = \frac{T(t)}{r} \quad (5.19)$$

where:

$$\begin{aligned} T(t) &= \text{total operating time} \\ r &= \text{number of failures} \end{aligned}$$

It is important to remember that MTBF only has meaning for repairable items, and, for that case, MTBF represents exactly the same parameter as mean life ( $\theta$ ). More important is the fact that a constant failure rate is assumed. Thus, given the two assumptions of replacement upon failure and constant failure rate, the reliability function is:

$$R(t) = e^{-\lambda t} = e^{-t/\theta} = e^{-t/MTBF} \quad (5.20)$$

and (for this case)

$$\lambda = \frac{1}{MTBF} \quad (5.21)$$

Figure 5.2-1 provides a convenient summary of the basic concepts developed in this section.

Failure Density Function (time to failure)	$f(t)$
Reliability Function	$R(t) = \int_t^{\infty} f(t) dt = \exp \left[ -\int_0^t h(t) dt \right]$
Hazard Rate (Failure Rate)	$h(t) = f(t)/R(t)$ $\lambda(t) = \int_0^t h(t) dt$
Mean Time to Failure (MTTF) (no repair)	$MTTF = \int_0^{\infty} R(t) dt$
Mean Time Between Failure (constant failure rate, $\lambda$ , with repair)	$MTBF = \frac{T(t)}{r} = 1/\lambda$

FIGURE 5.2-1: SUMMARY OF BASIC RELIABILITY CONCEPTS



---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

**5.3 Statistical Distributions Used in Reliability Models**

There are many standard statistical distributions which may be used to model the various reliability parameters. It has been found that a relatively small number of statistical distributions satisfies most needs in reliability work. The particular distribution used depends upon the nature of the data, in each case. The following is a short summary of some of the distributions most commonly used in reliability analysis, criteria for their use, and examples of application. Figures 5.3-1 and 5.3-2 are summaries of the shape of common failure density, reliability, and hazard rate functions for the distributions described. Each distribution will be described in more detail, with reliability examples, in the following sections.

**5.3.1 Continuous Distributions**
**5.3.1.1 Normal (or Gaussian) Distribution**

There are two principal applications of the normal distribution to reliability. One application deals with the analysis of items which exhibit failure due to wear, such as mechanical devices. Frequently the wear-out failure distribution is sufficiently close to normal that the use of this distribution for predicting or assessing reliability is valid.

Another application is in the analysis of manufactured items and their ability to meet specifications. No two parts made to the same specification are exactly alike. The variability of parts leads to a variability in systems composed of those parts. The design must take this part variability into account, otherwise the system may not meet the specification requirement due to the combined effect of part variability. Another aspect of this application is in quality control procedures.

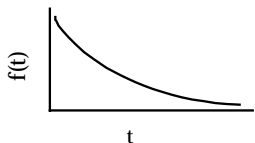
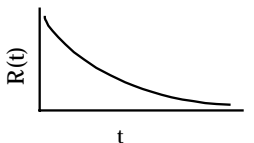
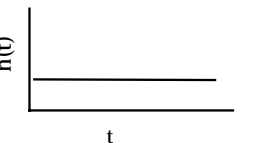
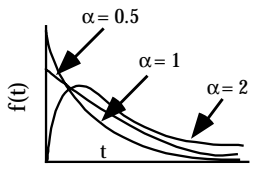
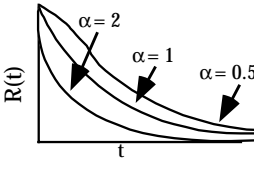
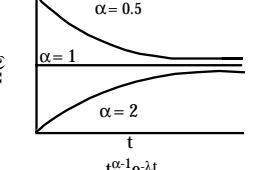
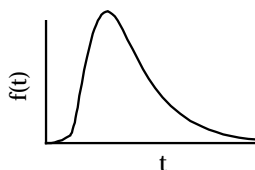
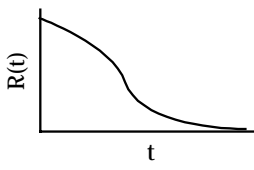

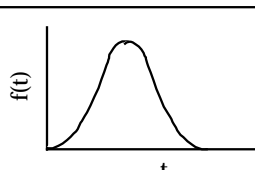
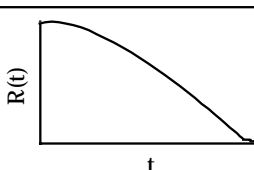
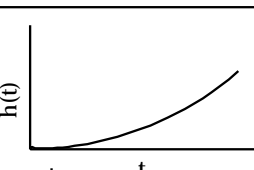
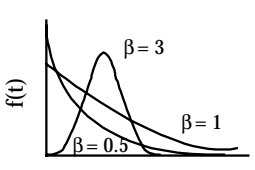
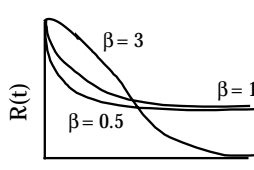
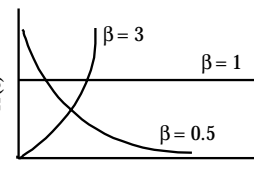
The basis for the use of normal distribution in this application is the central limit theorem which states that the sum of a large number of identically distributed random variables, each with finite mean and variance, is normally distributed.

Thus, the variations in value of electronic component parts, for example, due to manufacturing are considered normally distributed.

The failure density function for the normal distribution is

$$f(t) = \frac{1}{s\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}, \text{ where } -\infty < t < \infty \quad (5.22)$$

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TYPE OF DISTRIBUTION	PROBABILITY DENSITY FUNCTION, f(t)	RELIABILITY FUNCTION R(t) = 1 - f(t)	HAZARD FUNCTION h(t) = $\frac{f(t)}{R(t)}$
EXPONENTIAL	 $f(t) = \lambda e^{-\lambda t}$	 $R(t) = e^{-\lambda t}$	 $h(t) = \lambda = \theta^{-1}$
GAMMA	 $f(t) = \frac{\lambda}{\Gamma(\alpha)} (\lambda t)^{\alpha-1} e^{-\lambda t}$	 $R(t) = \frac{\lambda \alpha}{\Gamma(\alpha)} \int_t^{\infty} t^{\alpha-1} e^{-\lambda t} dt$	 $h(t) = \frac{t^{\alpha-1} e^{-\lambda t}}{\int_t^{\infty} t^{\alpha-1} e^{-\lambda t} dt}$
LOGNORMAL	 $f(t) = \frac{1}{\sigma t (2\pi)} e^{-\frac{1}{2} \left( \frac{\ln t - \mu}{\sigma} \right)^2}$	 $R(t) = 1 - \Phi \left( \frac{\ln t - \mu}{\sigma} \right)$ <p>See Note</p>	 $h(t) = \frac{f(t)}{1 - \Phi \left( \frac{\ln t - \mu}{\sigma} \right)}$
NORMAL	 $f(t) = \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{1}{2} \left( \frac{t - \mu}{\sigma} \right)^2}$	 $R(t) = 1 - \Phi \left( \frac{t - \mu}{\sigma} \right)$ <p>See Note</p>	 $h(t) = \frac{f(t)}{1 - \Phi \left( \frac{t - \mu}{\sigma} \right)}$
WEIBULL	 $f(t) = \frac{\beta}{\eta} \left( \frac{t - \gamma}{\eta} \right)^{\beta-1} e^{-\left[ \left( \frac{t - \gamma}{\eta} \right)^\beta \right]}$	 $R(t) = e^{-\left[ \left( \frac{t - \gamma}{\eta} \right)^\beta \right]}$	 $h(t) = \frac{\beta}{\eta} \left( \frac{t - \gamma}{\eta} \right)^{\beta-1}$

Note:  $\Phi \left( \frac{\ln t - \mu}{\sigma} \right)$  (lognormal) and  $\Phi \left( \frac{t - \mu}{\sigma} \right)$  (normal) is the standardized form of these distributions and is equal to the integral of the pdfs for those distributions (i.e., the cumulative distribution function).

FIGURE 5.3-1: SHAPES OF FAILURE DENSITY, RELIABILITY AND HAZARD RATE FUNCTIONS FOR COMMONLY USED CONTINUOUS DISTRIBUTIONS

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

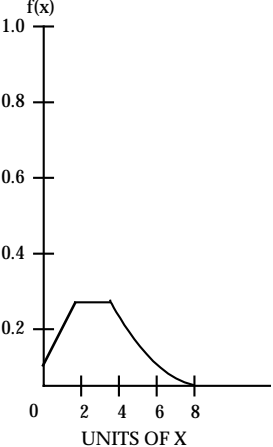
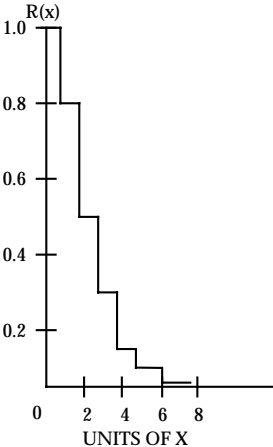
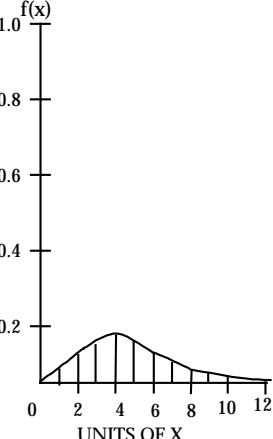
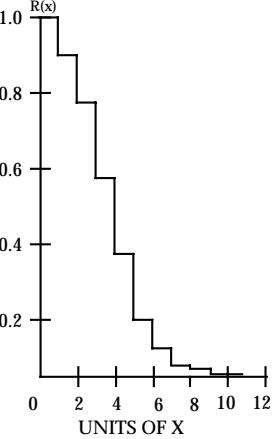
TYPE OF DISTRIBUTION	PARAMETERS	PROBABILITY DENSITY FUNCTION $f(x)$	RELIABILITY FUNCTION $R(x) = 1 - F(t)$
BINOMIAL	MEAN, $\mu = np$ Standard Deviation, $\sigma = \sqrt{npq}$ $\binom{n}{x} = \frac{n!}{(n-x)!x!}$ $q = 1 - p$		
	Sample data used to plot charts shown	$f(x) = \binom{n}{x} p^x q^{n-x}$ $\left\{ \begin{array}{l} n=8 \\ p=2/3 \end{array} \right\}$	$R(x) = \sum_{i=x}^n \binom{n}{i} p^i q^{n-i}$ $\left\{ \begin{array}{l} n=8 \\ p=2/3 \end{array} \right\}$
POISSON	MEAN, $\mu = a$ , Standard Deviation, $\sigma = \sqrt{a} = \sqrt{\lambda t}$		
	Sample data used to plot charts shown	$f(x) = \frac{a^x e^{-a}}{x!}$ $= \frac{(\lambda t)^x e^{-\lambda t}}{x!}$ $a = \lambda t = 4$	$R(x) = \sum_{i=x}^{\infty} \frac{a^i e^{-a}}{i!}$ $= \sum_{i=x}^{\infty} \frac{(\lambda t)^i e^{-\lambda t}}{i!}$ $a = \lambda t = 4$

FIGURE 5.3-2: SHAPES OF FAILURE DENSITY AND RELIABILITY FUNCTIONS OF COMMONLY USED DISCRETE DISTRIBUTIONS

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

where:

- $\mu$  = the population mean
- $\sigma$  = the population standard deviation, which is the square root of the variance

For most practical applications, probability tables for the standard normal distribution are used (See Table 5.3-1). The standard normal distribution density function is given by

$$f(z) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{z^2}{2}\right) \quad (5.23)$$

where:

$$\begin{aligned} \mu &= 0 \\ \sigma^2 &= 1 \end{aligned}$$

One converts from the normal to standard normal distribution by using the transformations

$$z = \frac{t - \mu}{\sigma} \quad (5.24)$$

$$f(t) = \frac{f(z)}{\sigma} \quad (5.25)$$

$$F(t) = P[t \leq t] = \int_{-\infty}^t \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2\right] dt \quad (5.26)$$

$$R(t) = 1 - F(t) \quad (5.27)$$

where:

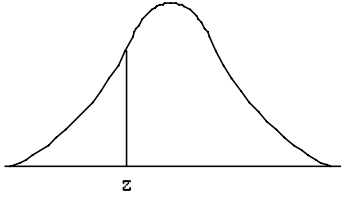
F(t) is the cumulative distribution function

R(t) is the reliability function

This integral cannot be evaluated in closed form; however, using the transformations in equations 5.24 and 5.25 along with Table 5.3-2, the probabilities for any normal distribution can be determined.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.3-1: VALUES OF THE STANDARD NORMAL DISTRIBUTION FUNCTION

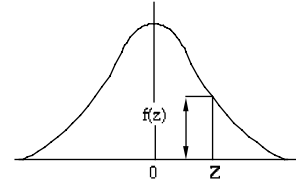


$$\Phi(z) = \int_{-\infty}^z \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}z^2} dz = P(Z \leq z)$$

z	0	1	2	3	4	5	6	7	8	9
-3.0	.0013	.0010	.0007	.0005	.0003	.0002	.0002	.0001	.0001	.0000
-2.9	.0019	.0018	.0017	.0017	.0016	.0016	.0015	.0015	.0014	.0014
-2.8	.0026	.0025	.0024	.0023	.0023	.0022	.0021	.0021	.0020	.0019
-2.7	.0035	.0034	.0033	.0032	.0031	.0030	.0029	.0028	.0027	.0026
-2.6	.0047	.0045	.0044	.0043	.0041	.0040	.0039	.0038	.0037	.0036
-2.5	.0062	.0060	.0059	.0057	.0055	.0054	.0052	.0051	.0049	.0048
-2.4	.0082	.0080	.0078	.0075	.0073	.0071	.0069	.0068	.0066	.0064
-2.3	.0107	.0104	.0102	.0099	.0096	.0094	.0091	.0089	.0087	.0084
-2.2	.0139	.0136	.0132	.0129	.0126	.0122	.0119	.0116	.0113	.0110
-2.1	.0179	.0174	.0170	.0166	.0162	.0158	.0154	.0150	.0146	.0143
-2.0	.0228	.0222	.0217	.0212	.0207	.0202	.0197	.0192	.0188	.0183
-1.9	.0287	.0281	.0274	.0268	.0262	.0256	.0250	.0244	.0238	.0233
-1.8	.0359	.0352	.0344	.0336	.0329	.0322	.0314	.0307	.0300	.0294
-1.7	.0446	.0436	.0427	.0418	.0409	.0401	.0392	.0384	.0375	.0367
-1.6	.0548	.0537	.0526	.0516	.0505	.0495	.0485	.0475	.0465	.0455
-1.5	.0668	.0655	.0643	.0630	.0618	.0606	.0594	.0582	.0570	.0559
-1.4	.0808	.0793	.0778	.0764	.0749	.0735	.0722	.0708	.0694	.0681
-1.3	.0968	.0951	.0934	.0918	.0901	.0885	.0869	.0853	.0838	.0823
-1.2	.1151	.1131	.1112	.1093	.1075	.1056	.1038	.1020	.1003	.0985
-1.1	.1357	.1335	.1314	.1292	.1271	.1251	.1230	.1210	.1190	.1170
-1.0	.1587	.1562	.1539	.1515	.1492	.1469	.1446	.1423	.1401	.1379
-.9	.1841	.1814	.1788	.1762	.1736	.1711	.1685	.1660	.1635	.1611
-.8	.2119	.2090	.2061	.2033	.2005	.1977	.1949	.1922	.1894	.1867
-.7	.2420	.2389	.2358	.2327	.2297	.2266	.2236	.2206	.2177	.2148
-.6	.2743	.2709	.2676	.2643	.2611	.2578	.2546	.2514	.2483	.2451
-.5	.3085	.3050	.3015	.2981	.2946	.2912	.2877	.2843	.2810	.2776
-.4	.3446	.3409	.3372	.3336	.3300	.3264	.3228	.3192	.3156	.3121
-.3	.3821	.3783	.3745	.3707	.3669	.3632	.3594	.3557	.3520	.3483
-.2	.4207	.4168	.4129	.4090	.4052	.4013	.3974	.3936	.3897	.3859
-.1	.4602	.4562	.4522	.4483	.4443	.4404	.4364	.4325	.4286	.4247
-.0	.5000	.4960	.4920	.4880	.4840	.4801	.4761	.4721	.4681	.4641

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.3-2: ORDINATES  $F(z)$  OF THE STANDARD NORMAL CURVE AT  $z$



z	0	1	2	3	4	5	6	7	8	9
0.0	.3989	.3989	.3989	.3988	.3986	.3984	.3982	.3980	.3977	.3973
0.1	.3970	.3965	.3961	.3956	.3951	.3945	.3939	.3932	.3925	.3918
0.2	.3910	.3902	.3894	.3885	.3876	.3867	.3857	.3847	.3836	.3825
0.3	.3814	.3802	.3790	.3778	.3765	.3752	.3739	.3725	.3712	.3697
0.4	.3683	.3668	.3653	.3637	.3621	.3605	.3589	.3572	.3555	.3538
0.5	.3521	.3503	.3485	.3467	.3448	.3429	.3410	.3391	.3372	.3352
0.6	.3332	.3312	.3292	.3271	.3251	.3230	.3209	.3187	.3166	.3144
0.7	.3123	.3101	.3079	.3056	.3034	.3011	.2989	.2966	.2943	.2920
0.8	.2897	.2874	.2850	.2827	.2803	.2780	.2756	.2732	.2709	.2685
0.9	.2661	.2637	.2613	.2589	.2565	.2541	.2516	.2492	.2468	.2444
1.0	.2420	.2396	.2371	.2347	.2323	.2299	.2275	.2251	.2227	.2203
1.1	.2179	.2155	.2131	.2107	.2083	.2059	.2036	.2012	.1989	.1965
1.2	.1942	.1919	.1895	.1872	.1849	.1826	.1804	.1781	.1758	.1736
1.3	.1714	.1691	.1669	.1647	.1626	.1604	.1582	.1561	.1539	.1518
1.4	.1497	.1476	.1456	.1435	.1415	.1394	.1374	.1354	.1334	.1315
1.5	.1295	.1276	.1257	.1238	.1219	.1200	.1182	.1163	.1145	.1127
1.6	.1109	.1092	.1074	.1057	.1040	.1023	.1006	.0989	.0973	.0957
1.7	.0940	.0925	.0909	.0893	.0878	.0863	.0848	.0833	.0818	.0804
1.8	.0790	.0775	.0761	.0748	.0734	.0721	.0707	.0694	.0681	.0669
1.9	.0656	.0644	.0632	.0620	.0608	.0596	.0584	.0573	.0562	.0551
2.0	.0540	.0529	.0519	.0508	.0498	.0488	.0478	.0468	.0459	.0449
2.1	.0440	.0431	.0422	.0413	.0404	.0396	.0387	.0379	.0371	.0363
2.2	.0355	.0347	.0339	.0332	.0325	.0317	.0310	.0303	.0297	.0290
2.3	.0283	.0277	.0270	.0264	.0258	.0252	.0246	.0241	.0235	.0229
2.4	.0224	.0219	.0213	.0208	.0203	.0198	.0194	.0189	.0184	.0180
2.5	.0175	.0171	.0167	.0163	.0158	.0154	.0151	.0147	.0143	.0139
2.6	.0136	.0132	.0129	.0126	.0122	.0119	.0116	.0113	.0110	.0107
2.7	.0104	.0101	.0099	.0096	.0093	.0091	.0088	.0086	.0084	.0081
2.8	.0079	.0077	.0075	.0073	.0071	.0069	.0067	.0065	.0063	.0061
2.9	.0060	.0058	.0056	.0055	.0053	.0051	.0050	.0048	.0047	.0046
3.0	.0044	.0043	.0042	.0040	.0039	.0038	.0037	.0036	.0035	.0034
3.1	.0033	.0032	.0031	.0030	.0029	.0028	.0027	.0026	.0025	.0025
3.2	.0024	.0023	.0022	.0022	.0021	.0020	.0020	.0019	.0018	.0018
3.3	.0017	.0017	.0016	.0016	.0015	.0015	.0014	.0014	.0013	.0013
3.4	.0012	.0012	.0012	.0011	.0011	.0010	.0010	.0010	.0009	.0009
3.5	.0009	.0008	.0008	.0008	.0008	.0007	.0007	.0007	.0007	.0006
3.6	.0006	.0006	.0006	.0005	.0005	.0005	.0005	.0005	.0005	.0004
3.7	.0004	.0004	.0004	.0004	.0004	.0004	.0003	.0003	.0003	.0003
3.8	.0003	.0003	.0003	.0003	.0003	.0002	.0002	.0002	.0002	.0002
3.9	.0002	.0002	.0002	.0002	.0002	.0002	.0002	.0002	.0001	.0001

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

The standardized cumulative distribution function is,

$$\phi(t) = \int_{-\infty}^z \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{z^2}{2}\right) dz \quad (5.28)$$

then for a normally distributed variable  $t$ , with mean  $\mu$  and standard deviation  $\sigma$

$$P(t \leq t) = P\left(Z \leq \frac{t - \mu}{\sigma}\right) = \Phi\left(\frac{t - \mu}{\sigma}\right) \quad (5.29)$$

The hazard function for a normal distribution is a monotonically increasing function of  $t$ . This can be shown by proving  $h'(t) \geq 0$  for all  $t$ .

### 5.3.2 Examples of Reliability Calculations Using the Normal Distribution

#### 5.3.2.1 Microwave Tube Example

A microwave transmitting tube has been observed to follow a normal distribution with  $\mu = 5000$  hours and  $\sigma = 1500$  hours. Find the reliability of such a tube for a mission time of 4100 hours and the hazard rate of one of these tubes at age 4400 hours.

$$\begin{aligned} R(t) &= P\left(z > \frac{t - \mu}{\sigma}\right) \\ R(4100) &= P\left(z > \frac{4100 - 5000}{1500}\right) \\ &= P(z > -0.6) = 1 - P(z < -0.6) \\ &= 1 - 0.27 = 0.73 \end{aligned}$$

as found in Table 5.3-1. Remember  $P(z > -z_i) = P(z < z_i)$  by symmetry of the normal distribution.

$$\begin{aligned} h(t) &= \frac{f(t)}{R(t)} = \frac{f(z)/\sigma}{R(t)} \\ f(t = 4400) &= \frac{f\left(z = \frac{4400 - 5000}{1500}\right)}{1500} = \frac{1}{1500} f(z = -0.4) \end{aligned}$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

$$= (0.00067)(0.37) = 0.00025$$

where  $f(z = 0.4)$  was obtained from Table 5.3-2. Remember  $f(z) = f(-z)$  because of the symmetry of the normal distribution.

$$R(4400) = P\left(z > \frac{4400 - 5000}{1500}\right) = P(z > -0.4) = 1 - P(z < -0.4) = 0.65$$

$$h(4400) = \frac{f(4400)}{R(4400)} = \frac{0.00025}{0.65} = 0.00038 \text{ failures/hour}$$

### 5.3.2.2 Mechanical Equipment Example

A motor generator has been observed to follow a normal distribution with  $\mu = 300$  hours and  $\sigma = 40$  hours. Find the reliability of the motor generator for a mission time (or time before maintenance) of 250 hours and the hazard rate at 200 hours.

$$\begin{aligned} R(250) &= P\left(z > \frac{250 - 300}{40}\right) = P(z > -1.25) \\ &= 1 - P(z < -1.25) = 1 - 0.11 = 0.89 \end{aligned}$$

where  $P(z < -1.25)$  was interpolated from Table 5.3-1.

$$\begin{aligned} h(t) &= \frac{f(t)}{R(t)} = \frac{f(z)/\sigma}{R(t)} \\ f(t = 200) &= \frac{f\left(z = \frac{200 - 300}{40}\right)}{40} = \frac{1}{40} f(z = -2.5) \end{aligned}$$

$$f(z = -2.5) = (0.025)(0.0175) = 0.00044$$

where  $f(z = 2.5)$  was found in Table 5.3-2.

$$R(200) = P\left(z > \frac{200 - 300}{40}\right) = P(z > -2.5) = 1 - P(z < -2.5) = 0.994$$

$$h(200) = \frac{f(200)}{R(200)} = \frac{0.00044}{0.994} = 0.00044 \text{ failures/hour}$$



## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

5.3.3 Lognormal Distribution

The lognormal distribution is the distribution of a random variable whose natural logarithm is distributed normally; in other words, it is the normal distribution with  $\ln t$  as the variate. The density function is

$$f(t) = \frac{1}{\sigma t \sqrt{2\pi}} \exp \left[ -\frac{1}{2} \left( \frac{\ln(t) - \mu}{\sigma} \right)^2 \right] \quad \text{for } t \geq 0 \quad (5.30)$$

$$\text{where the mean} = \exp \left( \mu + \frac{\sigma^2}{2} \right) \quad (5.31)$$

$$\text{and the standard deviation} = \left[ \exp(2\mu + 2\sigma^2) - \exp(2\mu + \sigma^2) \right]^{1/2} \quad (5.32)$$

where  $\mu$  and  $\sigma$  are the mean and standard deviation (SD) of  $\ln(t)$ .

The lognormal distribution is used in reliability analysis of semiconductors and fatigue life of certain types of mechanical components. This distribution is also commonly used in maintainability analysis and will be further discussed in Section 5.6.2.1.

The cumulative distribution function for the lognormal is,

$$F(t) = \int_0^t \frac{1}{t\sigma\sqrt{2\pi}} \exp \left[ -\frac{1}{2} \left( \frac{\ln(t) - \mu}{\sigma} \right)^2 \right] dt \quad (5.33)$$

this can be related to the standard normal variant  $Z$  by

$$F(t) = P[t \leq t] = P \left[ Z \leq \left( \frac{\ln t - \mu}{\sigma} \right) \right] \quad (5.34)$$

the reliability function is  $1-F(t)$  or

$$R(t) = (1 - F(t)) = P \left[ Z > \left( \frac{\ln(t) - \mu}{\sigma} \right) \right] \quad (5.35)$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

the hazard function,  $h(t)$ , is given as follows

$$h(t) = \frac{f(t)}{R(t)} = \frac{\phi\left(\frac{\ln(t) - \mu}{\sigma}\right)}{t\sigma R(t)} \quad (5.36)$$

where  $\phi$  is the standard normal probability function and  $\mu$  and  $\sigma$  are the mean and  $t$  standard deviation of the natural logarithm of the random variable  $t$ .

### 5.3.3.1 Fatigue Failure Example

Suppose it has been observed that gun tube failures occur according to the lognormal distribution with  $\mu = 7$  and  $\sigma = 2$  (remember  $\mu$  and  $\sigma$  are the mean and SD of the  $\ln(t)$  data). Find the reliability for a 1000 round mission and the hazard rate at 800 rounds. For this case, the variable  $t$  is the number of rounds.

$$R(t) = P\left(z > \frac{\ln(t) - \mu}{\sigma}\right)$$

$$R(1000) = P\left(z > \frac{\ln(1000) - 7.0}{2.0}\right) = P(z > -0.045) = 0.52$$

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(z)/\sigma t}{R(t)} \quad \text{The numerator represents the transformation in the lognormal case.}$$

$$\begin{aligned} h(800) &= \frac{f(800)}{\sigma t R(800)} = \frac{f\left(z = \frac{\ln(800) - 7}{2}\right)}{(2)(800)R(800)} = \frac{f\left(z = \frac{\ln 800 - 7}{2}\right)}{(2)(800) P\left(z > \frac{\ln 800 - 7}{2}\right)} \\ &= \frac{f(z = -0.16)}{1600 P(z > -0.16)} = \frac{0.3939}{(1600)(0.5636)} = 0.0004 \text{ failures/round} \end{aligned}$$

where  $P(z > -0.16)$  was interpolated from Table 5.3-1 and  $f(z = -0.16)$  was obtained from Table 5.3-2.

### 5.3.4 Exponential Distribution

This is probably the most important distribution in reliability work and is used almost exclusively for reliability prediction of electronic equipment (Ref. MIL-HDBK-217). It describes the situation wherein the hazard rate is constant which can be shown to be generated by a Poisson

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

process. This distribution is valuable if properly used. It has the advantages of

- (1) A single, easily estimated parameter ( $\lambda$ )
- (2) Is mathematically very tractable
- (3) Has fairly wide applicability
- (4) Is additive - that is, the sum of a number of independent exponentially distributed variables is exponentially distributed

Some particular applications of this model include

- (1) Items whose failure rate does not change significantly with age
- (2) Complex and repairable equipment without excessive amounts of redundancy
- (3) Equipment for which the early failures or "infant mortalities" have been eliminated by "burning in" the equipment for some reasonable time period

The failure density function is

$$f(t) = \lambda e^{-\lambda t} \quad \text{for } t > 0, \quad (5.37)$$

where  $\lambda$  is the hazard (failure) rate, and the reliability function is

$$R(t) = e^{-\lambda t} \quad (5.38)$$

the mean life ( $\theta$ ) =  $1/\lambda$ , and, for repairable equipment, the MTBF =  $\theta = 1/\lambda$ .

#### 5.3.4.1 Airborne Fire Control System Example

The mean time to failure (MTTF =  $\theta$ , for this case) of an airborne fire control system is 10 hours. What is the probability that it will not fail during a 3 hour mission?

$$R(3) = e^{-\lambda t} = e^{-t/\theta} = e^{-3/10} = e^{-0.3} = 0.74$$

#### 5.3.4.2 Computer Example

A computer has a constant error rate of one error every 17 days of continuous operation. What is the reliability associated with the computer to correctly solve a problem that requires 5 hours time? Find the hazard rate after 5 hours of operation.

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

$$\text{MTTF} = \theta = 408 \text{ hours}$$

$$\lambda = \frac{1}{\theta} = \frac{1}{408} = 0.0024 \text{ failure/hour}$$

$$R(5) = e^{-\lambda t} = e^{-(0.0024)(5)} = e^{-0.012} = 0.99$$

$$h(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda = 0.0024 \text{ failures/hours}$$

### 5.3.5 Gamma Distribution

The gamma distribution is used in reliability analysis for cases where partial failures can exist, i.e., when a given number of partial failures must occur before an item fails (e.g., redundant systems) or the time to second failure when the time to failure is exponentially distributed. The failure density function is: [www.keakaoxing.com](http://www.keakaoxing.com)

$$f(t) = \frac{\lambda}{\Gamma(\alpha)} (\lambda t)^{\alpha-1} e^{-\lambda t} \quad \text{for } t > 0, \quad (5.39)$$

$$\alpha > 0,$$

$$\lambda > 0$$

where:

$$\lambda = \frac{\mu}{\sigma^2} \text{ and } \alpha = \lambda\mu \quad (5.40)$$

$\mu$  = mean of data

$\alpha$  = standard deviation

and  $\lambda$  is the failure rate (complete failure) and  $\alpha$  is the number of partial failures for complete failure or events to generate a failure.  $\Gamma(\alpha)$  is the gamma function:

$$\Gamma(\alpha) = \int_0^{\infty} x^{\alpha-1} e^{-x} dx \quad (5.41)$$

which can be evaluated by means of standard tables (See Table 5.3-3).

When  $(\alpha-1)$  is a positive integer,  $\Gamma(\alpha) = (\alpha-1)!$ , which is usually the case for most reliability analysis, e.g., partial failure situation. For this case the failure density function is

$$f(t) = \frac{\lambda}{(\alpha-1)!} (\lambda t)^{\alpha-1} e^{-\lambda t} \quad (5.42)$$

which, for the case of  $\alpha = 1$  becomes the exponential density function, previously described.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.3-3: GAMMA FUNCTION  $\Gamma(n)$ 

$$\Gamma(n) = \int_0^{\infty} e^{-x} X^{n-1} dx$$

n	$\Gamma(n)$	n	$\Gamma(n)$	n	$\Gamma(n)$	n	$\Gamma(n)$
1.00	1.00000	1.25	.90640	1.50	.88623	1.75	.9196
1.01	.99433	1.26	.90440	1.51	.88659	1.76	.92137
1.02	.98884	1.27	.90250	1.52	.88704	1.77	.92376
1.03	.98355	1.28	.99072	1.53	.88757	1.78	.92623
1.04	.97844	1.29	.89904	1.54	.88818	1.79	.92877
1.05	.97350	1.30	.89747	1.55	.88887	1.80	.93138
1.06	.96874	1.31	.89600	1.56	.88964	1.81	.93408
1.07	.96415	1.32	.89464	1.57	.89049	1.82	.93685
1.08	.95973	1.33	.89338	1.58	.89142	1.83	.93969
1.09	.95546	1.34	.89222	1.59	.89243	1.84	.94261
1.10	.95135	1.35	1.89115	1.60	.89352	1.85	.94561
1.11	.94739	1.36	.89018	1.61	.89468	1.86	.94869
1.12	.94359	1.37	.88931	1.62	.89592	1.87	.95184
1.13	.93993	1.38	.88854	1.63	.89724	1.88	.95507
1.14	.93642	1.39	.88785	1.64	.89864	1.89	.95838
1.15	.93304	1.40	.88726	1.65	.90012	1.90	.96177
1.16	.92980	1.41	.88676	1.66	.90167	1.91	.96523
1.17	.92670	1.42	.88636	1.67	.90330	1.92	.96878
1.18	.92373	1.43	.88604	1.68	.90500	1.93	.97240
1.19	.92088	1.44	.88580	1.69	.90678	1.94	.97610
1.20	.91817	1.45	.88565	1.70	.90864	1.95	.97988
1.21	.91558	1.46	.88560	1.71	.91057	1.96	.98374
1.22	.91311	1.47	.88563	1.72	.91258	1.97	.98768
1.23	.91075	1.48	.88575	1.73	.91466	1.98	.99171
1.24	.90852	1.49	.88595	1.74	.91683	1.99	.99527
						2.00	1.00000

Note:  $\Gamma(n+x) = (n-1+x)(n-2+x) \dots (1+x) \Gamma(1+x)$

e.g.,  $\Gamma(3.15) = (2.15)(1.15) \Gamma(1.15)$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

$$F(t) = \int_0^t \frac{\lambda^\alpha}{\Gamma(\alpha)} t^{\alpha-1} e^{-\lambda t} dt \quad (5.43)$$

If  $\alpha$  is an integer, it can be shown by integration by parts that

$$F(t) = \sum_{k=\alpha}^{\infty} \frac{(\lambda t)^k \exp[-\lambda t]}{K!} \quad (5.44)$$

$$\text{Then } R(t) = 1 - F(t) = \sum_{K=0}^{n-1} \frac{(\lambda t)^K \exp[-\lambda t]}{K!} \quad (5.45)$$

$$\text{and } h(t) = \frac{f(t)}{R(t)} = \frac{\frac{\lambda^\alpha}{\Gamma(\alpha)} t^{\alpha-1} e^{-\lambda t}}{\sum_{K=0}^{n-1} \frac{(\lambda t)^K \exp[-\lambda t]}{K!}} \quad (5.46)$$

The gamma distribution can also be used to describe an increasing or decreasing hazard (failure) rate. When  $\alpha > 1$ ,  $h(t)$  increases; when  $\alpha < 1$ ,  $h(t)$  decreases. This is shown in Figure 5.3-1.

### 5.3.5.1 Missile System Example

An anti-aircraft missile system has demonstrated a gamma failure distribution with  $\alpha = 3$  and  $\lambda = 0.05$  (failures/hour). Determine the reliability for a 24 hour mission time and the hazard rate at the end of 24 hours.

$$R(t) = \frac{\lambda^\alpha}{\Gamma(\alpha)} \int_t^{\infty} t^{\alpha-1} e^{-\lambda t} dt$$

Ordinarily, special tables of the Incomplete Gamma Function are required to evaluate the above integral. However, it can be shown that if  $\alpha$  is an integer

$$R(t) = \sum_{k=0}^{\alpha-1} \frac{(\lambda t)^k e^{-\lambda t}}{k!} \quad (5.47)$$

which later in the section will be shown to be a Poisson distribution. Using Eq. (5.47)

$$R(24) = \sum_{k=0}^2 \frac{[(0.05)(24)]^k e^{-(0.05)(24)}}{k!} = \sum_{k=0}^2 \frac{(1.2)^k (0.3)}{k!}$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

$$= (0.3) + (1.2)(0.3) + \frac{(1.2)^2(0.3)}{2} = 0.3 + 0.36 + 0.216 = 0.88$$

$$h(t) = \frac{f(t)}{R(t)}$$

$$f(t) = \frac{\lambda}{(\alpha - 1)!} (\lambda t)^{\alpha-1} e^{-\lambda t}$$

$$f(24) = \frac{0.05}{2} (1.2)^2 e^{-1.2} = (0.025)(0.434) = 0.011$$

$$h(24) = \frac{f(24)}{R(24)} = \frac{0.011}{0.88} = 0.012 \text{ failures/hour}$$

5.3.6 Weibull Distribution

The Weibull distribution is particularly useful in reliability work since it is a general distribution which, by adjustment of the distribution parameters, can be made to model a wide range of life distribution characteristics of different classes of engineered items.

One of the versions of the failure density function is

$$f(t) = \frac{\beta}{\eta} \left( \frac{t-\gamma}{\eta} \right)^{\beta-1} \exp \left[ - \left( \frac{t-\gamma}{\eta} \right)^\beta \right] \quad (5.48)$$

where:

- $\beta$  is the shape parameter
- $\eta$  is the scale parameter or characteristic life  
(life at which 63.2% of the population will have failed)
- $\gamma$  is the minimum life

In most practical reliability situations,  $\gamma$  is often zero (failure assumed to start at  $t = 0$ ) and the failure density function becomes

$$f(t) = \frac{\beta}{\eta} \left( \frac{t}{\eta} \right)^{\beta-1} \exp \left[ - \left( \frac{t}{\eta} \right)^\beta \right] \quad (5.49)$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

and the reliability and hazard functions become

$$R(t) = \exp \left[ - \left( \frac{t}{h} \right)^b \right] \quad (5.50)$$

$$h(t) = \left( \frac{b}{h} \right) \left( \frac{t}{h} \right)^{b-1} \quad (5.51)$$

Depending upon the value of  $\beta$ , the Weibull distribution function can take the form of the following distributions as follows,

$\beta < 1$	Gamma	$\beta = 1$	Exponential
$\beta = 2$	Lognormal	$\beta = 3.5$	Normal (approximately)

Thus, it may be used to help identify other distributions from life data (backed up by goodness of fit tests) as well as being a distribution in its own right. Graphical methods are used to analyze Weibull failure data and are described in Section 8.

### 5.3.6.1 Example of Use of Weibull Distribution

The failure times of a particular transmitting tube are found to be Weibull distributed with  $\beta = 2$  and  $\eta = 1000$  hours. Find the reliability of one of these tubes for a mission time of 100 hours, and the hazard rate after a tube has operated successfully for 100 hours.

$$R(t) = \exp \left[ - \left( \frac{t}{\eta} \right)^\beta \right]$$

$$R(100) = \exp \left[ - \left( \frac{100}{1000} \right)^2 \right] = e^{-(0.1)^2} \approx 0.99$$

$$h(100) = \left( \frac{\beta}{\eta} \right) \left( \frac{t}{\eta} \right)^{\beta-1} = \left( \frac{2}{1000} \right) \left( \frac{100}{1000} \right)^{2-1} = 0.0002 \text{ failures/hour}$$



---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

5.3.7 Discrete Distributions5.3.7.1 Binomial Distribution

The binomial distribution is used for those situations in which there are only two outcomes, such as success or failure, and the probability remains the same for all trials. It is very useful in reliability and quality assurance work. The probability density function (pdf) of the binomial distribution is

$$f(x) = \binom{n}{x} p^x q^{(n-x)} \quad (5.52)$$

$$\text{where } \binom{n}{x} = \frac{n!}{(n-x)!x!} \quad \text{and } q = 1 - p \quad (5.53)$$

$f(x)$  is the probability of obtaining exactly  $x$  good items and  $(n-x)$  bad items in a sample of  $n$  items where  $p$  is the probability of obtaining a good item (success) and  $q$  (or  $1-p$ ) is the probability of obtaining a bad item (failure).

The cumulative distribution function (cdf), i.e., the probability of obtaining  $r$  or fewer successes in  $n$  trials, is given by

$$F(x; r) = \sum_{x=0}^r \binom{n}{x} p^x q^{n-x} \quad (5.54)$$

5.3.7.1.1 Quality Control Example

In a large lot of component parts, past experience has shown that the probability of a defective part is 0.05. The acceptance sampling plan for lots of these parts is to randomly select 30 parts for inspection and accept the lot if 2 or less defectives are found. What is the probability,  $P(a)$ , of accepting the lot?

$$\begin{aligned} P(a) &= \sum_{x=0}^2 \binom{30}{x} (0.05)^x (0.95)^{30-x} \\ &= \frac{30!}{0! 30!} (0.05)^0 (0.95)^{30} + \frac{30!}{1! 29!} (0.05)(0.95)^{29} + \frac{30!}{2! 28!} (0.05)^2 (0.95)^{28} \\ &= 0.812 \end{aligned}$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

Note that in this example, the probability of success was the probability of obtaining a defective part.

### 5.3.7.1.2 Reliability Example

The binomial is useful for computing the probability of system success when the system employs partial redundancy. Assume a five channel VHF receiver as shown in Figure 5.3-3.

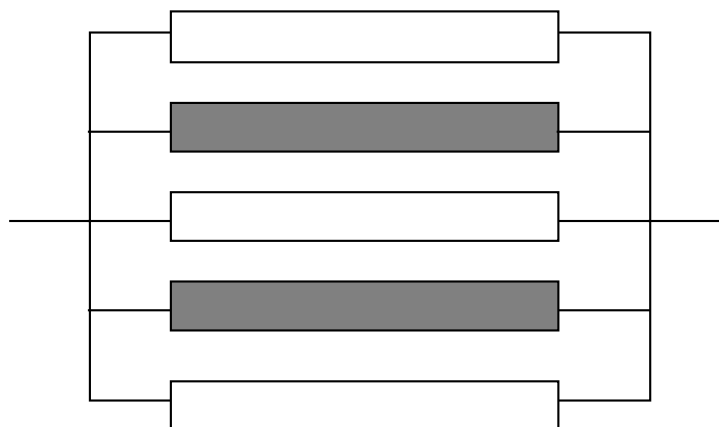


FIGURE 5.3-3: FIVE CHANNEL RECEIVER WITH TWO FAILURES ALLOWED

As long as three channels are operational, the system is classified as satisfactory. Thus, two channel failures are allowed. Each channel has a probability of 0.9 of surviving a 24 hour operation period without failure. What is the probability that the receiver will survive a 24 hour mission without loss of more than two channels?

Let

- $n = 5 =$  number of channels
- $r = 2 =$  number of allowable channel failures
- $p = 0.9 =$  probability of individual channel success
- $q = 0.1 =$  probability of individual channel failure
- $x =$  number of successful channels
- $P(S) =$  probability of system success

Then

$$P(S) = \sum_{x=3}^n \frac{n!}{x!(n-x)!} p^x q^{n-x}$$

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

$$= \frac{5!}{3!2!} (0.9)^3 (0.1)^2 + \frac{5!}{4!1!} (0.9)^4 (0.1)^1 + \frac{5!}{5!0!} (0.9)^5 (0.1)^0 = 0.99144$$

This is the probability that three or more of the five channels will survive the 24 hour operating period.

The problem can be solved another way, by subtracting the probability of three or more failures from one, e.g.:

$$\begin{aligned} P(S) &= 1 - P(F) \\ &= 1 - \sum_{x=(r+1)}^n \frac{n!}{n!(n-x)!} q^x p^{n-x} \\ &= 1 - \left[ \frac{5!}{3!2!} (0.1)^3 (0.9)^2 + \frac{5!}{4!1!} (0.1)^4 (0.9)^1 + \frac{5!}{5!0!} (0.1)^5 (0.9)^0 \right] \\ &= 1 - 0.00856 = 0.99144 \text{ as before} \end{aligned}$$

Note the change in notation (only) that  $x$  now represents the number of failures and  $q^x$  is the probability of  $x$  failures whereas before  $x$  represented the number of successes and  $p^x$  was the probability of  $x$  successes.

Computations involving the binomial distribution become rather unwieldy for even small sample sizes; however, complete tables of the binomial pdf and cdf are available in many statistics texts.

### 5.3.8 Poisson Distribution

This distribution is used quite frequently in reliability analysis. It can be considered an extension of the binomial distribution when  $n$  is infinite. In fact, it is used to approximate the binomial distribution when  $n \geq 20$  and  $p \leq 0.05$ .

If events are Poisson distributed, they occur at a constant average rate and the number of events occurring in any time interval are independent of the number of events occurring in any other time interval. For example, the number of failures in a given time would be given by

$$f(x) = \frac{a^x e^{-a}}{x!} \tag{5.55}$$

where  $x$  is the number of failures and  $a$  is the expected number of failures.

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

For the purpose of reliability analysis, this becomes

$$f(x; \lambda, t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!} \quad (5.56)$$

where:

$\lambda$  = failure rate  
 $t$  = length of time being considered  
 $x$  = number of failures

The reliability function,  $R(t)$ , or the probability of zero failures in time  $t$  is given by:

$$R(t) = \frac{(\lambda t)^0 e^{-\lambda t}}{0!} = e^{-\lambda t} \quad (5.57)$$

or our old friend, the exponential distribution.

In the case of redundant equipments, the  $R(t)$  might be desired in terms of the probability of  $r$  or fewer failures in time  $t$ . For that case

$$R(t) = \sum_{x=0}^r \frac{(\lambda t)^x e^{-\lambda t}}{x!} \quad (5.58)$$

### 5.3.8.1 Example With Permissible Number of Failures

A slide projector is needed for 500 hours of operation. Replacement of failed lamps is permitted, but there are only two spare bulbs on hand. If the lamp failure rate is 0.001 failures per hour, what is the reliability for the mission (i.e., the probability that no more than two lamp failures will occur)?

$$\lambda = 0.001 \quad t = 500 \quad \lambda t = 0.5 \quad r \leq 2$$

$$\begin{aligned} R(500) &= \sum_{r=0}^2 \frac{(0.5)^r e^{-0.5}}{r!} \\ &= e^{-0.5} + 0.5 e^{-0.5} + \frac{(0.5)^2 e^{-0.5}}{2} = 0.986 \end{aligned}$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

## 5.4 Failure Modeling

Failure modeling is a key to reliability engineering. Validated failure rate models are essential to the development of prediction techniques, allocation procedures, design and analysis methodologies, test and demonstration procedures/control procedures, etc. In other words, all of the elements needed as inputs for sound decisions to insure that an item can be designed and manufactured so that it will perform satisfactorily and economically over its useful life.

Inputs to failure rate models are operational field data, test data, engineering judgment, and physical failure information. These inputs are used by the reliability engineer to construct and validate statistical failure rate models (usually having one of the distributional forms described previously) and to estimate their parameters.

## 5.4.1 Typical Failure Rate Curve

Figure 5.4-1 shows a typical time versus failure rate curve for equipment. This is the "bathtub curve," which, over the years, has become widely accepted by the reliability community. It has proven to be particularly appropriate for electronic equipment and systems. The characteristic pattern is a period of decreasing failure rate (DFR) followed by a period of constant failure rate (CFR), followed by a period of increasing failure rate (IFR).

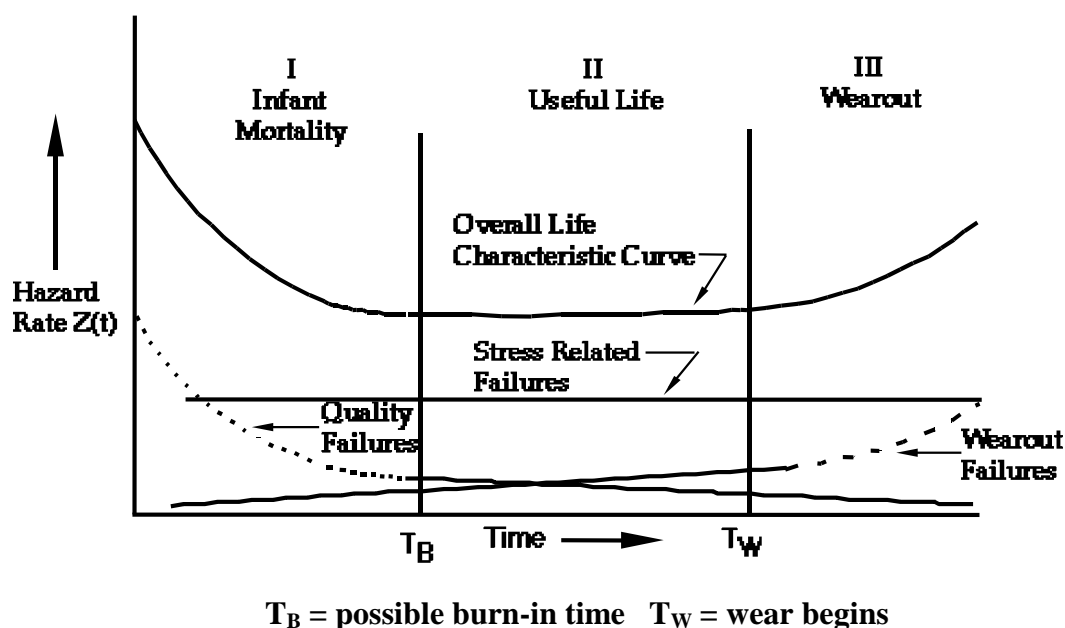


FIGURE 5.4-1: HAZARD RATE AS A FUNCTION OF AGE

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**

---

Zone I is the infant mortality (DFR) period characterized by an initially high failure rate. This is normally the result of poor design, the use of substandard components, or lack of adequate controls in the manufacturing process. When these mistakes are not caught by quality control inspections, an early failure is likely to result. Early failures can be eliminated from the customer by “burn in” during which time the equipment is operated at stress levels equal to the intended actual operating conditions. The equipment is then released for actual use only when it has passed through the “burn-in” period.

Zone II, the useful life period, is characterized by an essentially constant failure rate (CFR). This is the period dominated by chance failures. Chance failures are those failures that result from strictly random or chance causes. They cannot be eliminated by either lengthy burn-in periods or good preventive maintenance practices. Equipment is designed to operate under certain conditions and up to certain stress levels. When these stress levels are exceeded due to random unforeseen or unknown events, a chance failure will occur. While reliability theory and practice is concerned with all three types of failures, its primary concern is with chance failures, since they occur during the useful life period of the equipment. Figure 5.4-1 is somewhat deceiving, since Zone II is usually of much greater length than Zones I or III. The time when a chance failure will occur cannot be predicted; however, the likelihood or probability that one will occur during a given period of time within the useful life can be determined by analyzing the equipment design. If the probability of chance failure is too great, either design changes must be introduced or the operating environment made less severe.

This CFR period is the basis for application of most reliability engineering design methods. Since it is constant, the exponential distribution of time to failure is applicable and is the basis for the design and prediction procedures spelled out in documents such as MIL- HDBK-217.

The simplicity of the approach utilizing the exponential distribution, as previously indicated, makes it extremely attractive. Fortunately, it is widely applicable for complex equipments and systems. If complex equipment consists of many components, each having a different mean life and variance which are randomly distributed, then the system malfunction rate becomes essentially constant as failed parts are replaced.

Thus, even though the failures might be wearout failures, the mixed population causes them to occur at random time intervals with a constant failure rate and exponential behavior. Figure 5.4-2 indicates this for a population of incandescent lamps in a factory. This has been verified for many equipments from electronic systems to bus motor overhaul rates.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

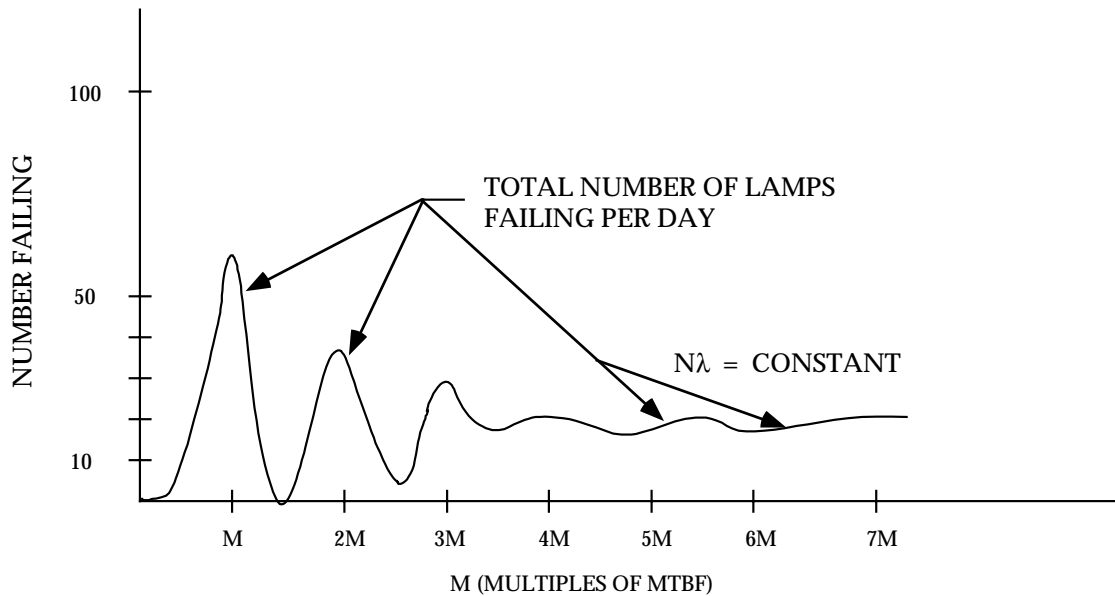


FIGURE 5.4-2: STABILIZATION OF FAILURE FREQUENCY

Zone III, the wearout period, is characterized by an IFR as a result of equipment deterioration due to age or use. For example, mechanical components such as transmission bearings will eventually wear out and fail, regardless of how well they are made. Early failures can be postponed and the useful life of equipment extended by good design and maintenance practices. The only way to prevent failure due to wearout is to replace or repair the deteriorating component before it fails.

Since modern electronic equipment is almost completely composed of semi-conductor devices which really have no short term wearout mechanism, except for perhaps electromigration, one might question whether predominantly electronic equipment will even reach Zone III of the bathtub curve.

From Figure 5.4-1, it can be seen that different statistical distributions might be used to characterize each zone. For example, the infant mortality period might be represented by gamma or Weibull, the useful life period by the exponential, and the wearout period by gamma or normal distributions.

The rest of this section will be devoted to models using the exponential distribution since it is applicable during the useful life period, which is the longest period of an equipment's life.

#### 5.4.2 Reliability Modeling of Simple Structures

In this section, the reliability functions of some simple, structures will be derived. These functions are based upon the exponential distribution of time to failure.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

5.4.2.1 Series Configuration

The simplest and perhaps most commonly occurring configuration in reliability mathematical modeling is the series configuration. The successful operation of the system depends on the proper functioning of all the system components. A component failure represents total system failure. A series reliability configuration is represented by the block diagram as shown in Figure 5.4-3 with  $n$  components. Further, assume that the failure of any one component is statistically independent of the failure or success of any other. This is usually the case for most practical purposes. If this is not the case, then conditional probabilities must be used, which only increase the complexity of the calculations.

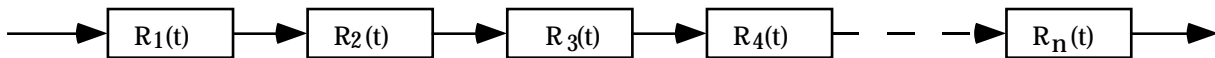


FIGURE 5.4-3: SERIES CONFIGURATION

Thus, for the configuration of Figure 5.4-3, under the assumptions made, the series reliability is given by

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \cdot \dots \cdot R_n(t) = \prod_{i=1}^n R_i(t) \quad (5.59)$$

If, as we said before, a constant failure rate,  $\lambda$ , is assumed for each component, which means the exponential distribution for the reliability function, then, is

$$R_S(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} \cdot \dots \cdot e^{-\lambda_n t} = \exp \left[ -\sum_{i=1}^n \lambda_i t \right] = \exp [-\lambda t] \quad (5.60)$$

where:

$$\lambda = \lambda_1 + \lambda_2 + \dots + \lambda_n = \frac{1}{\theta}$$

Thus, the system failure rate,  $\lambda$ , is the sum of the individual component failure rates and the system mean life,  $\theta = 1/\lambda$ .

Consider a system composed of 400 component parts each having an exponential time to failure density function. Let us further assume that each component part has a reliability of 0.99 for some time  $t$ . The system reliability for the same time  $t$  is

$$R(t) = 0.99^{400} = 0.018$$

Out of 1,000 such systems, 982 will be expected to fail by time  $t$ .



---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

Remember for the case of component replacement upon failure,

$$\text{MTBF} = \theta = \frac{1}{\lambda}, \text{ and, } R = e^{-t/\text{MTBF}}$$

The reader should keep in mind that, for the exponential distribution, the probability of surviving one MTBF without failure is

$$R = e^{-1} = 0.368 \text{ or } 37\%$$

#### 5.4.2.2 Parallel Configuration

The next most commonly occurring configuration encountered in reliability mathematical modeling is the parallel configuration as shown in the reliability block diagram of Figure 5.4-4.

For this case, assuming all the components are operating “on-line,” for the system to fail, all of the components would have to fail. Letting  $Q_i = 1 - R_i = 1 - e^{-\lambda_i t}$ , the probability of failure (or unreliability) of each component, the unreliability of the system would be given by

$$Q_S = Q_1 \cdot Q_2 \cdot \dots \cdot Q_n = \prod_{i=1}^n Q_i \quad (5.61)$$

And the reliability of the system would be

$$R_S = 1 - Q_S \quad (5.62)$$

since  $R + Q = 1$

Consider such a system composed of five parallel components, each with a reliability of 0.99. Then

$$Q_i = 1 - R_i = 1 - 0.99 = 0.01$$

$$Q_S = (0.01)^5 = 10^{-10} = 0.0000000001$$

$$R_S = 1 - Q_S = 0.9999999999$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

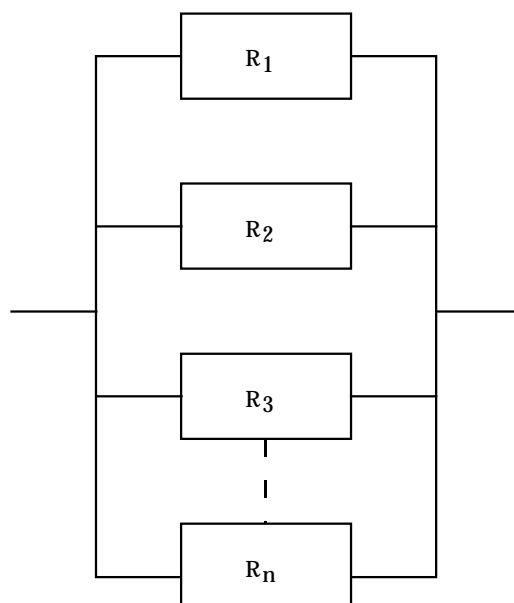


FIGURE 5.4-4: PARALLEL CONFIGURATION

Thus, parallel configurations, or the use of redundancy, is one of the design procedures used to achieve extremely high system reliability, greater than the individual component reliabilities. Of course, this is a very simple concept, which becomes more complicated in actual practice. Redundant equipment can be active (“on-line”) or turned off (“standby”), some redundant units can be repaired without shutting down the system, others can not, and the number of repair crews can vary. All these factors must be considered in formulating appropriate reliability models. Redundancy design techniques will be described in more detail in Section 7.

Most practical equipments and systems are combinations of series and parallel components as shown in Figure 5.4-5.

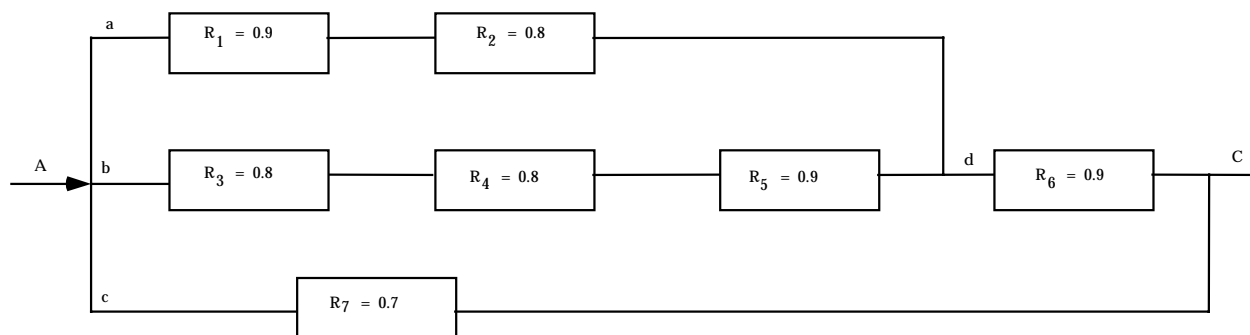


FIGURE 5.4-5: COMBINED CONFIGURATION NETWORK

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

To solve this network, one merely uses the previously given series and parallel relationships to decompose and recombine the network step by step. For example,

$$R_{ad} = R_1 \cdot R_2 = (0.9)(0.8) = 0.72$$

$$R_{bd} = R_3 \cdot R_4 \cdot R_5 = (0.8)(0.8)(0.9) = 0.576$$

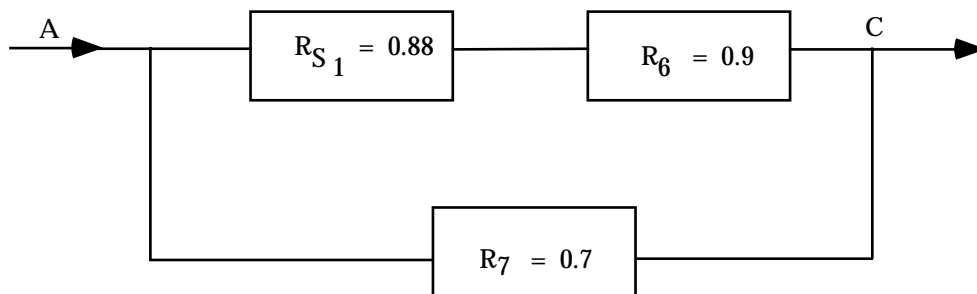
but  $R_{ad}$  and  $R_{bd}$  are in parallel; thus, the unreliability of this parallel subsystem ( $S_1$ ) is

$$\begin{aligned} Q_{S_1} &= Q_{ad} \cdot Q_{bd} = (1 - R_{ad}) \cdot (1 - R_{bd}) \\ &= (1 - 0.72)(1 - 0.576) = (0.28)(0.424) = 0.119 \end{aligned}$$

and its reliability is

$$R_{S_1} = 1 - Q_{S_1} = 1 - 0.119 = 0.88$$

Now the network has been decomposed to



Letting  $R_{S_2}$  equal the combined reliability of  $R_{S_1}$  and  $R_6$  in series

$$R_{S_2} = R_{S_1} \cdot R_6 = (0.88)(0.9) = 0.792$$

$$Q_{S_2} = 1 - R_{S_2} = 1 - 0.792 = 0.208$$

$$Q_7 = 1 - R_7 = 1 - 0.7 = 0.3$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

Since  $Q_{S_2}$  and  $Q_7$  are in parallel, the total system unreliability is

$$Q_{AC} = Q_{S_2} \cdot Q_7 = (0.208)(0.3) = 0.06$$

and the total network reliability is

$$R_{AC} = 1 - Q_{AC} = 1 - 0.06 = 0.94$$

thus, the reliability of the combined network is 0.94.

As the system network increases in complexity, the mathematics of system analysis becomes more laborious and are best handled by computerized techniques.

#### 5.4.2.3 K-Out-Of-N Configuration

A system consisting of  $n$  components or subsystems, of which only  $k$  need to be functioning for system success, is called a  $k$ -out-of- $n$  configuration. For such a system,  $k$  is less than  $n$ . An example of such a system might be an air traffic control system with  $n$  displays of which  $k$  must operate to meet the system reliability requirement.

For the sake of simplicity, let us assume that the units are identical, they are all operating simultaneously, and failures are statistically independent.

Then,

$$\begin{aligned} R &= \text{reliability of one unit for a specified time period} \\ Q &= \text{unreliability of one unit for a specified time period} \end{aligned}$$

$$\text{and } R + Q = 1$$

For  $n$  units

$$(R + Q)^n = 1$$

$$\begin{aligned} (R + Q)^n &= R^n + nR^{n-1}Q + \frac{n(n-1)}{2!}R^{n-2}Q^2 + \frac{n(n-1)(n-2)R^{n-3}Q^3}{3!} \\ &+ \dots + Q^n = 1 \end{aligned}$$

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

This is nothing more than the binomial expansion of  $(R + Q)^n$

Thus,

$$P [\text{at least } (n-1) \text{ surviving}] = R^n + nR^{n-1} Q$$

$$P [\text{at least } (n-2) \text{ surviving}] = R^n + nR^{n-1} Q + \frac{n(n-1)R^{n-2}Q^2}{2!}$$

$$P [\text{at least 1 surviving}] = 1 - Q^n$$

Let us look at the specific case of four display equipments which meet the previously mentioned assumptions.

$$(R + Q)^4 = R^4 + 4R^3 Q + 6R^2 Q^2 + 4RQ^3 + Q^4 = 1$$

from which

$$R^4 = P(\text{all four will survive})$$

$$4R^3 Q = P(\text{exactly 3 will survive})$$

$$6R^2 Q^2 = P(\text{exactly 2 will survive})$$

$$4RQ^3 = P(\text{exactly 1 will survive})$$

$$Q^4 = P(\text{all will fail})$$

We are usually interested in k out of n surviving.

$$R^4 + 4R^3 Q = 1 - 6R^2 Q^2 - 4RQ^3 - Q^4 = P(\text{at least 3 survive})$$

$$R^4 + 4R^3 Q + 6R^2 Q^2 = 1 - 4RQ^3 - Q^4 = P(\text{at least 2 survive})$$

$$R^4 + 4R^3 Q + 6R^2 Q^2 + 4RQ^3 = 1 - Q^4 = P(\text{at least 1 survives})$$

If the reliability of each display for some time t is 0.9, what is the system reliability for time t if 3 out of 4 displays must be working?

$$R_S = R^4 + 4R^3 Q = (0.9)^4 + 4(0.9)^3(0.1) = 0.6561 + 0.2916 = 0.9477$$

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

A similar example would be the case of launching 4 missiles, each of which had a probability of 0.9 of successfully hitting its target. What is the probability that at least 3 missiles will be on target? The procedure and result would be the same as the previous example.

For the case where all units have different reliabilities (or probabilities of success) the analysis becomes more difficult for the same assumptions. Let us look at the case of three units with reliabilities of  $R_1$ ,  $R_2$ , and  $R_3$ , respectively. Then,

$$(R_1 + Q_1)(R_2 + Q_2)(R_3 + Q_3) = 1 \quad (5.63)$$

The above equation can be expanded to permit analysis as was done for the previous case of equal reliabilities. An easy way of bookkeeping is to set up Boolean truth tables where  $R_i = 1$ ,  $Q_i = 0$ , as follows:

1	2	3		
0	0	0	$Q_1 Q_2 Q_3$	= all three fail
0	0	1	$Q_1 Q_2 R_3$	= 1 & 2 fail, 3 survives
0	1	0	$Q_1 R_2 Q_3$	= 1 & 3 fail, 2 survives
0	1	1	$Q_1 R_2 R_3$	= 1 fails, 2 & 3 survive
1	0	0	$R_1 Q_2 Q_3$	= 2 & 3 fail, 1 survives
1	0	1	$R_1 Q_2 R_3$	= 2 fails, 1 & 3 survive
1	1	0	$R_1 R_2 Q_3$	= 3 fails, 1 & 2 survive
1	1	1	$R_1 R_2 R_3$	= all three survive

For the previous example, if we are not interested in which particular unit fails, we can set up expressions for at least 1, 2 or 3 units surviving. For example,

$$P(\text{at least 2 units surviving}) = R_1 R_2 R_3 + R_1 R_2 Q_3 + R_1 Q_2 R_3 + Q_1 R_2 R_3$$

The simple combinational reliability models developed in this section were, primarily, for illustrative purposes to demonstrate the basic theory involved. More complex examples are addressed in the references at the end of this section and in Section 7.

### 5.5 Bayesian Statistics in Reliability Analysis

Bayesian statistics have been increasingly used in reliability analysis. The advantage to the use of Bayesian statistics is that it allows prior information (e.g., predictions, test results, engineering judgment) to be combined with more recent information, such as test or field data, in order to arrive at a prediction/assessment of reliability based upon a combination of all available data. It also permits the reliability prediction/assessment to be continually updated as more and more test

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

data are accumulated. The Bayesian approach is intuitively appealing to design engineers because it permits them to use engineering judgment, based upon prior experience with similar equipment designs, to arrive at an initial estimate of the reliability of a new design. It is particularly useful for assessing the reliability of new systems where only limited field data exists. For example, it can be argued that the result of a reliability test is not only information available on a product, but that information which is available prior to the start of the test, from component and subassembly tests, previous tests on the product, and even intuition based upon experience. Why should this information not be used to supplement the formal test result? Bayes' Theorem can be used to combine these results.

Thus, the basic difference between Bayesian and non-Bayesian (classical) approaches is that the former uses both current and prior data, whereas the latter uses current data only.

One of the main disadvantages to the use of the Bayesian approach is that one must be extremely careful in choosing the prior probabilities based upon part experience or judgment. If these are capriciously or arbitrarily chosen for Bayesian analysis, the end results of Bayesian analysis may be inaccurate and misleading. Thus, the key to the successful use of the Bayesian method resides in the appropriate choice of prior probability distributions. An objective prior such as existing test data is much better than a subjective prior based on opinion.

Bayes' analysis begins by assigning an initial reliability on the basis of whatever evidence is currently available. The initial prediction may be based solely on engineering judgment or it may be based on data from other similar types of items. Then, when additional test data is subsequently obtained, the initial reliabilities are revised on the basis of this data by means of Bayes' Theorem. The initial reliabilities are known as prior reliabilities in that they are assigned before the acquisition of the additional data. The reliabilities which result from the revision process are known as posterior reliabilities.

### 5.5.1 Bayes' Theorem

From basic probability theory, Bayes' Theorem is given by

$$\Pr [A|B] = \Pr [A] \frac{\Pr [B|A]}{\Pr [B]} \quad (5.64)$$

In the specific framework and context of reliability, the various terms in the equation may be motivated and defined as follows:

- |   |  |
|---|--|
| A | An hypothesis or statement of belief. (“The reliability of this component is 0.90.”)   |
| B | A piece of evidence, such as a reliability test result that has bearing upon the truth or credibility of the hypothesis. (“The component |

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

failed on a single mission trial.”)

- Pr [A]      The prior probability: the probability we assign to the hypothesis A before evidence B becomes available. (“We believe, based on engineering experience, that there is a 50-50 chance that the reliability of this component is about 0.90, as opposed to some-thing drastically lower, e.g., Pr [A] = 0.5.”)
- Pr [B|A]    The likelihood: the probability of the evidence assuming the truth of the hypothesis. (“The probability of the observed failure, given that the true component reliability is indeed 0.90, is obviously 0.10.”)
- Pr [B]      The probability of the evidence B, evaluated over the entire weighted ensemble of hypotheses  $A_i$
- Pr [A|B]    The posterior probability of A, given the evidence B

The posterior probability is the end result of the application of Bayes' Equation. The following examples illustrate the use of Bayesian statistics in reliability analysis.

#### 5.5.1.1 Bayes' Example (Discrete Distribution)

To demonstrate the use of Bayes' Equation within the framework of the binomial estimation of reliability, consider the following simplistic (but illustrative) example.

We wish to estimate the reliability of a simple pyrotechnic device which, upon being tested, either fires (success) or doesn't fire (failure). We have in the warehouse two lots of this component, one of which we have been assured has a reliability of  $R = 0.9$  (that is, in the long term, 9 of 10 randomly selected components will work). The other lot supposedly contains only 50% good items. Unfortunately, we have lost the identity of which lot is which.

After randomly selecting one of the lots (such that the probability for each lot is 0.50), we then randomly select a single item from it (each item has equal chance of being chosen), which fails in test. What can be said about all this in the context of Bayesian analysis?

First, terms must be defined (see Figure 5.5-1).

- $A_1$       “Lot chosen has  $R = 0.50$ ”
- $A_2$       “Lot chosen has  $R = 0.90$ ”



## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

Then, from above,

$$\Pr [A_1] = 0.5, \quad \Pr [A_2] = 0.5.$$

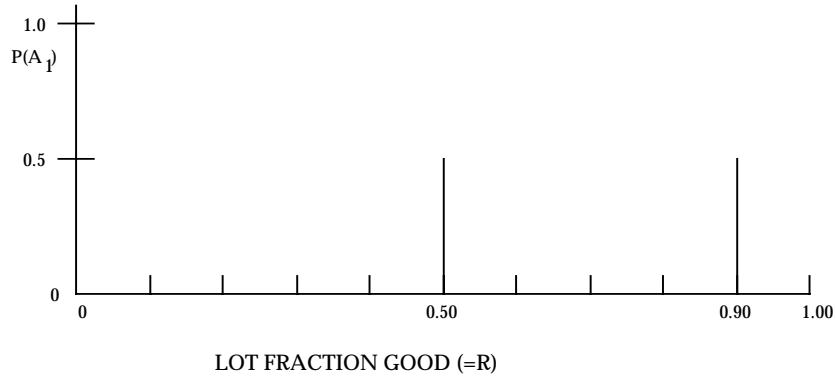


FIGURE 5.5-1: SIMPLE PRIOR DISTRIBUTION

Next, the test evidence must be considered. Therefore

B “One unit was tested and it failed.”

The likelihoods required for Bayes' Equation are obviously

$$\Pr[B|A_1] = \Pr[\text{single test failure}|R = 0.5] = (1 - 0.5) = 0.5$$

$$\Pr[B|A_2] = \Pr[\text{single test failure}|R = 0.9] = (1 - 0.9) = 0.1$$

If A is partitioned into a set of states  $[A_1, \dots, A_n]$  and if  $\Pr[A_i]$  and  $\Pr[B|A_i]$  are known for each i; then Eq. (5.64) becomes

$$\Pr[A_i | B] = \Pr[A_i] \frac{\Pr[B | A_i]}{\sum \Pr[B | A_j] \cdot \Pr[A_j]} = \Pr[A_i] \frac{\Pr[B|A_i]}{\Pr[B]}$$

where the sum is over all n values of i. For this example, we have

$$\Pr[B] = \Pr[B|A_1] \Pr[A_1] + \Pr[B|A_2] \Pr[A_2] = 0.5(0.5) + 0.1(0.5) = 0.30.$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

Finally, all necessary inputs having been obtained, Bayes' Equation now yields

$$\Pr[A_1|B] = \frac{\Pr[A_1] \Pr[B|A_1]}{\Pr[B]} = \frac{0.5(0.5)}{0.30} = 0.833,$$

$$\Pr[A_2|B] = \frac{\Pr[A_2] \Pr[B|A_2]}{\Pr[B]} = \frac{0.5(0.1)}{0.30} = 0.167$$

The prior distribution in Figure 5.5-1 has been transformed, under the impact of a single trial resulting in failure, to the posterior distribution shown in Figure 5.5-2. The analyst may already be somewhat dubious that he has picked the lot with  $R = 0.9$ .

The process is usually a sequential one, i.e., as successive packets of new information ( $B_1, B_2, B_3, \dots$ ) become available, the posterior degree of belief in proposition  $A_i$  is successively modified by each new increment of information.

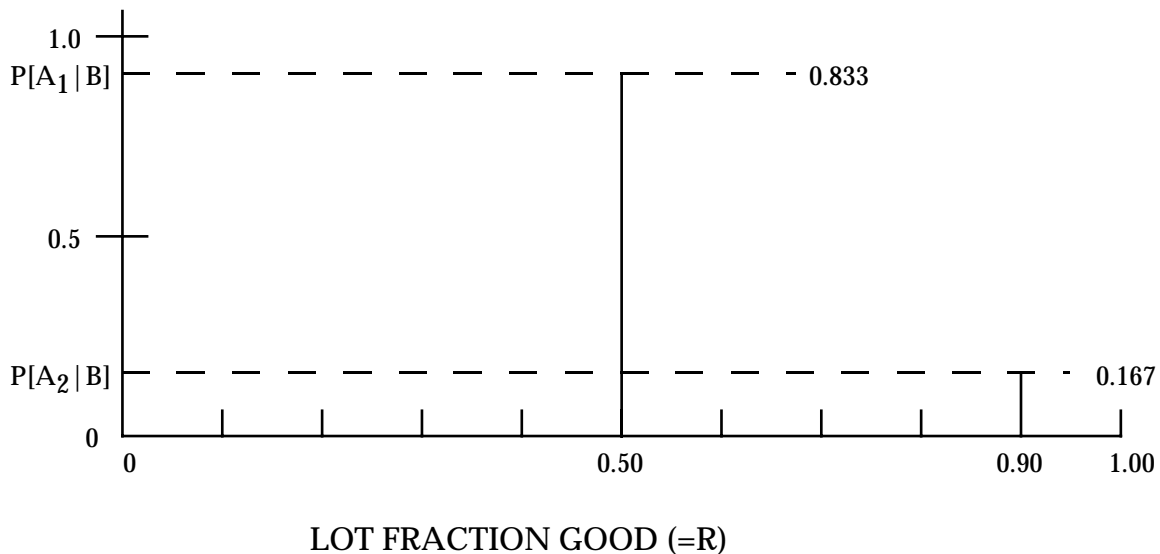


FIGURE 5.5-2: SIMPLE POSTERIOR DISTRIBUTION

Another way of visualizing this situation is by constructing a tree diagram like the one shown in Figure 5.5-3, where the probability of the final outcome "B" is given by the products of the probabilities corresponding to each individual branch.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

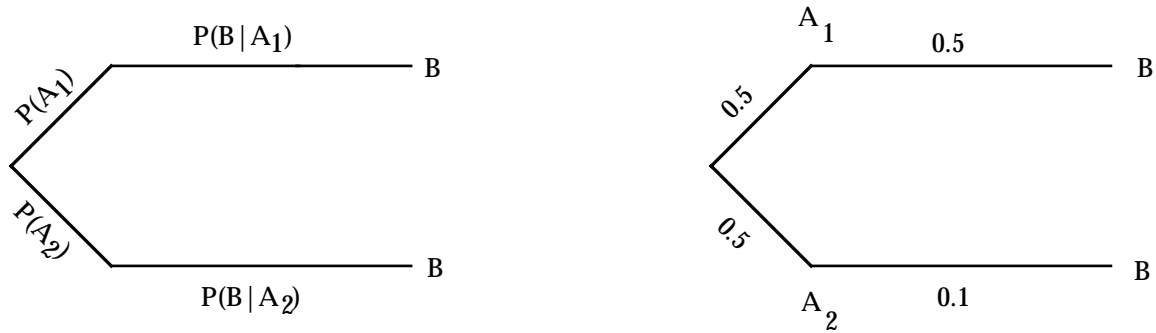


FIGURE 5.5-3: TREE DIAGRAM EXAMPLE

$$P[B] = (0.5)(0.5) + (0.5)(0.1) = 0.3$$

$$P[A_1|B] = \frac{P[A_1]P[B|A_1]}{P[B]} = \frac{(0.5)(0.5)}{(0.3)} = 0.8333$$

$$P[A_2|B] = \frac{P[A_2]P[B|A_2]}{P[B]} = \frac{(0.5)(0.1)}{(0.3)} = 0.167$$

5.5.1.2 Bayes' Example (Continuous Distribution)

As with the discrete example, the basic equation can be extended to cover continuous probability distributions. For example, assume that based upon prior test results, engineering judgment, etc. it has been observed that  $r$  failures occur in time  $t$ . The probability density function of  $t$  is a gamma distribution given by

$$f(\lambda) = \frac{(t)\lambda^{r-1}e^{-\lambda t}}{\Gamma(r)} \quad (5.65)$$

where:

$t$  is the amount of testing time (scale parameter)

$r$  is the number of failures (shape parameter)

From Section 5.3.5, we know that (note changes in notation)

$$\hat{\mu}_0 \text{ (mean failure rate)} = \frac{\text{shape parameter}}{\text{scale parameter}} = \frac{r}{t} \quad (5.66)$$

and

$$\hat{\sigma}_0^2 = \frac{r}{t^2} \quad (5.67)$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

Eqs. (5.64 and 5.65) represent the prior failure rate and the prior variance. Let us assume that these are given by 0.02 and  $(0.01)^2$ , respectively. Assume that we then run a reliability test for 500 hours ( $t'$ ) and observe 14 failures ( $r'$ ). What is the posterior estimate of failure rate?

The basic expression for the continuous posterior distribution is given by

$$f(\lambda|t) = \frac{f(\lambda) f(t|\lambda)}{f(t)} \quad (5.68)$$

where:

$f(\lambda)$  is the prior distribution of  $\lambda$ , Eq. (5.65)

$f(t|\lambda)$  is the sampling distribution of  $t$  based upon the new data

$$f(t) \text{ is } \int_0^{\infty} f(\lambda) f(t|\lambda) d\lambda$$

$f(\lambda|t)$  is the posterior distribution of combining the prior distribution and the new data.

It can be shown that the posterior distribution resulting from performing the operations indicated in Eq. (5.68) is

$$f(\lambda|t) = \frac{(t + t')\lambda^{r+r'-1} \exp[-\lambda(t + t')]}{\Gamma(r + r')} \quad (5.69)$$

which is another gamma distribution with

shape parameter =  $(r + r')$

scale parameter =  $(t + t')$

Using Eqs. (5.66) and (5.67) to solve for  $r$  and  $t$ , we obtain

$$r = \hat{\mu}_0 t = \hat{\sigma}_0^2 t^2$$

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

Therefore,

$$t = \frac{\hat{\mu}_0}{\hat{\sigma}_0^2} = \frac{0.02}{(0.01)^2} = \frac{2 \times 10^{-2}}{1 \times 10^{-4}} = 200$$

$$r = \hat{\mu}_0 t = (2 \times 10^{-2}) (200) = 4$$

Returning to the posterior gamma distribution, Eq. (5.69) we know that the posterior failure rate is

$$\hat{\mu}_1 = \frac{\text{shape parameter}}{\text{scale parameter}} = \frac{(r+r')}{(t+t')}$$

From the test data  $r' = 14$ ,  $t' = 500$ , and we found that  $r = 4$ , and  $t = 200$ ; thus

$$\hat{\mu}_1 = \frac{4 + 14}{200 + 500} = \frac{18}{700} = 0.0257$$

This compares with the traditional estimate of failure rate from the test result,  $14/500 = 0.028$ . Thus, the use of prior information resulted in a failure rate estimate lower than that given by the test results.

### 5.6 Maintainability Theory

In reliability, one is concerned with designing an item to last as long as possible without failure; in maintainability, the emphasis is on designing an item so that a failure can be repaired as quickly as possible. The combination of high reliability and high maintainability results in high system availability; the theory of which is developed in Section 5.7.

Maintainability, then, is a measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure. It is a function of the equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed.

As with reliability, maintainability parameters are also probabilistic and are analyzed by the use of continuous and discrete random variables, probabilistic parameters, and statistical distributions. An example of a discrete maintainability parameter is the number of maintenance actions completed in some time  $t$ , whereas an example of a continuous maintainability parameter is the time to complete a maintenance action.

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**

---

**5.6.1 Basic Concepts**

A good way to look at basic maintainability concepts is in terms of functions which are analogous to those in reliability. They may be derived in a way identical to that done for reliability in the previous section by merely substituting  $t$  (time-to-restore) for  $t$  (time-to-failure),  $\mu$  (repair rate) for  $\lambda$  (failure rate), and  $M(t)$  (probability of successfully completing a repair action in time  $t$ , or  $P(T \leq t)$ ) for  $F(t)$  (probability of failing by age  $t$ , or  $P(T \leq t)$ ). In other words, the following correspondences prevail in maintainability and reliability engineering functions.

- (1) The time-to-failure probability density function (pdf) in reliability corresponds to the time-to-maintain pdf in maintainability.
- (2) The failure rate function in reliability corresponds to the repair rate function in maintainability. Repair rate is the rate with which a repair action is performed and is expressed in terms of the number of repair actions performed and successfully completed per hour.
- (3) The probability of system failure, or system unreliability, corresponds to the probability of successful system maintenance, or system maintainability. These and other analogous functions are summarized in Table 5.6-1.

Thus, as illustrated in Figure 5.6-1, maintainability can be expressed either as a measure of the time ( $T$ ) required to repair a given percentage ( $P\%$ ) of all system failures, or as a probability ( $P$ ) of restoring the system to operational status within a period of time ( $T$ ) following a failure.

Some of the commonly used maintainability engineering terms are portrayed graphically in Figure 5.6-2 as a maintainability “function” derived as illustrated for the case where the pdf has a lognormal distribution. Points (1), (2), and (3) shown in the figure identify the mean, median, and maximum corrective time-to-repair, respectively.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.6-1: COMPARISON OF BASIC RELIABILITY AND MAINTAINABILITY FUNCTIONS

RELIABILITY	MAINTAINABILITY
<u>Time to Failure (pdf)</u> $f(t)$	<u>Time to Repair (pdf)</u> $g(t)$ (5.70)
<u>Reliability</u> $R(t) = \int_t^{\infty} f(t) dt$	<u>Maintainability</u> $M(t) = \int_0^t g(t) dt$ (5.71)
<u>Failure Rate</u> $\lambda(t) = \frac{f(t)}{R(t)}$	<u>Repair Rate</u> $\mu(t) = \frac{g(t)}{1 - M(t)}$ (5.72)
<u>Mean-Time-to-Failure</u> $\begin{aligned} \text{MTTF} &= \int_{-\infty}^{\infty} t f(t) dt \\ &= \int_0^{\infty} R(t) dt \end{aligned}$	<u>Mean Time to Repair</u> $\text{MTTR} = \int_{-\infty}^{\infty} t g(t) dt$ (5.73)
<u>Pdf of Time to Failure</u> $\begin{aligned} f(t) &= \lambda(t) \cdot R(t) \\ &= \lambda(t) \exp \left[ -\int_0^t \lambda(t) dt \right] \end{aligned}$	<u>Pdf of Time to Repair</u> $\begin{aligned} g(t) &= \mu(t) (1 - M(t)) \\ &= \mu(t) \exp \left[ -\int_0^t \mu(t) dt \right] \end{aligned}$ (5.74)

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

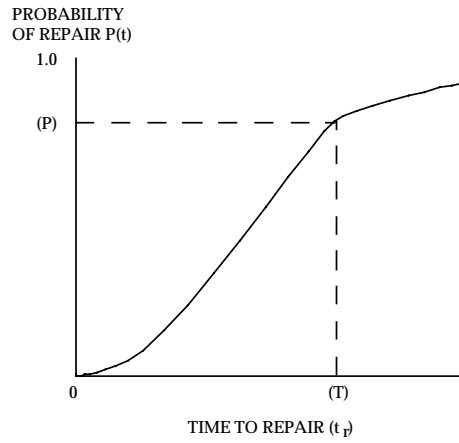


FIGURE 5.6-1: BASIC METHODS OF MAINTAINABILITY MEASUREMENT

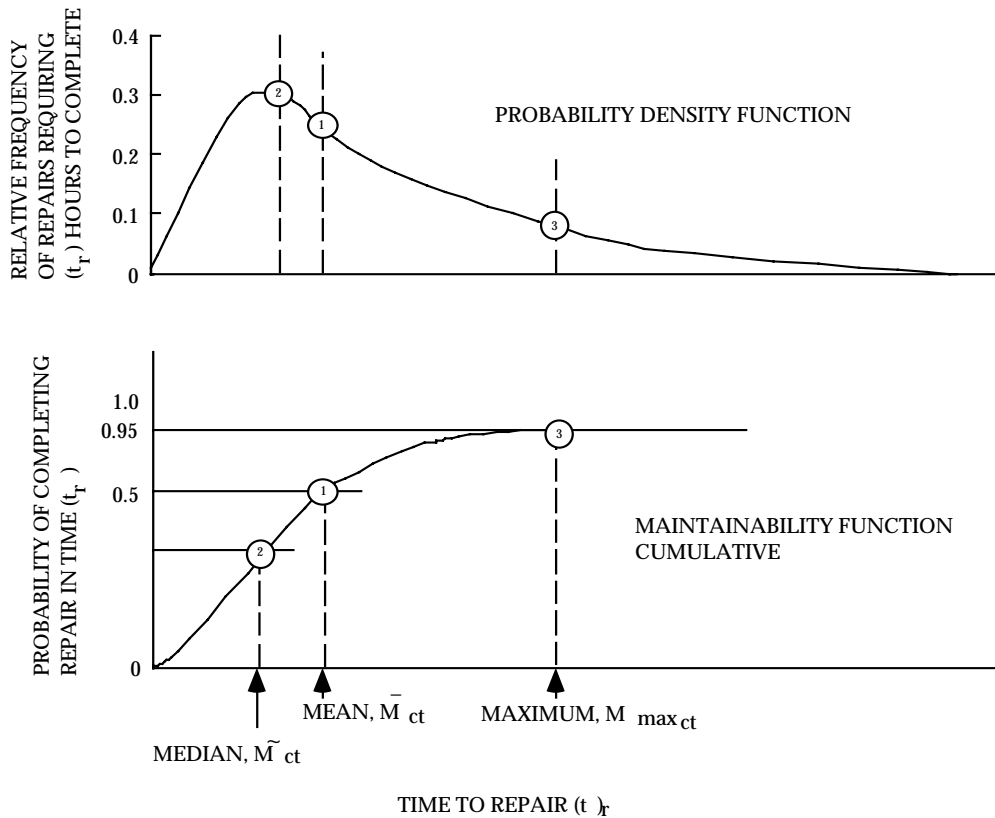


FIGURE 5.6-2: EXAMPLE MAINTAINABILITY FUNCTION DERIVED FROM TIME-TO-REPAIR DISTRIBUTION



---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

Points (1), (2), and (3) are defined as follows:

- (1) Mean Time to Repair,  $\overline{M}_{ct}$  : The mean time required to complete a maintenance action, i.e., total maintenance downtime divided by total maintenance actions for a given period of time, given as

$$\overline{M}_{ct} = \frac{\sum(\lambda_i \overline{M}_{ct_i})}{\sum\lambda_i} \quad (5.75)$$

where:  $\lambda_i$  = failure rate for the  $i^{\text{th}}$  repairable element of the item for which maintainability is to be determined, adjusted for duty cycle, catastrophic failures, tolerance and inter-action failures, etc., which will result in deterioration of item performance to the point that a maintenance action will be initiated.

$\overline{M}_{ct_i}$  = average corrective time required to repair the  $i^{\text{th}}$  repairable element in the event of its failure.

- (2) Median Time to Repair,  $\tilde{M}_{ct}$  : The downtime within which 50% of all maintenance actions can be completed.
- (3) Maximum Time to Repair: The maximum time required to complete a specified, e.g., 95%, percentage of all maintenance actions.

These terms will be described in more detail in the following sections, in terms of the form that they take, given the statistical distribution of time-to-repair.

### 5.6.2 Statistical Distributions Used in Maintainability Models

A smaller number of statistical distributions is used for maintainability analysis than for reliability analysis. This may be due to the fact that maintainability has traditionally lagged reliability theory in development.

The most commonly used distributions for maintainability analysis have been the normal, lognormal, and exponential. Just as the exponential distribution has been the one most widely used in reliability analysis of equipment/systems, the lognormal distribution is the most commonly used for equipment/system maintainability analysis. A number of studies have validated the lognormal as being the most appropriate for maintainability analysis (Ref. [25]).

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

However, use of other distributions such as the Weibull and gamma is also possible, depending upon the analysis of the data and the use of “goodness of fit” tests.

Since the form and expressions for the more commonly used distributions were previously given in Section 5.2.2, this section will concentrate on the use of the normal, exponential, and lognormal distribution, and give examples of their use in maintainability analysis.

### 5.6.2.1 Lognormal Distribution

This is the most commonly used distribution in maintainability analysis. It applies to most maintenance tasks and repair actions comprised of several subsidiary tasks of unequal frequency and time duration.

The probability density function is given by

$$g(t = M_{ct_i}) = \frac{1}{M_{ct_i} S_{ln M_{ct}} \sqrt{2\pi}} \exp \left[ -\frac{1}{2} \left( \frac{\ln M_{ct_i} - \overline{\ln M_{ct}}}{S_{ln M_{ct}}} \right)^2 \right] \quad (5.76)$$

$$= \frac{1}{t \sigma_{t'} \sqrt{2\pi}} \exp \left[ -\frac{1}{2} \left( \frac{t' - \overline{t'}}{\sigma_{t'}} \right)^2 \right] \quad (5.77)$$

where:

$t = M_{ct_i}$  = repair time from each failure

$$\overline{\ln M_{ct}} = \frac{\sum \ln M_{ct_i}}{N}$$

$$S_{ln M_{ct}} = \sigma_{t'} = \sqrt{\frac{\sum (\ln M_{ct_i})^2 - (\sum \ln M_{ct_i})^2 / N}{N-1}} \quad (5.78)$$

$$S_{ln M_{ct}} = \sqrt{\frac{\sum t_i'^2 - (\sum t_i')^2 / N}{N-1}} = \text{standard deviation of } \ln \text{ of repair times.}$$

$$t' = \ln M_{ct_i} = \ln t$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

$$\bar{t}' = \overline{\ln M_{ct}} = \frac{\sum t_i'}{N}$$

$$N = \text{number of repair actions} \quad (5.79)$$

The mean time to repair is given by

$$MTTR = \overline{M_{ct}} = \bar{t} = \int_0^{\infty} t g(t = M_{ct_i}) dt \quad (5.80)$$

(also see Eq. (5.76))

$$= \exp \left[ \overline{\ln M_{ct}} + \frac{1}{2} (S_{\ln M_{ct}})^2 \right] \quad (5.81)$$

$$= \exp \left[ \bar{t}' + \frac{1}{2} (\sigma_{t'})^2 \right] \quad (5.82)$$

The median time to repair is given by

$$\tilde{M}_{ct} = \tilde{t} = \text{antiln} \frac{\sum \lambda_i \overline{\ln M_{ct}}}{\sum \lambda_i} \quad (5.83)$$

$$= \exp \left( \overline{\ln M_{ct_i}} \right) \quad (5.84)$$

$$= \exp \left( \bar{t}' \right) \quad (5.85)$$

The maximum time to repair is given by

$$M_{\max_{ct}} = t_{\max} = \text{antiln} \left( \overline{\ln M_{ct}} + \phi S_{\ln M_{ct}} \right) \quad (5.86)$$

$$= \text{antiln} \left[ \bar{t}' + z(t'_{1-\alpha}) \sigma_{t'} \right] \quad (5.87)$$

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

where  $\phi = z(t'_{1-\alpha})$  = value from normal distribution function corresponding to the percentage point  $(1-\alpha)$  on the maintainability function for which  $M_{\max_{ct}}$  is defined.

Most commonly used values of  $\phi$  or  $z(t'_{1-\alpha})$  are shown in Table 5.6-2.

TABLE 5.6-2: VALUES OF  $\phi$  OR  $Z(T'_{(1-\alpha)})$  MOST COMMONLY USED IN MAINTAINABILITY ANALYSIS

$1-\alpha$	$\phi$ or $Z(t'_{(1-\alpha)})$
0.80	0.8416
0.85	1.036
0.90	1.282
0.95	1.645
0.99	2.326

Following is an example of maintainability analysis of a system which has a lognormal distribution of repair times.

#### 5.6.2.1.1 Ground Electronic System Maintainability Analysis Example

Given the active repair times data of Table 5.6-3 on a ground electronic system find the following:

- (1) The probability density function,  $g(t)$
- (2) The MTTR of the system
- (3) The median time to repair the system
- (4) The maintainability function
- (5) The maintainability for a 20 hour mission
- (6) The time within which 90% and 95% of the maintenance actions are completed
- (7) The repair rate,  $u(t)$ , at 20 hours

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.6-3: TIME-TO-REPAIR DATA ON A GROUND ELECTRONIC SYSTEM

Group No. j	Times to Repair $t_j$ (hr.)	Frequency of Observation $n_j$
1	0.2	1
2	0.3	1
3	0.5	4
4	0.6	2
5	0.7	3
6	0.8	2
7	1.0	4
8	1.1	1
9	1.3	1
10	1.5	4
11	2.0	2
12	2.2	1
13	2.5	1
14	2.7	1
15	3.0	2
16	3.3	2
17	4.0	2
18	4.5	1
19	4.7	1
20	5.0	1
21	5.4	1
22	5.5	1
23	7.0	1
24	7.5	1
25	8.8	1
26	9.0	1
27	10.3	1
28	22.0	1
$N' = 29$	24.5	1

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

1. Probability Density Function of  $g(t)$ 

To determine the lognormal pdf of the times-to-repair given in Table 5.6-3, the values of  $\bar{t}'$  and  $\sigma_{t'}$  should be calculated from

$$\bar{t}' = \frac{\sum_{j=1}^{N'} n_j t'_j}{\sum_{j=1}^{N'} n_j} \quad (5.88)$$

where  $n_j$  is the number of identical observations given in the third column of Table 5.6-3,  $N'$  is the number of different-in-value observed times-to-repair, or number of data groups, which for this problem is  $N' = 29$ , given in the second column of Table 5.6-3, and  $N$  is the total number of observed times-to-repair,

$$N = \sum_{i=1}^{N'} n_i$$

which, for this example, is 46,

and

$$\sigma_{t'} = \left[ \frac{\sum_{i=1}^N (t'_i)^2 - N(\bar{t}')^2}{N-1} \right]^{\frac{1}{2}} = \left[ \frac{\sum_{j=1}^{N'} n_j (t'_j)^2 - N(\bar{t}')^2}{N-1} \right]^{\frac{1}{2}} \quad (5.89)$$

To facilitate the calculations, Table 5.6-4 was prepared. From Table 5.6-4,  $\bar{t}'$  and  $\sigma_{t'}$ , are obtained as follows:

$$\bar{t}' = \frac{\sum_{j=1}^{N'} n_j t'_j}{\sum_{j=1}^{N'} n_j} = \frac{30.330439}{46} = 0.65879$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.6-4: CALCULATIONS TO DETERMINE  $\bar{t}'$  AND  $\sigma_T$   
FOR THE DATA IN TABLE 5.6-3

j	$t_j$	$\ln t_j=t'_j$	$(t'_j)^2$	$n_j$	$n_j t'_j$	$n_j (t'_j)^2$
1	0.2	-1.60944	2.59029	1	-1.60944	2.59029
2	0.3	-1.20397	1.44955	1	-1.20397	1.44955
3	0.5	-0.69315	0.48045	4	-2.77260	1.92180
4	0.6	-0.51083	0.26094	2	-1.02166	0.52188
5	0.7	-0.35667	0.12721	3	-1.07001	0.38163
6	0.8	-0.22314	0.04979	2	-0.44628	0.09958
7	1.0	0.00000	0.00000	4	0.00000	0.00000
8	1.1	0.09531	0.00908	1	0.09531	0.00908
9	1.3	0.26236	0.06884	1	0.26236	0.06884
10	1.5	0.40547	0.16440	4	1.62188	0.65760
11	2.0	0.69315	0.48045	2	1.38630	0.96090
12	2.2	0.78846	0.62167	1	0.78846	0.62167
13	2.5	0.91629	0.83959	1	0.91629	0.83959
14	2.7	0.99325	0.98655	1	0.99325	0.98655
15	3.0	1.09861	1.20695	2	2.19722	2.41390
16	3.3	1.19392	1.42545	2	2.38784	2.85090
17	4.0	1.38629	1.92181	2	2.77258	3.84362
18	4.5	1.50408	2.26225	1	1.50408	2.26225
19	4.7	1.54756	2.39495	1	1.54756	2.39495
20	5.0	1.60994	2.59029	1	1.60994	2.59029
21	5.4	1.68640	2.84394	1	1.68640	2.84394
22	5.5	1.70475	2.90617	1	1.70475	2.90617
23	7.0	1.94591	3.78657	1	1.94591	3.78657
24	7.5	2.01490	4.05983	1	2.01490	4.05983
25	8.8	2.17475	4.72955	1	2.17475	4.72955
26	9.0	2.19722	4.82780	1	2.19722	4.82780
27	10.3	2.33214	5.43890	1	2.33214	5.43890
28	22.0	3.09104	9.55454	1	3.09104	9.55454
29	24.5	3.19867	10.23151	1	3.19867	10.23151
Sum				46	30.30439	75.84371
$\sum_{j=1}^{N'=29} n_j = 46 = N$				$\sum_{j=1}^{N'} n_j t'_j = 30.30439$		$\sum_{j=1}^{N'} n_j (t'_j)^2 = 75.84371$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

and from Eq. (5.89)

$$\sigma_{t'} = \left[ \frac{75.84371 - 46(0.65879)^2}{46 - 1} \right]^{\frac{1}{2}} = 1.11435$$

Consequently, the lognormal pdf representing the data in Table 5.6-3 is

$$g(t) = \frac{1}{t s_{\tau_3} \sqrt{2\rho}} \exp \left[ -\frac{1}{2} \left( \frac{t' - \bar{t}'}{\sigma_{t'}} \right)^2 \right]$$

or

$$g(t) = \frac{1}{t(1.11435)\sqrt{2\rho}} \exp \left[ -\frac{1}{2} \left( \frac{t' - 0.65879}{1.11435} \right)^2 \right]$$

where  $t' = \ln t$ . The plot of this pdf is given in Figure 5.6-3 in terms of the straight times in hours. See Table 5.6-5 for the  $g(t)$  values used.

The pdf of the  $\ln t$  or of the  $t'$  is

$$g(t') = \frac{t}{t \sigma_{t'} \sqrt{2\pi}} \exp \left[ -\frac{1}{2} \left( \frac{t' - \bar{t}'}{\sigma_{t'}} \right)^2 \right] = t g(t)$$

or

$$g(t') = \frac{1}{(1.11435)\sqrt{2\pi}} \exp \left[ -\frac{1}{2} \left( \frac{t' - 0.65879}{1.11435} \right)^2 \right]$$

This pdf is that of a normal distribution which is what one should expect since if  $t$  follows a lognormal distribution,  $\ln t$  should be normally distributed. This is shown plotted in Figure 5.6-3, the values of  $g(t')$  were obtained from Table 5.6-5.



SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

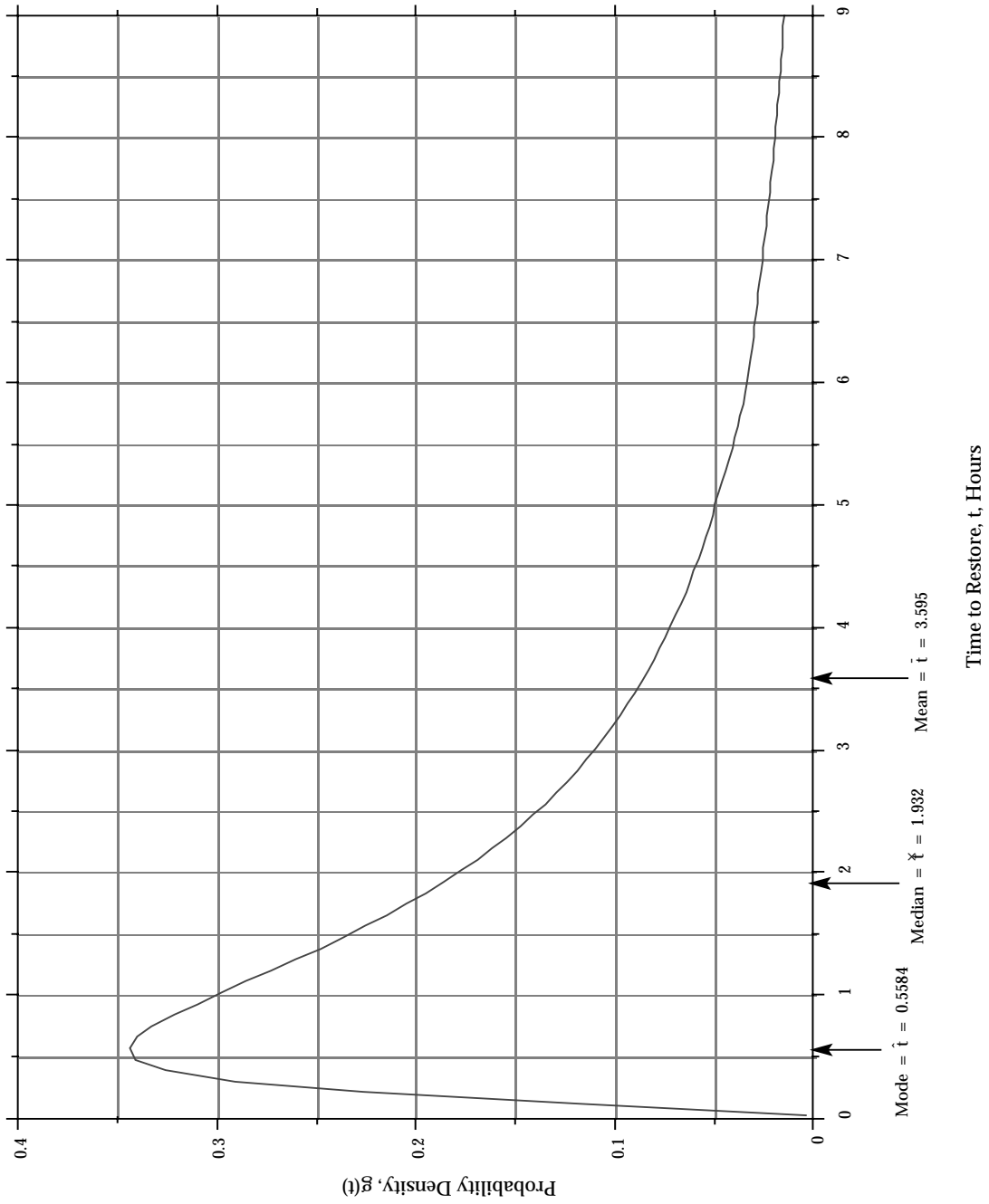


FIGURE 5.6-3: PLOT OF THE LOGNORMAL OF THE TIMES-TO-RESTORE DATA GIVEN IN TABLE 5.6-5 IN TERMS OF THE STRAIGHT  $t$ 's

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.6-5: THE PROBABILITY DENSITY OF TIME-TO-REPAIR DATA  
(FROM TABLE 5.6.2.1.1-1 BASED ON THE STRAIGHT TIMES TO REPAIR AND  
THE NATURAL LOGARITHM OF THE TIMES TO REPAIR USED TO PLOT  
FIGURES 5.6-3 AND 5.6-4, RESPECTIVELY.\*)

Time to restore, t hours	Probability density, g(t)	Probability density g(t') = g(ln t)
0.02	0.00398	7.95 x 10 <sup>-5</sup>
0.1	0.10480	0.01048
0.2	0.22552	0.04510
0.3	0.29510	0.08853
0.5	0.34300	0.17150
0.7	0.33770	0.23636
1.0	0.30060	0.30060
1.4	0.24524	0.34334
1.8	0.19849	0.35728
2.0	0.17892	0.35784
2.4	0.14638	0.35130
3.0	0.11039	0.33118
3.4	0.09260	0.31483
4.0	0.07232	0.28929
4.4	0.06195	0.27258
5.0	0.04976	0.24880
6.0	0.03559	0.21351
7.0	0.02625	0.18373
8.0	0.01985	0.15884
9.0	0.01534	0.13804
10.0	0.01206	0.12061
20.0	0.00199	0.03971
30.0	0.00058	0.01733
40.0	---	0.00888
80.0	---	0.00135

\*At the mode,  $\hat{t} = 0.5584$ ,  $g(\hat{t}) = 0.34470$  and  $g(\hat{t}') = 0.19247$ .

At the median,  $\check{t} = 1.932$ ,  $g(\check{t}) = 0.18530$  and  $g(\check{t}') = 0.35800$ .

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

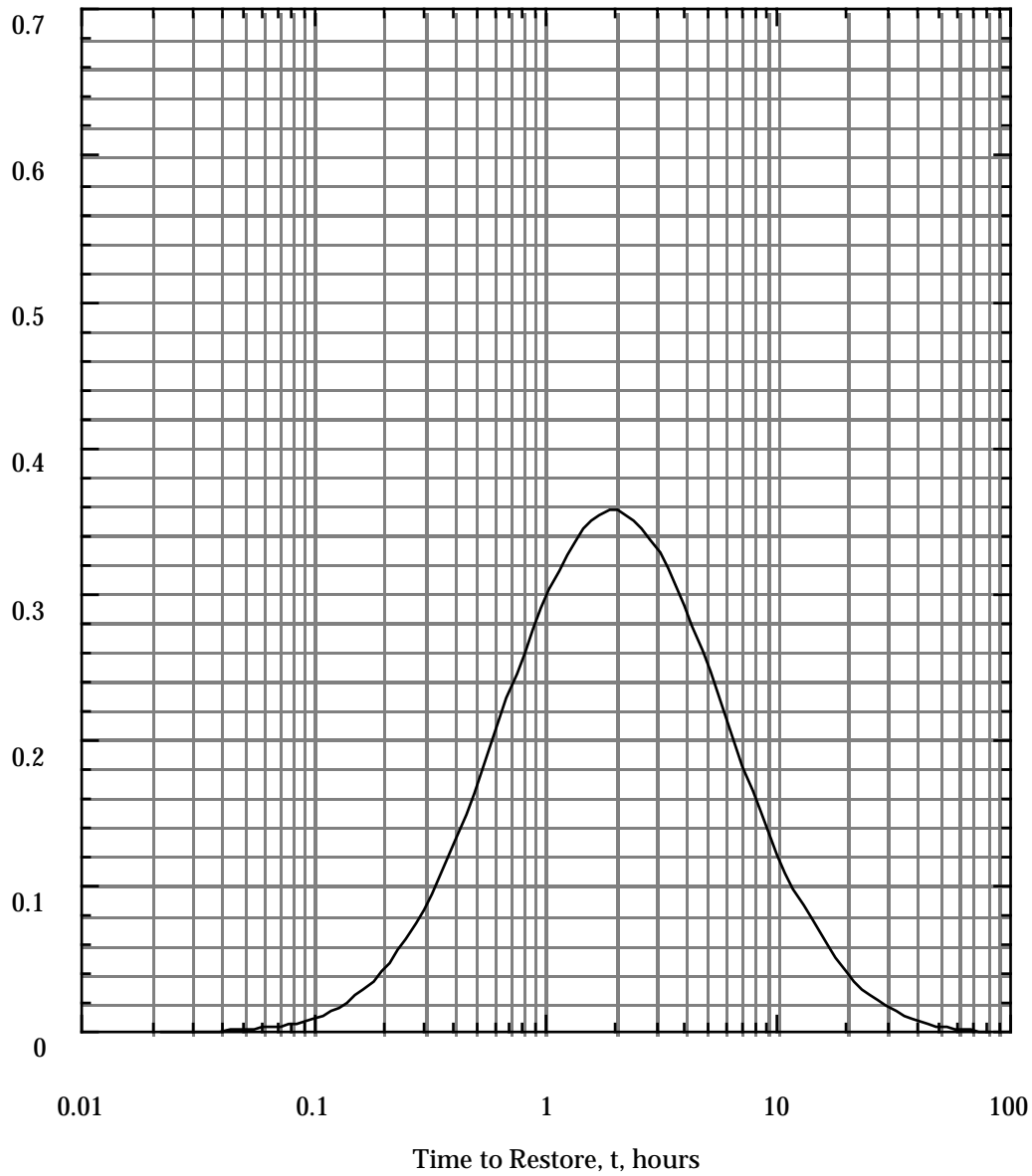


FIGURE 5.6-4: PLOT OF THE LOGNORMAL PDF OF THE TIMES-TO-RESTORE DATA GIVEN IN TABLE 5.6-5 IN TERMS OF THE LOGARITHMS OF T, OR  $\ln t$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

2. MTTR (Mean Time to Repair) of the System

The mean time to repair of the system,  $\bar{t}$ , is obtained from Eq. (5.83).

$$\bar{t} = \exp \left[ t' + \frac{1}{2} (\sigma_{t'})^2 \right] = \exp \left[ 0.65879 + \frac{1}{2} (1.11435)^2 \right] = 3.595 \text{ hr.}$$

3. Median Time to Repair

The median of the times-to-repair the system,  $\check{t}$ , is obtained from Eq. (5.85)

$$\check{t} = \exp(\bar{t}') = e^{0.65879} = 1.932 \text{ hr.}$$

This means that in a large sample of  $t$ 's, half of the  $t$ 's will have values smaller than  $\check{t}$ , and the other half will have values greater than  $\check{t}$ . In other words, 50% of the repair times will be  $\leq \check{t}$ .

4. Maintainability Function M(t)

The maintainability of a unit can be evaluated as follows, using Eq. (5.71):

$$M(t_1) = \int_0^{t_1} g(t) dt = \int_{-\infty}^{t'_1} g(t') dt' = \int_{-\infty}^{z(t'_1)} \phi(z) dz \quad (5.90)$$

$$\text{where } t' = \ln t, \quad (5.90a)$$

$$z(t'_1) = \frac{t'_1 - \bar{t}'}{\sigma_{t'}} \quad (5.90b)$$

and  $\bar{t}'$  and  $\sigma_{t'}$  are given by Eq. (5.88) and (5.91), respectively.

By means of the transformations shown in Eqs. (5.90a) and (5.90b), the lognormal distribution of the pdf of repair times,  $g(t)$ , is transformed to the standard normal distribution  $\phi(z)$  which enables the use of standard normal distribution tables (Table 5.3-3).

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

The maintainability function for the system,  $M(t)$ , from (5.90) is:

$$M(t) = \int_{-\infty}^{z(t')} \phi(z) dz$$

where:

$$z(t') = \frac{t' - \bar{t}'}{\sigma_{t'}}$$

$$t' = \ln t$$

From the data in Table 5.6-3 we previously calculated

$$\bar{t}' = 0.65879$$

$$\sigma_{t'} = 1.11435$$

The quantified  $M(t)$  is shown in Figure 5.6-5. The values were obtained by inserting values for  $t' = \ln t$  into the expression,

$$z(t') = \frac{t' - 0.65879}{1.11435}$$

solving for  $z(t')$ , and reading the value of  $M(t)$  directly from the standard normal tables in Table 5.3-3.

### 5. Maintainability for a 20 Hour Mission

$$M(20) = \int_{-\infty}^{z(\ln 20)} \phi(z) dz$$

where  $\ln 20 = 2.9957$

and

$$z(\ln 20) = \frac{2.9957 - 0.65879}{1.111435} = 2.0972$$

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

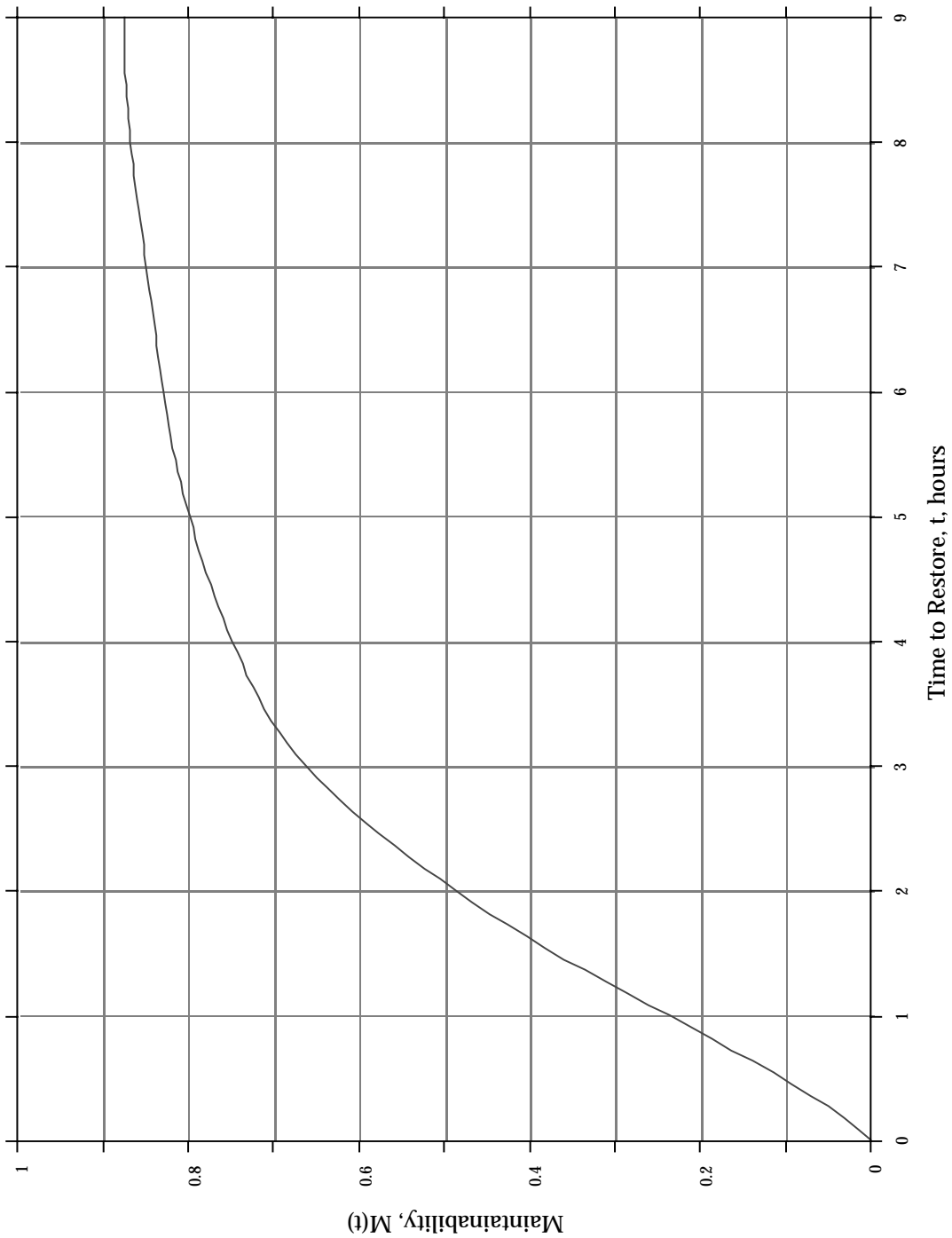


FIGURE 5.6-5: PLOT OF THE MAINTAINABILITY FUNCTION FOR THE TIMES-TO-REPAIR DATA OF EXAMPLE 2

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

From Table 5.3-3 we find that for  $z = 2.0972$

$$M(20) = \int_{-\infty}^{2.0972} \phi(z) dz = 1 - 0.018 = 0.982 \text{ or } 98.2\%$$

6. The time within which 90% and 95% of the Maintenance Actions are Completed ( $M_{\max_{ct}}$ )

This is the time  $t_{1-\alpha}$  for which the maintainability is  $1-\alpha$ , or

$$M(t_{1-\alpha}) = P(t \leq t_{1-\alpha}) = \int_0^{t_{1-\alpha}} g(t) dt = \int_{-\infty}^{t'_{1-\alpha}} g(t') dt' = \int_{-\infty}^{z(t'_{1-\alpha})} \phi(z) dz \quad (5.91)$$

and

$$z(t'_{1-\alpha}) = \frac{t'_{1-\alpha} - \bar{t}'}{\sigma_{t'}} \quad (5.92)$$

The commonly used maintainability, or  $(1-\alpha)$ , values are 0.80, 0.85, 0.90, 0.95, and 0.99. Consequently, the  $z(t'_{1-\alpha})$  values which would be used most commonly would be those previously given in Table 5.6-2. Using Eq. (5.92) the time  $t'_{1-\alpha}$  would then be calculated from

$$t'_{1-\alpha} = \bar{t}' + z(t'_{1-\alpha}) \cdot \sigma_{t'}$$

or

$$t'_{1-\alpha} = \text{antiln}(t'_{1-\alpha}) = \text{antiln} [\bar{t}' + z(t'_{1-\alpha}) \sigma_{t'}] \quad (5.93)$$

Thus, for 90%  $M_{\max_{ct}}$ , from the previously obtained value of  $\bar{t}'$  and  $\sigma_{t'}$

$$\begin{aligned} t_{0.90} &= \text{antiln} [\bar{t}' + z(t'_{0.90}) \sigma_{t'}] = \text{antiln} [0.65879 + 1.282(1.11435)] \\ &= \text{antiln} (2.08737) = 8.06 \text{ hrs.} \end{aligned}$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

For 95%  $M_{\max_{ct}}$

$$t_{0.95} = \text{antiln} \left[ 0.65879 + 1.645(1.11435) \right] = \text{antiln} (2.491896) = 12.08 \text{ hrs.}$$

### 7. Repair Rate at t = 20 hours

Using Eq. (5.60) and substituting the values for  $g(20)$  from Table 5.6-5 and the previously calculated value for  $M(20)$

$$\mu(20) = \frac{g(20)}{1 - M(20)} = \frac{0.00199}{1 - 0.982} = \frac{0.00199}{0.018} = 0.11 \text{ repairs/hr.}$$

#### 5.6.2.2 Normal Distribution

The normal distribution has been adequately treated in Section 5.3.2.1 in the discussion on reliability theory. The same procedures and methodology apply for maintainability if one merely uses repair time for  $t$ , mean repair time for  $\mu$ , and standard deviation of repair times for  $\sigma$ .

In maintainability, the normal distribution applies to relatively straightforward maintenance tasks and repair actions (e.g., simple removal and replacement tasks) which consistently require a fixed amount of time to complete. Maintenance task times of this nature are usually normally distributed, producing a probability density function given by

$$g(t = M_{ct}) = \frac{1}{S_{M_{ct}} \sqrt{2\pi}} \exp \left[ \frac{-(M_{ct_i} - \overline{M}_{ct})^2}{2(S_{M_{ct}})^2} \right] \quad (5.94)$$

where:

$M_{ct_i}$  = repair time for an individual maintenance action

$\overline{M}_{ct} = \frac{\Sigma(M_{ct_i})}{N}$  = average repair time for N observations

$S_{M_{ct}} = \sqrt{\frac{\Sigma(M_{ct_i} - \overline{M}_{ct})^2}{N-1}}$  = standard deviation of the distribution of repair times, based on N observations



SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

$N$  = number of observations

The mean time to repair ( $\overline{M}_{ct}$ ) is given by

$$\overline{M}_{ct} = \frac{\sum M_{ct_i}}{N} \quad (5.95)$$

The median time to repair ( $\tilde{M}_{ct}$ ) is given by

$$\tilde{M}_{ct} = \frac{\sum M_{ct_i}}{N} \quad (5.96)$$

which is equal to the mean time to repair because of the symmetry of the normal distribution (see Fig. 5.3-1).

The maximum time to repair is given by

$$M_{\max_{ct}} = \overline{M}_{ct} + \phi S_{M_{ct}} \quad (5.97)$$

where:

$$\phi = z(t_{1-\alpha})$$

= value from normal distribution function corresponding to the percentage point  $(1-\alpha)$  on the maintainability function for which  $M_{\max_{ct}}$  is defined. Values of  $\phi$  as a function of  $(1-\alpha)$  are shown in Table 5.6-6. Note that this is the same as Table 5.6-2 with rounded-off values.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.6-6: VALUES OF  $\phi$  FOR SPECIFIED  $\alpha$ 

1- $\alpha$	$\phi$ or $z(t_{1-\alpha})$
95%	1.65
90%	1.28
85%	1.04
80%	0.84

5.6.2.2.1 Equipment Example

An equipment whose repair times are assumed to be normally distributed was monitored and the following repair times were observed (in minutes):

6.5, 13.25, 17.25, 17.25, 19.75, 23, 23, 24.75, 27.5, 27.5, 27.5, 32, 34.75, 34.75, 37.5, 37.5, 40.25, 42.5, 44.75, 52

Find the following parameters.

- (1) The pdf of  $g(t)$  and its value at 30 minutes
- (2) The MTTR and median times to repair
- (3) The maintainability for 30 minutes
- (4) The time within which 90% of the maintenance actions are completed
- (5) The repair rate,  $u(t)$ , at 30 minutes

(1) Pdf of  $g(t)$ 

$$\bar{M}_{ct} = \frac{\Sigma M_{ct_i}}{N} = \frac{583.25}{20} = 29.16 \text{ minutes}$$

$$S_{M_{ct}} = \sqrt{\frac{\Sigma(M_{ct_i} - \bar{M}_{ct})^2}{N-1}}$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

$$= \sqrt{\frac{\Sigma(M_{ct_i})^2 - N(\overline{M}_{ct})^2}{N-1}} = \sqrt{\frac{19527 - 17006}{19}} = 11.5 \text{ minutes}$$

$$g(t) = \frac{1}{11.5\sqrt{2p}} \exp\left[-\frac{(M_{ct_i} - 29.16)^2}{2(11.5)^2}\right]$$

$$g(30) = \frac{1}{28.82} \exp\left[-\frac{(30 - 29.16)^2}{2(11.5)^2}\right] = \frac{1}{28.82} e^{-0.0032}$$

$$= (0.035)(0.9973) = 0.035$$

(2) MTTR and Median Time to Repair

These are the same for the normal distribution because of its symmetry, and are given by

$$\overline{M}_{ct} = \frac{\Sigma M_{ct_i}}{N} = \frac{583}{20} = 29.16 \text{ minutes}$$

(3) Maintainability for 30 Minutes

$$M(30) = \int_{-\infty}^{30} g(t) dt = \int_{-\infty}^{z(30)} \phi(z) dz$$

$$z(30) = \frac{M_{ct_i} - \overline{M}_{ct}}{S_{M_{ct}}} = \frac{30 - 29.16}{11.5} = \frac{0.84}{11.5} = 0.07$$

From the standard normal table (Table 5.3-3).

$$\phi(0.07) = 1 - .4721 = 0.5279 = 0.53$$

$\therefore M(30) = 0.53$  or 53% probability of making a repair in 30 minutes.

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

- (4)
- Time within which 90% of the Maintenance Actions are completed

$$M_{0.9} = \overline{M}_{ct} + \phi S_{M_{ct}} \quad \phi = 1.28 \text{ from Table 5.6-6}$$

$$= 29.16 + (1.28)(11.5) = 43.88 \text{ minutes}$$

- (5)
- Repair Rate at 30 Minutes

$$\mu(30) = \frac{g(30)}{1 - M(30)} = \frac{0.035}{1 - 0.53} = \frac{0.035}{0.47} = 0.074 \text{ repairs/minute}$$

5.6.2.3 Exponential Distribution

In maintainability analysis, the exponential distribution applies to maintenance tasks and maintenance actions whose completion times are independent of previous maintenance experience (e.g., substitution methods of failure isolation where several equally likely alternatives are available and each alternative is exercised, one at a time, until the one which caused the failure is isolated), producing a probability density function given by

$$g(t = M_{ct}) = \frac{1}{M_{ct}} \exp\left(-\frac{M_{ct}t}{M_{ct}}\right) \quad (5.98)$$

The method used in evaluating the maintainability parameters is similar to that previously shown in Section 5.3.4 for analyzing reliability with exponential times-to-failure. The fundamental maintainability parameter is repair rate,  $\mu(t)$ , which is the reciprocal of  $\overline{M}_{ct}$ , the mean-time-to-repair (MTTR). Thus, another expression for  $g(t)$  in terms of  $\mu(t)$ , the repair rate, is

$$g(t) = \mu e^{-\mu t} \quad (5.99)$$

where  $\mu$  is the repair rate (which is constant for the exponential case).

The maintainability function is given by

$$M(t) = \int_0^t g(t) dt = \int_0^t \mu e^{-\mu t} dt = 1 - e^{-\mu t} \quad (5.100)$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

The MTTR is given by

$$\overline{M}_{ct} = \frac{1}{\mu} = \frac{\sum M_{ct_i}}{N} \quad (5.101)$$

If the maintainability function,  $M(t)$ , is known, the MTTR can also be obtained from

$$\text{MTTR} = \overline{M}_{ct} = \frac{-t}{\{\ln[1 - M(t)]\}} \quad (5.102)$$

The median time to repair  $\tilde{M}_{ct}$  is given by

$$\tilde{M}_{ct} = 0.69 \overline{M}_{ct} \quad (5.103)$$

The maximum time to repair is given by

$$M_{\max ct} = k_e \overline{M}_{ct} \quad (5.104)$$

where:

$k_e$  = value of  $M_{ct_i} / \overline{M}_{ct}$  at the specified percentage point  $\alpha$   
on the exponential function at which  $M_{\max ct}$  is defined.

Values of  $k_e$  are shown in Table 5.6-7.

TABLE 5.6-7: VALUES OF  $k_e$  FOR SPECIFIED  $\alpha$

$\alpha$	$k_e$
95%	3.00
90%	2.31
85%	1.90
80%	1.61

#### 5.6.2.3.1 Computer Example

For a large computer installation, the maintenance crew logbook shows that over a period of a month there were 15 unscheduled maintenance actions or downtimes, and 1200 minutes in

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

emergency maintenance status. Based upon prior data on this equipment, the maintainability analyst knew that the repair times were exponentially distributed. A warranty contract between the computer company and the government calls for a penalty payment of any downtime exceeding 100 minutes.

Find the following:

1. The MTTR and repair rate
2. The maintainability function  $M(t)$  for 100 minutes, or the probability that the warranty requirement is being met
3. The median time to repair
4. The time within which 95% of the maintenance actions can be completed

1. MTTR and Repair Rate

$$\text{MTTR} = \overline{M}_{ct} = \frac{1200}{15} = 80 \text{ minutes}$$

$$\mu(\text{repair rate}) = \frac{1}{\overline{M}_{ct}} = 1/80 = 0.0125 \text{ repairs/minute}$$

2. Maintainability Function for 100 Minutes

$$M(100) = 1 - e^{-\mu t} = 1 - e^{-(0.0125)(100)} = 1 - e^{-1.25} = 1 - 0.286 = 0.714$$

or a 71% probability of meeting the warranty requirement.

3. Median Time to Repair

$$\tilde{M}_{ct} = 0.69 \overline{M}_{ct} = (0.69)(80) = 55.2 \text{ minutes}$$

4. Time within which 95% of the Maintenance Actions can be Completed

$$M_{\max ct} = M_{0.95} = 3 \overline{M}_{ct} = 3(80) = 240 \text{ minutes}$$

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

**5.6.2.4 Exponential Approximation**

In general, the repair time density function is lognormally distributed. In practice, however, the standard deviation of the logarithms of repair times ( $\sigma \ln M_{ct}$ ) is not usually known and must be estimated in order to compute the probability of repair for any value of repair time. A value of  $\sigma = 0.55$  has been suggested by some prediction procedures, based on maintenance experience data accumulated on equipment. In the absence of justifiable estimates of  $\sigma$ , it is practicable to use the exponential distribution as an approximation of the lognormal.

Figure 5.6-6 compares the exponential function with several lognormal functions of different standard deviations. All functions in the figure are normalized to a common  $\bar{M}_{ct}$  at  $M_{ctj}/\bar{M}_{ct} = 1.0$ . The exponential approximation is, in general, conservative over the region shown. Probability of repair in time  $t$  in the exponential case is given by

$$M(t) \approx 1 - e^{-t/\bar{M}_{ct}} = 1 - e^{-\mu t}$$

where:

$M(t)$  = probability of repair in a specified time  $t$

$\bar{M}_{ct}$  = known mean corrective maintenance time

This approximation will be used in the next section on availability theory because it allows for a relatively simple description of the basic concepts without becoming overwhelmed by the mathematics involved.

**5.7 Availability Theory**

The concept of availability was originally developed for repairable systems that are required to operate continuously, i.e., round the clock, and are at any random point in time either operating or “down” because of failure and are being worked upon so as to restore their operation in minimum time. In this original concept a system is considered to be in only two possible states - operating or in repair - and availability is defined as the probability that a system is operating satisfactorily at any random point in time  $t$ , when subject to a sequence of “up” and “down” cycles which constitute an alternating renewal process (Ref. [35]). In other words, availability is a combination of reliability and maintainability parameters.

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

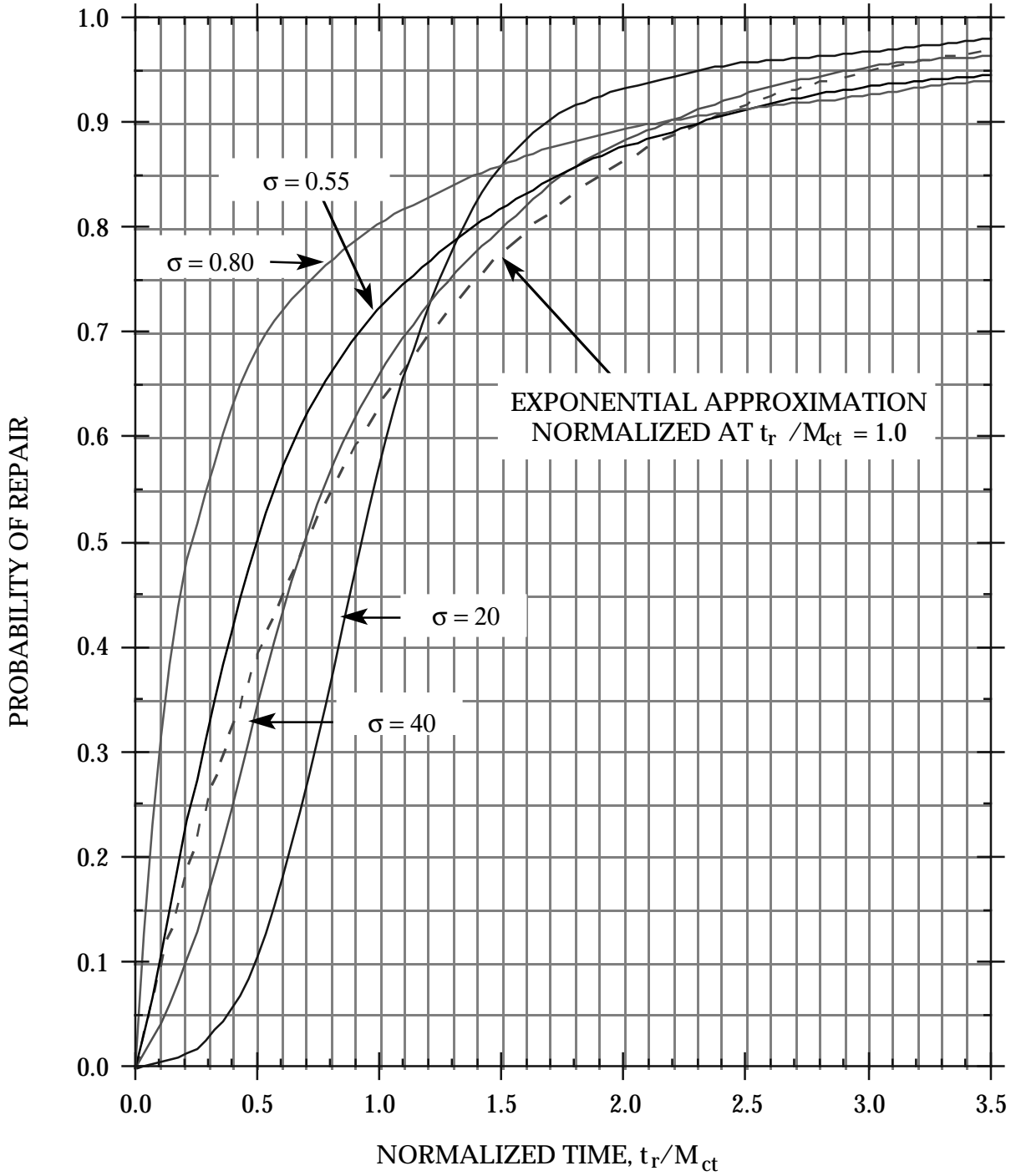


FIGURE 5.6-6: EXPONENTIAL APPROXIMATION OF LOGNORMAL MAINTAINABILITY FUNCTIONS

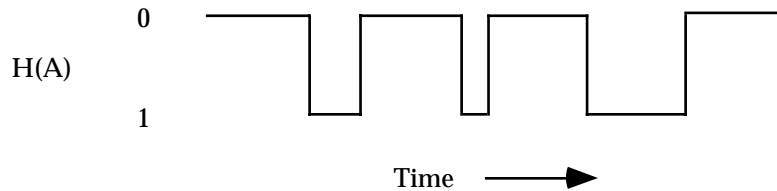


---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**


---

For simplicity, consider a single equipment which is to be operated continuously. If a record is kept on when the equipment is operating or down over a period of time, it is possible to describe its availability as a random variable defined by a distribution function  $H(A)$  as illustrated.



The expected value availability is simply the average value of the function over all possible values of the variable. When we discuss a system's steady state availability, we are referring, on the other hand, to the behavior of an ensemble of equipments. If we had a large number of equipments that have been operating for some time, then at any particular time we would expect the number of equipments that are in state 0 (available) to be  $NP_0$ . Thus, the ratio of the number of equipments available to the total number of equipments is simply  $NP_0/N = P_0$ , where  $N$  = total number of equipments and  $P_0$  is fraction of total equipment ( $N$ ) in state 0 (available).

### 5.7.1 Basic Concepts

System availability can be defined in the following ways:

- (1) Instantaneous Availability:  $A(t)$  Probability that a system will be available for use at any random time  $t$  after the start of operation.
- (2) Mission Availability:  $A_m(t_2 - t_1)$  The proportion of time in an interval  $(t_2 - t_1)$ , during a mission, that a system is available for use, or

$$A_m(t_2 - t_1) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t) dt \quad (5.105)$$

This is also called average availability,  $A_{AV}$

- (3) Steady State of Availability:  $A_S$  Probability a system will be available for use at a point in time  $t$  after the start of system operation as  $t$  becomes very large, or as  $t \rightarrow \infty$ , or

$$A_S = \lim_{t \rightarrow \infty} A(t)$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

These three availabilities are illustrated in Figure 5.7-1.

(4) Achieved Availability:  $A_A$

$$A_A = 1 - \frac{\text{Downtime}}{\text{Total Time}} = \frac{\text{Uptime}}{\text{Total Time}} \quad (5.106)$$

Downtime includes all repair time (corrective and preventive maintenance time), administrative time and logistic time.

(5) Intrinsic Availability:  $A_i$

$$A_i = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \quad (5.107)$$

This does not include administrative time and logistic time; in fact, it usually does not include preventive maintenance time.  $A_i$  is primarily a function of the basic equipment/system design.

### 5.7.2 Availability Modeling (Markov Process Approach)

A Markov process (Ref. [2]) is a mathematical model that is useful in the study of the availability of complex systems. The basic concepts of the Markov process are those of “state” of the system (e.g., operating, nonoperating) and state “transition” (from operating to nonoperating due to failure, or from nonoperating to operating due to repair).

A graphic example of a Markov process is presented by a frog in a lily pond. As time goes by, the frog jumps from one lily pad to another according to his whim of the moment. The state of the system is the number of the pad currently occupied by the frog; the state transition is, of course, his leap.

Any Markov process is defined by a set of probabilities  $p_{ij}$  which define the probability of transition from any state  $i$  to any state  $j$ . One of the most important features of any Markov model is that the transition probability  $p_{ij}$  depends only on states  $i$  and  $j$  and is completely independent of all past states except the last one, state  $i$ ; also  $p_{ij}$  does not change with time.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

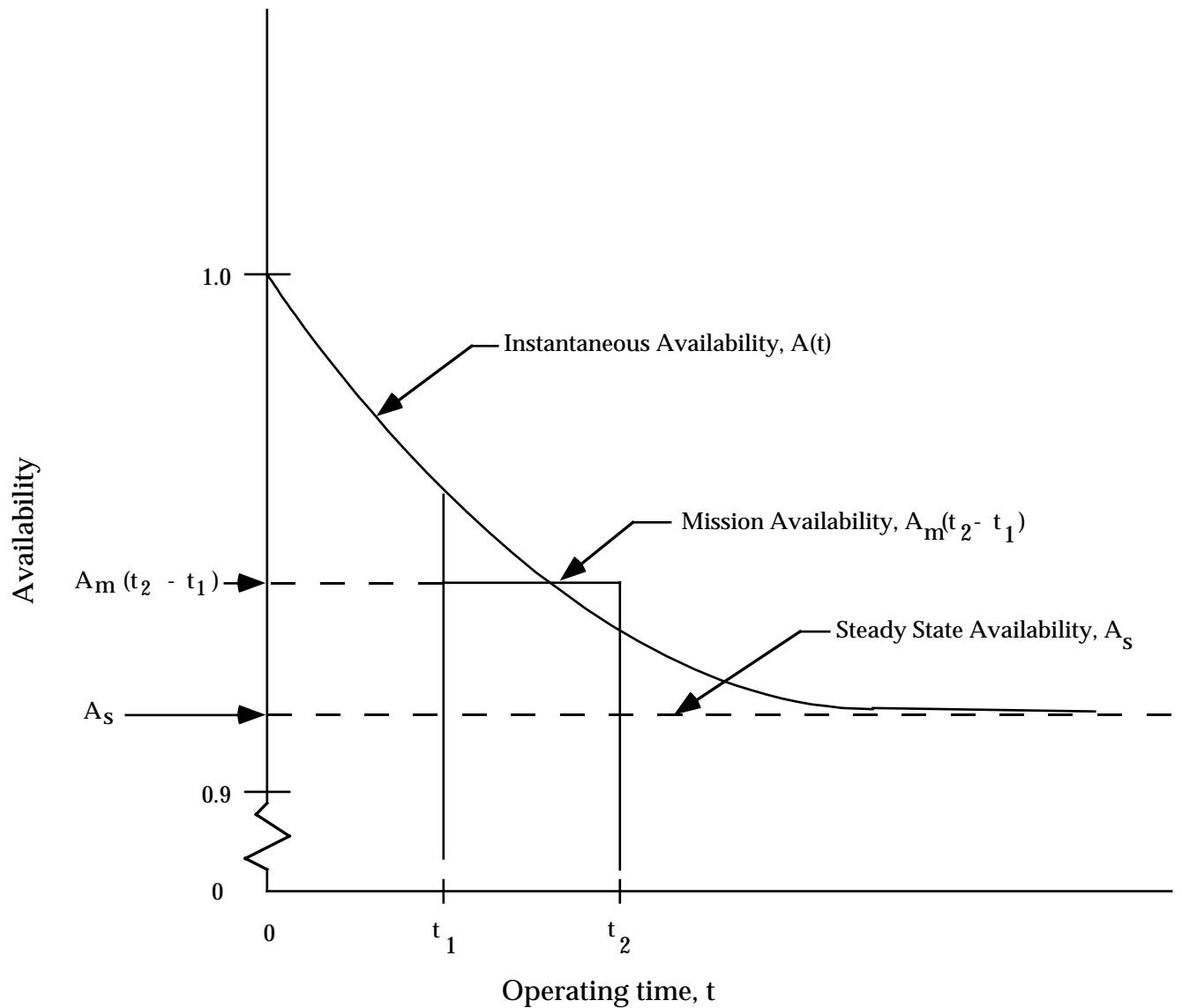


FIGURE 5.7-1: THE RELATIONSHIP BETWEEN INSTANTANEOUS, MISSION, AND STEADY STATE AVAILABILITIES AS A FUNCTION OF OPERATING TIME

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

In system availability modeling utilizing the Markov process approach, the following additional assumptions are made:

- (1) The conditional probability of a failure occurring in time  $(t, t + dt)$  is  $\lambda dt$ .
- (2) The conditional probability of a repair occurring in time  $(t, t + dt)$  is  $\mu dt$ .
- (3) The probability of two or more failures or repairs occurring simultaneously is zero.
- (4) Each failure or repair occurrence is independent of all other occurrences.
- (5)  $\lambda$  (failure rate) and  $\mu$  (repair rate) are constant (e.g., exponentially distributed).

Let us now apply the Markov process approach to the availability analysis of a single unit with failure rate  $\lambda$  and repair rate  $\mu$ .

#### 5.7.2.1 Single Unit Availability Analysis (Markov Process Approach)

The Markov graph for a single unit is shown in Figure 5.7-2.

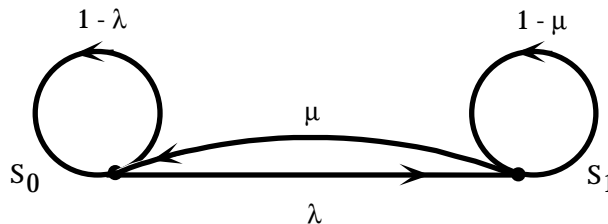


FIGURE 5.7-2: MARKOV GRAPH FOR SINGLE UNIT

where:

$S_0$  = State 0 = the unit is operating and available for use

$S_1$  = State 1 = the unit has failed and is being repaired

$\lambda$  = failure rate

$\mu$  = repair rate

Now since the conditional probability of failure in  $(t, t + dt)$  is  $\lambda dt$ , and the conditional probability of completing a repair in  $(t, t + dt)$  is  $\mu dt$ , we have the following transition matrix

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

$$P = \begin{matrix} 0 \\ 1 \end{matrix} \begin{pmatrix} 0 & 1 \\ 1-\lambda & \lambda \\ \mu & 1-\mu \end{pmatrix}$$

For example, the probability that the unit was in state 0 (operating) at time  $t$  and remained in state 0 at time  $t + dt$  is the probability that it did not fail in time  $dt$ , or  $(1 - \lambda) dt$ . On the other hand, the probability that the unit transitioned from state 0 (operating) to state 1 (failed) in time  $t + dt$  is the probability of systems failure in time  $dt$ , or  $\lambda dt$ . Similarly, the probability that it was in state 1 (failed) at time  $t$  and transitioned to state 0 (operating) in time  $dt$  is the probability that it was repaired in  $dt$ , or  $\mu dt$ . Also, the probability that it was in state 1 (failed) at time  $t$  and remained in state 1 at time  $t + dt$  is the probability that it was not repaired in  $dt$ , or  $(1 - \mu) dt$ .

The single unit's availability is

$$A(t) = P_0(t) \quad (\text{probability that it is operating at time } t)$$

and

$$P_0(t) + P_1(t) = 1 \quad (\text{it is either operating or failed at time } t)$$

The differential equations describing the stochastic behavior of this system can be formed by considering the following: the probability that the system is in state 0 at time  $t + dt$  is derived from the probability that it was in state 0 at time  $t$  and did not fail in  $(t, t + dt)$ , or that it was in state 1 at the time  $t$  and (was repaired) returned to state 0 in  $(t, t + dt)$ . Thus, we have

$$P_0(t + dt) = P_0(t) (1 - \lambda dt) + P_1(t) \mu dt$$

Similarly the probability of being in state 1 at time  $t + dt$  is derived from the probability that the system was in state 0 at time  $t$  and failed in  $(t, t + dt)$ ; or it was in state 1 at time  $t$ , and the repair was not completed in  $(t, t + dt)$ . Therefore

$$P_1(t + dt) = P_0(t) \lambda dt + P_1(t) (1 - \mu dt)$$

It should be noted that the coefficients of these equations represent the columns of the transition matrix. We find the differential equations by defining the limit of the ratio

$$\frac{P_i(t + dt) - P_i(t)}{dt}$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

which yields

$$P_0'(t) = -\lambda P_0(t) + \mu P_1(t) \quad (5.108)$$

$$P_1'(t) = \lambda P_0(t) - \mu P_1(t)$$

The above equations are called differential - difference equations.

If we say that at time  $t = 0$  the system was in operation, the initial conditions are  $P_0(0) = 1$ ,  $P_1(0) = 0$ . It is also of interest to consider the case where we begin when the system is down and under repair. In this case, the initial conditions are  $P_0(0) = 0$ ,  $P_1(0) = 1$ .

Transforming Equation [5.108] into LaPlace transforms under the initial conditions that  $P_0(0) = 1$ ,  $P_1(0) = 0$  we have

$$sP_0(s) - 1 + \lambda P_0(s) - \mu P_1(s) = 0$$

$$sP_1(s) - \lambda P_0(s) + \mu P_1(s) = 0$$

and simplifying

$$(s + \lambda) P_0(s) - \mu P_1(s) = 1 \quad (5.100)$$

$$-\lambda P_0(s) + (s + \mu) P_1(s) = 0 \quad (5.109)$$

Solving these simultaneously for  $P_0(s)$  yields

$$P_0(s) = \frac{\begin{vmatrix} 1-\mu \\ 0 & s+\mu \end{vmatrix}}{\begin{vmatrix} s+\lambda & -\mu \\ -\lambda & s+\mu \end{vmatrix}} = \frac{s+\mu}{s(s+\lambda+\mu)} = \frac{s}{s(s+\lambda+\mu)} + \frac{\mu}{s(s+\lambda+\mu)}$$

or

$$P_0(s) = \frac{1}{s+\lambda+\mu} + \frac{\mu}{s_1-s_2} \left( \frac{1}{s-s_1} - \frac{1}{s-s_2} \right)$$

where:

$$s_1 = 0 \text{ and } s_2 = -(\lambda + \mu).$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

Therefore,

$$P_0(s) = \frac{1}{s + \lambda + \mu} + \frac{\mu}{\lambda + \mu} \left\{ \frac{1}{s} - \frac{1}{s - [-(\lambda + \mu)]} \right\}$$

or, taking the inverse Laplace transform

$$P_0(t) = L^{-1}[P_0(s)]$$

The use of LaPlace transform,  $L[f(t)]$  and inverse LaPlace transform,  $L^{-1}[f(t)]$ , for availability analysis is described in a number of texts (see Refs. [35], [36]).

Therefore,

$$P_0(t) = e^{-(\lambda + \mu)t} + \frac{\mu}{\lambda + \mu} \left[ 1 - e^{-(\lambda + \mu)t} \right]$$

and

$$A(t) = P_0(t) = \underbrace{\frac{\mu}{\lambda + \mu}}_{\substack{\uparrow \text{---} \uparrow \\ \text{Steady state} \\ \text{component}}} + \underbrace{\frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t}}_{\substack{\uparrow \text{---} \uparrow \\ \text{Transient component}}} \quad (5.110)$$

$$1 - A(t) = P_1(t) = \underbrace{\frac{\lambda}{\lambda + \mu}}_{\substack{\uparrow \text{---} \uparrow \\ \text{Steady state} \\ \text{component}}} - \underbrace{\frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t}}_{\substack{\uparrow \text{---} \uparrow \\ \text{Transient component}}}$$

If the system was initially failed, the initial conditions are  $P_0(0) = 0$ ,  $P_1(0) = 1$ , and the solutions are

$$A(t) = P_0(t) = \frac{\mu}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \quad (5.111)$$

and

$$1 - A(t) = P_1(t) = \frac{\lambda}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \quad (5.111a)$$

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

We note that as  $t$  becomes very large, Eqs. (5.110) and (5.111) become equivalent. This indicates that after the system has been operating for some time its behavior becomes independent of its starting state.

We will show later that the transient term becomes negligible when

$$t = \frac{4}{\lambda + \mu} \quad (5.112)$$

For a mission of  $(t_1 - t_2)$  duration, the mission availability is

$$\begin{aligned} A_m(t_2 - t_1) &= \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t) dt = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} P_0(t) dt \\ &= \frac{\mu}{\lambda + \mu} - \frac{\lambda}{(\lambda + \mu)^2 T} \exp [-(\lambda + \mu)T] \end{aligned} \quad (5.113)$$

The steady state availability,  $A_s$ , is

$$A_s = \lim_{t \rightarrow \infty} A(t) = A(\infty),$$

Therefore Eq. (5.111) becomes

$$A_s = \frac{\mu}{\lambda + \mu} = \frac{1}{1 + \frac{\lambda}{\mu}}$$

As  $\lambda = \frac{1}{MTBF}$  and  $\mu = \frac{1}{MTTR}$  the steady state availability becomes

$$A_s = \frac{MTBF}{MTBF + MTTR}$$

Usually  $\mu$  is much larger in value than  $\lambda$ , and  $A_s$  may be written as



## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

$$A_s = \frac{1}{1 + \frac{\lambda}{\mu}} = 1 - \frac{\lambda}{\mu} + \frac{2}{\mu^2} - \dots \cong 1 - \frac{\lambda}{\mu}$$

As was previously stated, the transient part decays relatively fast and becomes negligible before

$$t = \frac{4}{\lambda + \mu}$$

If  $\mu$  is substantially greater than  $\lambda$ , then the transient part becomes negligible before

$$t = \frac{4}{\mu}$$

Figure 5.7-3 gives the availability of a single unit with repairs, showing how it approaches the steady state availability, as a function of

$$\frac{i}{\lambda + \mu} \quad \text{where } i = 1, 2, \dots$$

The instantaneous and steady state availabilities for a single exponential unit are tabulated as a function of operating time in Table 5.7-1.

The same technique described for a single unit can be applied to different equipment/system reliability configurations, e.g., combinations of series and parallel units. As the systems become more complex, the mathematical manipulations can be quite laborious. The important trick is to set up the Markov graph and the transition matrix properly; the rest is just mechanical. Reference [5] contains an extensive list of solutions for different system configurations.

For example, for the most general case of  $n$  equipments and  $r$  repairmen where  $r = n$ , the steady state availability,  $A_s$ , is

$$A_s = \left[ \sum_{k=0}^{n-1} \frac{n!}{(n-k)!k!} \rho^k + \sum_{k=r}^n \frac{n!}{(n-k)!r!} \rho^r \left( \frac{\rho}{r} \right)^{k-1} \right] \quad (5.114)$$

where  $\rho = \frac{\lambda}{\mu}$

More details on availability modeling and applications are presented in Section 10.

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

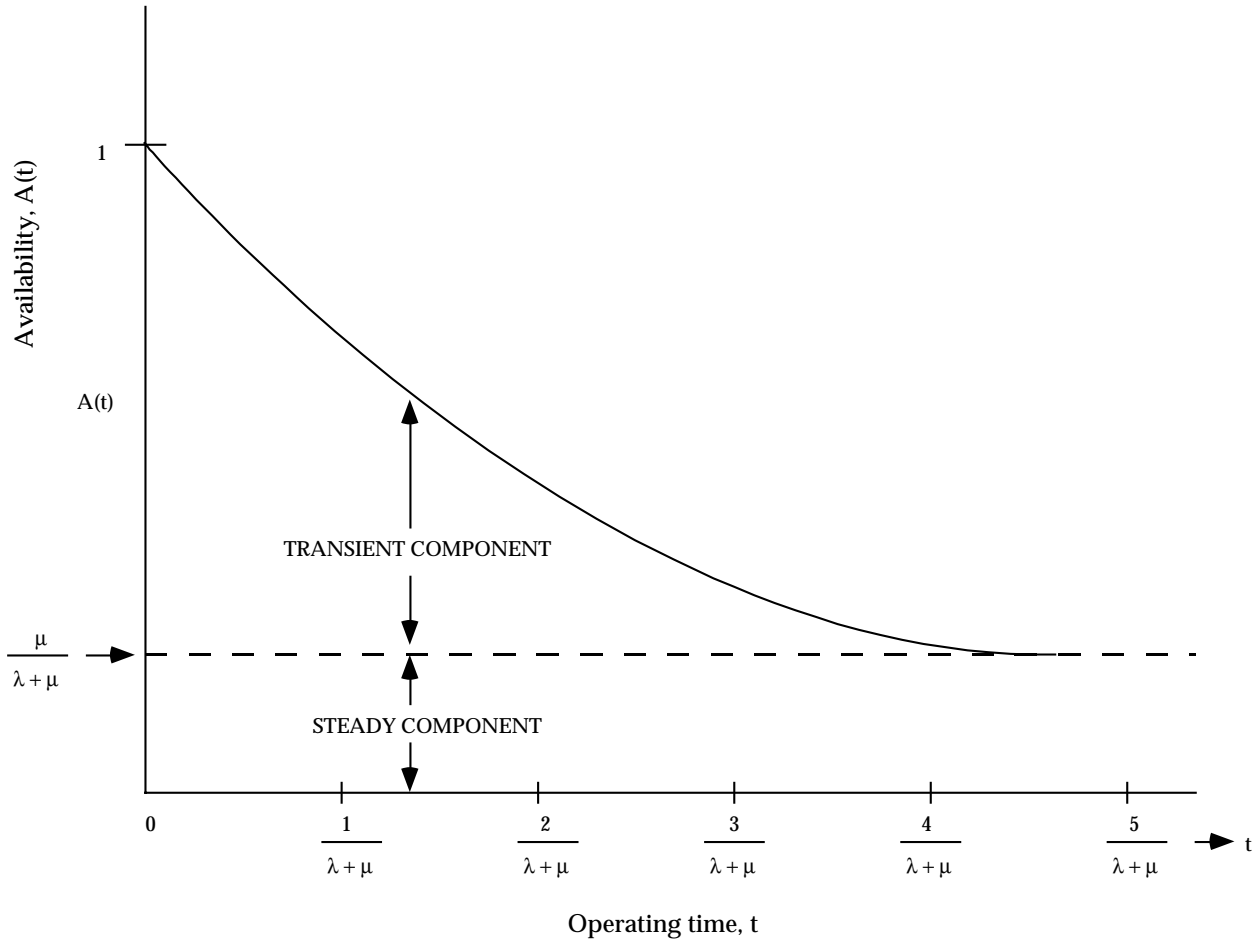


FIGURE 5.7-3: SINGLE UNIT AVAILABILITY WITH REPAIR

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

TABLE 5.7-1: THE AVAILABILITY OF A SINGLE SYSTEM OR UNIT

- (a) instantaneous or point availability  
 (b) steady state availability or inherent uptime ratio.  
 $\lambda = 0.01$  failures/hr (fr/hr);  
 $\mu = 1.0$  repairs/hr (rp/hr).

Operating Time (Hrs.)	(a) Point Availability A(t)	(b) Steady State Availability $A_s$  $= \frac{\mu}{\lambda + \mu}$
0.25	0.997791	
0.50	0.996074	
0.75	0.994741	$= \frac{1}{0.01 + 1}$
1.00	0.993705	
1.50	0.992275	
2.00	0.991412	$= \frac{1}{1.01}$
2.50	0.990892	
3.00	0.990577	
3.50	0.990388	$= 0.990099$
4.00	0.990273	
5.00	0.990162	
6.00	0.990122	
7.00	0.990107	
8.00	0.990102	
9.00	0.990100	
10.00	0.990099	
$\infty$		0.990099

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

5.8 R&M Trade-Off Techniques

System effectiveness and cost/effectiveness models provide the best tools for performing trade-off studies on the system level. Because of the complexities involved, most of these models are computerized. Through the computerized models any changes in any of the multitude of reliability, maintainability, performance, mission profile, logistic support, and other parameters can be immediately evaluated as to their effect on the effectiveness and total cost of a system. Thus cost effectiveness modeling and evaluation, besides being used for selecting a specific system design approach from among several competing alternatives, is a very powerful tool for performing parametric sensitivity studies and tradeoffs down to component level when optimizing designs to provide the most effective system for a given budgetary and life cycle cost constraint or the least costly system for a desired effectiveness level.

At times, however, especially in the case of the more simple systems, tradeoffs may be limited to achieving a required system availability while meeting the specified reliability and maintainability requirements. Comparatively simple trade-off techniques can then be used as shown in the paragraphs below. The maintainability design trade-off aspects and the cost oriented trade-offs are discussed further in Sections 10 and 12.

5.8.1 Reliability vs. Maintainability

As stated earlier in this section, reliability and maintainability jointly determine the inherent availability of a system. Thus, when an availability requirement is specified, there is a distinct possibility of trading-off between reliability and maintainability since, in the steady state, availability depends only on the ratio or ratios of MTTR/MTBF that is referred to as maintenance time ratio (MTR) and uses the symbol  $\alpha$ , i.e.,

$$\alpha = \text{MTTR/MTBF} \quad (5.115)$$

so that the inherent availability equation assumes the form

$$A_i = 1/(1+\alpha) = (1 + \alpha)^{-1} \quad (5.116)$$

Now, obviously innumerable combinations of MTTR and MTBF will yield the same  $\alpha$  and, therefore, the same availability  $A_i$ . However, there is usually also a mission reliability requirement specified and also a maintainability requirement. Both of these requirements must also be met in addition to the availability requirement. Following is a tradeoff example. Figure 5.8-1 represents a system consisting of five major subsystems in a series arrangement. The MTBF of this system is

$$\text{MTBF} = (\sum \lambda_i)^{-1} = (0.0775)^{-1} = 12.9 \text{ hour}$$

## SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

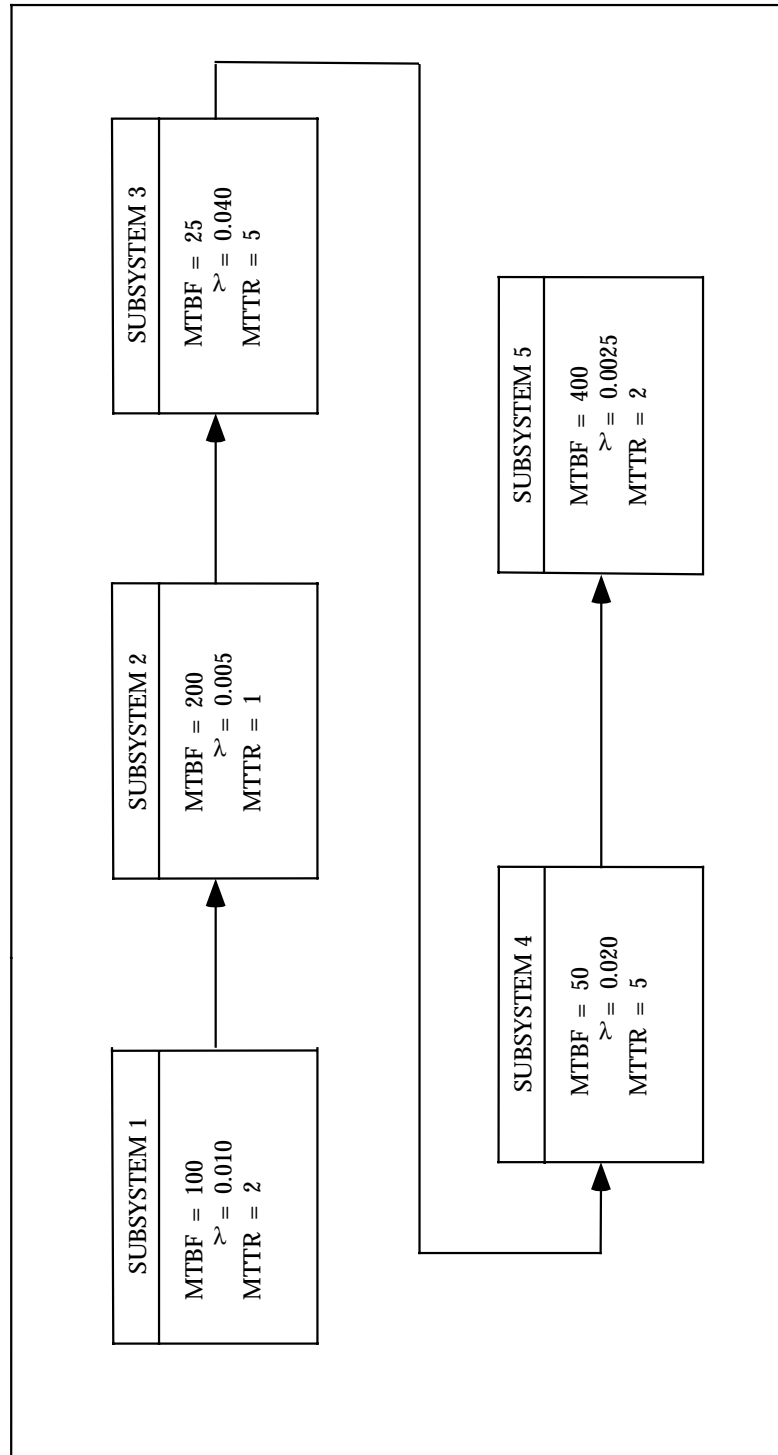


FIGURE 5.8-1: BLOCK DIAGRAM OF A SERIES SYSTEM

---

 SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY
 

---

and its MTTR is

$$MTTR = \sum \lambda_i (MTTR)_i / \sum \lambda_i = 0.33(0.0775)^{-1} = 4.26 \text{ hr}$$

Since the maintenance time ratio equals

$$\alpha = 4.26(12.9)^{-1} = 0.33 \quad (5.117)$$

which is the sum of the maintenance ratios of the five serial subsystems

$$\alpha = \sum \alpha_i = 2/100 + 1/200 + 5/25 + 5/50 + 2/400 = 0.33 \quad (5.118)$$

then

$$A_i = [1 + (4.26/12.9)]^{-1} = .752$$

By inspection of Eq. (5.118) we see that Subsystems 3 and 4 have the highest maintenance time ratios, i.e., 0.2 and 0.1, and therefore are the “culprits” in limiting system availability to 0.752 which may be completely unacceptable.

If, because of state-of-the-art limitations it is not possible to increase the MTBFs of these two subsystems and their MTTRs cannot be reduced by repackaging, the first recourse could be the adding of a parallel redundant subsystem to Subsystem 3. Now two cases may have to be considered: (a) the case where no repair of a failed redundant unit is possible until both fail and the system stops operating, or (b) repair is possible while the system is operating.

In the first case the MTBF of Subsystem 3, which now consists of two parallel units, becomes 1.5 times that of a single unit, i.e.,  $1.5 \times 25 = 37.5$  hr. With both units failed, both must be repaired. If a single crew repairs both in sequence, the new MTTR becomes 2 hr and availability actually drops. If two repair crews simultaneously repair both failed units, and repair time is assumed exponentially distributed, the MTTR of both units is again 1.5 times that of a single unit, or 1.5 hr., and system availability remains the same as before, with nothing gained. But if repair of a failed redundant unit is possible while the system operates, the steady-state availability of Subsystem 3 becomes

$$A_3 = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + 2\lambda^2)$$

for a single repair crew. Since, for a single unit in this subsystem the failure rate  $\lambda = 0.04$  and the repair rate  $\mu = 1/5 = 0.2$ , we get

$$A_3 = (0.04 + 2 \cdot 0.04 \cdot 0.2) / (0.04 + 2 \cdot 0.04 \cdot 0.02 + 2 \cdot 0.0016)^{-1}$$

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

$$= 0.056(0.0592)^{-1} = 0.946$$

as compared to 0.883 (e.g., 25/30) when no redundancy was used. The value of  $A_1 = 0.946$  of the redundant configuration corresponds to a maintenance time ratio of

$$\alpha_s = (1 - A_3)A_3^{-1} = 0.054(0.946)^{-1} = 0.057$$

The whole system maintenance time ratio now becomes

$$\alpha = \sum \alpha_i = 0.02 + 0.005 + 0.057 + 0.1 + 0.005 = 0.187$$

and system availability  $A$  is

$$A = (1 + 0.187)^{-1} = (1.187)^{-1} = 0.842$$

as compared with 0.752 without redundancy in Subsystem 3. If this new value of availability is still not acceptable, redundancy would also have to be applied to Subsystem 4. But to achieve these gains in availability, repair of failed redundant units must be possible while the system is operating. This is called availability with repair. Otherwise, redundancy will not increase availability and may even reduce it, even though it increases system reliability.

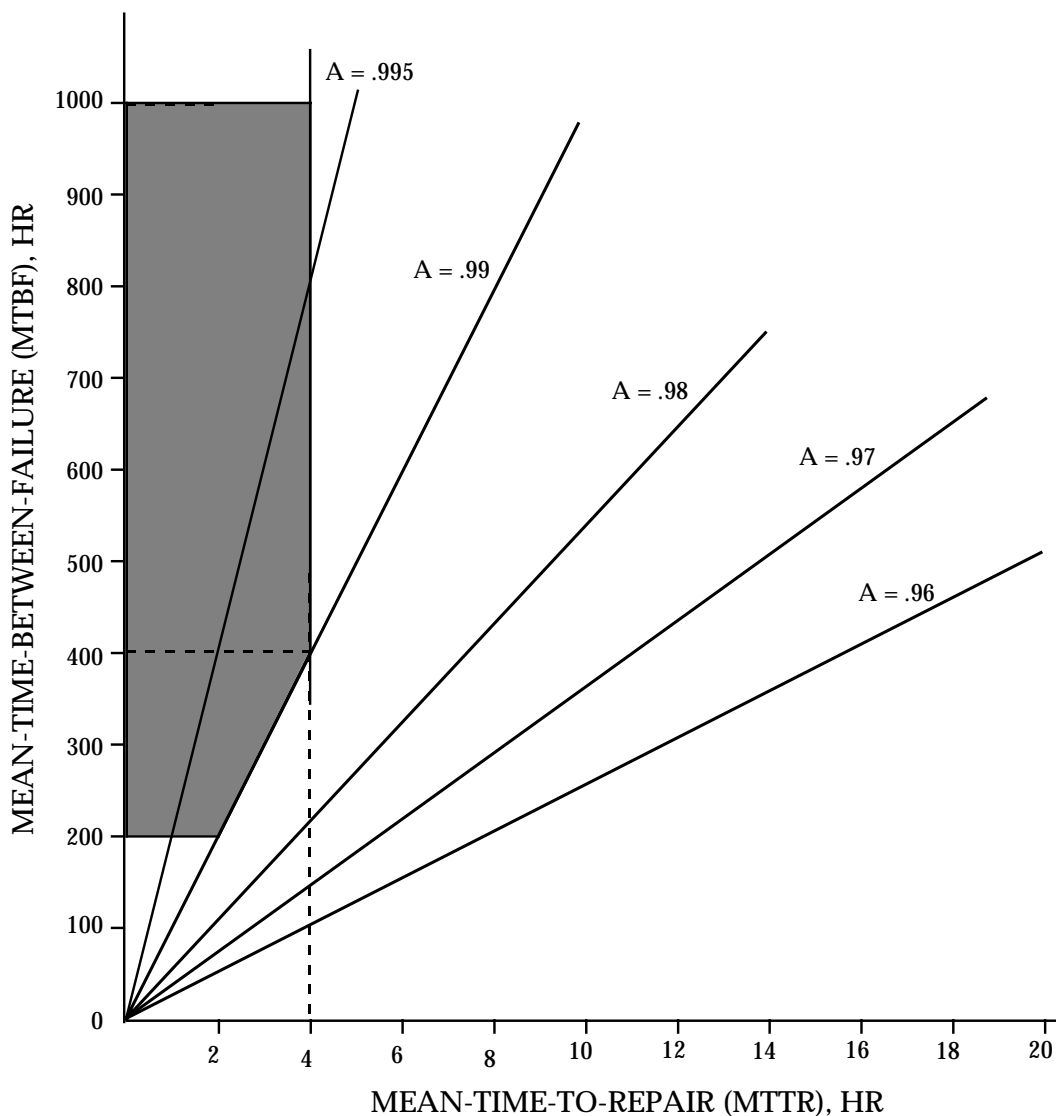
A different method of straightforward trade-off between reliability and maintainability is shown in Figure 5.8-2. The specific trade-off example shown in this figure is based on a requirement that the inherent availability of the system must be at least  $A = 0.99$ , the MTBF must not fall below 200 hr, and the MTTR must not exceed 4 hr. The trade-off limits are within the shaded area of the graph, resulting from the equation for inherent availability

$$A_i = \text{MTBF}/(\text{MTBF} + \text{MTTR})$$

The straight line  $A = 0.99$  goes through the points (200,2) and (400,4), the first number being the MTBF and the second number being the MTTR. Any system with an MTBF larger than 200 hr and an MTTR smaller than 2 hr will meet or exceed the minimum availability requirement of  $A = 0.99$ . If there are several system design alternatives that comply with the specification requirements, the design decision is made by computing the life cycle costs of each alternative and usually selecting the least expensive system, unless substantial gains in system effectiveness are achieved which would warrant increasing the expenditures.

More examples of R&M tradeoffs are given in Section 10.

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY



 TRADE-OFF AREA WITHIN SPECIFICATION

 OUT OF SPECIFICATION

REQUIREMENT  
 A = 99%  
 MTBF = 200 HR MIN  
 MTTR = 4 HR MAX

FIGURE 5.8-2 RELIABILITY-MAINTAINABILITY TRADE-OFFS



---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**

---

5.9 References For Section 5

1. Amstader, B. Reliability Mathematics. New York, NY: McGraw-Hill, 1971.
2. ARINC Research Corporation, Reliability Engineering, Englewood Cliffs, NJ: Prentice-Hall, 1963.
3. Arsenault, J.E. and J.A. Roberts, "Reliability and Maintainability of Electronic Systems." Computer Science Press, Potomac, MD, 1980.
4. Ascher, H. and H. Feingold, Repairable Systems Reliability. New York, NY, Marcel Dekker, 1984
5. Barlow, R.E. and F. Proschan, Mathematical Theory of Reliability. New York, NY: John Wiley & Sons, Inc., 1965.
6. Bazovsky, I., Reliability Theory and Practice. Englewood Cliffs, NY: Prentice-Hall, 1961.
7. Blanchard, B.S., Jr., and E. Lowery, Maintainability, Principles and Practice. New York, NY: McGraw-Hill, 1969.
8. Bourne, A.J. and A.E. Greene, Reliability Technology. London, UK: Wiley, 1972.
9. Calabro, S.R., Reliability Principles and Practice. New York, NY: McGraw-Hill, 1962.
10. Cox, D.R., Renewal Theory. New York, NY: John Wiley & Sons, 1962.
11. Cunningham, C.E. and Cox, W., Applied Maintainability Engineering. New York, NY: Wiley, 1972.
12. Dummer, G.W., and N.B. Griffin, Electronic Reliability: Calculation and Design. Elmsford, NY: Pergamon, 1966.
13. Enrick, N.L., Quality Control and Reliability. New York, NY: Industrial Press, 1972.
14. Fuqua, N., Reliability Engineering for Electronic Design. New York, NY: Marcel Dekker, 1987.
15. Gnedenko, B.J. Belyayev and A.D. Solovyev, Mathematical Methods of Reliability. (translation edited by Richard E. Barlow), New York, NY: Wiley, 1969.

---

**SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY**

---

16. Goldberg, M., et al., "Comprehensive Failure Mechanism Theory - Metal Film Resistor Behavior," Proceedings of Second Annual Symposium on the Physics of Failure in Electronics, RADC, Griffiss Air Force Base, NY, 1963.
17. Goldman, A.S. and T.B. Slattery, Maintainability: A Major Element of System Effectiveness, New York, NY: Wiley, 1964.
18. Ireson, W.G., Reliability Handbook. New York, NY: McGraw-Hill, 1966.
19. Ireson, W.G. and C.F. Coombs, Handbook of Reliability Engineering and Management. New York, NY: McGraw-Hill, 1988.
20. Kececioglu, D., Reliability Engineering Handbook. Englewood Cliffs, NJ: Prentice-Hall, 1991.
21. Klion, J., Practical Electronic Reliability Engineering. New York, NY: Van Nostrand, 1992.
22. Krishnamoorthi, K.S., "Reliability Methods for Engineers," Milwaukee, WI, ASQC, 1992.
23. Kozlov, B.A. and I.A. Ushakov, Reliability Handbook. Winston, NY: Holt, Rinehart, 1970.
24. Landers, R.R., Reliability and Product Assurance. Englewood Cliffs, NJ: Prentice-Hall, 1963.
25. Lloyd, D.K. and M. Lipow, Reliability Management, Methods, and Mathematics. (second edition published by the authors), TRW, Inc., Redondo Beach, CA, 1977.
26. Locks, M.O., Reliability, Maintainability, and Availability Assessment. Rochelle Park, NJ: Hayden Book Co., 1973.
27. Mann, N.R., R.E. Schafer and N.D. Singpurwallar, Methods for Statistical Analysis of Reliability and Life Data. New York, NY: Wiley, 1974.
28. Myers, R.H. (ed.), Reliability Engineering for Electronic Systems. New York, NY: Wiley, 1964.
29. O'Connor, P. and D.T. O'Connor, Practical Reliability Engineering. Philadelphia, PA: Heyden & Son, 1981.
30. Pieruschka, E., Principles of Reliability. Englewood Cliffs, NJ: Prentice-Hall, 1963.

SECTION 5: RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

---

31. Polovko, A.M., Fundamentals of Reliability Theory. (translation edited by William H. Pierce), New York, NY: Academic Press, 1968.
32. Rau, J.G., Optimization and Probability in Systems Engineering. New York, NY: Van Nostrand-Reinhold, 1970.
33. Reheja, D.E., Assurance Technologies: Principles and Practices. New York, NY: McGraw-Hill, 1991.
34. Roberts, N.H., Mathematical Methods in Reliability Engineering. New York, NY: McGraw-Hill, 1964.
35. Sandler, G.W., System Reliability Engineering. Englewood Cliffs, NJ: Prentice-Hall, 1963.
36. Shooman, M., Probabilistic Reliability: An Engineering Approach. New York, NY: McGraw-Hill, 1968.
37. Smith, D.J., Reliability Engineering. New York, NY: Barnes and Noble, 1972.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

### 6.0 RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

#### 6.1 Introduction

Section 5 of this handbook laid the theoretical, mathematical foundation for the reliability engineering discipline; this section emphasizes the practical approaches to specifying, allocating and predicting equipment/system reliability.

Section 6.2 discusses methods for specifying reliability, quantitatively; Section 6.3 describes procedures for allocating reliability to each of the elements of an equipment or system so as to meet the overall equipment/system reliability requirement; Section 6.4 provides details on methods for modeling equipment/system reliability and describes the techniques for predicting equipment/system reliability; and Section 6.5 ties it all together in a step-by-step procedure for performing reliability allocation and prediction.

#### 6.2 Reliability Specification

The first step in the reliability engineering process is to specify the required reliability that the equipment/system must be designed to achieve. The essential elements of a reliability specification are:

- (1) A quantitative statement of the reliability requirement
- (2) A full description of the environment in which the equipment/system will be stored, transported, operated and maintained
- (3) Clear identification of the time measure (operating hours, flying hours, cycles, etc.) and mission profile
- (4) A clear definition of what constitutes failure
- (5) A description of the test procedure with accept/reject criteria that will be used to demonstrate the specified reliability

##### 6.2.1 Methods of Specifying the Reliability Requirement

To be meaningful, a reliability requirement must be specified quantitatively. Three basic ways in which a reliability requirement may be defined are:

- (1) As a “mean life” or mean-time-between-failure, MTBF. This definition is useful for long life systems in which the form of the reliability distribution is not too critical or where the planned mission lengths are always short relative to the specified mean life. Although this definition is adequate for specifying life, it gives no positive assurance of

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

a specified level of reliability in early life, except as the assumption of an exponential distribution can be proven to be valid.

- (2) As a probability of survival for a specified period of time,  $t$ . This definition is useful for defining reliability when a high reliability is required during the mission period but mean-time-to-failure beyond the mission period is of little tactical consequence, except as it influences availability.
- (3) As a probability of success, independent of time. This definition is useful for specifying the reliability of one-shot devices, such as the flight reliability of missiles. It is also useful for items that are cyclic, such as the reliability of launch equipment.

The reliability requirement may be specified in either of two ways as: a **NOMINAL** or design value with which the customer would be satisfied, on the average; or a **MINIMUM** acceptable value below which the customer would find the system totally unacceptable and which could not be tolerated in the operational environment -- a value based upon the operational requirements.

Whichever value is chosen as the specified requirement, there are two rules that should be applied; (a) when a nominal value is specified as a requirement, always specify a minimum acceptable value which the system must exceed, (b) when a minimum value alone is used to specify the requirement, always insure that it is clearly defined as minimum. In MIL-HDBK-781, "Reliability Test Methods, Plans and Environments for Engineering Development, Qualification and Production," (Ref. [1]), the nominal value is termed the "upper test MTBF" and the minimum acceptable value is the "lower test MTBF."

Of the two methods, the first is by far the best, since it automatically establishes the design goal at or above a known minimum.

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

Example 1:

A complex radar has both search and track functions. It is also possible to operate the search function in both a low and high power mode. The reliability requirement for this system could be expressed as:

“The reliability of the system shall be at least:

- Case I - High power search: 28 hours MTBF
- Case II - Low power search: 40 hours MTBF
- Case III - Track: 0.98 probability of satisfactory performance for 1/2 hour”

The definition of satisfactory performance must include limits for each case. These are necessary since if the radar falls below the specified limits for each case, it is considered to have failed the reliability requirement. A portion of the Satisfactory Performance Table for the radar is shown in Figure 6.2-1.

An important consideration in developing the reliability requirement is that it be realistic in terms of real need, yet consistent with current design state-of-the-art. Otherwise, the requirement may be unattainable or attainable only at a significant expenditure of time and money.

### 6.2.2 Description of Environment and/or Use Conditions

The reliability specification must cover all aspects of the use environment to which the item will be exposed and which can influence the probability of failure. The specification should establish in standard terminology the “use” conditions under which the item must provide the required performances. “Use” conditions refer to all known use conditions under which the specified reliability is to be obtained, including the following:

Temperature	Penetration/Abrasion
Humidity	Ambient Light
Shock	Mounting Position
Vibration	Weather (wind, rain, snow)
Pressure	Operator Skills

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

System Characteristic	Units	Performance Limits		
		Case 1	Case 2	Case 3
Range	Yards	300,000	120,000	120,000
Resolution - Range	Yards	±50	±50	± 10
- Bearing	Degrees	±0.1	±0.1	±0.1
- Velocity	Ft./Sec.	±100	±100	±25

FIGURE 6.2-1: SATISFACTORY PERFORMANCE LIMITS FOR EXAMPLE RADAR

The “Use” conditions are presented in two ways:

- (1) Narrative: Brief description of the anticipated operational conditions under which the system will be used.

Example 2:

- (a) The MK 000 Computer will be installed in a 15 to 30°C temperature-controlled space aboard the aircraft.
  - (b) The TOY missile must be capable of withstanding exposed airborne environments encountered while suspended from the launcher for periods up to three hours. This includes possible ice-loading conditions, subzero weather, etc.
- (2) Specific: Itemized list of known or anticipated ranges of environments and conditions. When changes of environment are expected throughout an operating period, as in an aircraft flight, an environmental profile should be included.

Example 3:

- (a) MK 000 Computer shall operate as specified under the following environments, either singly or combined:
 

Vibration:	Vehicle Motion 10-25 Hz at 2.5g
Roll:	47°
Pitch:	10°
Yaw:	20°
Temperature:	45°F to 80°F
Humidity:	to 95%
Input Power:	Nominal 440 Hz 110V ± 20%
- (b) The AN/ARC-000 shall meet its performance requirements when subjected to the mission temperature profile, as illustrated in Figure 6.2-2.

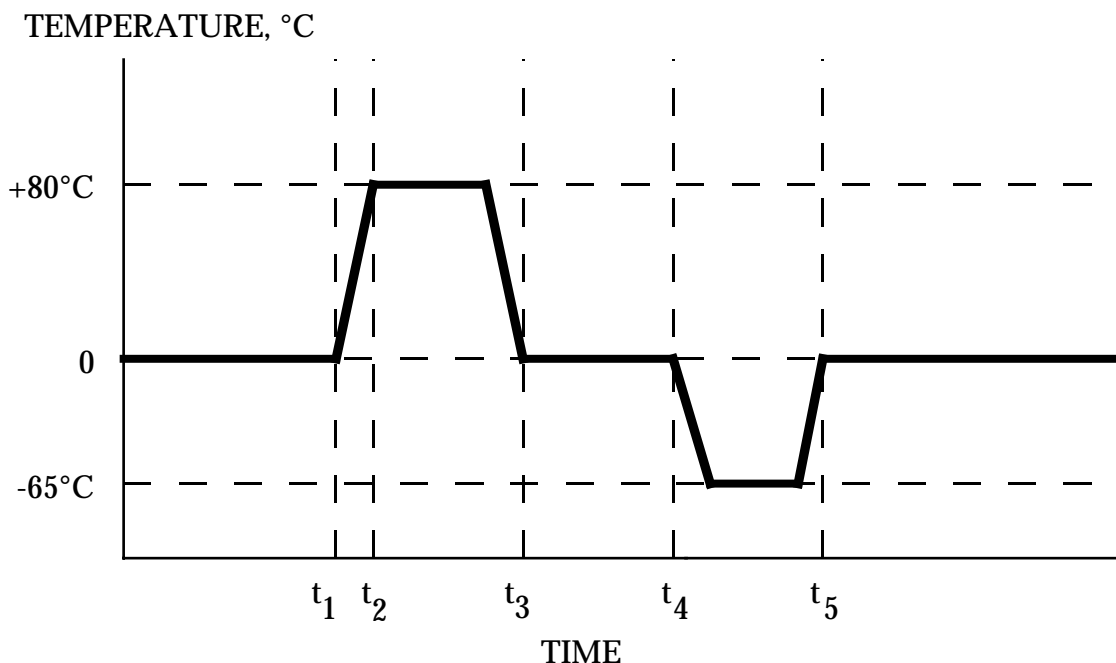
SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

FIGURE 6.2-2: TEMPERATURE PROFILE

Many individual specifications for specific categories of systems provide environmental classifications which may be referenced, providing the standard environments adequately cover the specified system's planned use. The practice of stating extreme environmental ranges for systems which will be used under controlled or limited conditions leads to undue costs.

### 6.2.3 Time Measure or Mission Profile

Time is vital to the quantitative description of reliability. It is the independent variable in the reliability function. The system usage from a time standpoint, in large measure, determines the form of the reliability expression of which time is an integral part. The types of mission times commonly encountered are given in Figure 6.2-3. For those cases where a system is not designed for continuous operation, a total anticipated time profile or time sequences of operation should be defined, either in terms of duty cycles or profile charts.

#### Example 4:

The mission reliability for an airborne fire control system shall be at least 0.9 for a six-hour mission having the typical operational sequence illustrated in Figure 6.2-3.



## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

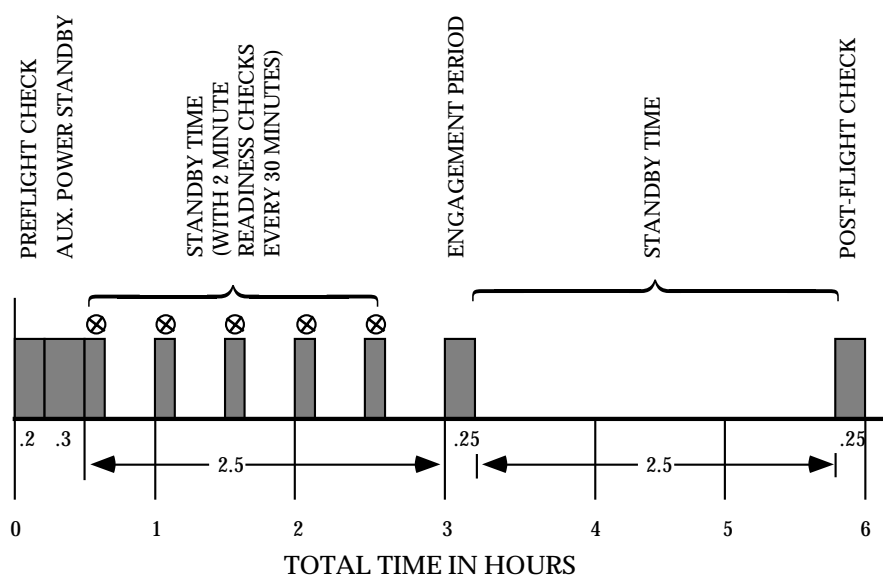


FIGURE 6.2-3: TYPICAL OPERATIONAL SEQUENCE FOR AIRBORNE FIRE CONTROL SYSTEM

From the example it can be seen that a large portion of time is standby time rather than full power-on time.

### 6.2.4 Clear Definition of Failure

A clear, unequivocal definition of "failure" must be established for the equipment or system in relation to its important performance parameters. Successful system (or equipment) performance must be defined. It must also be expressed in terms which will be measurable during the demonstration test.

Parameter measurements will usually include both go/no-go performance attributes and variable performance characteristics. Failure of go/no-go performance attributes such as channel switching, target acquisition, motor ignition, warhead detonation, etc., are relatively easy to define and measure to provide a yes/no decision boundary. Failure of a variable performance characteristic, on the other hand, is more difficult to define in relation to the specific limits outside of which system performance is considered unsatisfactory. The limits of acceptable performance are those beyond which a mission may be degraded to an unacceptable level. The success/failure boundary must be determined for each essential system performance characteristic to be measured. They must be defined in clear, unequivocal terms. This will minimize the chance for subjective interpretation of failure definition, and post-test rationalization (other than legitimate diagnosis) of observed failures.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

### 6.2.5 Description of Method(s) for Reliability Demonstration

It is not enough to merely specify the reliability requirement. One must also delineate the test(s) that will be performed to verify whether the specified requirement has been met. In essence, the element of reliability specification should answer the following questions:

- (1) How the equipment/system will be tested.
  - The specified test conditions, e.g., environmental conditions, test measures, length of test, equipment operating conditions, accept/reject criteria, test reporting requirements, etc.
- (2) Who will perform the tests.
  - Contractor, Government, independent organization.
- (3) When the tests will be performed.
  - Development, production, field operation.
- (4) Where the tests will be performed.
  - Contractor's plant, Government facility.

Examples of several forms of reliability specifications are given in Figure 6.2-4.

### 6.3 Reliability Apportionment/Allocation

#### 6.3.1 Introduction

System-level requirements are not usually sufficient to scope the design effort. For example, a requirement that a truck have an MTBF of 1000 hours doesn't help the designers of the transmission, engine, and other components. How reliable must these components be? Consequently, the requirement process for "complex" products usually involves allocating the reliability requirements to lower levels. When a product contains "few" parts, the allocation of product requirements may not be necessary or cost-effective. Functional complexity, parts counts, and challenge to the state-of-the-art are some considerations in a typical allocation process. In some cases, the process is iterative, requiring several attempts to satisfy all requirements. In other cases, the requirements can't be satisfied (components are needed with unattainable levels of reliability) and trade-off discussions with the customer may be required.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

3.2.3	<b>Reliability</b>
(1)	Avionics
3.2.3.1	<b>Operational Stability.</b> The equipment shall operate with satisfactory performance, continuously or intermittently, for a period of at least _____ hours or _____ year (whichever occurs first) without the necessity for readjustment of any controls which are inaccessible to the operator during normal use.
3.2.3.2	<b>Operating Life.</b> The equipment shall have a minimum total operating life of _____ hours with reasonable servicing and replacement of subassemblies. Complete information on parts requiring scheduled replacement due to wear during the life of the equipment, and the wearout life of such subassemblies, shall be determined by the contractor and submitted to the procuring agency for approval.
3.2.3.3	<b>Reliability in Mean Time Between Failures (MTBF).</b> The equipment shall be designed to meet a _____ hour specified mean (operating) time between failure demonstration as outlined under the requirements of paragraph _____ .
(2)	Missile System
3.2.3.1	<b>System Reliability.</b> The system (excluding _____) shall have a mission reliability of _____ as a design objective and a minimum acceptable value of _____. A mission is defined as one catapult launch and recovery cycle consisting of captive flight and missile free flight, with total system performance within specifications.
3.2.3.2	<b>Missile Free Flight Reliability.</b> The missile shall have a free flight reliability of _____ as a design objective and _____ as a minimum acceptable value. Free flight is defined as the mission profile from launch to target including motor action, guidance to target with terminal fuze and warhead actions within specifications.
3.2.3.3	<b>Missile Captive Flight Reliability.</b> The missile shall have a captive flight MTBF of _____ hours as a design objective and _____ hours as a minimum acceptable value. Captive flight includes catapult launch or take-off and recovery, accrued flight time, and missile component operation within specifications up to missile launch. The missile shall have a _____ percent probability of surviving _____ successive captive-flight cycles of _____ hours each without checkout or maintenance as a design objective, and a _____ percent probability of surviving _____ successive captive-flight cycles without checkout or maintenance as the minimum acceptable value.
(3)	Aircraft
3.2.3.1	<b>Mission Reliability.</b> The mission reliability expressed as the probability that the Airplane Weapon System can perform all the mission functions successfully, shall equal or exceed _____ based on a _____ mission duration, with _____ as a goal.
3.2.3.2	<b>Refly Reliability.</b> The refly reliability, expressed as the probability that the Airplane Weapon System can be returned to full operating capability without corrective maintenance between missions, shall equal or exceed _____ based on a _____ mission duration, with _____ as a goal .
3.2.3.3	<b>Aircraft Equipment Subsystem Reliability.</b> The avionics equipment/aircraft installation shall have a design objective mean time between failure (MTBF) of _____ hours and a minimum acceptable MTBF of _____ hours. The launcher minimum acceptable reliability shall be _____ .

FIGURE 6.2-4: EXAMPLE DEFINITION OF RELIABILITY DESIGN REQUIREMENTS IN A SYSTEM SPECIFICATION FOR (1) AVIONICS, (2) MISSILE SYSTEM AND (3) AIRCRAFT

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

The allocation of system reliability involves solving the basic inequality:

$$f(\hat{R}_1, \hat{R}_2, \dots, \hat{R}_n) \geq R^* \quad (6.1)$$

where:

- $\hat{R}_i$  is the allocation reliability parameter for the  $i^{\text{th}}$  subsystem
- $R^*$  is the system reliability requirement parameter
- $f$  is the functional relationship between subsystem and system reliability

For a simple series system in which the  $\hat{R}$ 's represent probability of survival for  $t$  hours, Eq. (6.1) becomes:

$$\hat{R}_1(t) \cdot \hat{R}_2(t) \dots \cdot \hat{R}_n(t) \geq R^*(t) \quad (6.2)$$

Theoretically, Eq. (6.2) has an infinite number of solutions, assuming no restrictions on the allocation. The problem is to establish a procedure that yields a unique or limited number of solutions by which consistent and reasonable reliabilities may be allocated. For example, the allocated reliability for a simple subsystem of demonstrated high reliability should be greater than for a complex subsystem whose observed reliability has always been low.

The allocation process is approximate. The reliability parameters apportioned to the subsystems are used as guidelines to determine design feasibility. If the allocated reliability for a specific subsystem cannot be achieved at the current state of technology, then the system design must be modified and the allocations reassigned. This procedure is repeated until an allocation is achieved that satisfies the system level requirement, within all constraints, and results in subsystems that can be designed within the state of the art.

In the event that it is found that, even with reallocation, some of the individual subsystem requirements cannot be met within the current state of the art, the designer must use one or any number of the following approaches (assuming that they are not mutually exclusive) in order to achieve the desired reliability:

- (1) Find more reliable component parts to use.
- (2) Simplify the design by using fewer component parts, if this is possible without degrading performance.
- (3) Apply component derating techniques to reduce the failure rates below the averages.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

- (4) Use redundancy for those cases where (1), (2) and (3) do not apply.

It should be noted that the allocation process can, in turn, be performed at each of the lower levels of the system hierarchy, e.g., equipment, module, component.

This section will discuss six different approaches to reliability allocation. These approaches differ in complexity, depending upon the amount of subsystem definition available and the degree of rigor desired to be employed. References [2] through [5] contain a more detailed treatment of allocation methods, as well as a number of more complex examples.

### 6.3.2 Equal Apportionment Technique

In the absence of definitive information on the system, other than the fact that “n” subsystems are to be used in series, equal apportionment to each subsystem would seem reasonable. In this case, the nth root of the system reliability requirement would be apportioned to each of the “n” subsystems.

The equal apportionment technique assumes a series of “n” subsystems, each of which is to be assigned the same reliability goal. A prime weakness of the method is that the subsystem goals are not assigned in accordance with the degree of difficulty associated with achievement of these goals. For this technique, the model is:

$$R^* = \prod_{i=1}^n R_i^* \quad (6.3)$$

or

$$R_i^* = (R^*)^{1/n} \text{ for } i = 1, 2, \dots, n \quad (6.4)$$

where:

- $R^*$  is the required system reliability
- $R_i^*$  is the reliability requirement apportioned to subsystem “i,” and each subsystem has the same reliability requirement

#### Example 5:

Consider a proposed communication system which consists of three subsystems (transmitter, receiver, and coder), each of which must function if the system is to function. Each of these subsystems is to be developed independently. Assuming each to be equally expensive to develop, what reliability requirement should be assigned to each subsystem in order to meet a system requirement of 0.729?

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

The apportioned subsystem requirements are found as:

$$R_T^* = R_R^* = R_C^* = (R^*)^{1/n} = (0.729)^{1/3} = 0.90$$

Then a reliability requirement of 0.90 should be assigned to each subsystem.

### 6.3.3 ARINC Apportionment Technique (Ref. [6])

This method assumes series subsystems with constant failure rates, such that any subsystem failure causes system failure and that subsystem mission time is equal to system mission time. This apportionment technique requires expression of reliability requirements in terms of failure rate.

The following steps apply:

- (1) The objective is to choose  $\lambda_i^*$  such that:

$$\sum_{i=1}^n \lambda_i^* \leq \lambda^* \quad (6.5)$$

where:

$\lambda_i^*$  is the failure rate allocated to subsystem “i”

$\lambda^*$  is the maximum allowable failure rate

- (2) Determine the subsystem failure rates ( $\lambda_i$ ) from past observation or estimation
- (3) Assign a weighting factor ( $w_i$ ) to each subsystem according to the failure rates determined in (2) above

$$w_i = \frac{\lambda_i}{\sum_{i=1}^n \lambda_i} \quad (6.6)$$

- (4) Allocate subsystem failure rate requirements

$$\lambda_i^* = w_i \lambda^* \quad (6.7)$$

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

### Example 6:

To illustrate this method, consider a system composed of three subsystems with predicted failure rates of  $\lambda_1 = 0.003$ ,  $\lambda_2 = 0.001$ , and  $\lambda_3 = 0.004$  failures per hour, respectively. The system has a mission time of 20 hours and 0.90 reliability is required. Find the subsystem requirements.

The apportioned failure rates and reliability goals are found as follows:

$$(1) \quad R^*(20) = \exp [-\lambda^* (20)] = 0.90$$

Solving (1) for  $\lambda^*$  gives

$$\lambda^* = 0.005 \text{ failures per hour}$$

$$(2) \quad \lambda_1 = 0.003, \quad \lambda_2 = 0.001, \quad \lambda_3 = 0.004$$

$$(3) \quad w_1 = \frac{0.003}{0.003 + 0.001 + 0.004} = 0.375$$

$$w_2 = \frac{0.001}{0.003 + 0.001 + 0.004} = 0.125$$

$$w_3 = \frac{0.004}{0.003 + 0.001 + 0.004} = 0.5$$

$$(4) \quad \lambda_1^* = 0.375(0.005) = 0.001875$$

$$\lambda_2^* = 0.125(0.005) = 0.000625$$

$$\lambda_3^* = 0.5(0.005) = 0.0025$$

(5) The corresponding allocated subsystem reliability requirements are

$$R_1^*(20) = \exp [-20 (0.001875)] = 0.96$$

$$R_2^*(20) = \exp [-20 (0.000625)] = 0.99$$

$$R_3^*(20) = \exp [-20 (0.0025)] = 0.95$$

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

6.3.4 Feasibility-Of-Objectives Technique (Ref. [7])

This technique was developed primarily as a method of allocating reliability without repair for mechanical-electrical systems. In this method, subsystem allocation factors are computed as a function of numerical ratings of system intricacy, state of the art, performance time, and environmental conditions. These ratings are estimated by the engineer on the basis of his experience. Each rating is on a scale from 1 to 10, with values assigned as discussed:

- (1) System Intricacy. Intricacy is evaluated by considering the probable number of parts or components making up the system and also is judged by the assembled intricacy of these parts or components. The least intricate system is rated at 1, and a highly intricate system is rated at 10.
- (2) State-of-the-Art. The state of present engineering progress in all fields is considered. The least developed design or method is a value of 10, and the most highly developed is assigned a value of 1.
- (3) Performance Time. The element that operates for the entire mission time is rated 10, and the element that operates the least time during the mission is rated at 1.
- (4) Environment. Environmental conditions are also rated from 10 through 1. Elements expected to experience harsh and very severe environments during their operation are rated as 10, and those expected to encounter the least severe environments are rated as 1.

The ratings are assigned by the design engineer based upon his engineering know-how and experience. They may also be determined by a group of engineers using a voting method such as the Delphi technique.

An estimate is made of the types of parts and components likely to be used in the new system and what effect their expected use has on their reliability. If particular components had proven to be unreliable in a particular environment, the environmental rating is raised.

The four ratings for each subsystem are multiplied together to give an overall rating for the subsystem. Each subsystem rating will be between 1 and 10. The subsystem ratings are then normalized so that their sum is 1.

The basic equations are:

$$\lambda_s T = \sum \bar{\lambda}_k T \quad (6.8)$$

$$\bar{\lambda}_k = C_k' \lambda_s \quad (6.9)$$



## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

where:

$\lambda_s$	=	system failure rate
T	=	mission duration
$\bar{\lambda}_k$	=	failure rate allocated to each subsystem
$C_k$	=	complexity of subsystem "k"

Further:

$$C_k' = \frac{w_k'}{W'} \quad (6.10)$$

$$w_k' = r_{1k}' r_{2k}' r_{3k}' r_{4k}' \quad (6.11)$$

$$W' = \sum_{k=1}^N w_k' \quad (6.12)$$

where:

$w_k'$	=	rating for subsystem k
$W'$	=	sum of the rated products
$r_{ik}'$	=	rating for each of the four factors for each subsystem
N	=	number of subsystems

### Example 7:

A mechanical-electrical system consists of the following subsystems: propulsion, ordnance, guidance, flight control, structures, and auxiliary power. A system reliability of 0.90 in 120 hours is required. Engineering estimates of intricacy, state-of-the-art, performance time, and environments can be made. The subsystems and their ratings are described in Table 6.3-1, Columns 1-5. Compute the allocated failure rate for each subsystem.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

<u>Procedure</u>	<u>Example</u>
(1) Compute the product of the rating $r_i$ for each subsystem and their sums, i.e., fill in column 6, Table 6.3-1 by Eq. (6.11) and (6.12).	$w_1 = 5 \cdot 6 \cdot 5 \cdot 5 = 750$ $w_6 = 6 \cdot 5 \cdot 5 \cdot 5 = 750$ $W' = 750 + 840 + 2500 + 2240 + 640 + 750 = 7720$
(2) Compute the complexity factors $C_k$ for each subsystem, i.e., fill in Column 7, Table 6.3-1 by Eq. (6.10).	$C_1 = 750/7720 = 0.097$ $C_6 = 750/7720 = 0.097$
(3) Compute system failure rate $\lambda_s$ from system specifications; $R=0.90$ and $T=120$ hr.	$\lambda_s = -\ln(0.90)/120 \text{ hr}$ $\lambda_s = 878.0 \text{ per } 10^6 \text{ hr}$
(4) Compute the allocated subsystem failure rate $\lambda_k$ , i.e., fill in Column 8, Table 6.3-1 by Eq. (6.9).	$\bar{\lambda}_1 = 0.097 \cdot (878.0 \text{ per } 10^6 \text{ hr})$ $\bar{\lambda}_1 = 85.17 \text{ per } 10^6 \text{ hr}$ $\bar{\lambda}_6 = 0.097 \times (878.0 \text{ per } 10^6 \text{ hr})$ $\bar{\lambda}_6 = 85.17 \text{ per } 10^6 \text{ hr}$
(5) Round-off failure rates, $\bar{\lambda}_k$ , so that too much accuracy will not be implied; sum and compare with $\lambda_s$ , Step (3).	$\sum_{k=1}^{k=6} \bar{\lambda}_k = 85+96+284+255+73+85$ $\sum \bar{\lambda}_k = 878$ $\sum \bar{\lambda}_k \text{ compare to } \lambda_s$ $878 \leq 878$

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

TABLE 6.3-1: MECHANICAL-ELECTRICAL SYSTEM

(1) Subsystem	(2) Intricacy $r'_1$	(3) State-of- the-art $r'_2$	(4) Performance time $r'_3$	(5) Environmentr ' <sub>4</sub>	(6) Overall Rating $w'_k$	(7) Complexity $C'_k$	(8) Allocated Failure Rate (per $10^6$ hours)
1. Propulsion	5	6	5	5	750	.097	85
2. Ordnance	7	6	10	2	840	.109	96
3. Guidance	10	10	5	5	2500	.324	284
4. Flight Control	8	8	5	7	2240	.290	255
5. Structure	4	2	10	8	640	.083	73
6. Auxiliary Power	6	5	5	5	750	.097	85
Total					7720	1.000	878

System reliability = 0.90

Mission time = 120 hours

$\lambda_s = 878$  failures per  $10^6$  hours

### 6.3.5 Minimization of Effort Algorithm

This algorithm considers minimization of total effort expended to meet system reliability requirements. It assumes a system comprised of  $n$  subsystems in series. Certain assumptions are made concerning the effort function. It assumes that the reliability of each subsystem is measured at the present stage of development, or is estimated, and apportions reliability such that greater reliability improvement is demanded of the lower reliability subsystems.

Let  $R_1, R_2, \dots, R_n$  denote subsystem reliabilities, and the system reliability  $R$  would be given by:

$$R = \prod_{i=1}^n R_i \quad (6.13)$$

Let  $R^*$  be the required reliability of the system, where  $R^* > R$ . It is then required to increase at least one of the values of the  $R_i$  to the point that the required reliability  $R^*$  will be met. To accomplish such an increase takes a certain effort, which is to be allocated in some way among the subsystems. The amount of effort would be some function of the number of tests, amount of engineering manpower applied to the task, etc.

The algorithm assumes that each subsystem has associated with it the same effort function,  $G(R_i, R_i^*)$ , which measures the amount of effort needed to increase the reliability of the  $i^{\text{th}}$  subsystem from  $R_i$  to  $R_i^*$ .

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

The problem, then, is to determine  $R_i^*$  such that:

$$\sum_{i=1}^n G(R_i, R_i^*) \quad (6.14)$$

is minimized subject to the condition:

$$\prod_{i=1}^n R_i^* = R^* \quad (6.15)$$

With the preceding assumptions, it can be shown that the unique solution is:

$$R_i^* = \begin{cases} R_o^* & \text{if } i \leq K_o \\ R_i & \text{if } i > K_o \end{cases}$$

where the subsystem reliabilities  $R_1, R_2, \dots, R_n$  are ordered in an increasing fashion (assuming such an ordering is implicit in the notation).

$$R_1 \leq R_2 \leq \dots \leq R_n$$

and the number  $K_o$  is determined as:

$K_o =$  maximum value of  $j$  such that

$$R_j < \left[ \frac{R^*}{\prod_{i=j+1}^{n+1} R_i} \right]^{1/j} = r_j \quad (6.16)$$

where  $R_{n+1} = 1$  by definition.

The number  $R_o^*$  is determined as

$$R_o^* = \left[ \frac{R^*}{\prod_{j=K_o+1}^{n+1} R_j} \right]^{1/K_o} \quad (6.17)$$

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

It is evident that the system reliability will then be  $R^*$ , since the new reliability is:

$$(R_o^*)^{K_o} (R_{K_o+1}) \dots (R_{n+1}) = (R_o^*)^{K_o} \left( \prod_{j=K_o+1}^{n+1} R_j \right) = R^* \quad (6.18)$$

when the relationship for  $R_o^*$  is substituted.

Example 8:

As an example, consider a system that consists of three subsystems (A, B, and C), all of which must function without failure in order to achieve system success. The system reliability requirement has been set at 0.70. We have predicted subsystem reliabilities as  $R_A = 0.90$ ,  $R_B = 0.80$ , and  $R_C = 0.85$ . How should we apportion reliability to the subsystem in order that the total effort be minimized and that the system reliability requirement be satisfied? Assume identical effort functions for the three subsystems.

The resulting minimum effort apportionment goals are found as follows:

- (1) Arrange subsystem reliability values in ascending order:

$$R_1 = R_B = 0.80, \quad R_2 = R_C = 0.85, \quad R_3 = R_A = 0.90$$

- (2) Determine  $K_o$ , the maximum value of  $j$ , such that:

$$R_j < \left[ \frac{R^*}{\prod_{i=j+1}^{n+1} R_i} \right]^{1/j} = r_j$$

- (3) When  $j = 1$ ,

$$R_1 = 0.80 < r_1 = \frac{0.7}{R_2 R_3 (1.0)} = \frac{0.7}{(0.85)(0.9)(1.0)} = \frac{0.7}{0.765} = 0.915$$

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

Note that  $R_{n+1}$  was previously defined as 1 (Eq. 6.16).

(4) When  $j = 2$ ,

$$R_2 = 0.85 < r_2 = \left( \frac{0.7}{(0.9)(1.0)} \right)^{1/2} = \left( \frac{0.7}{0.9} \right)^{1/2} = 0.882$$

(5) When  $j = 3$ ,

$$R_3 = 0.90 > r_3 = \left( \frac{0.7}{1.0} \right)^{1/3} = 0.888$$

(6) Since  $R_1 < r_1$ ,  $R_2 < r_2$ , but  $R_3 > r_3$ , then  $K_O = 2$  because 2 is the largest subscript  $j$  such that  $R_j < r_j$ . Thus,

$$R_O^* = \left( \frac{0.7}{0.9} \right)^{1/2} = 0.882$$

which means that the effort is to be allotted so that subsystem B increases in reliability from 0.80 to 0.882, and subsystem C increases in reliability from 0.85 to 0.882, whereas subsystem A is left alone with a reliability of 0.90. The resulting reliability of the entire system is, as required,  $0.70 = (0.882)^2(0.90)$ . This means that effort should be expended on subsystems C and B to raise their respective reliabilities to 0.882 with no developmental effort spent on subsystem A. This policy would minimize the total expended effort required to meet system reliability requirements. The minimization, however, is dependent upon the effort in meeting the initial assumptions, which may not be possible.

## 6.4 Reliability Modeling and Prediction

### 6.4.1 Introduction

Reliability modeling and prediction are essential functions in evaluating a design. The real worth of the quantitative expression lies in the information conveyed with the numerical value and the use which is made of that information. Reliability models and predictions do not, in themselves, contribute significantly to system reliability.

Predictions do, however, provide a rational basis for design decisions such as the choice between alternative concepts, choice of part quality levels, derating factors to be applied, use of proven versus state-of-the-art techniques, and other factors. Some of the important uses of reliability models and predictions are summarized in Table 6.4-1.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

Reliability models and predictions are not used as a basis for determining the attainment of reliability requirements. Attainment of these requirements is based on representative test results such as those obtained by using tests plans from MIL-HDBK-781 (see Section 8 and Ref. [1]). However, predictions are used as the basis against which reliability performance is measured. Therefore, all ground rules and assumptions used in the prediction process must be thoroughly understood and carefully documented.

Reliability modeling and prediction is a methodology for estimating an item's ability to meet specified reliability requirements. A Mission Reliability prediction estimates the probability that an item will perform its required functions during the mission. A Basic Reliability prediction estimates the demand for maintenance and logistic support caused by an item's unreliability. When used in combination, the two predictions provide a basis for identifying areas wherein special emphasis or attention is needed, and for comparing the ownership cost-effectiveness of various design configurations. The two predictions may also be used as a basis for the apportionment (allocation) of ownership cost and operational effectiveness requirements to various subdivisions.

Reliability modeling and prediction should be initiated early in the configuration definition stage to aid in the evaluation of the design and to provide a basis for item reliability allocation (apportionment) and establishing corrective action priorities. Reliability models and predictions are updated when there is a significant change in the item design, availability of design details, environmental requirements, stress data, failure rate data, or service use profile.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

TABLE 6.4-1: USES OF RELIABILITY MODELS AND PREDICTIONS

- (1) Evaluate reliability requirements in planning documents, preliminary design specifications and requests for proposals, and determination of the feasibility of proposed reliability requirements.
- (2) Compare established reliability requirements with state-of-the-art feasibility, and provide guidance in budget and schedule decisions.
- (3) Provide a basis for uniform proposal preparation, evaluation and contractor selection.
- (4) Evaluate potential reliability through predictions submitted in technical proposals and reports in pre-contract transactions.
- (5) Identify and rank potential problem areas and suggest possible solutions.
- (6) Allocate reliability requirements among the subsystems and lower-level items.
- (7) Evaluate the choice of proposed parts, materials, and processes.
- (8) Conditionally evaluate the design before prototype fabrication.
- (9) Provide a basis for trade-off analysis and evaluate design alternatives.

#### 6.4.2 General Procedure

The steps set forth below define the procedure for developing a reliability model and performing a reliability prediction. Effort to develop the information, for the steps below, should be closely coordinated with related program activities (such as design engineering, system engineering, maintainability, and logistics) to minimize duplications and to assure consistency and correctness. Comprehensive documentation of all the following definitions, their sources, ground rules and assumptions, and limitations of data is essential for the success of follow-on activities (Sections 7 and 8).

- (1) Define the item for which the prediction is applicable.
- (2) Define the service use (life cycle) for which item reliability will be modeled and predicted.
- (3) Define the item reliability block diagrams.



## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

- (4) Define the mathematical or simulation models for computing item reliability.
- (5) Define the parts of the item.
- (6) Define the environmental profile and expected conditions.
- (7) Define the stress conditions.
- (8) Define the failure distribution.
- (9) Define the failure rates.
- (10) Compute the item reliability.

### 6.4.2.1 Item Definition

Item definition includes performance requirements and hardware concept to the extent known at the time the model and prediction are prepared. Characteristics of the item are stated in terms of range, altitude, speed, maneuverability, environmental conditions, power, or such other parameters as may be applicable. The manner in which the item and its subdivision operate is usually expressed by means of functional diagrams which become the basis for the reliability block diagrams. Normally, the initial item definition used for the feasibility prediction will be lacking several details and will require certain assumptions as to environmental conditions, design configuration, etc. The item definition is defined and updated as more information becomes available to support the preliminary design prediction, and subsequently, the detailed design prediction. As the item description is progressively updated, higher levels of accuracy will be attained for prediction results.

### 6.4.2.2 Service Use Profile

The service use (life cycle) profile is a thorough description of all events and environments associated with an item from final factory acceptance through its terminal expenditure or removal from inventory. Each significant service use event, such as transportation, storage, test and checkout, operational deployment, etc., is addressed. Figure 6-4-1 illustrates the major service use events to be considered in the logistic and operational cycles. The profile depicts expected time spans, environments, operating modes (including standby and ready modes), etc., for each event. Information from logistic cycles, operational cycles, mission profiles, and environmental profiles is used to develop the service use profile.

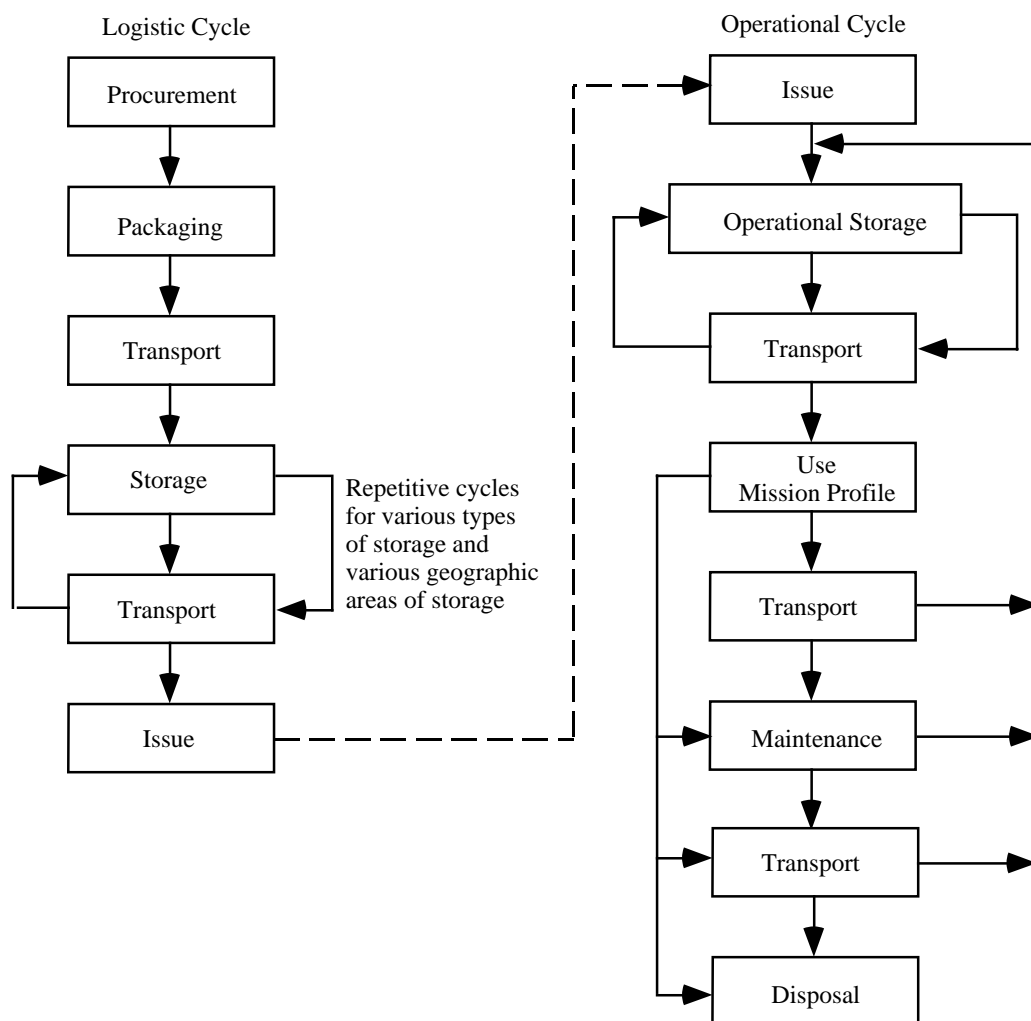
SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
 AND PREDICTION


FIGURE 6.4-1: SERVICE USE EVENTS IN THE LOGISTIC AND OPERATIONAL CYCLES

- (1) Logistic cycle describes the expected duration and sequence of events which maintain, transport, and store an item to assure operational availability.
- (2) Operational cycle describes the expected duration and sequence of events of the period from an item's assignment to an operational user through expenditure or return to some phase of the logistic cycle.
- (3) Mission profile describes events and conditions associated with a specific operational usage of an item. A mission profile is one segment of the operational cycle. The profile depicts the time spans of the events and operational conditions to be anticipated.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

Multiple mission profiles may be required to adequately describe an item's multimission capabilities.

- (4) Environmental profile describes the specific natural and induced environments (nominal and worst case) with the operations, events, and functions described by the logistic and operational cycles. Each mission profile has an associated environmental profile.

### 6.4.2.3 Reliability Block Diagrams

Reliability block diagrams are prepared to show interdependencies among all elements (subsystems, equipments, etc.) or functional groups of the item for item success in each service use event. The purpose of the reliability block diagram is to show by concise visual shorthand the various series-parallel block combinations (paths) that result in item success. A complete understanding of the item's mission definition, and service use profile is required to produce the reliability diagram.

### 6.4.2.4 Mathematical/Simulation Models

Models need to be derived to relate reliability block diagrams to time-event relationships and failure rate data. This can be done through purely mathematical means or computer generated simulation models. The solution of the models will be the item predicted reliability. The mathematical model shall be capable of being readily updated with information resulting from reliability and other relevant tests as well as changes in item configuration, mission parameters and operational constraints.

### 6.4.2.5 Part Description

Part and application descriptions needs to be provided for any prediction based upon part failure rates. The part identification number from the schematic diagram, the applicable specification and the specification type number needs to be included.

### 6.4.2.6 Environmental Data

Environmental data affecting part failure rates must be defined. These data include the specific natural and induced environments (nominal and worst case) associated with the operations, events, and functions described by the logistic and operational cycles.

### 6.4.2.7 Stress Analysis

Analyses will be performed to determine the operating stresses to be experienced by each part commensurate with the prediction classification and the design detail available. Failure rates can be modified by appropriate factors to account for the effect of applied stress. Stress ratios cited

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

in the prediction report shall be individually identified as Estimated (E), Calculated (C), or Measured (M).

### 6.4.2.8 Failure Distributions

The failure distribution appropriate to the specific electronic, electrical, electromechanical, mechanical, and ordnance item will be in used in computation. In instances where the failure distribution for the item is not known, the Weibull failure distribution may be assumed. The failure distribution utilized needs to be cited and any assumptions substantiated in the prediction report.

### 6.4.2.9 Failure Rates

Failure rates for all electronic, electrical, electromechanical, mechanical, and ordnance items are required for each significant event and environment defined by the service use profile. All sources of failure data shall be approved by the procuring activity prior to use. Basic failure rates from most data sources must be modified with appropriate factors to account for the specific item application under consideration. Factors used shall be cited and substantiated in the prediction report.

### 6.4.2.10 Item Reliability

Item reliability will be computed using mathematical or simulation based models and applicable failure rate data. The prediction results should be expressed in terms consistent with the specified reliability requirements.

## 6.4.3 Tailoring Reliability Models and Predictions

Since the reliability prediction process is iterative in nature, tailoring of the reliability model and prediction is based primarily upon the program procurement phase. As the design progresses, the hardware relationships become better defined, thus the model of the system depicting the relationship between basic reliability and mission reliability is refined and it must be exercised iteratively to provide reliability predictions up through the system level.

Tailoring of these tasks involves, primarily, the selection of the prediction method utilized and the rigor with which it is applied. For relatively simple systems (i.e., those containing no redundant elements and without alternate modes of operation or degraded modes of operation) the basic reliability model and the mission reliability model will be identical and a single reliability prediction will suffice.

An example of tailoring based upon the procurement phase may be as follows: in the conceptual design phase reliability predictions are based primarily upon comparison with similar equipment, in the preliminary design phase, a simple part count prediction is used, in the final design phase, as more detailed design information becomes available, a detailed stress reliability prediction

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

would be made, and in the test phase, test or field data would be integrated in the prediction model.

Reliability modeling and prediction is only as accurate as the assumptions and data sources used in its preparation, and to the extent all pertinent influences are considered. The primary value of the reliability prediction is as a design tool for comparison of alternative approaches. Although the absolute value of item reliability derived by the prediction may be used in the determination of expected field use reliability, it must be used with great caution and with full disclosure of the data sources and assumptions used. As an example, when field experience data for similar items in a like environment are utilized, the prediction reflects anticipated field performance after design maturity has been achieved. Conversely, when laboratory data are utilized, the prediction reflects expected performance under laboratory conditions.

### 6.4.4 Reliability Modeling

The reliability model consists of a reliability block diagram and an associated mathematical or simulation model (Ref. [8]). Elements of the item intended for redundancy or alternate modes of operation are modeled in a parallel configuration or similar construct appropriate to the mission phase and mission application.

#### 6.4.4.1 Reliability Block Diagrams

A reliability block diagram shows the interdependencies among all elements (subsystems, equipments, etc.) or functional groups of the item for item success in each service use event. A progressive example of a reliability block diagram is illustrated in Figure 6.4-2. The purpose is to show, by concise visual shorthand, the various series-parallel block combinations (paths) that result in item success. A complete understanding of the item's mission definition, and service use profile is required.

Each reliability block diagram will have a title including identification of the item, the mission identification or portion of the service use profile addressed, and a description of the mode of operation for which the prediction is to be performed.

Each reliability block diagram should include a statement of conditions listing all constraints which influence the choice of block presentation, the reliability parameters or reliability variables utilized in the analysis, and the assumptions or simplifications utilized to develop the diagram. Once established, these conditions are observed throughout the analysis.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

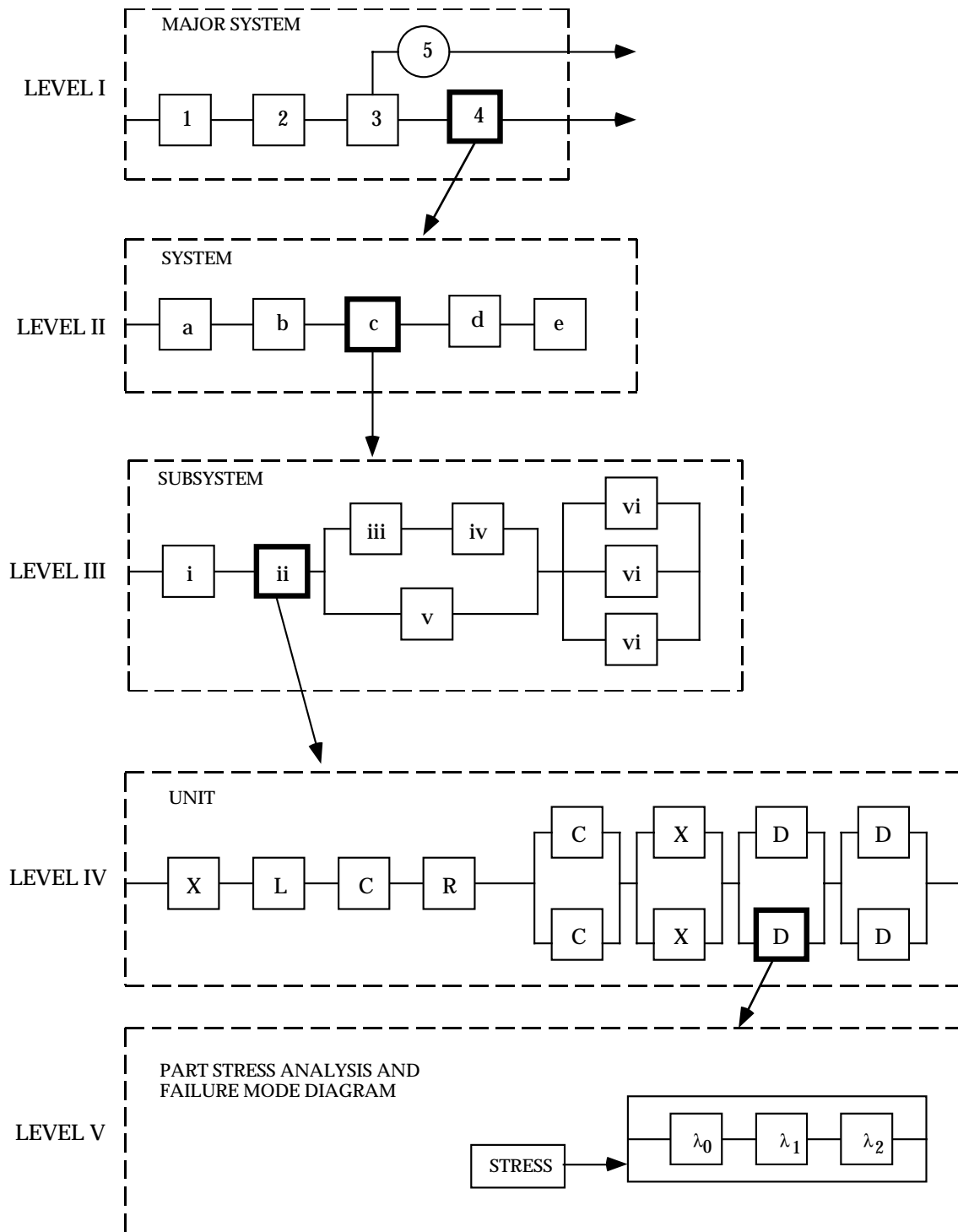


FIGURE 6.4-2: PROGRESSIVE EXPANSION OF RELIABILITY BLOCK DIAGRAM AS DESIGN DETAIL BECOMES KNOWN

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

The blocks in the diagram follow a logical order which relates the sequence of events during the prescribed operation of the item. The reliability block diagram is drawn so that each element or function employed in the item can be identified. Each block of the reliability block diagram represents one element of function contained in the item. All blocks are configured in series, parallel, standby, or combinations thereof as appropriate.

- (1) Identification of blocks. The coding system should be based upon a uniform identification system that will permit unambiguous traceability of the reliability block to its hardware (or functional) equivalent as defined in program documentation. Hardware or functional elements of the item which are not included in the reliability model are identified in a separate listing.
- (2) Reliability variable. For each block include the units of the reliability or mean life value. Examples include; time, cycles, events, etc. kekaoxing.com
- (3) Block diagram assumptions. The following general assumptions apply to reliability block diagrams:
  - (a) Blocks denote elements or functions of the items that are considered when evaluating reliability and which have reliability values associated with them.
  - (b) Lines connecting blocks have no reliability values. The lines serve only to give order to the diagram. Cabling and connectors are incorporated into a single block or included as part of the block for an element or function.
  - (c) All inputs to the item are within specification limits.
  - (d) Failure of any element or function denoted by a block in the diagram will cause failure of the entire item, except where alternative modes of operation may be present; i.e., redundant units or paths.
  - (e) Each element or function denoted by a block in the diagram is independent, with regard to probability of failure, from all other blocks.
- (4) Software reliability and human reliability assumptions. The impact of software and human reliability needs to be stated and considered in the reliability model.

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

6.4.4.2 Reliability Modeling Methods

Four reliability modeling methods presented are: the conventional probability model, the Boolean Truth table model, the logic diagram model and the simulation model. These models are described as follows:

6.4.4.2.1 Conventional Probability Modeling Method

The conventional probability method may be used to prepare a reliability mathematical model from a reliability block diagram. The conventional probability method makes use of the equations developed for redundancy to handle series, parallel, and series-parallel combinations of equipments. For non-series parallel or complex configurations, use or repeated use of the following equation is required.

$$P_S = P_S \text{ (if X is good)} R_X + P_S \text{ (if X is bad)} Q_X \quad (6.19)$$

where:

$P_S$  = reliability of mission

$P_S$  (if X is good) = reliability of mission if X is good

$P_S$  (if X is bad) = reliability of mission if X is bad

$R_X$  = reliability of X

$Q_X$  = unreliability of X =  $1 - R_X$

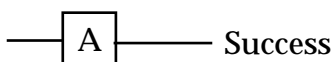
In other words, the reliability of the mission is equal to the reliability of the mission given a specific portion of the system works times the probability that the portion of the system will work plus the reliability of the mission given that the specific portion of the system fails times the probability that the portion fails.

The above formula can also be used to generate probability of success equations for series-parallel configurations.

Formulas for probability of success,  $P_S$ , for various system configurations are derived as follows for various success diagrams. Each formula shown can be used as a building block to evaluate a more complex success diagram.

6.4.4.2.1.1 Series Model

If there is only one equipment in the system and it is required, then the reliability diagram is:





## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

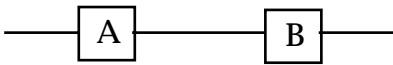
---

The probability of success for the system is obviously the probability of success of equipment A, or

$$P_S = P_A \quad (6.20)$$

The probability of A failing would be  $1 - P_A$ .

For a two equipment serial system the reliability diagram is:



The probability of success for the system is the probability of success of equipment A and B, or

$$P_S = P_A P_B \quad (6.21)$$

If A and B are identical, then

$$P_S = (P_A)^2 \quad (6.22)$$

For a three equipment serial system the reliability diagram is:

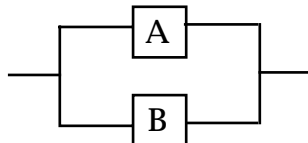


The probability of success for the system is the probability of success of equipment A, B and C, or

$$P_S = P_A P_B P_C \quad (6.23)$$

### 6.4.4.2.1.2 Parallel Models

For a two equipment active parallel system the reliability diagram is:



$$P_S = P(\text{mission success with A working}) P_A + \\ P(\text{mission success with A failed}) (1 - P_A)$$

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

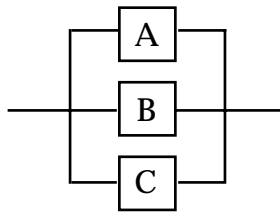
---

$$\begin{aligned}
 P_S &= (1) P_A + P_B (1 - P_A) \\
 P_S &= P_A + P_B - P_A P_B
 \end{aligned}
 \tag{6.24}$$

If A and B are identical, then

$$P_S = 2P_A - (P_A)^2 \tag{6.25}$$

For a three equipment active parallel system the reliability diagram is:

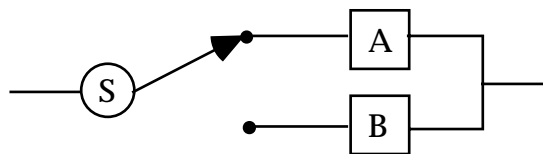


$$P_S = P_A + P_B + P_C - P_A P_B - P_A P_C - P_B P_C + P_A P_B P_C \tag{6.26}$$

If A, B, and C are identical, then

$$P_S = 3P_A - 3(P_A)^2 + (P_A)^3 \tag{6.27}$$

For a two equipment standby parallel system with a switch, the reliability diagram is:



The switch, "S," detects a failure of the operative element and instantaneously switches from the failed element to a standby element.

The switch may fail in two ways: (1) the switch may fail to operate when required,  $Q_1$  and (2) the switch may operate without command (i.e., prematurely),  $Q_2$ .  $Q_1$  and  $Q_2$  can be represented as  $(1-P_1)$  and  $(1-P_2)$  as the probability of failure (Q) plus the probability of success (P) equals one.

$$\begin{aligned}
 P_S &= P(\text{mission success with A working}) P_A + \\
 &\quad P(\text{mission success with A failed}) (1 - P_A) \\
 P_S &= P_2 P_A + (1 - P_2) P_B P_A + P_1 P_B (1 - P_A) \\
 P_S &= P_A P_B (1 - P_1 - P_2) + P_A P_2 + P_B P_1
 \end{aligned}
 \tag{6.28}$$

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

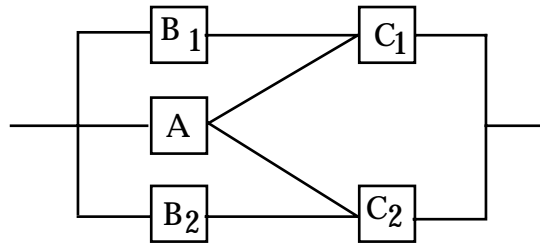
---

The equivalent series reliability mathematical model for this system is:

$$P_S = P_A P_B P_1 P_2 \quad (6.29)$$

### 6.4.4.2.1.3 Series-Parallel Models

As one example of a complex series-parallel combination of equipments the reliability diagram is:



The system requirement would be that equipment A and either equipment  $C_1$  or  $C_2$  work, or that equipments  $B_1$  and  $C_1$  work, or that  $B_2$  and  $C_2$  work for success. Equipments with the same letter are identical, i.e.,  $C_1 = C_2$  and  $B_1 = B_2$ .

$$\begin{aligned}
 P_S &= P(\text{mission success with A working}) P_A \\
 &\quad + P(\text{mission success with A failed}) (1 - P_A) \\
 P_S &= (2P_C - P_C^2) P_A + [2P_B P_C - (P_B P_C)^2] (1 - P_A) \quad (6.30)
 \end{aligned}$$

An example involving the above diagram is as follows:

Given that,

$$\begin{aligned}
 P_A &= 0.3 \\
 P_{B_1} &= P_{B_2} = 0.1 \\
 P_{C_1} &= P_{C_2} = 0.2
 \end{aligned}$$

Evaluating the probability of success for a given mission using equation 6.30 is:

$$P_S = (.4 - .04) .3 + [.04 - .0004] (.7)$$

$$P_S = 0.13572$$

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

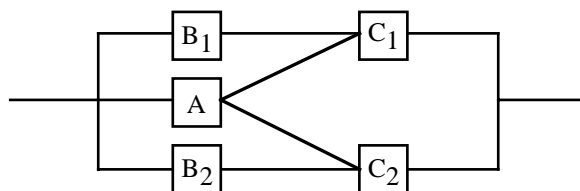
The equivalent series reliability mathematical model for this system is:

$$P_S = P_A P_B^2 P_C^2 \quad (6.31)$$

and the reliability is 0.00012.

#### 6.4.4.2.2 Boolean Truth Table Modeling Method

A Boolean Truth Table may also be used to prepare a reliability mathematical model from a reliability block diagram. This method is applicable to single functioned and malfunctioned systems. The method is more tedious than the conventional probability method but is useful when there is familiarity with Boolean algebra. The procedure for the Boolean Truth Table approach for a single function system is illustrated by the following example. The system reliability diagram is given as:



where:

$$\begin{array}{ll}
 P_A = 0.3 & 1 - P_A = 0.7 \\
 P_{B_1} = P_{B_2} = 0.1 & \text{and therefore} \quad 1 - P_B = 0.9 \\
 P_{C_1} = P_{C_2} = 0.2 & 1 - P_C = 0.8
 \end{array}$$

The Boolean algebra approach lists all equipments in a truth table form (See Table 6.4-2). The truth table has  $2^n$  entries where  $n$  is the number of equipments in the system. The table has a 1 or 0 entry in each column indicating success or failure respectively on each equipment. All possible combinations of all equipments working and failing are thus listed. The procedure is to examine each row of the truth table and decide whether the combination of equipments working and failed yields system success (S) or failure (F). Insert an S or F respectively in the next column in the table. For each S entry, multiply the respective probabilities for the indicated state of each equipment to yield a  $P_S$  for that entry.

Entry number 4 is the entry with a success indicated and .03888 is obtained by multiplying

$$(1 - P_{B_1}) (1 - P_{B_2}) (1 - P_{C_1}) P_{C_2} P_A \quad \text{or}$$

$$(.9) (.9) (.8) (.2) (.3) = .03888$$

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

All figures in the  $P_S$  column are then added for a system reliability probability of .13572 in this example.

The equivalent series reliability mathematical model for this system is:

$$P_S = P_A P_{B_1} P_{B_2} P_{C_1} P_{C_2} \quad (6.32)$$

and the probability is 0.00012.

A Boolean algebra reliability equation can be written from the truth table (Table 6.4-2) if it is desired. In this case it would look like the following:

$$\begin{aligned} P_S = & \bar{B}_1 \bar{B}_2 \bar{C}_1 C_2 A + \bar{B}_1 \bar{B}_2 C_1 \bar{C}_2 A + \bar{B}_1 \bar{B}_2 C_1 C_2 A + \bar{B}_1 B_2 \bar{C}_1 C_2 \bar{A} + \bar{B}_1 B_2 \bar{C}_1 C_2 A + \bar{B}_1 B_2 C_1 \bar{C}_2 A + \\ & \bar{B}_1 B_2 C_1 C_2 \bar{A} + \bar{B}_1 B_2 C_1 C_2 A + B_1 \bar{B}_2 \bar{C}_1 C_2 A + B_1 \bar{B}_2 C_1 \bar{C}_2 \bar{A} + B_1 \bar{B}_2 C_1 \bar{C}_2 A + B_1 \bar{B}_2 C_1 C_2 \bar{A} + \\ & B_1 \bar{B}_2 C_1 C_2 A + B_1 B_2 \bar{C}_1 C_2 \bar{A} + B_1 B_2 \bar{C}_1 C_2 A + B_1 B_2 C_1 \bar{C}_2 \bar{A} + B_1 B_2 C_1 \bar{C}_2 A + B_1 B_2 C_1 C_2 \bar{A} + B_1 B_2 C_1 C_2 A \end{aligned} \quad (6.33)$$

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTIONTABLE 6.4-2: TRUTH TABLE CALCULATION FOR THE  
SYSTEM RELIABILITY DIAGRAM

Entry No.	B <sub>1</sub>	B <sub>2</sub>	C <sub>1</sub>	C <sub>2</sub>	A	Success OR FAILURE	P <sub>S</sub>
1	0	0	0	0	0	F	-
2	0	0	0	0	1	F	-
3	0	0	0	1	0	F	-
4	0	0	0	1	1	S	.03888
5	0	0	1	0	0	F	-
6	0	0	1	0	1	S	.03888
7	0	0	1	1	0	F	-
8	0	0	1	1	1	S	.00972
9	0	1	0	0	0	F	-
10	0	1	0	0	1	F	-
11	0	1	0	1	0	S	.01008
12	0	1	0	1	1	S	.00432
13	0	1	1	0	0	F	-
14	0	1	1	0	1	S	.00432
15	0	1	1	1	0	S	.00252
16	0	1	1	1	1	S	.00108
17	1	0	0	0	0	F	-
18	1	0	0	0	1	F	-
19	1	0	0	1	0	F	-
20	1	0	0	1	1	S	.00432
21	1	0	1	0	0	S	.01008
22	1	0	1	0	1	S	.00432
23	1	0	1	1	0	S	.00252
24	1	0	1	1	1	S	.00108
25	1	1	0	0	0	F	-
26	1	1	0	0	1	F	-
27	1	1	0	1	0	S	.00112
28	1	1	0	1	1	S	.00048
29	1	1	1	0	0	S	.00112
30	1	1	1	0	1	S	.00048
31	1	1	1	1	0	S	.00028
32	1	1	1	1	1	S	.00012
$\Sigma$ All success paths = .13572							

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

A bar above a letter indicates the complement or unreliability, e.g.,  $\bar{A} = (1 - A)$ .

With the aid of a reduction technique the nineteen terms of (6.33) can be reduced as follows:

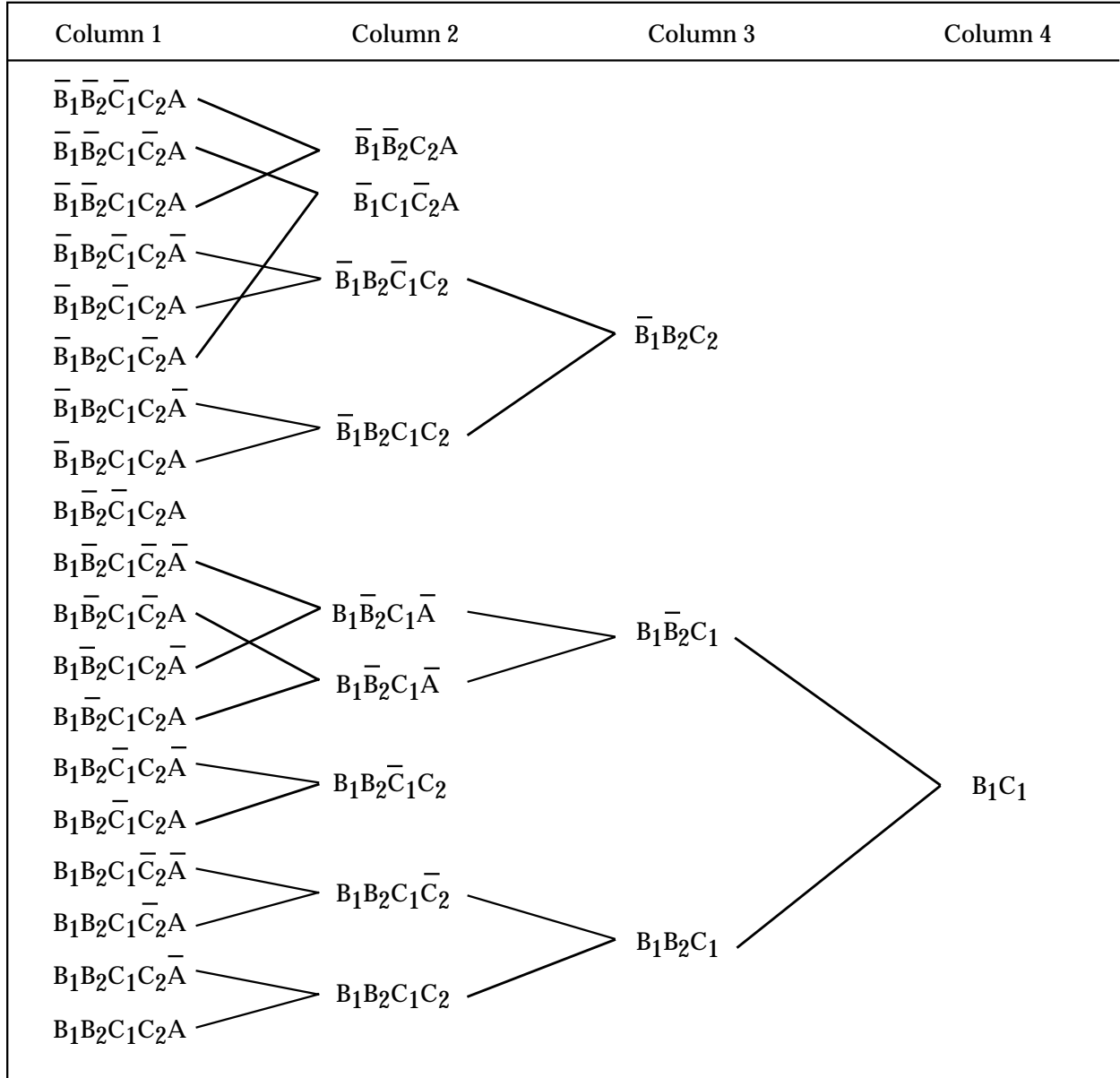
- (1) A reduction table (Table 6.4-3) is constructed which allows the reduction of the 19 Boolean success terms to a simplified expression for the given mission reliability model. All 19 success paths are first listed in Column 1 of Table 6.4-3.
- (2) By a comparative process, product pairs are formed for those terms in Column 1 of Table 6.4-3 which differ only by a letter inverse, thus forming a new product term which has this letter missing. For example, in Column 1 the two terms  $\bar{B}_1 \bar{B}_2 \bar{C}_1 C_2 A$  and  $\bar{B}_1 \bar{B}_2 C_1 C_2 A$  differ only in the letter  $C_1$  and therefore can be combined to form the product term  $\bar{B}_1 \bar{B}_2 C_2 A$  entered in Column 2. Again, this process is repeated by comparing product terms in Column 2 which differ only by a letter inverse, thus forming a new product term which is then entered in Column 3. It should be noted that once a term is used in a comparison, it is eliminated from all further comparisons, thus ensuring that all remaining terms are still mutually exclusive. The order of terms selected for the comparison process in Table 6.4-3 is not a necessary consideration; the resulting disjoint group of Boolean terms can always be interpreted, on a one-for-one basis, as the simplified probability of success (reliability) expression. For the given model, the probability of success has been reduced to the following terms:
- (3) Substituting the reliabilities and unreliabilities used previously into (equation 6.34), we obtain:

$$P_S = (.1)(.2) + (.9)(.1)(.2) + (.9)(.9)(.2)(.3) + (.9)(.2)(.8)(.3) + (.1)(.1)(.8)(.2) + (.1)(.9)(.8)(.2)(.3) = .13572$$

which is the same probability of success shown in the summation for Table 6.4-2.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

TABLE 6.4-3: REDUCTION TABULATION



$$\begin{aligned}
 P_S = & B_1 C_1 + \bar{B}_1 B_2 C_2 + \bar{B}_1 \bar{B}_2 C_2 A + \bar{B}_1 C_1 \bar{C}_2 A + B_1 \bar{B}_2 \bar{C}_1 C_2 \\
 & + B_1 \bar{B}_2 \bar{C}_1 C_2 A
 \end{aligned}
 \tag{6.34}$$



## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

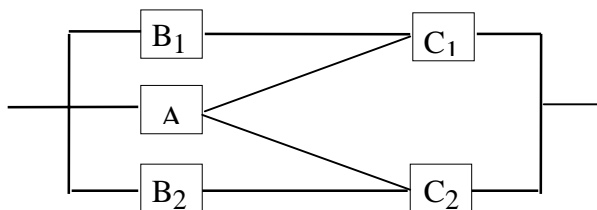
### 6.4.4.2.3 Logic Diagram Modeling Method

Logic diagrams may also be used to prepare a reliability mathematical model from a reliability block diagram. This method is applicable to single functioned and multifunctioned systems. This method is more tedious than the conventional probability method but is a short cut method for the Boolean truth table approach in combining terms to simplify the reliability equation.

The logic diagram procedure for a single function system is to translate the reliability block diagram into a switching network. A closed contact represents equipment success, an open contact equipment failure. Each complete path of contacts represents an alternate mode of operation. Each equipment that is required for each alternative mode of operation is identified by a contact along a path. All paths terminate at the same point (success). The logic diagram is developed so that all paths are mutually exclusive; by use of a few simple manipulations, the amount of effort involved over the Boolean truth table method can be shortened.


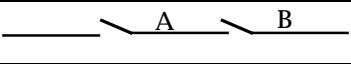
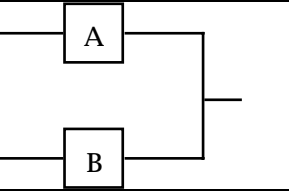
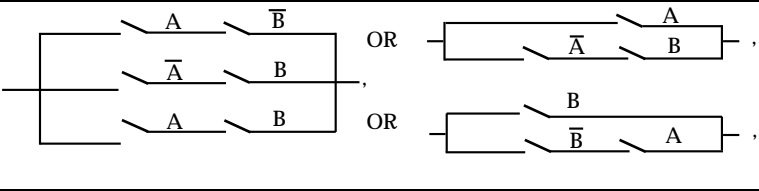
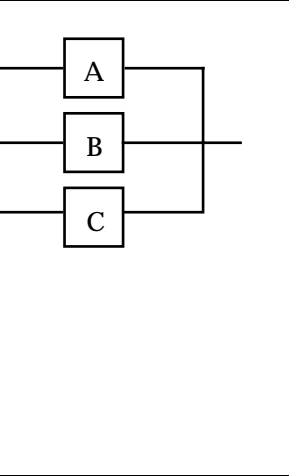
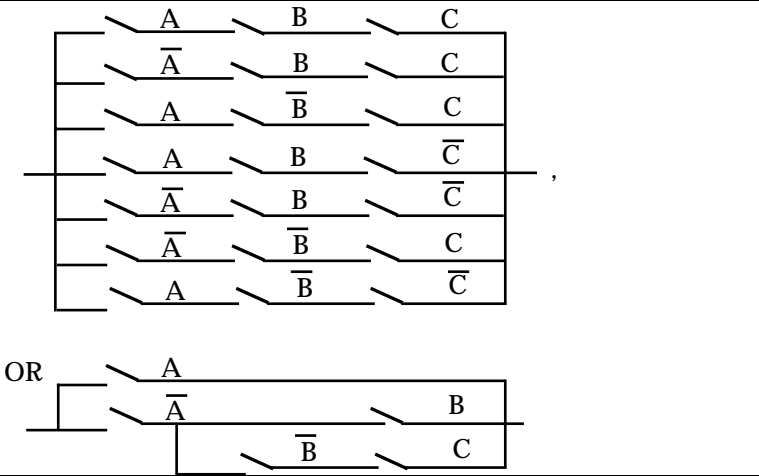
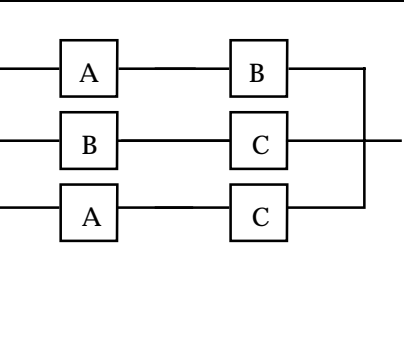
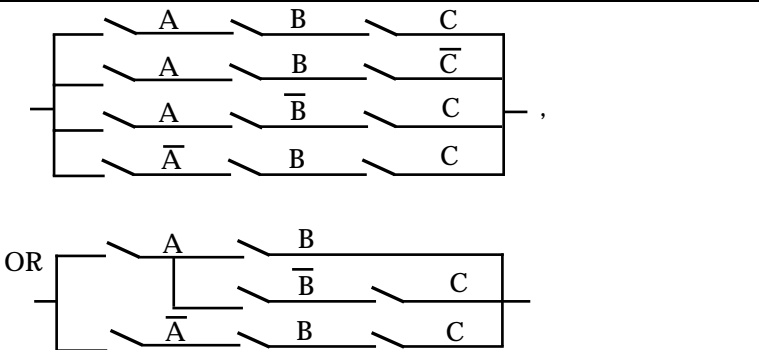
Logic diagrams for series, parallel, and series-parallel diagrams are easy to draw as shown in Table 6.4-4.

For complex configurations the procedure is to reduce the reliability diagram to a series-parallel configuration by successively splitting the diagram into subdiagrams by removing one equipment and replacing it with a short circuit and an open circuit. An example will clarify the procedure.



SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

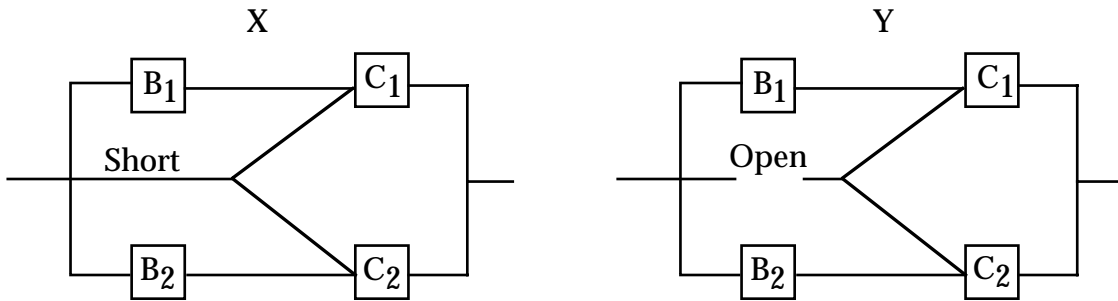
TABLE 6.4-4: LOGIC DIAGRAM EXAMPLES

Mission Reliability Diagram	Logic Diagram
	
	
	
	
<p>Other series parallel combinations can be quite simply drawn.</p>	
<p>NOTE: When one logic switch A is open, all must be open and all <math>\bar{A}</math> must be closed and similarly for B and C logic switches.</p>	

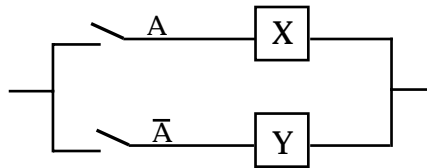
SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

Remove equipment A by splitting the diagram as follows:

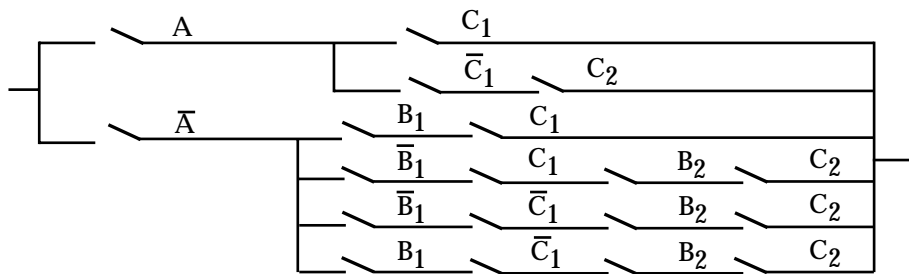
(In the diagrams which follow, the term "Short" indicates a circuit which is always operative; the term "open" indicates a circuit which is never operative).



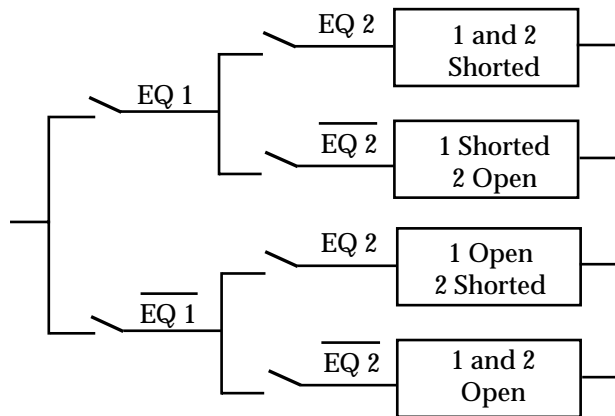
start the logic diagram



X and Y are now in series parallel form and can be drawn directly, therefore, the logic diagram would appear as follows:



If removing one equipment by replacing it by an open and short circuit will not reduce the system to two series parallel diagrams, two equipments must be removed. The logic diagram would then look as follows:

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

After the logic diagram is drawn, two approaches are possible for a numerical answer. The first involves writing an equation for the probability of success,  $P_S$ , by writing down every path with an addition sign joining all paths. The second approach is to insert values for the various probabilities directly into the logic diagram and multiply series terms and add parallel terms until just one series term remains. This result is the answer. For the above example:

$$P_S = A [C_1 + \bar{C}_2 C_2] + \bar{A} [B_1 C_1 + \bar{B}_1 C_1 B_2 C_2 + \bar{B}_1 \bar{C}_1 B_2 C_2 + B_1 \bar{C}_1 B_2 C_2] \quad (6.35)$$

6.4.4.2.4 Complex System Modeling Methods

The closed form techniques for modeling, as described in paragraph 6.4.4.2.1 through 6.4.4.2.3, are difficult to use on complex configurations that include high levels of fault-tolerance, standby spares and complex repair methods. Markov modeling is one method that can assist in providing needed performance and dependability prediction. Simulation tools are another method which may be more attractive as they are even more flexible.

6.4.4.2.4.1 Markov Modeling (Ref. [9])

Markov modeling processes are stochastic processes using random variables to describe the states of the process, transition probabilities for changes of state and time or event parameters for measuring the process. A stochastic process is said to be a Markov property if the conditional probability of any future event, given any past events and the present state, is independent of the past events and depends only on the present state of the process (Ref. [10]).

The advantages for using Markov modeling methods include the flexibility in expressing dynamic system behavior. These types of behavior include:

- (1) Complex repair. Situations consisting of repairs of either individual components or groups of components or partial repair of components.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

- (2) Standby spares. Standby conditions include hot, warm and cold spares. Hot spares are power-on units with identical stresses as apply to the active units, where warm spares have power-on but have lower stresses. Cold spares are power-off units.
- (3) Sequence dependent. This behavior includes: functional dependency in which the failure of one component can cause the unavailability of other components; priority dependency in which behavior will differ depending on whether an event occurs before or after another; and sequence enforcement in which it is impossible for certain events to occur before others have occurred.
- (4) Imperfect fault coverage. Imperfect fault coverage conditions arise when a dynamic reconfiguration process that is invoked in response to a fault or component failure has a chance of not being successful leading to system failure.

The disadvantages of using Markov modeling techniques include state size and model construction. Solving models with thousands of states can challenge the computer resources available. Also, the problem of identifying all the states and transitions correctly can be a difficult assignment.

Software tools for performing dependability analysis, such as Markov modeling include (see the RAC Web Site; the URL is <http://rac.iitri.org/DATA/RMST>):

- (1) HARP, Hybrid-Automated Reliability Predictor was developed to input system conditions directly in the form of a Markov model or in the form of a dynamic fault tree.
- (2) SHARPE, Symbolic Hierarchical Automated Reliability and Performance Evaluation, is an integrated tool that allows models to be solved either individually or combined hierarchically. In addition to Markov models, SHARPE can solve reliability block diagrams, fault trees and generalized stochastic Petri nets.
- (3) CARMS, Computer-Aided Rate Modeling and Simulation, is an interactive Markov modeling tool designed for reliability analysis of redundant systems.
- (4) CARSA, Computer-Aided Redundant System Reliability Analysis, utilizes Markov modeling for failure effect coverage. CARSA by-passes disadvantages of Markov modeling (larger number of states) by partitioning the system so that the model is a lower dimension.

### 6.4.4.2.4.2 Monte Carlo Simulation Method

Monte Carlo simulation may be used to synthesize a system reliability prediction from a reliability block diagram by means of random sampling. Monte Carlo simulation is employed in instances where individual equipment probabilities (or equivalent reliability parameter) are

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

known but the mission reliability model is exceedingly complex to derive a general equation for solution. The method does not result in a general probability of success equation but computes the system probability of success from the individual equipment probabilities and the reliability block diagram. Monte Carlo simulation is performed by computer due to the large number of repetitive trials and calculations required to obtain a significant result. Monte Carlo simulation is applicable to single functioned and multifunctioned systems.

Monte Carlo simulation determines the distribution of a function of one or more variables from the distribution of the individual variables. The method involves random sampling from the distributions of all variables and inserting the values so obtained in the equation for the function of interest. Suppose the function whose probability of success distribution is to be estimated is,  $P(x_1, \dots, x_n)$  and that the  $x_1, x_2, \dots, x_n$  are independent random variables whose distributions are presumed to be known. The procedure is to pick a set of  $x$ 's randomly from the distributions of the  $x$ 's, calculate  $P$  for that set, and store that value of  $P$ . This is repeated many times until enough values of  $P$  are obtained. From this sample of  $P$  values, its distribution and parameters can be estimated.

Monte Carlo simulation is based on several principles of probability and on the techniques of probability transformation. One underlying principle is the law of large numbers, which states that the larger the sample the more certainly the sample mean will be a good estimate of the population mean.

Software tools for simulation modeling include (see the RAC Web Site; the URL is <http://rac.iitri.org/DATA/RMST>):

- (1) AvSim, Availability Simulator allows the user to predict and optimize system and component performance. Uses Monte Carlo simulation techniques.
- (2) CARE, Computer-Aided Reliability Estimation helps estimate the reliability of complex, redundant, or fault-tolerant systems. Capable of modeling very large systems that incorporate some form of system management strategy which controls hardware/software resources in the presence of multiple faults or errors.
- (3) ETARA, Event Time Availability, Reliability Analysis is an interactive event driven simulation program. The program simulates the behavior of a system over a specified period of time using Monte Carlo methods to generate block failure and repair times as a function of exponential or Weibull distributions.
- (4) REST, (RADC Reliability Simulation Tool, is a Monte Carlo simulation used to evaluate reliability figures of merit for fault tolerant systems. Given a fault tolerant system configuration component MTBF's and repair rates, the program calculates the system MTBCF, MTTR, reliability and availability. REST also synthesizes reliability demonstration plans for fault tolerant systems. Can be used to model systems with full, standby, or partial standby redundancy.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

- (5) RAPTOR, The Rapid Availability Prototyping for Testing Operational Readiness (RAPTOR) software tool was developed by Headquarters Air Force Operational Test and Evaluation Center, Logistics Studies and Analysis Team (HQ AFOTEC/SAL). Its primary purpose is Reliability, Maintainability & Availability (RM&A) analysis of systems undergoing Operational Test and Evaluation (OT&E). Other applications include test planning, requirements definition, reliability prediction and sensitivity analysis. It can be downloaded over the Internet  
(URL: <http://www.afotec.af.mil/sa/safrmset.htm>).

### 6.4.5 Reliability Prediction

Predictions are a means of determining the feasibility of requirements and of assessing progress toward achieving those requirements. In general, there is a hierarchy of reliability prediction techniques available to the designer depending upon (1) the depth of knowledge of the design and (2) the availability of historical data on equipment and component part reliabilities. As the system design proceeds from conceptual, through detailed design, data describing the system evolves from a qualitative description of systems functions to detailed specifications and drawings suitable for hardware production. Therefore, a hierarchy of reliability prediction techniques have been developed to accommodate the different reliability study and analysis requirements and the availability of detailed data as the system design progresses as shown in Figure 6.4-3. These techniques can be roughly classified in four categories, depending on the type of data or information availability for the analysis. The categories are:

- (1) Similar Item Analysis. Each item under consideration is compared with similar items of known reliability in estimating the probable level of achievable reliability, then combined for higher level analyses.
- (2) Part Count Analysis. Item reliability is estimated as a function of the number of parts and interconnections included. Items are combined for higher level analysis.
- (3) Stress Analyses. The item failure rate is determined as a function of all the individual part failure rates as influenced by operational stress levels and derating characteristics for each part.
- (4) Physics-of-Failure Analysis. Using detailed fabrication and materials data, each item or part reliability is determined using failure mechanisms and probability density functions to find the time to failure for each part. The physics-of-failure (PoF) approach is most applicable to the wearout period of an electronic product's life cycle and is not suited to predicting the reliability during the majority of its useful life. In addition, at the time this handbook was being revised, a practical and economic method for applying a PoF prediction method was not available. The pros and cons of PoF prediction models are shown in Table 6.4-5.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

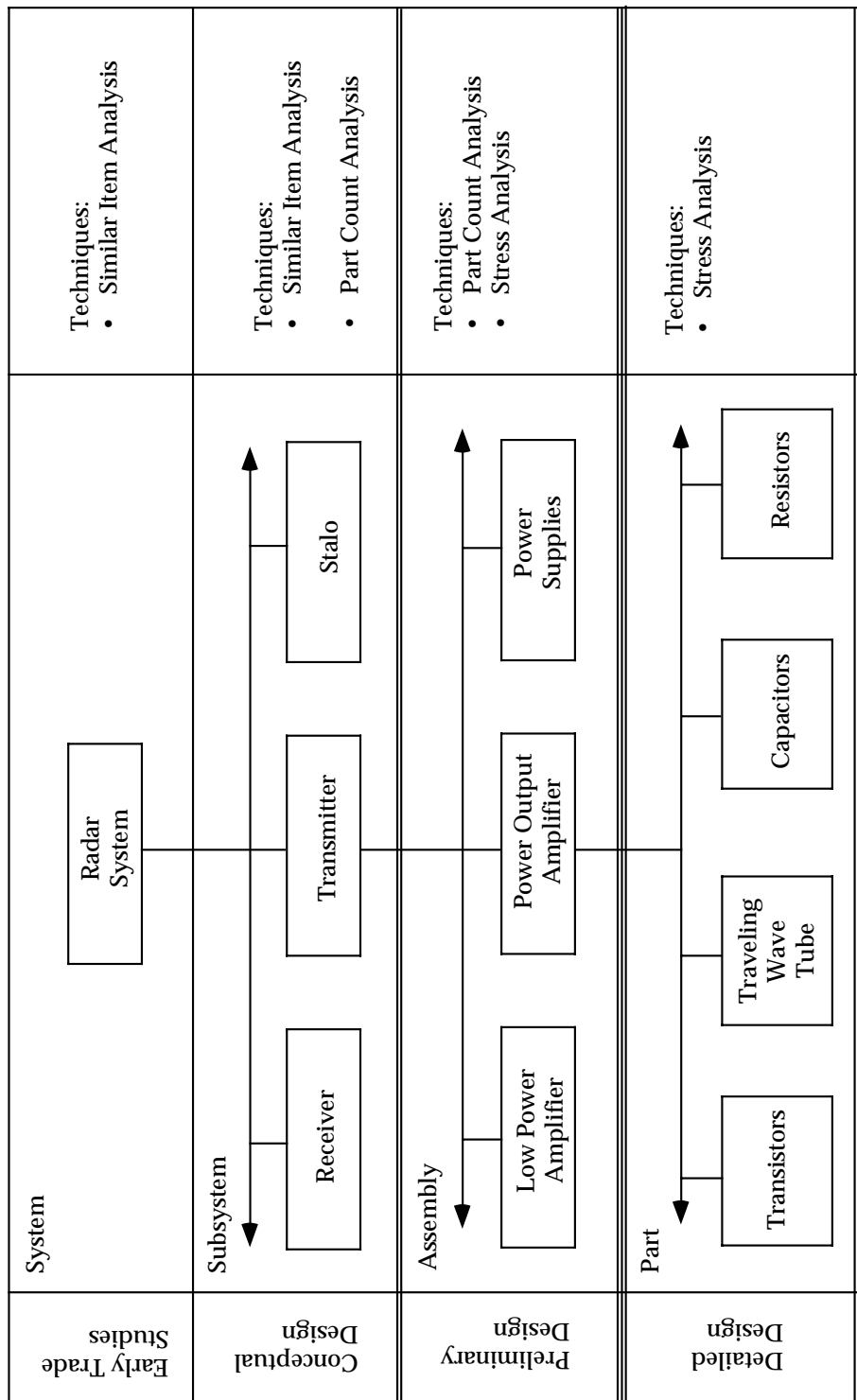


FIGURE 6.4-3: RADAR SYSTEM HIERARCHY (PARTIAL LISTING)



## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

TABLE 6.4-5: PROS AND CONS OF PHYSICS-OF-FAILURE PREDICTION MODELS

Advantages	Disadvantages
More accurate than generic models for wearout mechanisms	Can only be used by those having access to detailed fabrication and materials data
Based on fundamental reliability parameters	Relatively complex and difficult to use
Can be developed sooner since they require only fabrication & materials data	Do not address early and mid-life failure

### 6.4.5.1 General

To perform a satisfactory reliability analysis of a system, basic information is needed and should include:

- (1) Description. Part or component descriptions should be provided for any prediction based upon part failure rates. The identification numbers from the schematic diagram, the applicable specification and the specification type number should be included.
- (2) Environmental Data. Environmental data affecting part failure rates must be defined. These data include the specific natural and induced environments (nominal and worst case) associated with the operations, events, and functions described by the logistic and operational cycles. Environmental categories should be defined for each service use event using Table 6.4-6 as a guide of typical categories. Data sources, such as MIL-HDBK-217 (Ref. [11]) and NPRD-95 (Ref. [12]) which utilize environmental factors to adjust failure rates, should apply the environmental factor which most closely matches the intended environment. Factors utilized should be cited and substantiated.
- (3) Operating Temperature. Part or component temperatures used for prediction purposes should include the item internal temperature rise as determined by thermal analysis or test data.
- (4) Stress Analysis. Analyses should be performed to determine the operating stresses experienced by each part commensurate with the prediction classification and the design detail available. Failure rates are modified by appropriate factors to account for the effect of applied stress.
- (5) Failure Distributions. The failure distribution appropriate to the specific electronic, electrical, electromechanical, mechanical, and ordnance item should be used in computation. In instances where the failure distribution for the item is not known, the exponential, binomial, Weibull, or other failure distribution may be assumed. The failure distributions utilized should be cited and any assumptions substantiated in the prediction report.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

- (6) **Failure Rates.** Failure rates for all electronic, electrical, electromechanical, mechanical, and ordnance items are needed for each significant event and environment defined by the service use profile. Basic failure rates from most data sources must be modified with appropriate factors to account for the specific item application under consideration. Factors used should be cited and substantiated in the prediction report. These include:
- (a) Functional group failure rates may be derived from failure rate data for functionally similar groups or items. The GIDEP Failure Rate Summaries are an available source for locating group and item failure rates.

TABLE 6.4-6: ENVIRONMENTAL SYMBOL IDENTIFICATION  
AND DESCRIPTION

Environment	Symbol	Nominal Environmental Conditions
Ground, Benign	G <sub>B</sub>	Nonmobile, temperature and humidity controlled environments.
Space, Flight	S <sub>F</sub>	Earth orbital. Approaches Ground Benign conditions. Vehicle neither under powered flight nor in atmospheric reentry.
Ground, Fixed	G <sub>F</sub>	Conditions less than ideal to include installation in permanent racks with adequate cooling air and possible installation in unheated buildings.
Ground, Mobile	G <sub>M</sub>	Conditions more severe mostly for vibration and shock. Equipment installed on wheeled or tracked vehicles.
Naval, Sheltered	N <sub>S</sub>	Sheltered or below deck conditions on surface ships and submarines.
Naval, Unsheltered	N <sub>U</sub>	Unprotected surface shipborne equipments exposed to weather conditions and salt water.
Airborne, Inhabited, Cargo	A <sub>IC</sub>	Typical conditions in cargo compartments occupied by aircrew without environmental extremes of pressure, temperature, shock and vibration.
Airborne, Inhabited, Fighter	A <sub>IF</sub>	Same as A <sub>IC</sub> but installed on high performance aircraft such as fighters and interceptors.
Airborne, Uninhabited, Cargo	A <sub>UC</sub>	Uncontrolled areas with environmental extremes of pressure, temperature and shock.
Airborne, Uninhabited, Fighter	A <sub>UF</sub>	Same as A <sub>UC</sub> but installed on high performance aircraft such as fighters and interceptors.
Airborne, Rotary Winged	A <sub>RW</sub>	Equipment installed on helicopters, internally and externally.
Missile, Launch	M <sub>L</sub>	Severe conditions of noise, vibration, and other environments related to missile launch, and space vehicle boost into orbit, vehicle re-entry and landing by parachute. Conditions may also apply to installation near main rocket engines during launch operations.
Missile, Flight	M <sub>F</sub>	Typical conditions of pressure, vibration and temperature experienced in atmospheric flight to target.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

- (b) Operating failure rates for electronic and electromechanical parts may be found in MIL-HDBK-217 (Ref. [11]) and Bellcore TR-NWT-00332 (Ref. [13]). Failure rates for other parts may be found in NPRD-95 (Ref. [12]), Electronic Parts Reliability Data, 1997 (Ref. [14]), the GIDEP Failure Rate Summaries, and other sources.
- (c) Nonoperating failure rates take into consideration pertinent environmental influences or other stresses of the application. Data sources such as RADC-TR-85-91 (Ref. [15]) and NONOP-1 (Ref. [16]), provide nonoperating failure rates.

### 6.4.5.2 Mathematical Models for Reliability Prediction

For the simplest case of equipment or system configurations consisting of N independent elements or subsystems in series, the reliability equation is:

$$R_s = \prod_{i=1}^N R_i \quad (6.36)$$

where:

$R_s$  is the equipment or system reliability

$R_i$  is the reliability of each of the elements or subsystems

For the case where time is a factor

$$R_s(t) = \prod_{i=1}^N R_i(t) \quad (6.37)$$

where:

$R_s(t)$  = The probability that the system will not fail before time t. (In this case a "system" is considered to be any device consisting of n elements, none of which can fail without system failure).

$R_i(t)$  = The probability that the  $i^{\text{th}}$  element of the system will not fail before time t.

Finally, if one assumes that each of the  $R_i(t)$  's is exponentially distributed with constant failure rate of  $\lambda_i$ , then

$$R_i(t) = \exp(-\lambda_i t) \quad (6.38)$$

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

Then,

$$R_s(t) = \prod_{i=1}^N \exp(-\lambda_i t) \quad (6.39)$$

Also,

$$\lambda_s = \sum_{i=1}^N \lambda_i \quad (6.40)$$

where:

$\lambda_s$  = system failure rate

$\lambda_i$  = failure rate of each of the independent elements of the system

And,

$$MTBF = \frac{1}{\lambda_s} = \frac{1}{\sum_{i=1}^N \lambda_i} \quad (6.41)$$

Eqs. (6.38), (6.39), and (6.41) are the basic equations used in the reliability prediction of electronic equipment/systems.

The use of the exponential distribution of time to failure for complex systems is usually justified because of the many forces that can act upon the system and produce failure. For example, different deterioration mechanisms, different part hazard-rate functions, and varying environmental conditions often result in, effectively, random system failures.

Another justification for assuming the exponential distribution in long-life complex systems is the so called "approach to a stable state," wherein the system hazard rate is effectively constant regardless of the failure pattern of individual parts. This state results from the mixing of part ages when failed elements in the system are replaced or repaired. Over a period of time, the system hazard rate oscillates, but this cyclic movement diminishes in time and approaches a stable state with a constant hazard rate.

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

### 6.4.5.3 Reliability Prediction Methods

Four prediction methods are described as follows:

#### 6.4.5.3.1 Similar Item Prediction Method

Several techniques have been developed and used in performing very early predictions of item reliability before any characteristics of the system design have been established. The most basic of these techniques involves a simple estimate of item reliability in terms of MTBF, failure rate, or similar parameters, based on experience gained from operational items of similar function.

In general, these similar item prediction techniques involve the following steps:

- (1) Defining the new item in terms such as general equipment type (e.g., radar), operational use (e.g., ground based) and other known characteristics.
- (2) Identifying an existing item or class of equipment that most nearly compares with the new item.
- (3) Obtaining and analyzing historical data generated during operation of the existing equipment to determine as nearly as possible the reliability of the items under the stated operating environment.
- (4) Drawing conclusions concerning the level of reliability that will be demonstrated by the new items. Such conclusions assume that similar equipment will exhibit similar reliability and that reliability achievement evolves in an orderly manner from one generation of equipments to the next. These reliability prediction techniques permit very early estimation of the failure rate of a new item based on experience gained from operational items of similar function. The accuracy of the estimates, however, depends on the quality of historical data and the similarity between the existing and new equipments. If the technology of the new items is too advanced, then the operational data for the old items will not be relevant and another technique will have to be considered.

The similar item prediction method utilizes specific experience on similar items. The more rapid way of estimating reliability is to compare the item under consideration with a similar item whose reliability has previously been determined by some means and has undergone field evaluation. The method has a continuing and meaningful application for items undergoing orderly evolution. Not only is the contemplated new design similar to the old design, but small differences can be easily isolated and evaluated. In addition, difficulties encountered in the old design are signposts to improvements in the new design.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

Major factors for a direct comparison of similar items should include:

- (1) Item physical and performance comparison
- (2) Design similarity
- (3) Manufacturing similarity
- (4) Similarity of the service use profile (logistic, operational, and environmental)
- (5) Program and project similarity
- (6) Proof of reliability achievement

The validity of the similar item method is dependent upon the degree of equivalence between the items and not simply the generic term used to describe the items. For example, although both are power supplies (generic type), the achieved reliability of a ten watt power supply should not normally be used as a prediction method for a proposed one kilowatt power supply as the much higher power level of the proposed power supply may result in much lower reliability achievement due to significant design differences and stresses. A comparison may be made if there are scale factors to realistically relate reliability with item parameters such as power levels.

An example of this technique is: a new computer product which is composed of a processor, a display, a modem and a keyboard is expected to operate in a 20°C environment. Data on similar items indicates mean-time-between-failure (MTBF) values as shown in the second column of Table 6.4-7. The similar item data is for a computer operating in a 30°C environment. If a 30% reliability improvement factor (as a result of improved technology) is expected, what MTBF can we expect?

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

TABLE 6.4-7: RELIABILITY ANALYSIS SIMILAR ITEM

Item	Similar Data MTBF (hrs.)	Temperature Factor*	Improvement Factor	New Product MTBF (Hrs.)
Processor	5,000	1.1	1.3	7,150
Display	15,000	1.1	1.3	21,450
Modem	30,000	1.1	1.3	42,900
Keyboard	60,000	1.1	1.3	85,800
System	3,158			4,516

\*Each item MTBF is corrected using temperature conversion factors from the “Reliability Toolkit: Commercial Practices Edition,” page 176 (Ref. [8]).

Each item MTBF is corrected for the change in temperature of 30°C to 20°C. Technology improvement factors are also included and the system MTBF is calculated using the expression:

$$MTBF_s = \sum_i^n \frac{1}{\lambda_i}$$

where:

$MTBF_s$  = mean-time-between-failure of the system

$\lambda_i$  = failure rate of the i component which equals 1/MTBF<sub>i</sub>

#### 6.4.5.3.2 Parts Count Prediction Method

This technique is used when one has a “feel” for the number of component parts (actual or estimated) by class or type that will be used in an equipment/system but does not have enough data as to the stresses to which each part will be subjected in the final design. It involves counting the number of parts of each class or type, multiplying this number by the generic failure rate for each part class or type, and summing these products to obtain the failure rate for the equipment. The procedure distinguishes a part class as being all parts of a given function (e.g., resistors, capacitors, transformers). Part types are used to further define parts within a class (e.g., fixed composition resistors, fixed wire wound resistors).

This method is used in the preliminary design stage when the number of parts in each generic type class such as capacitors, resistors, etc., are reasonably fixed and the overall design complexity is not expected to change appreciably during later stages of development and production. The parts count method assumes the time to failure of the parts is exponentially distributed (i.e., a constant failure rate).

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

The item failure rate can be determined directly by the summation of part failure rates if all elements of the item reliability model are in series or can be assumed in series for purposes of an approximation. In the event the item reliability model consists of non-series elements (e.g., redundancies, alternate modes of operation), item reliability can be determined either by considering only the series elements of the model as an approximation or by summing part failure rates for the individual elements and calculating an equivalent series failure rate for the non-series elements of the model.

The information needed to support the parts count method includes:

- (1) Generic part types (including complexity for microelectronics),
- (2) Part quantity,
- (3) Part quality levels (when known or can be assumed), and
- (4) Item environment.

The general expression for item failure rate with this method is:

$$\lambda_{\text{ITEM}} = \sum_{i=1}^n N_i (\lambda_{G_i} \pi_{Q_i}) \quad (6.42)$$

where:

$\lambda_{\text{ITEM}}$	=	total failure rate
$\lambda_{G_i}$	=	generic failure rate for the $i^{\text{th}}$ generic part
$\pi_{Q_i}$	=	quality factor for the $i^{\text{th}}$ generic part
$N_i$	=	quantity of $i^{\text{th}}$ generic part
$n$	=	number of different generic part categories

Equation 6.42 applies to an entire item being used in one environment. If the item comprises several units operating in different environments (such as avionics with units in airborne, inhabited, fighter ( $A_{\text{IF}}$ ) and uninhabited, fighter ( $A_{\text{UF}}$ ) environment), then equation 6.42 should be applied to the portions of the item in each environment. These “environment-item” failure rates should be added to determine total item failure rate.

Quality factors are to be applied to each part type where quality level data exists or can be reasonably assumed. Multi-quality levels and data exist for parts, such as microelectronics, discrete semiconductors, and for established reliability (ER) resistors and capacitors. For other parts such as nonelectronics,  $\pi_Q = 1$  providing that parts are procured in accordance with applicable parts specifications.



## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

The generic (average) failure rate ( $\lambda_{Gi}$ ) and the quality factor ( $\pi_{Qi}$ ) can be obtained from the latest version of MIL-HDBK-217 (Ref. [11]) or manufacturer's data. MIL-HDBK-217 contains a number of tables of generic failure rates for various classes and types of parts, as well as the associated quality factors. Tables 6.4-8 and 6.4-9 (taken from MIL-HDBK-217F, Notice 2), are specific examples of generic failure rates and quality factors for diodes and transistors.

An example of how this technique might be applied to predict the MTBF and reliability of a mobile electronic receiver is shown in Figure 6.4-4. The part failure rates for a ground mobile environmental condition are presented from MIL-HDBK-217 for the various part types.

### 6.4.5.3.3 Parts Stress Analysis Prediction Method

The previous method described was based upon average failure rates for each component part type. It is well known that part failure rates vary significantly with applied stresses, sometimes by several orders of magnitude. For example, a 110 volt light bulb does not operate very long when subjected to 220 volts. It is this interaction between strength of the component and the stress level at which the component operates which determines the failure rate of a component in a given situation. Thus, at different stress levels component parts assume different failure rates. This is the rationale for the stress analysis prediction technique. This technique is based upon a knowledge of the stress to which the part will be subjected, e.g., temperature, humidity, vibration, etc., and the effect of those stresses on the part's failure rate. Some of the factors that influence part reliability, for a sample of part types, are shown in Table 6.4-10.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTIONTABLE 6.4-8: GENERIC FAILURE RATE -  $\lambda_0$  (FAILURES/10<sup>6</sup> HOURS) FOR DISCRETE SEMICONDUCTORS

Section #	Part Type	Env. $T_j$ (°C) →	$G_1$	$G_2$	$N_1$	$A_1$	$A_2$	$A_{3c}$	$A_{3f}$	$A_{3M}$	$S_f$	$M_f$	$M_f$	$C_f$
		60	65	75	85	75	75	80	80	80	50	65	75	80
6.1	DIODES													
6.1	General Purpose Analog Switching	.0036 .00094	.028 .075	.049 .013	.043 .011	.092 .024	.21 .054	.20 .054	.44 .12	.17 .045	.0018 .00047	.076 .020	.23 .060	1.5 4.0
6.1	Fast Recovery Pwr. Rectifier	.065	.52	.99	.78	1.7	3.7	3.7	8.0	3.1	.032	1.4	4.1	28
6.1	Power Rectifier/Schottky Pwr.	.0028	.022	.038	.034	.073	.16	.16	.35	.13	.0014	.060	.18	1.2
6.1	Transient Suppressor/Varistor	.0029	.023	.040	.035	.075	.17	.17	.36	.14	.0015	.062	.18	1.2
6.1	Voltage Ref/Reg. (Avalanche and Zener)	.0033	.024	.039	.035	.066	.15	.13	.27	.12	.0016	.060	.16	1.3
6.1	Current Regulator	.0056	.040	.066	.060	.11	.25	.22	.46	.21	.0028	.10	.28	2.1
6.2	Si Impatt (f < 35 GHz)	.86	2.8	8.9	5.6	20	11	36	62	44	.43	16	67	350
6.2	Gunn/Bulk Effect	.31	.76	2.1	1.5	4.6	2.0	4.5	7.6	7.9	.16	3.7	12	94
6.2	Tunnel and Back	.004	.0086	.0026	.0019	.025	.032	.057	.097	.10	.002	.048	.15	1.2
6.2	PIN	.028	.088	.19	.14	.41	.18	.40	.69	.71	.014	.34	1.1	8.5
6.2	Schottky Barrier and Point Contact (see whz's in chz)	.047	.11	.31	.23	.68	.30	.67	1.1	1.2	.023	.56	1.8	14
6.2	Varactor	.0043	.010	.029	.021	.063	.028	.062	.11	.11	.0022	.052	.17	1.3
6.10	Thyristor/SCR	.0025	.020	.034	.030	.064	.14	.14	.31	.12	.0012	.053	.16	1.1
6.3	TRANSISTORS													
6.3	NPN/PNP (f < 200 MHz)	.00015	.0011	.0017	.0017	.0030	.0067	.0060	.013	.0056	.000073	.0027	.0074	.056
6.3	Power NPN/PNP (f < 200 MHz)	.0087	.042	.089	.063	.15	.26	.23	.50	.22	.0029	.11	.29	2.2
6.4	Si FET (f < 400 MHz)	.014	.099	.16	.15	.34	.62	.53	1.1	.51	.0069	.25	.68	5.3
6.5	Unijunction	.016	.12	.20	.18	.42	.36	.74	1.6	.66	.0079	.31	.88	6.4
6.6	RF, Low Noise (f > 200 MHz, P < 1W)	.094	.23	.63	.46	1.4	.60	1.3	2.3	2.4	.047	1.1	3.6	28
6.7	RF, Power (P > 1W)	.074	.15	.37	.29	.81	.29	.52	.88	.037	.33	.66	1.8	18
6.8	GaAs FET (P < 100 mW)	.17	.51	1.5	1.0	3.4	1.8	5.4	9.2	7.2	.083	2.8	11	63
6.8	GaAs FET (P > 100 mW)	.42	1.3	3.9	2.5	8.5	4.5	13	23	18	.21	6.9	27	160
6.9	Si FET (f > 400 MHz)	.099	.24	.64	.47	1.4	.61	1.3	2.3	2.4	.049	1.2	3.6	30

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTIONTABLE 6.4-9: DISCRETE SEMICONDUCTOR QUALITY FACTORS -  $\pi_Q$ 

Section Number	Part Types	JANTX V	JANTX	JAN	Lower	Plastic
6.1, 6.3, 6.4, 6.5, 6.10, 6.11, 6.12	Non-RF Devices/ Opto-Electronics*	.70	1.0	2.4	5.5	8.0
6.2	High Freq Diodes	.50	1.0	5.0	25	50
6.2	Schottky Diodes	.50	1.0	1.8	2.5	----
6.6, 6.7, 6.8, 6.9	RF Transistors	.50	1.0	2.0	5.0	----
6.13	*Laser Diodes	$\pi_Q$ = 1.0 Hermetic Package = 1.0 Nonhermetic with Facet Coating = 3.3 Nonhermetic without Facet Coating				

Part Type	Failure Rate ( $\lambda_G$ ) per $10^6$ Hrs.)	Quantity Used (N)	Quality Factor ( $\pi_Q$ )	Total Failure rate per $10^6$ Hrs. ( $\lambda_G \times N \times \pi_Q$ )
Microcircuit				
Linear	0.18	20	2	7.20
Memory	0.07	5	2	0.70
Diode				
General Purpose	0.05	30	1	1.50
Regulator	0.04	20	1	0.80
Transistor				
Power	0.07	20	1	1.40
FET	0.16	5	1	0.80
Resistor				
Composition	0.05	80	.3	1.20
Variable	0.07	20	.3	0.42
Capacitor				
Ceramic	0.06	60	.3	1.08
Tantalum	0.04	40	.3	0.48
Switch				
Rocker	0.41	5	2	4.10
Rotary	2.00	5	2	20.00
Transformer				
Power	0.80	2	1	1.60
Connector				
Edge	0.45	2	1	0.90
Circular	0.10	10	1	1.00
Circuit Board				
Two Layer	0.16	2	1	0.32
Total		326		43.50

$$MTBF_{TOTAL} = 1/\lambda_T = 1/43.5 \times 10^{-6} = 22,989 \text{ hours}$$

FIGURE 6.4-4: SAMPLE RELIABILITY CALCULATION

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

TABLE 6.4-10: MAJOR INFLUENCE FACTORS ON PART RELIABILITY

Part Type	Influence Factors
Integrated Circuits	<ul style="list-style-type: none"> <li>• Temperature</li> <li>• Complexity</li> <li>• Supply Voltage</li> </ul>
Semiconductors	<ul style="list-style-type: none"> <li>• Temperature</li> <li>• Power Dissipation</li> <li>• Voltage Breakdown</li> </ul>
Capacitors	<ul style="list-style-type: none"> <li>• Temperature</li> <li>• Voltage</li> <li>• Type</li> </ul>
Resistors	<ul style="list-style-type: none"> <li>• Temperature</li> <li>• Power Dissipation</li> <li>• Type</li> </ul>
Inductors	<ul style="list-style-type: none"> <li>• Temperature</li> <li>• Current</li> <li>• Voltage</li> <li>• Insulation</li> </ul>

#### 6.4.5.3.3.1 Stress Analysis Techniques

A number of empirical stress analysis prediction techniques exist to estimate the reliability in the operating domain. The best known are:

- (1) MIL-HDBK-217F, "Reliability Prediction of Electronic Equipment"
- (2) Bellcore Reliability Prediction Procedures for Electronic Equipment (Bellcore RPP)
- (3) Nippon Telegraph and Telephone Cooperation Standard Reliability Tables for Semiconductor Devices (NTT Procedure)
- (4) British Telecom Handbook of Reliability Data for Components in Telecommunications Systems (British Telecom HRD-4)
- (5) French National Center for Telecommunications Study (CNET Procedure)
- (6) Siemens Reliability and Quality Specification Failure Rates of Components (Siemens Procedure)

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

Examples of the models used in each technique are shown in Table 6.4-11 for microcircuit parts.

TABLE 6.4-11: FORMULAS FOR CALCULATING MICROCIRCUIT RELIABILITY

Technique	Microcircuit Model
MIL-HDBK-217	$\lambda = \pi_Q (C_1 \pi_T \pi_V + C_2 \pi_E) \pi_L$
Bellcore	$\lambda = \lambda_G \pi_Q \pi_S \pi_T$
British HRD-4	$\lambda = \lambda_b \pi_T \pi_Q \pi_E$
NTT Procedure	$\lambda = \lambda_b \pi_Q (\pi_E + \pi_T \pi_V)$
CNET Procedure	$\lambda = (C_1 \pi_T \pi_t \pi_V + C_2 \pi_B \pi_\sigma \pi_E) \pi_L \pi_Q$
Siemens Procedure	$\lambda = \lambda_b \pi_U \pi_T$

The factors cited for each of the models are the stress parameters and base part failure rate values. The factors for failure rate calculation are as follows:

- (1)  $\pi_Q$  equals the quality factor based on test and inspection
- (2)  $C_1$  and  $C_2$  equal the complexity and technology factors
- (3)  $\pi_T$  equals the temperature acceleration factor
- (4)  $\pi_V$ ,  $\pi_S$  and  $\pi_U$  equals the voltage acceleration factors
- (5)  $\pi_E$  equals the environment that the part is expected to operate
- (6)  $\pi_L$  equals the part manufacturing or process learning factor
- (7)  $\lambda_G$  equals the generic or average failure rate assuming average operating conditions
- (8)  $\lambda_b$  equals the base failure rate depending on part complexity and technology
- (9)  $\pi_t$  equals the technology function factor
- (10)  $\pi_B$  equals the packaging factor

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

(11)  $\pi_{\circ}$  equals the package factor based on the number of pins

#### 6.4.5.3.3.2 Sample Calculation

The best way to illustrate the stress analysis prediction technique is to perform a sample calculation. The example is; a 60,000 gate dual-in-line 64 pin digital bipolar microcircuit which will be operated in a ground fixed environment. General commercial practices apply to the manufacturing which has been on-going for two years. The formula for determining the failure rate of the microcircuit is from MIL-HDBK-217 (Ref. [11]):

$$\lambda_p = (C_1\pi_T + C_2\pi_E)\pi_Q\pi_L$$

where:

$\lambda_p$	=	bipolar failure rate in failure per $10^6$ hours
$C_1$	=	complexity factor for 60,000 gates
$\pi_T$	=	temperature factor based on junction temperature
$C_2$	=	complexity factor for the package type
$\pi_E$	=	operating environment factor
$\pi_Q$	=	quality inspection and test factor
$\pi_L$	=	the learning factor based on years in production

**STEP 1:** Given: 60,000 gate bipolar microcircuit, with 64 pin non-hermetic dual-in-line package, to be operated in a ground fixed condition. The manufacturing has been on-going for 2 years and is considered good commercial practices. The case temperature is expected to be no greater than 45°C, and the thermal resistance factor is 11 degrees centigrade per watt. The microcircuit maximum power dissipation is 200 milliwatts.

**STEP 2:** Determine  $C_1$ : From MIL-HDBK-217, the complexity factor for a 60,000 gate digital microcircuit is 0.08 as shown in Table 6.4-12.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

TABLE 6.4-12: BIPOLAR COMPLEXITY FAILURE RATE C1

Digital		Linear	
No. Gates	C <sub>1</sub>	No Transistors	C <sub>1</sub>
1 to 100	.0025	1 to 100	.01
101 to 1,000	.005	101 to 300	.02
1,001 to 3,000	.010	301 to 1,000	.04
3,001 to 10,000	.020	1,001 to 10,000	.06
10,001 to 30,000	.040		
30,001 to 60,000	.080		

**STEP 3:** Determine junction temperature: The standard junction temperature is calculated using the following relationship:

$$T_J = T_C + \theta_{JC} P$$

where:

$$T_J = \text{junction temperature in degrees centigrade}$$

$$T_C = \text{case temperature in degrees centigrade}$$

$$\theta_{JC} = \text{junction to case thermal resistance in degrees centigrade per watt}$$

$$P = \text{power dissipated in watts}$$

Values for the factors are given, so

$$\begin{aligned} T_J &= 45 + 11(.20) \\ &= 47.2^\circ\text{C} \end{aligned}$$

**STEP 4:** Determine the temperature acceleration factor,  $\pi_T$  from the temperature equation as stated in MIL-HDBK-217. The equation is:

$$\pi_T = 0.1 \exp \left[ -A \left( \frac{1}{T_J + 273} - \frac{1}{298} \right) \right]$$

where:

$$A = \text{temperature coefficient, 4642}$$

$$T_J = \text{junction temperature } (^\circ\text{C})$$

$$\pi_T = .29$$

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

**STEP 5:** Determine the packaging factor  $C_2$  given a 64 pin non-hermetic dual-in-line package from the equation in MIL-HDBK-217. The equation is:

$$C_2 = 3.6 \times 10^{-4} (N_p)^{1.08}$$

where:

$$\begin{aligned} C_2 &= 3.6 \times 10^{-4} (64)^{1.08} \\ &= .032 \end{aligned}$$

**STEP 6:** Find the environmental factor from MIL-HDBK-217 which is shown in Table 6.4-13. For ground fixed conditions, the value is 2.0.

TABLE 6.4-13: ENVIRONMENTAL FACTOR -  $\pi_E$

Environment	$\pi_E$
$G_B$ (Ground Benign)	0.5
$G_F$ (Ground Fixed)	2.0
$G_M$ (Ground Mobile)	4.0

**STEP 7:** Select the quality value from MIL-HDBK-217. Since the product is a commercial device with an unknown screening level, the quality factor has a value of 10.0 as shown in Table 6.4-14. When the screening level is known, MIL-HDBK-217 has a table that relates  $\pi_Q$  values (lower than 10.0) to the specific screening level.

TABLE 6.4-14: QUALITY FACTORS -  $\pi_Q$

Description	$\pi_Q$	Description	$\pi_Q$
Class S	0.25	Class B-1	2.00
Class B	1.00	Commercial	10.00

**STEP 8:** Using the equation for manufacturing learning from MIL-HDBK-217 which is:

$$\pi_L = 0.1 \exp(5.35 - .354/Y)$$

$$\pi_L = 1 \text{ for production lines in operation longer than 2 years}$$



## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

where:

$$\begin{aligned}
 Y &= \text{years, which is 2} \\
 \pi_L &= .01 \exp(5.35 - .35(2)) \\
 &= 1.05, \text{ which is rounded to 1.}
 \end{aligned}$$

**STEP 9:** Perform the calculation.

$$\begin{aligned}
 \lambda_p &= [C_1\pi_T + C_2\pi_E] \pi_Q\pi_L \\
 &= [(0.08)(.29) + (.032)(2.0)] (10) (1.0) \\
 &= 0.87 \text{ failures per } 10^6 \text{ hours}
 \end{aligned}$$

After one has calculated the failure rate for each component, the equipment failure rate is determined by summing the failure rates of the individual components as shown in equation 6.43.

$$\lambda_{\text{EQUIP}} = \sum_{i=1}^n \lambda_i \quad (6.43)$$

and the MTBF is

$$\text{MTBF} = \frac{1}{\lambda_{\text{EQUIP}}} \quad (6.44)$$

Stress analysis failure rate predictions such as this permit extremely detailed analyses of equipment or system reliability. However, since details of the system design are required in determining stress ratios, temperature and other application and environmental data, these techniques are only applicable during the later stages of design. Because of the high level of complexity of modern systems, the application of the procedure is time consuming.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

6.4.5.3.3 Modification for Non-Exponential Failure Densities (General Case)

Although the exponential technique indicated in the previous sections can be used in most applications with little error, it must be modified (1) if the system contains parts for which the density function of failure times cannot be approximated by an exponential distribution over the time period of interest; or (2) if the parts which are the dominant factor in overall system unreliability do not follow an exponential density function of times to failure. Mechanical parts such as gears, motors, and bearings usually fall into this category.

In these cases, one cannot add the failure rates of all parts because there are some parts whose failure rates vary significantly with time. The method used is to consider separately within each block diagram the portion of the block containing parts with constant failure rates, and the portion containing parts with time varying failure rates. If the former portion contains  $n$  parts, then the reliability of this portion is

$$R_1(t) = \exp \left( - \left( \sum_{i=1}^n \lambda_i \right) t \right) \quad (6.45)$$

The reliability of the second portion at time  $t$  is formed by using the appropriate failure density function for each part whose parameters have been determined through field experience or testing. If this portion contains  $B$  parts, then

$$R_2(t) = \prod_{i=1}^B R_i(t) \quad (6.46)$$

where:

$$R_i(t) = \int_t^{\infty} f_i(t) dt \quad (6.47)$$

and  $f_i(t)$  is the probability density function, general expression, of each of the  $B$  parts.

As discussed in 5.3.6, the Weibull distribution can be used to describe the distribution of times to failure in a wide variety of cases. If we use the Weibull to describe the portion of the block diagram containing parts with varying failure rate, equation 6.47 becomes:

$$R_2(t) = \prod_{i=1}^B \left( \int_t^{\infty} \frac{\beta}{\theta} \left( \frac{t}{\theta} \right)^{\beta-1} e^{-\left( \frac{t}{\theta} \right)^{\beta}} \right) = \prod_{i=1}^B \left( e^{-\left( \frac{t}{\theta} \right)^{\beta}} \right) \quad (6.48)$$

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

where:

B	=	numbered parts
t	=	time
$\theta_i$	=	Weibull scale parameter for part i
$\beta_i$	=	Weibull shape parameter for part i

The reliability for the block diagram, under the assumption of independence between the two portions, is

$$R(t) = R_1(t) R_2(t) \quad (6.49)$$

For example, consider the failure rates of two elements, x and y, that make up a system. Let x be a microprocessor controller with a constant failure of 2 failures per million hours. Let y be a roller bearing operating at 1000 revolutions per minute for which 90% of the population will operate without failure for  $3.6 \times 10^9$  revolutions. Bearing life test results have been fitted to the Weibull distribution with a shape parameter,  $\beta$ , of 1.5.

**STEP 1:** The microcircuit reliability is found by using equation 6.38.

$$\begin{aligned} R_1(t) &= \exp(-\lambda t) \\ &= \exp [ - (2 \times 10^{-6})(50,000) ] \\ R_1(t) &= 0.905 \end{aligned}$$

**STEP 2:** The bearing reliability is determined by converting the revolutions into hours given that the speed is 60,000 revolutions per hour. This is  $3.6 \times 10^9$  revolutions divided by 60,000 revolutions per hours which equals 60,000 hours.

Then scale parameter  $\theta$ , is determined from the standard Weibull equation shown as 6.48.

$$R(t) = \exp - \left( \frac{t}{\theta} \right)^\beta$$

---

 SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION
 

---

where:

$$\begin{aligned}
 R(t) &= 0.9 \text{ at } 60,000 \text{ hours (given)} \\
 t &= 60,000 \text{ hours} \\
 \beta &= \text{Weibull shape of } 1.5 \text{ for product characteristic of early wearout} \\
 \theta &= \text{mean-time-to-failure}
 \end{aligned}$$

$$R(t) = 0.9 = \exp - \left( \frac{60,000}{\theta} \right)^{1.5}$$

$$\theta = 60,000 / (-\ln 0.9)^{1/1.5}$$

$$\theta = 268,967 \text{ hours}$$

This scale parameter is used to determine the reliability at the 50,000-hour point using equation 6.48.

$$R(t) = \exp - \left( \frac{t}{\theta} \right)^{\beta}$$

$$R(t) = 0.9 = \exp - \left( \frac{50,000}{268,976} \right)^{1.5}$$

$$= 0.923$$

**STEP 3:** The system reliability is found using equation 6.49 where

$$\begin{aligned}
 R(t) &= R_1(t) R_2(t) \\
 &= (0.905) (0.923) \\
 &= 0.835
 \end{aligned}$$

**STEP 4:** Calculate the system MTBF as follows:

$$\text{MTBF} = \frac{\int_0^T R(t) dt}{1 - R(T)} = \frac{\int_0^T \left( e^{-\lambda t} \left\{ e^{-\left( \frac{t}{\theta} \right)^{\beta}} \right\} \right) dt}{1 - \left[ e^{-\lambda T} \left\{ e^{-\left( \frac{T}{\theta} \right)^{\beta}} \right\} \right]}$$

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

where T is the time period of interest (T = 50,000 hours in this case).

$$\text{MTBF} = \frac{\int_0^{50,000} R(t) dt}{1 - R(50,000)} = 279,795 \text{ hours}$$

### 6.4.5.3.3.4 Nonoperating Failure Rates

The component failure rates in MIL-HDBK-217 (Ref. [11]) and in the Nonelectronic Parts Reliability Data (Ref. [12]) are based upon operating time. There are, however, equipment and systems in which nonoperating time represents a significant portion of the useful life, e.g., missiles, fuses, projectiles, etc.

Nonoperating component failure rate prediction models have been developed in the technical report, RADC-TR-85-91, *Impact of Nonoperating Periods on Equipment Reliability* (Ref. [15]). These models are patterned after those found in MIL-HDBK-217 and are applicable to equipment/systems subjected to nonoperating conditions.

Nonoperating failure rates are computed in a manner similar to operating failure rates only using somewhat different models and different multiplying factors. A typical nonoperating failure rate model is as shown in the following equation for discrete semiconductors.

$$\lambda_p = \lambda_{nb} \pi_{NT} \pi_{NQ} \pi_{NE} \pi_{cyc} \text{ failures}/10^6 \text{ nonoperating hours} \quad (6.50)$$

where:

$\lambda_p$  = predicted transistor or diode nonoperating failure rate

$\lambda_{nb}$  = nonoperating base failure rate

$\pi_{NT}$  = nonoperating temperature factor, based on device style

$\pi_{NE}$  = nonoperating environmental factor

$\pi_{NQ}$  = nonoperating quality factor

$\pi_{cyc}$  = equipment power on-off cycling factor

The nonoperating failure rate prediction models can be used separately to predict nonoperating failure rate and reliability, or they can be used to complement the operating failure rate prediction models in the other sections of the Handbook. The following equations illustrate the methods for

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

predicting equipment (or system) level nonoperating reliability ( $R_n$ ), service life failure rate ( $\lambda_{sl}$ ) and combined operating/nonoperating reliability ( $R_{(o/n)}$ ).

$$R_{n_i} = \exp(-\lambda_{ni}t_{ni}) \quad R_n = \prod_{i=1}^n R_{n_i}$$

$$\lambda_{(sl)_i} = D_{o_i} \lambda_{o_i} + D_{n_i} \lambda_{n_i} \quad \lambda_{sl} = \sum_{i=1}^n \lambda_{(sl)_i}$$

$$R_{(o/n)_i} = \exp(-(\lambda_{ni}t_{ni} + \lambda_{oi}t_{oi})) \quad R_{(o/n)} = \prod_{i=1}^n R_{(o/n)_i}$$

where:

$R_{n_i}$  = nonoperating reliability of the  $i^{\text{th}}$  item

$\lambda_{ni}$  = nonoperating failure rate in the  $i^{\text{th}}$  nonoperating environment

$t_{ni}$  = nonoperating time in the  $i^{\text{th}}$  nonoperating environment

$\lambda_{(sl)_i}$  = service life failure rate of the  $i^{\text{th}}$  item, equal to the number of failures per unit time regardless of operational mode

$D_{o_i}$  = duty cycle in the  $i^{\text{th}}$  operating environment, equal to the time in the  $i^{\text{th}}$  operating environment divided by total operating time plus total nonoperating time

$\lambda_{oi}$  = operating failure rate in the  $i^{\text{th}}$  operating environment

$D_{n_i}$  = duty cycle in the nonoperating environment, equal to the time in the  $i^{\text{th}}$  nonoperating environment divided by total operating time plus total nonoperating time

$\lambda_{ni}$  = nonoperating failure rate in the  $i^{\text{th}}$  nonoperating environment

$R_{(o/n)_i}$  = reliability of the  $i^{\text{th}}$  item for the mission duration plus nonoperating time between missions

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

The following cautions are offered to prevent the misuse of the nonoperating failure rate models:

- (1) Temperature in the models for discrete semiconductors and microelectronic devices is the ambient nonoperating temperature, not operating case or junction temperatures.
- (2) Nonoperating environment is the actual environment to which the component is exposed. For example, an airborne radar between missions is most likely exposed to a ground fixed environment.
- (3) Equipment power on-off cycling is determined at the equipment level. The parameter does not refer to actuations of switches or relays, nor specific circuit applications within the operating state.

### 6.4.5.3.4 Reliability Physics Analysis (Ref. [17] and [18])

Reliability physics is a technique for identifying and understanding the physical processes and mechanisms of failure. The concept has been around for decades and has resulted in great strides in component reliability design, even as component complexity has increased. The purpose of a reliability physics analysis is to identify components and processes that exhibit wearout failure before the expected end of use and to isolate the root cause of the failure.

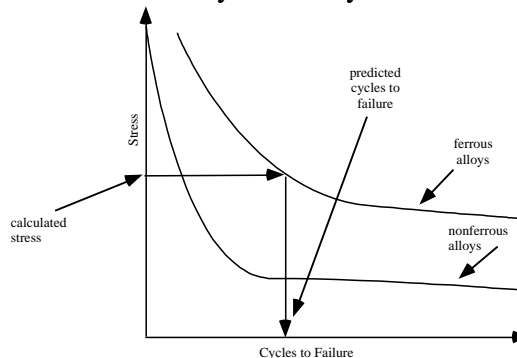
The basic approach to this analysis, which is applicable to new or old components or processes, is outlined in Table 6.4-15.

An example of reliability physics approach is determine the average failure rate of a pinion during the first 1,500 hours of operation given a speed of 90,000 revolutions per hour. The  $L_{10}$  life of the pinion is  $450 \times 10^6$  revolutions with a Weibull slope of 3.0.  $L_{10}$  life is the length of time that 90% of the pinions will meet or exceed during use before they fail. Table 6.4-16 illustrates the steps involved.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

TABLE 6.4-15: BASIC APPROACH TO RELIABILITY PHYSICS ANALYSIS

Step	Discussion
1. Define the operating and nonoperating life requirements	Length of time or number of cycles expected or needed for both operating and nonoperating periods should be determined.
2. Define the life environment	Temperature, humidity, vibration and other parameters should be determined so that the load environment can be quantified and the cycle rates determined. For example, a business computer might expect a temperature cycle once each day from 60°F to 75°F ambient. This would quantify the maximum and minimum temperatures and a rate of one cycle per day.
3. Identify the material properties	Usually this involves determining material characteristics from a published handbook. If unique materials are being considered, then special test programs will be necessary.
4. Identify potential failure sites	Failure areas are usually assumed to fall into categories of new materials, products or technologies. Considerations should include high deflection regions, high temperature cycling regions, high thermal expansion materials, corrosion sensitive items, and test failures.
5. Determine if a failure will occur within the time or number of cycles expected	A detailed stress analysis using either a closed form or finite element simulation method should be performed. Either analysis will result in a quantifiable mechanical stress for each potential failure site.
6. Calculate the component or process life	Using fatigue cycle curves from material handbooks, estimate the number of cycles to failure. The following figure shows a typical fatigue curve for stress versus cycles to failure. Specific material fatigue data can be obtained from databases maintained by the Center for Information and Numerical Data Analysis and Synthesis.



STRESS VERSUS CYCLES TO FAILURE



SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

TABLE 6.4-16: EXAMPLE OF A PINION RELIABILITY ANALYSIS

Step	Parameters and Calculations
1. Identify the pinion life characteristics	<ul style="list-style-type: none"> <li>• <math>L_{10} = 450 \times 10^6</math> revolutions</li> <li>• Weibull slope (<math>\beta</math>) = 3.0</li> <li>• Speed = 90,000 revolutions/hour</li> </ul>
2. Convert $L_{10}$ revolutions to hours	$L_{10} (\text{Hours}) = \frac{L_{10} \text{ Revolutions}}{\text{Revolutions/Hour}}$ $\frac{450 \times 10^6}{90,000} = 5,000$
3. Determine the characteristic life using the Weibull reliability function	$R(t) = \exp\left(-\frac{t}{\theta}\right)^\beta$ $\theta = \frac{t}{[-R(t)]^{1/\beta}}$ <p>where: <math>t</math> = time in hours  <math>\theta</math> = mean-time-to-failure  <math>\beta</math> = Weibull slope of 3.0  <math>R(t)</math> = 0.9 at 5,000 hours</p>
4. Compute the failure rate for 1,500 hours	$\theta = \frac{5,000}{[-\ln(0.9)]^{1/3}} = 10,586 \text{ hours}$ $\lambda(t) = H(t) = \frac{t^{\beta-1}}{\theta^\beta}$ <p>where: <math>\lambda(t)</math> = instantaneous failure rate  <math>t</math> = time in hours  <math>\theta</math> = mean time between failure</p> $\lambda(t) = \frac{(1,500)^{3-1}}{(10,586)^3} = 1.9 \text{ failures}/10^6 \text{ hours}$

---

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

#### 6.4.5.4 Computer Aided Reliability Prediction

Reliability prediction for a modern complex system requires a tremendous amount of computation. To overcome this obstacle, various commercial software packages have been developed to automate MIL-HDBK-217 (Ref. [11]) and other reliability predictions. In fact, some of the more elaborate commercial software packages also handle intricate mission reliability modeling of complex systems.

An ever-growing abundance of reliability prediction software packages are available in a variety of price ranges, each offering an assortment of common attributes and various unique features. Due to the changes occurring daily in this field it is not possible to include a detailed discussion of each such program. A comprehensive listing of the various commercial packages currently available is beyond the scope of this handbook, but may be found at the RAC world wide web site at (<http://rome.iitri.com/RAC/DATA/RMST/>).

#### 6.5 Step-By-Step Procedure for Performing Reliability Prediction and Allocation

In summary, the following basic steps apply to the prediction and allocation of reliability requirements:

- Step (1) Definition of equipment
- Step (2) Definition of failure
- Step (3) Definition of operational and maintenance conditions
- Step (4) Develop the reliability block diagram(s)
- Step (5) Establish mathematical model(s)
- Step (6) Compilation of equipment, component or part lists
- Step (7) Performance of “similar item,” “parts count,” “parts stress analysis,” “reliability physics analysis predictions”
- Step (8) Assignment of failure rates or reliability
- Step (9) Combination of failure rates or reliability
- Step (10) Computation of equipment reliability
- Step (11) Allocate failure rates and reliability
- Step (12) Allocate among redundant configurations

## SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING AND PREDICTION

---

### Step (13) Evaluate feasibility of allocated requirements

The procedures for making pre-design or interim reliability predictions are basically the same as for final design predictions except that the difference lies in the degree of precision (and details) with which the basic steps are implemented.

For predictions made at any stage of development, each of the steps will be carried out to the maximum extent possible. The system failure and operating and maintenance conditions should be defined as explicitly as possible. Reliability block diagrams are constructed to the lowest identifiable function, and appropriate system reliability formulas are established.

Precise parts lists, of course, cannot be compiled prior to design of an equipment. It is necessary, however, to make the best possible estimate of the parts complements of the various item subdivisions (blocks on the reliability diagram).

Stress analyses obviously cannot be made prior to design. However, for portions of the equipment that have not been designed, gross stress analyses can be accomplished. Stress levels may be assumed and failure rate estimates can be made by applying failure rate vs. stress tradeoffs to the assumed failure rate data. The process of combining part failure rates to obtain preliminary block failure rates or reliabilities, of adjusting block rates or probabilities, and of computing equipment reliability is the same for pre-design and interim predictions as for final predictions.

### 6.6 References for Section 6

1. MIL-HDBK-781, "Reliability Test Methods, Plans and Environments for Engineering Development, Qualification and Production," 1987.
2. Arsenault, J.E., et al., "Reliability of Electronic Systems," Computer Science Press, Inc., 1980.
3. Fuqua, N.B., "Reliability Engineering for Electronic Design," Marcel Dekker, Inc., New York, NY, 1987.
4. Klion, J., "Practical Electronic Reliability Engineering," Van Norstrand Reinhold, 1992.
5. Shooman, M.L., "Probabilistic Reliability, An Engineering Approach," McGraw Hill, 1968.
6. Von Alven, W.H., "Reliability Engineering," Prentice Hall, Inc., Englewood Cliff, NJ, 1964.
7. "Engineering Design Handbook: Design for Reliability," AMCP 706-196, ADA 027370, 1976.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

8. "Reliability Toolkit: Commercial Practices Edition," Reliability Analysis Center and Rome Laboratory, 1995.
9. Boyd, M.A., "What Markov Modeling Can Do For You," Annual Reliability and Maintainability Symposium - Tutorial Notes, 1996.
10. Regulinski, T.L., "Availability Function for Communicating Computer Net," Proceedings Reliability and Maintainability Symposium, 1980.
11. "Reliability Prediction of Electronic Equipment," MIL-HDBK-217F, 1995.
12. "Nonelectronic Parts Reliability Data," (NPRD), Reliability Analysis Center, 1995.
13. Bellcore, TR-332, "Reliability Prediction Procedure," Issue 5, December 1995.
14. "Electronic Parts Reliability Data," (EPRD), Reliability Analysis Center, 1997.
15. "Impact of Nonoperating Periods on Equipment Reliability," RADC-TR-85-91, 1985.
16. "Nonoperating Reliability Data Book," (NONOP-1), Reliability Analysis Center, 1987.
17. "Reliability Assessment Using Finite Element Techniques," RADC-TR-89-281, Rome Laboratory, 1989.
18. "Computer-Aided Assessment of Reliability Using Finite Element Methods," RADC-TR-91-155, Rome Laboratory, 1991.

SECTION 6: RELIABILITY SPECIFICATION, ALLOCATION, MODELING  
AND PREDICTION

---

THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.0 RELIABILITY ENGINEERING DESIGN GUIDELINES****7.1 Introduction**

Reliability engineering is the technical discipline of estimating, controlling, and managing the probability of failure in devices, equipment and systems. In a sense, it is engineering in its most practical form, since it consists of two fundamental aspects:

- (1) Paying attention to detail
- (2) Handling uncertainties

However, merely to specify, allocate, and predict reliability is not enough. One has to do something about it in terms of having available a family of design guidelines which the designer can use to achieve a desired reliability. These guidelines are provided in this section.

During a product development program, a design is developed to meet previously defined quantitative reliability requirements. The importance of designing in the required degree of reliability initially cannot be overemphasized, for once the design is approved, inherent reliability is fixed.

There are a host of design principles and tools of which the designer should be aware and should use as required to achieve a reliable electronic equipment/system design. They include:

- (1) Parts Management
- (2) Part derating
- (3) Reliable circuit design
- (4) Redundancy
- (5) Environmental design
- (6) Human factors design
- (7) Failure modes and effects analysis (FMEA)
- (8) Fault tree analysis (FTA)
- (9) Sneak circuit analysis
- (10) Design reviews
- (11) Design for testability
- (12) System safety program
- (13) Finite element analysis

Each of these will be briefly discussed in this section in terms of its role in the design of reliable equipment/systems.

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

### 7.2 Parts Management

Many factors affect the ultimate levels of quality and reliability of parts. Possibly the most important factor is the degree to which the manufacturer is able to fabricate them in a defect-free manner. This factor is a strong function of the volume and continuity of part production. Additional factors affecting part reliability are the levels to which the part is screened, the application, and the manner in which the part is integrated into the system.

The volume of parts produced usually impacts field reliability, since manufacturers producing large numbers of parts on a continuous basis can easily benefit from Statistical Process Control (SPC). When used wisely, SPC has proven to be an effective tool for improving processes, thereby increasing the quality and reliability levels of manufactured parts. Manufacturing lines intermittently producing small numbers of parts on a line with non-standard manufacturing processes typically do not exhibit the reliability levels of fully loaded manufacturing lines using well-controlled manufacturing processes.

Critical parts are often highly reliable, simply due to the attention given to them by both the part manufacturers and by the users. As an example, consider integrated circuits. When first used extensively twenty years ago, they often were the predominant device type limiting system reliability. Since then, due to their critical nature, part manufacturers have improved their reliability by orders of magnitude and part users are learning how to apply them in a manner which results in a robust design. These efforts have resulted in integrated circuits that are much more reliable than many other part types used in systems.

Therefore, high usage, highly critical and high volume parts often show rapid technology maturation, whereas low usage, noncritical or low volume parts can exhibit slower reliability improvement and result in lower levels of field reliability. As an example, consider the items identified by field data as being high failure rate parts: fasteners, actuators, connectors, transducers and switches. These are ordinary and necessary parts which are not considered state-of-the-art, but yet can significantly impact field reliability.

The general elements of an effective Parts Management Plan (PMP) are (MIL-HDBK-965, "Acquisition Practices for Parts Management" provides guidance in selecting tasks to include in a PMP):

- (1) Preferred Parts List
- (2) Vendor and Device Selection
- (3) Critical Devices/Technologies/Vendors
- (4) Device Specifications
- (5) Screening
- (6) Part Obsolescence
- (7) Failure Reporting, Analysis and Corrective Action (FRACAS)

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

Each of these elements can be tailored to meet the specific needs of each system. Reference [1] "Parts Selection, Application and Control" provides generic guidance in the development of this process.

Each of these elements are discussed in the following subsections.

A comprehensive PMP defines the manner in which each of the aforementioned elements will be addressed. It should identify the responsible personnel and include a milestone schedule. This plan can also be tailored in accordance with specific requirements of the system for each of the PMP elements. Tailoring should be accomplished considering:

- |                            |   |
|----------------------------|---|
| (1) Development Cycle Time | (6) Budget                                |
| (2) Warranty Period        | (7) Screenability                         |
| (3) Maintainability        | (8) Preventive Maintenance                |
| (4) Cost of Failure        | (9) Customer Requirements                 |
| (5) System Characteristics | (10) Severity (or Criticality) of Failure |
| (a) volume                 |   |
| (b) weight                 |   |
| (c) performance            |   |
| (d) operating environment  |   |

Understanding, defining and then implementing all the tasks involved in a PMP program is the key to its success. The representation and active participation of the following disciplines, as a minimum, are necessary to enable, in a concurrent engineering fashion, an effective PMP:

- |                                    |                               |
|------------------------------------|-------------------------------|
| (1) Parts (components) engineering | (3) Design engineering        |
| (2) Reliability engineering        | (4) Manufacturing engineering |

Successful implementation of a PMP requires a disciplined approach, and must have management participation and support to ensure cooperation among disciplines and resolve any differences based on the ultimate impacts on cost, schedule and performance.

### 7.2.1 Establishing a Preferred Parts List (PPL)

In the course of a design effort, equipment designers need to select the parts and materials to be used to meet specified equipment requirements for performance, reliability, quality, producibility and cost. This selection task is greatly enhanced if the designer has a list of preferred parts available to help in this selection process.

Preferred parts are those whose quality and reliability are well-known to the industry, and are probably parts that the company is already using in other equipments. Without a preferred parts list (PPL), designers may tend to choose parts in haphazardly. The result is the uncontrolled proliferation of parts throughout a manufacturer's product line, all varying in performance and reliability. All potential candidate parts should undergo an independent assessment before being



---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

placed on the preferred parts list. Information sheets or data sheets from part suppliers may paint an optimistic picture of the part's capabilities, but may omit information regarding the part's inherent characteristics that are critical to proper operation of the final product.

The absence of a PPL may have wide-ranging consequences for manufacturing, purchasing, and logistics. Manufacturing engineers may have to cope with parts that require a variety of assembly methods and unique tooling. More inventory may be needed and, as a result, inventory costs can mushroom out of control. Manufacturing automation may also be adversely affected. Purchasing representatives may have to deal with many different suppliers, making it hard for them to monitor quality and timely delivery, and to obtain volume cost discounts. Logistics specialists must now provide spares for many different parts, enter them into the supply system, and find storage space for all of them.

Some consequences of designing equipment without a PPL are:

- (1) Proliferation of non-preferred parts and materials with identical functions
- (2) Increased need for development and preparation of engineering justification for new parts and materials
- (3) Increased need for monitoring suppliers and inspecting/screening parts and materials
- (4) Selection of obsolete (or potentially obsolete) and sole-sourced parts and materials
- (5) Possibility of diminishing sources
- (6) Use of unproven or exotic technology ("beyond" state-of-the-art)
- (7) Incompatibility with the manufacturing process
- (8) Inventory volume expansion and cost increases
- (9) Increasing supplier base and audit requirements
- (10) Loss of "ship-to-stock" or "just-in-time" purchase opportunities
- (11) Limited ability to benefit from volume buys
- (12) Increased cost and schedule delays
- (13) Nonavailability of reliability data
- (14) Additional tooling and assembly methods may be required to account for the added variation in part characteristics
- (15) Decreased part reliability due to the uncertainty and lack of experience with new parts
- (16) Impeded automation efforts due to the added variability of part types
- (17) Difficulty in monitoring vendor quality due to the added number of suppliers
- (18) More difficult and expensive logistics support due to the increased number of part types that must be spared.

When a PPL is available at the beginning of the design process, designers avoid using non-approved parts and the laborious task of having to supply engineering justification for their use.

---

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

Preferred parts databases help to flag obsolete parts and also indicate a part's long term availability (i.e., how long a given part may actually be available in the market).

The PMP must provide some level of standardization to minimize the number of new parts entering the system/equipment, or the logistic support and supply system, and yet still be flexible enough to effectively capitalize on the advantages offered by alternative technologies. To be truly effective, the PMP must first ensure that the parts selected will provide the necessary level of performance and reliability over the projected life of the system/equipment. It must also be tailored to the expected life of the equipment to ensure, among other things, that replacement spares will continue to be available throughout the effective life of the system/equipment. The PPL should be updated periodically to ensure a proactive approach to minimizing the impact of part obsolescence.

### 7.2.2 Vendor and Device Selection

Major factors to consider when implementing a PMP is the evaluation of vendors and the selection of components. It is imperative that engineers select and use components from manufacturers in which they have confidence. This confidence can be attained either empirically through adequate past performance of the part manufacturer, or from verification that the manufacturer is indeed producing high quality parts. The latter can be achieved via evaluation of the part manufacturing processes through testing and subsequent data analysis.

To ensure the supply of adequate parts, both vendors and subcontractors must be effectively managed. A procedure is needed in which each vendor/technology is evaluated, certified and qualified in a cost-effective manner. Traditionally, this procedure was to test all devices and audit all vendors. Due to the increased emphasis on quality (especially in microcircuits), a more generic approach to vendor certification/qualification of processes is recommended. Then, existing data from technology families can be used for qualification by similarity. Ongoing vendor/customer testing programs on representative products may be used to determine acceptability. Procedures for performing and monitoring vendor/product testing and incoming inspection are still necessary, but should be tailored to allow each vendor to be handled on a case-by-case basis. For example, outgoing vendor quality and user incoming inspection and board level testing can be monitored to determine device quality and product design/manufacturing process compatibility. Data analysis can then determine the need for vendor testing, incoming inspection and increased vendor surveillance. These data can also form the basis for determining whether a "ship to stock" program (i.e., acceptance of a product without incoming inspection) is feasible.

Parts must be selected based on a knowledge of both the application environment in which the part is to operate and the conditions it is exposed to during part manufacturing, assembly, handling and shipping. It is equally important to understand how the failure rate during the part's useful life, and its wearout characteristics (lifetime), are impacted by the specific application conditions. Only with this understanding are robust designs possible.

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

One specific area of importance is the continuity of production. As mentioned earlier, facilities/production lines that manufacture parts on a continuous basis often produce higher quality parts than those manufactured on an intermittent basis. Intermittent production can be a characteristic of custom, low usage parts. High volume, continuous production is usually controlled in a statistical manner, whereas intermittent production may not be able to implement SPC. Additionally, intermittent lines often run into unanticipated problems associated with start-up which can adversely affect the quality, availability, and reliability of the part.

Many successful organizations have developed a qualified manufacturers list (QML) on which procurement decisions are based. A QML lists manufacturers who have proven that they can supply good parts with a high degree of confidence. The DoD is also using this methodology in the procurement of microcircuit devices, via the QML program (i.e. MIL-PRF-38535).

Part manufacturers can be evaluated in many ways. For suppliers of parts that have been manufactured for some time, analysis of historical reliability/quality data is usually the optimum method. In many cases, these data are readily available from the manufacturer and, in some cases, are published in their data catalogs. To be meaningful, historical data must be representative of the same, or a similar, part with few changes, and must be for a similar application under similar operational stresses.

Vendor evaluation can be accomplished by analyzing design, manufacturing, quality, and reliability practices. Figure 7.2-1 illustrates a methodology to evaluate potential vendors.

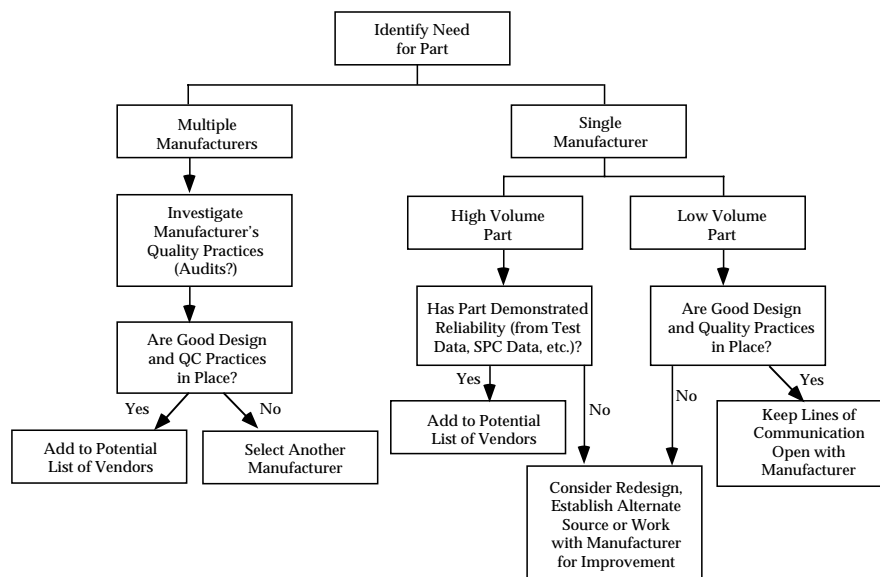


FIGURE 7.2-1: VENDOR SELECTION METHODOLOGIES

An audit/validation should focus on whether a documented baseline system exists and is being used. Additionally, required demonstration of generic product manufacturability, verified by

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

reliability testing, is necessary. Representative questions such as those in Table 7.2-1 should be asked.

TABLE 7.2-1: QUESTIONS FOR PART SUPPLIERS

<ul style="list-style-type: none"><li>• Is a quality program defined and implemented?</li><li>• Have potential failure mechanisms been identified?</li><li>• Are the manufacturing materials and processes documented?</li><li>• Are there process controls in place?</li><li>• Are parts manufactured continuously or is there intermittent production?</li><li>• What defect levels are present?</li><li>• Is there a goal in place for continuous improvement?</li><li>• Have life limiting failure mechanisms been designed out?</li><li>• If it is not practical to design or screen out life limiting mechanisms, have they been modeled such that the user can quantify the part's lifetime in a specific application?</li><li>• Are efforts being taken to identify the causes of part failure and to improve the manufacturing process to alleviate their occurrence?</li><li>• Is the part screening and qualification process effective?</li><li>• Are design rules used and adhered to that result in high quality and reliability?</li><li>• Are design changes made only after analyzing and quantifying possible reliability impact?</li><li>• What is the on-time delivery success rate?</li></ul>
--

Recent improvements in customer/supplier relationships have resulted in alliances or partnerships where both parties work together to improve the quality and reliability of delivered products. However, to achieve these alliances, it is necessary to understand that:

- (1) Effective preferred parts selection is a dynamic process which minimizes the number of different parts used, while providing designers an adequate choice of components to meet equipment performance requirements.
- (2) Vendor selection certification and qualification criteria based on technical expertise are used to minimize the number of vendors.
- (3) Good production suppliers are willing to support problem analysis and corrective actions.

A process based on these considerations should be formalized to assess and validate potential suppliers' quality, reliability and manufacturing systems, and delivery, cost and service performance. The resulting data, when reviewed by cognizant personnel (i.e., purchasing, design

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

engineering and manufacturing), can be used to select the appropriate suppliers. Once this step is accomplished, alliances or partnerships can be established that can result in a win-win situation, where the procurement process changes from an adversarial to a cooperative relationship. To establish the continuous improvement process and manage the supplier, a reassessment and information exchange program can be put in place. The validation/audit plan results that were used to select a vendor can now be the reference from which progress is measured.

### 7.2.2.1 Critical Devices/Technology/Vendors

Critical part types are considered to be those that require additional attention due to potential reliability, safety or availability problems. Many parts programs focus too much attention on standard or non-controversial part types. It is imperative that special attention be given to critical parts, since they are often the parts driving the system reliability. The establishment of a listing of critical devices, technology and vendors, and a monitoring/action plan, should be part of every PMP, and should address components exhibiting the following characteristics:

- (1) Performance Limitations: due to stringent environmental conditions or non-robust design practice.
- (2) Reliability Limitations: component/materials with life limitations or use of unrealistic derating requirements.
- (3) Vendors: those with a past history of delivery, cost performance or reliability problems
- (4) Old Technology: those with availability problems
- (5) New Technology: parts fabricated using immature design and manufacturing technology

The first three categories require historical data to track and define actions to minimize their occurrence or provide alternate solutions. In addition, sound component engineering judgment and the combined efforts of design, reliability, and manufacturing engineering, and vendors, are needed to ensure the identification and management of critical components.

The subject of old and new technology can involve the generation of different procurement procedures for tracking technology maturity, obsolescence and hidden hybrids (i.e., those devices that fall between generic device categories and, as a result, are incorrectly specified and tested, see 7.2.2.3).

The PMP should address the identification and control of limited or critical parts and off-the-shelf equipment. Also, the PMP must ensure that parts engineering, design, manufacturing and reliability personnel are notified of potential risks in using critical parts/technology. As stated previously, a PMP program must be tailored to account for the unique failure mechanisms associated with the parts being used. For example, if plastic packaged microcircuits are used, their expected lifetime must be determined as a function of the use environment (temperature, humidity, dissipated power, etc.) and then compared to the design life of the equipment in which the component operates. As another example, consider off-the-shelf equipment. In this case, the

---

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

equipment must be analyzed to assess its suitability for use in its intended application. This is especially true for commercial equipment designed for benign environments that are to be used in more severe environments. A determination should be made of its reliability and performance, since it would be neither cost-effective nor practical for the vendor to change the design or production procedures. The task becomes one of evaluating subcontractor procedures, reliability design analyses and past performance.

### 7.2.2.1.1 ASIC Devices

The rapid technology changes in the field of microelectronics, both hybrid and monolithic, have to be monitored closely. Application Specific Integrated Circuits (ASICs) are one part type usually considered to be critical. The advent of ASICs requires a change in the device selection procedure. The term "ASIC" describes a wide variety of different types of devices which can include custom and semicustom standard cells, gate arrays, Programmable Logic Devices (PLD) and Field Programmable Gate Arrays (FPGA) typically designed for a specific application. Advantages include a relatively short development cycle and customized performance and functionality. Disadvantages are that the equipment schedule may be impacted because system designers are involved in the device design cycle, and unproven vendors and technologies may be used for the first time.

Typically, ASIC devices are designed for a very specific application and then produced and sold in very limited quantities. Thus, there is no market for marginal devices. Historically, generic ICs have been produced in a tiered market environment. Parts not meeting the highest level of performance could usually be sold to a less demanding customer at a reduced price. This is simply not the case with ASICs. Either they are 100% perfect or they are scrap. Given this fact, there is a very strong incentive to reduce or eliminate all possible variation in the part manufacturing processes to attain a very high yield of good parts. Thus, Total Quality Management (TQM) and SPC become imperative to the manufacture of these types of parts. To use ASICs, a supplier must select and certify a silicon foundry and design the device using foundry design rules. Performance would be demonstrated through simulation tools. The foundry would then fabricate wafers and packaged devices for test. The planning and management of ASIC design requires a very rigorous and controlled procedure to achieve desired device functionality, reliability, cost and delivery schedules.

### 7.2.2.1.2 GaAs and MMIC Devices

Gallium arsenide (GaAs) devices are now being used in military and commercial systems. GaAs offers some significant advantages over silicon that can result in improved device performance. It has unique qualities which allow the fabrication of devices that can operate at frequencies which outperform their silicon counterparts. In addition, GaAs offers inherent radiation hardness and improved power efficiency for high frequency digital and analog circuitry.

Monolithic Microwave Integrated Circuits (MMIC) are replacing hybrid microwave devices throughout the industry as a result of the Defense Advanced Research Project Agency (DARPA)

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

sponsored Monolithic Microwave Millimeter Wave Integrated Circuit (MIMIC) program. Before the development of GaAs MMIC technology, discrete packaged devices and multifunction assemblies were commonly utilized in microwave applications. MMIC technology, however, offers several advantages including weight/size reduction, process tolerance and uniform performance with a reduced need of tuning circuits. These advantages, combined with GaAs's inherent performance advantages, have led to significant interest in the technology.

To date, information concerning the reliability of GaAs and MMIC components has shown varying results and inconsistent activation energies for a specific failure mechanism. Thus, the absolute reliability of GaAs devices is not easy to predict with accuracy, though an approximation can be made based on government/industry reliability studies.

### 7.2.2.2 Plastic Encapsulated Microcircuits (PEMs)

Plastic packaging is a leading factor in the growth of microelectronics companies and has had a significant positive effect in the telecommunications, computer and automotive industries. PEMs have demonstrated cost effectiveness while providing improved performance and reliability in these applications environments. Now, acquisition reform initiatives and continued improvements in plastic packaging and die protection (i.e., silicon nitride passivation) have led to their consideration and limited use in military environments. The RAC publication PEM2 (Ref. 2) provides additional information.

### 7.2.2.3 Hidden Hybrids

Quality and reliability efforts for microcircuits have been more intense than for any other commodity items, resulting in orders of magnitude improvement in their performance since the 1960's. However, the procurement of complementary devices/modules sometimes ignores the lessons learned in this area. We have chosen to call these devices "hidden hybrids," indicating a mix or composite of technologies.

Examples include the following:

- |                                     |                        |
|-------------------------------------|------------------------|
| (1) Crystal Oscillators             | (4) Solid State Relays |
| (2) Multichip and Microwave Modules | (5) Transformers       |
| (3) Power Regulators (Supplies)     |                        |

In many cases, these items have escaped the traditional testing and technology/vendor evaluation that has led to the successes achieved for microelectronics devices. Crystal oscillators evolved from a combination of discrete components mounted on a printed wiring board to hybrid microcircuits made up of chip components (including the crystal), all contained in a single hermetic package. Solid state relays are essentially a hybrid device containing discrete semiconductor components which should be individually tested and controlled.

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

The problem is presently being compounded by the various types of multichip and high frequency (i.e., R.F. and microwave) modules being introduced. Multichip modules (MCM) are taking advantage of integrated circuit, hybrid and printed wiring board (PWB) technologies, and are being used to fabricate state-of-the-art high performance products.

It is specifically recommended that packaged items be reviewed to uncover potential "hidden hybrids" as shown in Table 7.2-2. Once located, the appropriate component procurement approach (such as MIL-PRF-38534) should be used to ensure reliable and quality products. Incorporation of appropriate evaluation, audit and testing requirements could eliminate costly testing and corrective action procedures at a later date, while ensuring customer satisfaction.

TABLE 7.2-2: HIDDEN HYBRID CHECKLIST

<p><b>Analyze:</b></p> <ul style="list-style-type: none"><li>• Fabrication Process - uses hybrid microcircuit assembly techniques</li><li>• Technology - contains microcircuits and/or semiconductors</li><li>• Packaging - potted/encapsulated modules</li></ul> <p><b>Take Action:</b></p> <ul style="list-style-type: none"><li>• Testing Requirements - per applicable test procedure</li></ul>
---

#### 7.2.2.4 Device Specifications

Part electrical, mechanical and physical characteristics should be defined in a device specification to be used for design and procurement. Applicable device electrical performance parameters that ensure product performance objectives are met for all operating conditions should be specified, including reliability parameters. This information may be available in vendor catalogs/data sheets. Special care should be taken for electrical parameters that are "guaranteed but not tested," or other special features which should be discussed and agreed to with each vendor. The part specification should be based on several factors, including operating environments, worst case stress levels, and quality requirements.

The Defense Electronic Supply Center (DESC) Standard Microcircuit Drawing format is an example of how to prepare a company specification for microcircuits and other applicable components. This format has been reviewed and coordinated with industry and can be used to develop a specification that provides realistic, clearly stated requirements. Details are provided in MIL-HDBK-780 "Standardized Microcircuit Drawings." Reference [3] "Analog Testing Handbook (ATH)" provides information for the specification for analog and mixed mode (analog/digital) devices.



---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.2.2.5 Screening**

Screening, or 100% testing similar to that included in MIL-PRF-38534 and -38535, is recommended, pending vendor validation and use experience. Data from appropriate in-process and reliability testing can be used to justify deletion of end-of-line tests. Vendor/customer trust and alliances can result in practical cost-effective testing.

**7.2.2.6 Part Obsolescence and Diminishing Manufacturer Sources (DMS)**

Obsolescence occurs when parts that are required for system support are no longer manufactured (usually due to insufficient market demand). It is a common occurrence within the DoD for systems to have lifetimes greater than the life cycle of their supporting part technologies. Hence, part obsolescence is typically more of a problem for military systems than for commercial systems. Also, parts qualified for military use have historically represented more mature technologies relative to those used in non-military applications. The potential for diminishing manufacturing sources, causing parts that are not yet obsolete to become unavailable, must also be considered. This unavailability can be the result of the manufacturer experiencing limited orders, downsizing, market instability, or the result of other business decisions to exit the market for a particular technology or device. Regardless of the reason, the part is unavailable, and the effect is essentially the same as if the part had become obsolete.

Part and vendor obsolescence management should be a basic part of a company's operating, design, and manufacturing procedures (i.e., best commercial practices) and be substantially product independent, evolve around needed components, operating environments and package styles. Implementation of an effective PMP requires diligent management in maintaining part availability for system support, including taking the actions necessary to maintain availability of parts that are, or will be, obsolete during the equipment life cycle. Such actions can be grouped into two categories: management and technical.

Management solutions to part availability problems include preventive measures to alleviate the use of potentially obsolete parts, detection of the use of potentially unavailable parts, and identification of the need to procure an adequate quantity of parts to support the equipment throughout its life cycle. Management solutions include the use of a PPL and the lifetime purchase of parts to ensure part availability in the event that they become obsolete. This latter solution carries its own risks and burdens (for example, provisions for storing the parts in a sufficiently benign environment that precludes the occurrence of storage-related failure mechanisms).

Technical solutions include replacement of the unavailable part with an equivalent part, device emulation, and system redesign. If there is a direct replacement available, substitution is usually the easiest and least costly solution. There are several semiconductor information sources that can assist in the identification of equivalent parts. These include the IC Master and Part Master (available from International Handling Services), and Computer Aided Product Selection (CAPS) (available from Cahners Publishing).

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

Early notification of part/vendor end-of-life status provides time to select an acceptable solution that will minimize the identified problem's impact on manufacturing. External sources such as the Defense Logistics Agency/Defense Supply Center Columbus (DLA/DSCC), Government Industry Data Exchange Program (GIDEP) and vendors, as well as management of the company's internal PPL, can be used to provide early notification. Figure 7.2-2 illustrates a process flow for short and long term solutions that takes place when obsolete part notification is received. The major difference between short and long term solutions is that, in the long term solution, even when a part or vendor exists or another solution is found, the effort does not stop. As mentioned, it is critical that the solution is not just a stop gap and that long term support issues are addressed. Therefore, a trade study using the factors indicated in Figure 7.2-2 is performed to ensure a long term solution is not required in the future. (This concept is further described in reference [4] "767 AWACS Strategies For Reducing DMS Risk").

When a device has been identified as needed but unprocurable, the most practical solution is emulation. Device emulation is a process by which a direct replacement is designed and fabricated for an unavailable part. The design task may include reverse engineering, simulation, or direct design and fabrication (if original schematics and drawings are available). The Defense Logistics Agency (DLA) currently leads such an emulation program, referred to as the Generalized Emulation of Microcircuits (GEM).

System redesign is also a possible technical solution to alleviate the dependence on unavailable parts. Device emulation and system redesign can be very costly solutions to the unavailability problem. Implementation of preventive measures early in the part selection process can provide significant cost savings as the system reaches end-of-life.

The VHSIC Hardware Description Language (VHDL) is a valuable tool that can assist in the emulation or redesign of devices. VHDL is fast becoming the hardware description language of choice because it is an IEEE standard and has technology process and vendor independence, CAD tool support, and top-down design methodology capability. What is required is a VHDL behavioral description of the obsolete device or printed wiring assembly. The next step is to produce a structural VHDL description of the design to be emulated, which can then be processed by logic and layout synthesis tools of choice. This emulated design can then be processed by a compatible wafer foundry processing capability and packaged appropriately for insertion.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

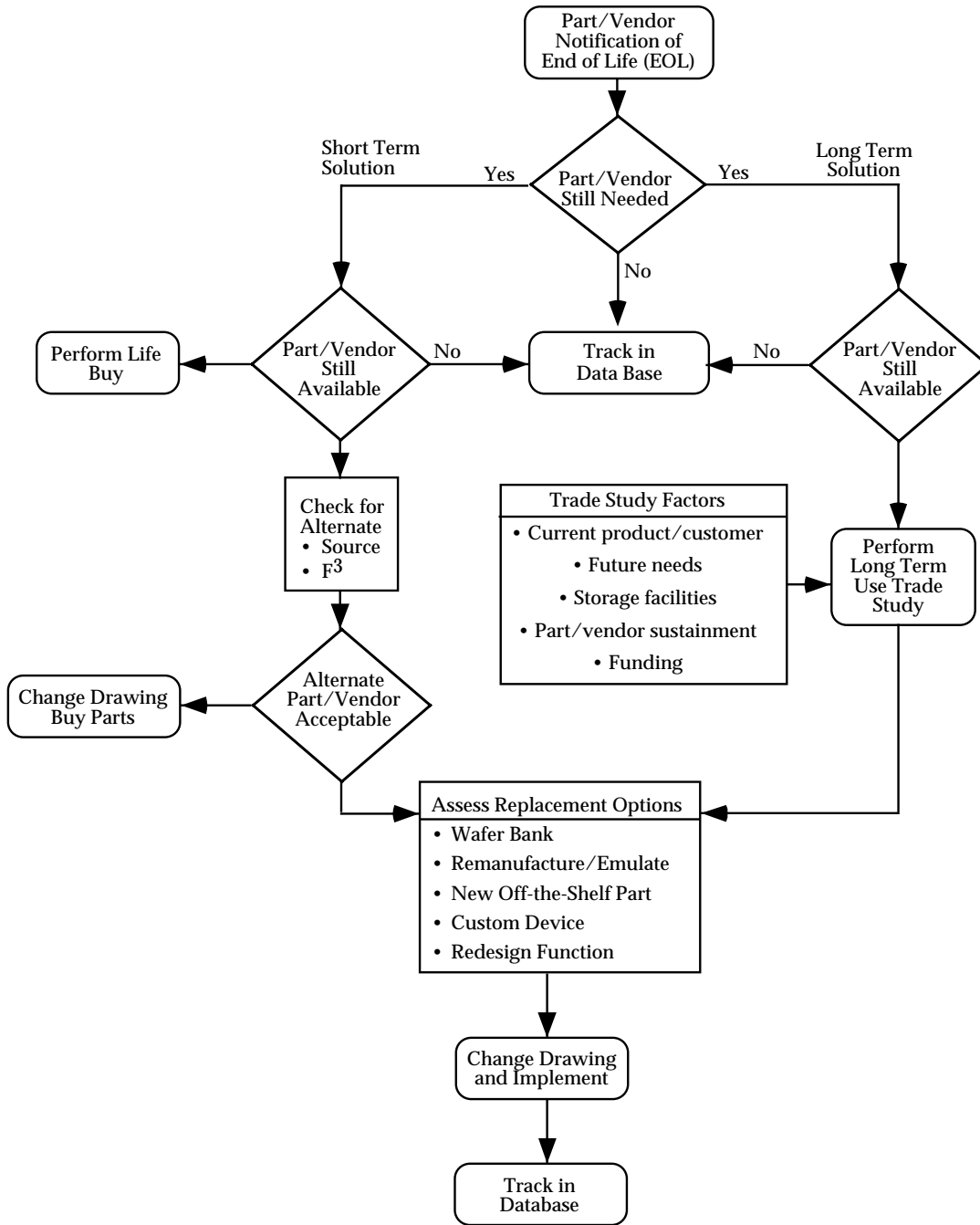


FIGURE 7.2-2: PART OBSOLESCENCE AND DMS PROCESS FLOW

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.2.2.7 Failure Reporting, Analysis, And Corrective Action System (FRACAS)**

FRACAS is a management tool established to identify and correct deficiencies in equipment and thus prevent further occurrence of these deficiencies. It is based upon the systematic reporting and analysis of failures during manufacturing, inspection, test and use. The closed-loop feature of FRACAS requires that the information obtained during the failure analysis be disseminated to all of the decision making engineers and managers in the program. See Section 8 for more information on FRACAS.

**7.2.3 Design for Reliability**

In Section 7.2, the elements of a traditional Parts Management Program were discussed. This section discusses some of the methodologies that can be used to ensure that systems are designed and parts are applied in a robust manner. It presents an overview of the analytical tools that can be used to ensure a robust design and discusses several considerations for ensuring a manufacturable product. Although this material is not part of a traditional parts management program, it is relevant since the manner in which a part is used is as important as ensuring an adequate part is obtained. This observation illustrates the inseparability of part selection and application in the design and manufacture of a reliable system, and illustrates the necessity of using a concurrent engineering approach.

In the course of developing a system or equipment, suppliers must determine the market the product will serve and the need they will fulfill (i.e., environment to be used in, quality/reliability to satisfy customer, guarantee/warranty, and performance when compared to competition and cost). Once this is determined, requirements for part quality levels, design guidelines, temperature range and packaging can be defined. Assembly procedures must be defined to determine the appropriate component packaging (i.e., surface mount, through-hole, etc.). Design guidelines for manufacturing producibility must be available to determine package lead pitch vs. printed wiring board capability, specification of component drift parameters and the many other factors leading to robust design. Once they are determined, the PMP function can attempt to provide the components and materials necessary to satisfy them. The output of this function should be company-specific procedures containing:

- (1) Guidelines for choosing component quality levels
- (2) Design guidelines
  - (a) Performance
  - (b) Environmental/temperature
  - (c) Assembly procedures
- (3) Manufacturing/assembly procedures
- (4) Performance/reliability demonstration plan

Correct application of parts means "using the best part for the job in an optimum/cost effective manner." Hence, electrical and electronic parts must be selected with the proper temperature, performance, reliability, testability, and environmental characteristics to operate correctly and

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

reliably when used in a specific application. Parts and materials should be selected based on their ability to meet functional requirements for a given period of time under the expected extremes of operating stresses, including shock/vibration, temperature, temperature cycling, humidity, contamination, mechanical stress, electrical stress, radiation and electromagnetic interference. Factors to be considered in optimum parts application are both numerous and complex, and should address each of the factors included in Table 7.2-3. Many of these part application factors can be specifically addressed by performing a reliability assessment.

Design for reliability is the process of selecting a part or material and applying it in such a manner that results in high reliability under the worst case actual use conditions. Such an effort requires a structured approach during the part selection and design process. This process should include:

- (1) Definition of operating environments
- (2) Establishment of lifetime requirements
- (3) Use of reliability models to estimate lifetime under use conditions
- (4) Estimates of reliability during the useful life
- (5) Stress derating
- (6) Analysis and design modifications to ensure robustness

Several analytical techniques are useful in robust design. These include derating, failure mode and effects analysis (FMEA) (with or without criticality analysis), fault tree analysis (FTA,) and finite element analysis (FEA) (see 7.3, 7.8, 7.9, and 7.14, respectively).

### 7.2.3.1 Electronic Part Reliability Assessment / Life Analysis

A reliable product requires that the applicable part reliability and life requirements be adequately defined. This effort requires accurate quantification of the environmental and operational stresses that the part will experience during use and an assessment of part reliability and life under these conditions. Typical stress profiles are frequently used, but worst case stress values may often be better suited for this assessment.

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.2-3: GENERIC PART APPLICATION FACTORS

**Operating Temperature Range** - parts should be selected which are rated for the operating temperature range to which they will be subjected.

**Electrical Characteristics** - parts should be selected to meet EMI, frequency, waveform and signal requirements and maximum applied electrical stresses (singularly and in combination).

**Stability** - parts should be selected to meet parameter stability requirements based on changes in temperature, humidity, frequency, age, etc.

**Tolerances** - parts should be selected that will meet tolerance requirements, including tolerance drift, over the intended life.

**Reliability** - parts should be selected with adequate inherent reliability and properly derated to achieve the required equipment reliability. Dominant failure modes should be understood when a part is used in a specific application.

**Manufacturability** - parts should be selected that are compatible with assembly manufacturing process conditions.

**Life** - parts should be selected that have "useful life" characteristics (both operating and storage) equal to or greater than that intended for the life of the equipment in which they are used.

**Maintainability** - parts should be selected that consider mounting provisions, ease of removal and replacement, and the tools and skill levels required for their removal/replacement/repair.

**Environment** - parts should be selected that can operate successfully in the environment in which they will be used (i.e., temperature, humidity, sand and dust, salt atmosphere, vibration, shock, acceleration, altitude, fungus, radiation, contamination, corrosive materials, magnetic fields, etc.).

**Cost** - parts should be selected which are cost effective, yet meet the required performance, reliability, and environmental constraints, and life cycle requirements.

**Availability** - parts should be selected which are readily available, from more than one source, to meet fabrication schedules, and to ensure their future availability to support repairs in the event of failure.

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

Part test data is generally used to assess part reliability under specific operating stresses. Such data can take many different forms. Useful reliability assessment data are often gleaned from the analysis of life tests, performed either by the part manufacturer or by the user of the part. Helpful part reliability and life information may also be found in the literature. In any case, the data used for this assessment must address the specific predominant failure mechanisms applicable to that particular part and the specific materials used in the construction of that part. The use of appropriate data can help in ensuring adequate part life in a specific application, as well as in projecting anticipated part reliability. On the other hand, using inappropriate part life and reliability assessment data can give a false degree of confidence in the life estimate and thus provide a potential for early field failures or poor long term reliability.

Part failure mechanisms can generally be grouped into two categories: common cause and special cause. These two types of mechanisms have very different failure characteristics. This difference must be recognized, and properly addressed, in the data collection, analysis and assessment effort.

Common cause failures are due to inherent failure mechanisms; they have the potential of affecting the entire population of parts. These mechanisms are typically addressed through the design of the part itself and the part's fabrication process controls. These contributions help to ensure that the device is sufficiently robust to operate reliably for a given period of time. For these types of mechanisms, a physics-of-failure based reliability assessment is appropriate, since it is possible to gain a good understanding of the failure mechanisms. Such an assessment requires a fundamental knowledge of the device fabrication process, the appropriate process controls, and applicable materials data.

Special cause failure mechanisms result from defects or from specific events. An example of such a mechanism might be: capacitor failures resulting from a defective dielectric or from electrical overstress. Since special cause failure mechanisms are defect or event related, rather than process related, they tend to occur randomly. For such mechanisms, a purely physics-based assessment may not be appropriate, due to the random nature of failure occurrence. For these failure mechanisms, statistical analysis of the data is usually the more appropriate assessment approach.

Clearly, it is important that a combination of both a physics-based approach and a statistical analysis approach be used in any part reliability and life assessment. Because of the differences in the potential failure mechanisms involved, either approach used alone is unlikely to yield correct conclusions regarding part reliability or life assessment.

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.2.4 Design for Manufacturability**

Of equal importance to the selection and application of parts is the manufacturing process to be used for their implementation. The best part used in a good design is useless, unless it can be processed in a reliable and reproducible manner. Manufacturing process evaluation is especially important for new or immature technologies, or for technologies for which the manufacturer has little or no experience. Therefore, the manufacturability of equipment designs should be given equal weight with the part selection and application efforts. Reference [5] "Best Practices - How to Avoid Surprises in the World's Most Complicated Technical Process" is a good reference source for this task.

Procedures are required today to not only procure acceptable parts and materials, but also to ensure that the process steps from shipping to assembly do not destroy good components. It is not enough to qualify components to a standard qualification procedure, because some current assembly processes impose greater stress than those used in the past. A classic example is surface mount technology, which uses soldering processes (i.e., vapor phase, infrared heating) that provide a very fast temperature transition to 220°C, creating a thermal shock which is greater than that used for component verification testing. This is exemplified by the use of plastic surface mount packages which, in some cases, have resulted in the "popcorn effect." This refers to a phenomena in which moisture is absorbed by the plastic encapsulant material and, upon exposure to the soldering thermal shock, the moisture vaporizes, causing the package to delaminate or crack due to the resulting high internal pressures.

In order to determine if components will perform reliably after exposure to handling and assembly stresses, a preconditioning procedure emulating these processes should be developed and applied. Reference [6] describes a procedure generated to ensure that surface mount components can withstand severe printed wiring board assembly conditions and still meet expected reliability requirements. It can be used as a guide to define each test/procedure/operation/ material that is used in component handling and fabrication/assembly for establishing a process requirements procedure. This procedure should emulate all steps, from receipt of material through manufacturing. Additional or different preconditioning may be necessary for a specific process. After exposure, these devices should be subjected to appropriate testing to determine if performance degradation has occurred. Common tests for a molded plastic package include "85°C/85RH," Highly Accelerated Stress Testing (HAST), Autoclave, and Dye Penetrant. For a hermetic device, seal testing should be part of the test procedure. Residual Gas Analysis (RGA) is also sometimes performed.



---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.2.5 Parts Management Plan Evaluation Criteria**

The following paragraphs provide guidelines which customers can use to evaluate a supplier's PMP. This evaluation includes an assessment of the quality improvement program, quality assurance, assembly processes, and design criteria. These guidelines are based on industry-accepted quality standards and are practiced by world-class organizations. These paragraphs are provided to express the level of detail desired, highlight the subjects of interest, and provide concrete guidelines. It is intended that suppliers clearly describe their own processes and explain how these processes develop, maintain and improve the reliability of equipment.

**7.2.5.1 Quality Improvement Program**

Quality is defined as providing customers with products and services that consistently meet their needs and expectations. But quality goes beyond that of the product to include quality of work, service, information, processes, people, and management. Control of quality in every aspect of the contractor's operation is the basic approach to total quality management.

A quality improvement program should be instituted to apply quantitative methods and human resources to control processes. The objective is to achieve continuous improvement in the selection and application of components, their installation in subassemblies, and in end user satisfaction. Each supplier should document their plan for achieving the goal of continuous improvement in the development, manufacture, reliability, administration, and distribution of products and services that meet the customer's needs and expectations.

**7.2.5.2 Quality Assurance**

Quality assurance is the corporate effort that is specifically aimed at reducing process variation by improving process controls during product development and manufacture, and by taking measures to prevent recurrence of detected problems. Quality assurance also addresses those techniques that will give the customer confidence that future components and assembly processes will have equivalent or better reliability than current components and assembly processes.

Assurance of component and assembly quality should be established before the part and assembly process is approved for use. Suppliers should have procedures for verifying that selected components will operate reliably in the intended environment for the life of the equipment. Component qualification processes should be documented or referenced in the PMP. Testing should be conducted to verify that the proposed components will satisfactorily operate in the intended environment with acceptable reliability. This verification usually takes the form of a qualification test and screening. However, other methods may be proposed, such as extensive field experience of the proposed parts in similar applications or previous contractor qualification data which is valid for the intended application. Furthermore, evidence of quality assembly processes should be demonstrated and documented to ensure reliability at higher levels of integration. The supplier should ensure that the component quality is maintained during the

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

manufacture of equipment. The component reliability should not be compromised by equipment manufacturing processes such as handling or assembly.

#### 7.2.5.2.1 Part Qualification

Qualification is used to verify that components are able to function for the specified life in the intended environment. The goal of qualification should be to ensure long term mechanical and electrical integrity. Qualification requirements may be satisfied by similarity to existing qualified devices of similar packaging and technology. The process for the disposition of failures during the qualification procedures should be at the discretion of the supplier, but should be identified in the PMP. The following items should be accounted for during component qualification:

- (1) Hermetic and hygroscopic nature of unique package types
- (2) Operating characteristics over entire temperature range
- (3) Packaging capability for handling thermal shock
- (4) Internal circuitry and connection resistance to contamination and corrosion (passivation)
- (5) Internal connection fatigue life
- (6) Levels of inherent contamination in packaging
- (7) Solderability of leads

Detailed qualification processes should be documented or referenced in PMP and should address, as a minimum:

- (1) Goals/objectives
- (2) Procedures
- (3) Test reports
- (4) Pass/fail criteria
- (5) Failure detection and analysis
- (6) Requalification criteria
- (7) Failure resolution/corrective action procedures

Qualification Testing - Accelerated environmental qualification testing may be proposed for all components if adequate field data does not exist to indicate long term reliability has been achieved. The environmental testing is to verify that reliability performance is within specification. Electrical characteristics for all potential environmental conditions should be verified through qualification testing if it is not already verified by the manufacturer.

Field Data - Component field data can be used in lieu of qualification testing when the data verify an acceptable failure rate. Component failure rates are generated by dividing total accumulated component failures by total accumulated hours. Component failure rates may also be calculated using industry-accepted prediction methodologies, such as those presented previously. Component types used for failure rate calculations should be of similar families,

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

technologies or package types. The sample size should be statistically significant, with adequate field experience per component.

Component Manufacturer Data - Component manufacturer qualification data may also be used in lieu of field data, provided the data are adequately documented, statistically significant, and indicates that the components should function in the environment for the specified time. These data demonstrate that processes are in statistical process control and accelerated component testing data can be correlated to the intended application environment.

Component Reliability Assessment - Suppliers should have a plan for performing component reliability assessment. The formulas, data and assumptions used to generate the reliability assessments should be documented or referenced in the PMP. When required by contract, the supplier should explain to the customer how part reliability will allow the resulting product to meet or exceed the reliability requirements of the respective equipment performance specification.

When components are selected for use in an intended environment, a component quality and reliability assessment is necessary. The assessment technique and source of reliability data should be clearly defined or referenced in the PMP. The following reliability sections address only component reliability, and not assembly, LRU or system reliability assessments.

Reliability Analysis - A preliminary reliability analysis for each component should be performed prior to the preliminary design review and, as a minimum, should consist of a clear example of the content and format of the reliability analyses being proposed. The supplier is encouraged to base component reliability predictions on field data or other acceptable technical evaluations. Further, suppliers are encouraged to modify component reliability assessments based on methods used to improve the quality of components, such as component manufacturing process control, screening, qualification or other provisions. Failure rates based on the supplier's experience and modifications based on quality provisions should be available for customer review when required by contract.

A final reliability analysis for each component should be required at the critical design review. This analysis should be completed as early as possible, so that potential problems with parts selection or system architecture can be uncovered in time for a cost-effective correction.

Reliability Tracking - In order to perform root cause failure analysis and provide a basis for quality improvement, the component reliability and quality assessments should be verified on a continual basis. A verification should be made to show that the measured reliability exceeds the predicted reliability. This may include tracking field reliability measurements and analysis, tracking screen yield, and/or monitoring manufacturing floor rejects. Failure rate assessments should be updated for future reliability predictions, particularly when part reliability is measured to be less than predicted.

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

When field data are used to perform a part reliability assessment, the following information should be provided:

- (1) Component MTBF formulas correlating field performance to MTBF should be available to the customer. Details of operating hours should be included, as well as component part numbers, equipment part numbers, and failure analysis results.
- (2) Data submittals, if required, should include a summary of part types and failure mechanisms, and should include or reference the raw data used to arrive at these conclusions.
- (3) Component failure rates should be generated by dividing total accumulated component failures by total accumulated hours. Component types used for failure rate calculations should be of similar families, technologies or package types.
- (4) Accumulated operating hours and failures should be statistically significant to provide accurate failure rates. Suppliers should establish confidence intervals for the calculated failure rates using statistical techniques similar to the chi-square method.
- (5) Continue to track component in-service data on an ongoing basis until equipment production is completed.

Requalification - Requalification of the component should be performed when significant changes (i.e., form, fit or function) are made to the package or internal circuitry. The following are examples of significant changes that would require requalification, but do not constitute a complete list.

- (1) Changing the package material or component size.
- (2) Changing the component fabrication process.
- (3) Changing component materials.
- (4) Changing lead finish/material.
- (5) Internal circuit redesign.
- (6) Changing the assembly plant.
- (7) Substantial rejections from the field or infant mortality during testing.

The extent of the requalification should correspond to the changes made to the component. Partial qualification testing should be allowed, provided changed features are tested thoroughly. It is the purchaser's responsibility to establish the means of communication with component manufacturers such that major changes are identified to the purchaser in a timely fashion. The determination to requalify may be difficult if parts are procured through distributors, where design or material changes to the part may be unknown.

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.2.5.2.2 Production Quality Assurance**

Components should perform initially with minimal infant mortality and latent defect rates. Verification should be provided that current and future component reliability is not compromised by unpredictable variations in the manufacturing process. Suppliers should strive to continuously detect and eliminate component flaws that result in infant mortality failures, or changes which may unpredictably degrade future lot quality.

Screening - Product assurance can be accomplished by 100% part screening, but alternative processes may be proposed, such as analyzing key process measurements of the component during manufacture or sample screening. The screening procedures, if applicable, can be performed by either the purchaser, the part vendor or a qualified screening house. Periodic screening failure reports should be available to customers.

Reduced Screening - Reduced screening may be considered when screening, factory and in-service rejections are measured and are found to consistently exhibit an acceptable defect density. Available data, including those from the device manufacturer, should be provided to indicate that the current level of screening is not required. Reduced screening may consist of sample screening, or a reduction of electrical testing and/or burn-in. However, to eliminate screening, some kind of quantitative measure of lot quality should be offered to ensure continuing quality. Approval of an alternate assurance method should be based upon scientific techniques and statistical analysis.

Historically, screening data indicates that part quality may change over time. Future part quality can be adequately assessed by measuring past part quality performance. The reduced screen criteria is aimed at measuring the level of part defects over a period of time, and then making a determination as to whether the level of defects is acceptable. The criteria stated in this section represents one possible baseline. Changes to the criteria can occur based upon experience and a partnership with vendors that would allow other innovative approaches to be considered. A generalized process flow appears in Figure 7.2-3.

At the start, parts should be qualified and screened. All failures before, during, and after screening should be recorded. These failures can be used to determine the level of defects in the tested parts.

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

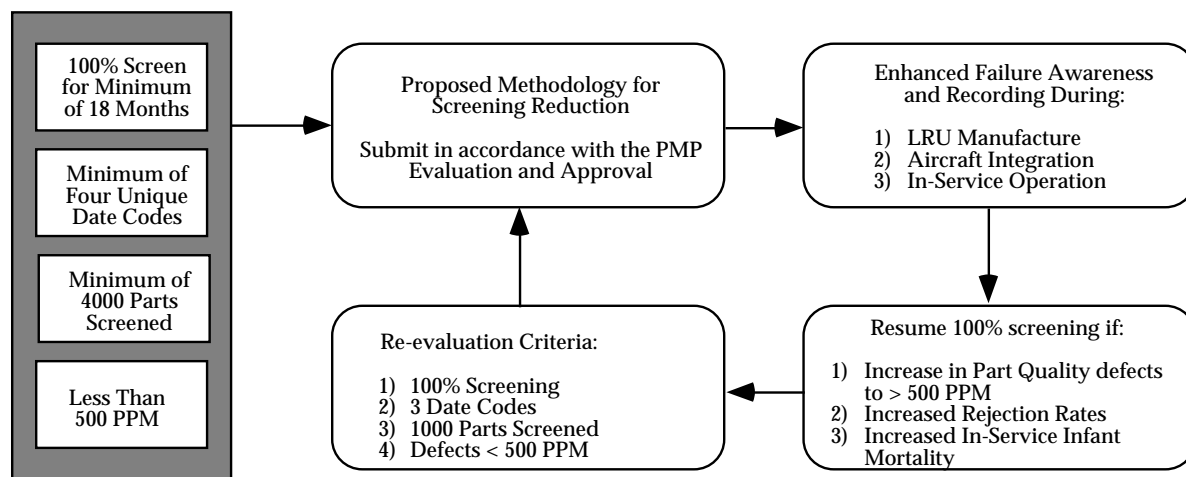


FIGURE 7.2-3: REDUCED SCREEN FLOW

In order to identify whether the part manufacturer consistently produces low defect levels in all lots (including future lots) and maintains configuration control of part specifications, the following data can be collected:

- (1) Parts being screened should come from a minimum of four separate lots (date codes).
- (2) 100% screening should be performed for at least 18 months.
- (3) 4,000 parts, minimum, should have been screened.

The defects measured should be below 500 parts per million (500 PPM = 1 failure in 2,000 parts). If the sample of parts tested has more than 500 PPM, then the reduction or elimination of screening should not be allowed. Failing this criteria indicates a possibility that future parts may also have more flaws than are acceptable.

As part of the original PMP, a failure recording system should be developed and implemented that will record failures during sample screening, equipment/item assembly, environmental stress screening, and field operation. If these measurements indicate a decline in part quality, 100% screening can be reinstated until 500 PPM quality is re-established.

**Screening Documentation** - Detailed screening processes should be documented in the supplier's program plan and should address, as a minimum:

- (1) Goals and objectives
- (2) Test methods
- (3) Data collection techniques
- (4) Test reports
- (5) Pass/fail criteria
- (6) Failure detection and analysis
- (7) Failure resolution and corrective action procedures

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

Data Retention - Results of all screening, qualification, tests, inspections, field history and failure analysis should be recorded and maintained on file. It is recognized that some yield, qualification or screening data may be proprietary to the component manufacturer. Suppliers should still collect and retain some evidence of component quality.

#### 7.2.5.3 Assembly Processes

Equipment manufacturing processes contribute to equipment reliability. Thus, when reviewing the process for selecting components, an assessment of the ability to manufacture the assembly using the proposed technology should be accomplished. The overall goal is to ensure that manufacturing processes are mature.

Processes In Manufacturing - A verification should be made that all manufacturing processes involving electronic components are mature. Further, the supplier should implement continuous improvement goals and quality assurance requirements.

This portion of the parts management plan should include a definition of the manufacturing processes used, how the piece parts flow through these processes, and where process controls are used. The use of statistical process control, design of experiments, and other methods of process control should be documented.

Process Maturity - Suppliers should document their ability to use the proposed processes successfully. If the proposed manufacturing techniques have been used on other products, identification of these existing processes, and a simple statement that these processes are in control and capable, should be adequate. If new techniques are being proposed (such as a change to surface mount technology), demonstration of process control and capability should be required. Suppliers should list the activities performed to identify all of the key process parameters, measurement criteria, and manufacturing procedures needed to minimize the learning curve during production. Examples of these activities include:

- (1) Development of manufacturing procedures
- (2) Personnel training
- (3) Identification of process measurements
- (4) Development of pass/fail criteria
- (5) Design of experiments
- (6) Product life testing after assembly

Process Control and Capability - The next item that should be demonstrated is a supplier's ability to keep their processes in statistical control and capable. Guidelines are provided in Reference [7].

Component Packaging - Maintainability of equipment can be enhanced through the use of standard part package types. Therefore, suppliers are encouraged to procure components with standard package outlines. Standard package outlines are contained in Reference [8].

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

Component Marking - Components which undergo screening should be permanently marked to indicate the individual component has received quality assurance testing. Markings should be visible when components are mounted on the PC board. This helps prevent components without quality assurance from being accidentally installed at the factory or at a remote repair facility.

Components should also be permanently and legibly marked by the manufacturer with the following information, where space allows:

- (1) Manufacturers name, trademark or logo
- (2) Manufacturers part number
- (3) Inspection lot identification or date code
- (4) Pin 1 locator or orientation designator

Components without adequate space for marking should have provisions to preclude accidental replacement with a different part. All component marking should be able to withstand normal use in the planned environment. For military products, marking should be able to pass the resistance-to-solvents test of MIL-STD-883, Method 2015.

Component Handling - Component quality assurance measures can be easily compromised by improper handling. Thus, the contractor PMP plan should reflect practical and proven handling procedures to maintain component quality. Considerations may include ESD prevention, lead formation maintenance and automated handling practices for standard and non-standard packages and humidity control (i.e., PEMs).

All components should be shipped in appropriate packing material. The program plan should address component handling issues, such as ESD, installation orientation, mounting techniques (tube, reel, etc.), contamination and humidity.

Procurement and Shipping Procedures - Component quality should not be degraded during handling or screening. Handling or screening provisions placed in effect with third party participants, such as manufacturers, distributors or screening facilities, should be identified or referenced. Suppliers should be encouraged to eliminate unnecessary processing which may degrade component quality.

The component manufacturer or screening house should obtain and keep on file written certification of specified shipments of components. The shipment certificate should include:

- (1) Manufacturer name and address
- (2) Customer or distributor name and address
- (3) Component type
- (4) Date code and latest re-inspection date, if applicable
- (5) Quantity of components in the shipment
- (6) Level of screen and specification reference



## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

To maintain quality as shipped from the part manufacturer, date codes should be no older than 12 months from receiving date of the purchase order by the manufacturer.

The supplier should ensure that the components are the correct type, date code, screening level, and package type prior to stocking. Incoming inspection is one way to ensure that the components are received with the proper information. This procedure should be properly identified in the PMP.

Discrepancy controls for non-conforming materials should be implemented. These controls should include flow charts describing corrective actions, actions taken to prevent recurrence of discrepancies, etc.

Storage Procedures - The PMP should also address relevant storage and stocking procedures. For instance, plastic packages absorb moisture over time, which may cause package cracking during the solder process. Dry storage may be necessary up until the time of soldering. An alternative process would involve a thermal pre-bake to drive out excessive moisture.

References [9] and [10] can be used in determining the sensitivity of particular ICs to moisture-induced package cracking.

Rotation of stock is also an important function of the storage process. The supplier's plan should identify how their process controls stock flow (i.e., First In/First Out, Last In/First Out, etc.).

Modification and Repair of PCBs and Assemblies - Repair and modification techniques for surface mounted components can be complicated, and may require special tooling and processes. Thus, the program plan should identify the governing documents and procedures for the modification and repair of PC boards.

### 7.2.5.4 Design Criteria

A reliability program should provide Line Replaceable Unit/Line Replaceable Module (LRU/LRM) design guidance and control early in an equipment design program. Misapplication of any part can affect the reliability and performance of that part. Many parts have unique packaging and performance characteristics that should be accounted for in the design of the equipment.

LRU/LRM design guidance should address such issues as thermal stresses, contamination and electrical derating. Appropriate industry standards or proven "in-house" standards should be followed rigorously. The parts management plan should reference these design standards and analytical methods. Design criteria should embody lessons learned by the supplier.

The reliability of components can be greatly improved by using the best equipment design standards and techniques available. Early equipment design analyses not only gives the customer confidence in the product, but gives the supplier time to implement design changes in an orderly

---

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

and cost-effective manner. This early analysis is an essential practice with the use of new technology parts.

Many of the design requirements are already defined by the equipment specification or other design guidelines. The objective is to have the existing design standards referenced, rather than being detailed in the contractor's PMP.

Electronic Parts Selection List - The contractor should prepare a parts selection list. The list should be initially submitted at the preliminary design review. This list is considered preliminary and should be updated as the design matures. The parts list should specify whether "preferred" or "non-preferred" parts (definitions follow) are being used.

Preferred Parts Selection - Preferred parts are those parts for which the contractor has demonstrated a successful history of use.

Non-Preferred Parts (NPPs) - Many component manufacturers are now producing high quality new technology components. If the reliability of these new technology parts can be shown to be acceptable in the intended environment, adequate quality assurance provisions exist which will ensure future production, and application of these NPPs will meet or exceed current reliability performance requirements, then these parts can be considered.

Component Descriptions - Components can be procured under a variety of product descriptions which include commercial item descriptions (CIDs), program-specific documents, and defense detail specifications (MIL-DTL). The selected component description should provide configuration (and interchangeability) control such that the manufacturer, supplier or distributor guarantees the electrical operating characteristics and package specifications.

Components should be tested to supplier requirements under control of the component specification. Lot tolerance percent defective, or other quality and performance guarantees, can be specified in the component description, and should be contracted with the screening house or vendor. The PMP plan should also identify the disposition of failed lots. Tips for selecting and developing product descriptions are presented in reference [11] "Buying Commercial and Nondevelopmental items: A Handbook."

Notification of Change - The component should be controlled to the greatest extent possible through a system of change control. Requalification may be necessary based on the significance of the change. Part specifications should be documented and performance to those specifications guaranteed.

The program plan should define the supplier's "notice of change" agreement. The agreement should ensure that the component is under configuration control at all times, and that quality is not compromised by manufacturer process changes. The component description should require the component vendor or distributor to notify the supplier of component process or design changes.

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

Thermal/Fatigue Analysis and Measurements - The equipment contractor should provide an engineering analysis of the component thermal operating characteristics early in the equipment design process, followed by a thermal test to verify the analysis accuracy. Equipment thermal requirements may necessitate a thermal management program, a thermal analysis, and a cooling evaluation. Thermal cycling fatigue analysis should also be accounted for in the design. This analysis may account for lead compliance during thermal cycling and identify coefficient of expansion mismatches.

### 7.3 Derating

Derating can be defined as the operation of an item at less severe stresses than those for which it is rated. In practice, derating can be accomplished by either reducing stresses or by increasing the strength of the part. Selecting a part of greater strength is usually the most practical approach.

Derating is effective because the failure rate of most parts tends to decrease as the applied stress levels are decreased below the rated value. The reverse is also true. The failure rate increases when a part is subjected to higher stresses and temperature. The failure rate model of most parts is stress and temperature dependent.

#### 7.3.1 Electronic Part Derating

Achieving high equipment reliability requires that each electronic part be both properly applied and capable of withstanding all of the stresses to which it will be subjected. Thus proper derating of electronic parts is a powerful tool for enhancing equipment reliability.

Electronic part derating is done with reference to the "Absolute Maximum Ratings." These ratings are defined in the manufacturer's specification or data sheet as those values which: "should not be exceeded under any service or test condition." There are various "absolute maximum ratings" for each part: voltage, current and power, etc. Each absolute maximum ratings is unique. It is applied individually, not in combination with other absolute maximum rating. Absolute maximum ratings include both operating and storage temperatures, e.g., the maximum junction or hot spot temperature. The "absolute maximum ratings" are typically based upon "DC power conditions measured in free air at 25°C."

Electronic part reliability is a function of both electrical and thermal stresses. Increased thermal stresses generate higher junction temperatures. The result is increased chemical activity within the part as described by the Arrhenius Reaction Rate Model and thus in an increased failure rate. Electronic part reliability is largely determined by the thermal stress.

The specific parameters to be derated vary with different types of parts as shown in Table 7.3-1. Capacitors are derated by reducing the applied voltage to a stated percentage of the absolute maximum rated. Transistors are derated by reducing applied voltage to avoid voltage

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

breakdown, reducing output current, power dissipation and maximum junction temperature. A sample set of derating values for transistors is shown in Table 7.3-2.

TABLE 7.3-1: PRINCIPLE RELIABILITY DEPENDENT STRESS FACTORS/DERATING FACTORS

COMPONENT FAMILY	TEMPERATURE °C	VOLTAGE	CURRENT	POWER	OTHER
Capacitors	Ambient	Ripple & Transient			
Circuit Breakers	Ambient		Contact		Load type
Connectors	Insert	Dielectric withstanding	Contact		
Crystals				Input	
Diodes	Junction	Reverse & Peak Inverse Voltage	Surge, Forward, Zener	Dissipation	
EMI & RF Filters	Ambient	Maximum Operating	Maximum Operating		
Fuses	Ambient	Maximum Operating	Surge		
Inductive Devices, Transformers	Hotspot	Dielectric withstanding	Maximum Operating		
Microcircuits	Junction	Supply & Input Signal	Output & Load	Dissipation	Frequency Fanout
Relays	Ambient		Contact		Load type Cycle Rate
Resistors	Hotspot	Maximum Operating		Dissipation	
Switches	Ambient		Contact		Load type Cycle Rate
Thermistors	Maximum Operating			Dissipation	
Transistors	Junction	Breakdown, $V_{CB}$ , $V_{CE}$ , $V_{BE}$	Output	Dissipation	Safe operating area

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.3-2: DERATING VALUES FOR TRANSISTORS<sup>1</sup>

PART TYPE	DERATING PARAMETER	DERATING LEVEL		
		I (Space)	II (Airborne)	III (Ground)
TRANSISTORS	On-State Current ( $I_t$ - % Rated)	50%	70%	70%
	• Thyristors (SCR/TRIAC)			
	Off-State Voltage ( $V_{DM}$ - % Rated)	70%	70%	70%
	Max T (°C)	95°	105°	125°
	• Field Effect			
	Power Dissipation (% Rated)	50%	60%	70%
	Breakdown Voltage (% Rated)	60%	70%	70%
	Max T (°C)	95°	105°	125°
	• Bipolar			
Power Dissipation (% Rated)	50%	60%	70%	
Breakdown Voltage (% Rated)	60%	70%	70%	
Max T (°C)	95°	105°	125°	

It is imperative that derating be cost effective. If derating is excessively conservative (e.g., lower than necessary part stresses are applied) part costs rise severely. At optimum derating, a rapid increase in failure rate is usually noted for a small increase in temperature or stress. However, there is usually a practical minimum derating value. Below this minimum stress level, circuit complexity increases drastically, offsetting any reliability gain achieved by further derating.

Derating helps to compensate for many of the variables inherent in any design. Electronic parts produced on an assembly line are not all identical. There are subtle differences and variations from one part to the next. Proper part derating helps to compensate for part-to-part variations and alleviate their impact upon equipment reliability. Electronic parts with identical part numbers may be purchased from a variety of suppliers. While these items are “electrically interchangeable” there may be significant design, material and manufacturing differences between them. Derating also compensates for these differences. Furthermore, critical part parameters are not necessarily stable over their entire life. Proper derating will help assure proper circuit operation in spite of these part parameter changes.

Data on failure rates vs. stress is available for a number of electronic parts. This data can be used to determine the reliability improvement through derating. The same is not true of mechanical and structural parts, as can be seen in the following subsection.

### 7.3.2 Derating of Mechanical and Structural Components

For mechanical and structural components, such failure rate versus stress data may be obtainable from the manufacturer or users, but time rate data may not be available. In using a manufacturer's rating and single design stress values, the design engineer must keep in mind that they are really distributions, not single values. Either the worst case “tolerances” for both stress

<sup>1</sup> Rome Laboratory, Part Derating Guide

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

and strength or a plot of the distributions must be utilized. When there is time dependency for the distributions (e.g., degradation, wear out), the stress and strength distributions must be related in the appropriate manner to the cyclic or time operation in the intended environment.

The classical approach to mechanical and structural design is to give every part enough strength to handle the worst stress it will encounter. Several references, such as MIL-HDBK-5 are available, providing data on the strength of materials. Some of these provide limited data on strength degradation with time, resulting from fatigue. Effective design procedures should provide for evaluating alternative configurations with respect to reliability. Since failure is not always related to time, the designer needs techniques for comparing stress vs. strength, and determining the quantitative reliability measure of the design. The traditional use of safety factors and safety margins is inadequate for providing a reliability measure of design integrity.

The concept of stress strength in design recognizes the reality that loads or stresses and strengths of particular items subjected to these stresses cannot be identified as a specific value but have ranges of values with a probability of occurrence associated with each value in the range. The ranges of values (variables) may be described with appropriate statistical distributions for the item. Stress/strength design requires knowledge of these distributions. After the strength and stress distributions are determined, a probabilistic approach can be used to calculate the quantitative reliability measure of the design, including confidence limits.

To illustrate the concept of stress and strength distributions related to reliable design, assume that a large number of tests of the strength of a given manufactured item have been run, with each test being run to failure. A relationship (frequency distribution) between the number failing at any particular value of strength (or band of values) and the value can be determined. Figure 7.3-1(a) shows a generalized frequency distribution of the results. If the exact relationship were known, the probability of a randomly selected specimen failing at a particular value of stress  $F'$  could be predicted. It would be that fraction of the population, whose strength was equal to or less than a stress  $F'$ . Similarly if a large number of experiments were conducted, and the stress was recorded on each experiment, a relationship between the relative frequency of stresses and the stress can be established. This relationship is shown in Figure 7.3-1(b). If the exact relationship were known, the probability that on any randomly selected trial the stress would exceed a strength  $S'$  could be predicted. This would be the fraction of the population (of possible trials) in which the stress exceeded the strength  $S'$ . With both of these distributions defined, unreliability is determined as the probability that the stress is greater than the strength. Unreliability can be determined analytically, graphically, by numerical integration or by probabilistic techniques such as "Monte Carlo" provided the form or shape of the two probability distribution functions are known. The curves from Figure 7.3-1(a) and 7.3-1(b) are combined in Figure 7.3-1(c) to illustrate the region of the unreliability given by the shaded area where stress exceeds strength. Figure 7.3-2 illustrates normal (gaussian) stress and strength distributions, where the stress and strength variables are identified as Kips (a thousand pounds).

Looking at Figure 7.3-2, two things may happen with time and repeated stress. The variance of the strength distribution may change; for example the curve may extend from 13 to 23 Kips rather than the original 16 to 20 Kips. This would result in an increased unreliability since the

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

shaded area would now extend from 13 to 20 Kips. This is shown in Figure 7.3-3(a). The other factor that could change with time and stress is that the mean of the strength distribution might be lowered, to say 15 Kips. This, in turn, would result in a decreased reliability as shown by the shaded area of Figure 7.3-3(b).

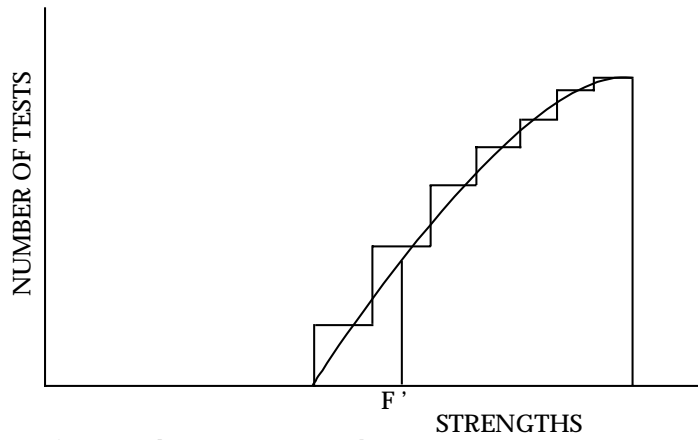
The purpose of stress strength analysis is to improve the reliability of the design. That is, to find the optimum comparison of stress and strength that will have an acceptable probability of success and compete favorably with other constraints such as weight, cost, and availability of material.

There are four basic procedures the designer may use to increase reliability.

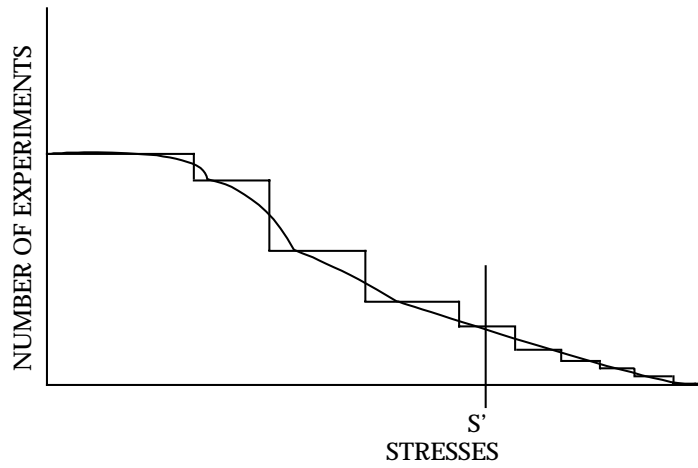
- (1) Increase Average Strength: This approach is tolerable if size, weight, and cost increases can be accepted or if a stronger material is available.
- (2) Decrease Average Stress: Occasionally the average allowable stress on a component can be reduced without greatly affecting its performance.
- (3) Decrease Stress Variation: The variation in stress is usually hard to control. However, the stress distribution can be effectively truncated by putting limitations on use conditions.
- (4) Decrease Strength Variation: The inherent part-to-part variation in strength can be reduced by improving the basic process, holding tighter control over the process, or by utilizing tests to eliminate the less desirable parts.

References [12], [13] and [14] provide more details on this procedure and its application to mechanical and structural components.

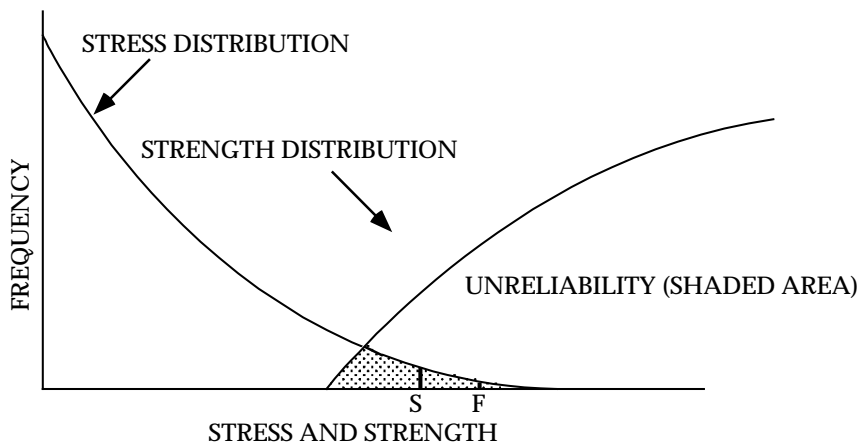
SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



a) Strength Frequency Distribution



b) Stress Frequency Distribution



c) Probability of Stress Exceeding Strength

FIGURE 7.3-1: STRESS-STRENGTH DISTRIBUTIONS AND UNRELIABILITY IN DESIGN



## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

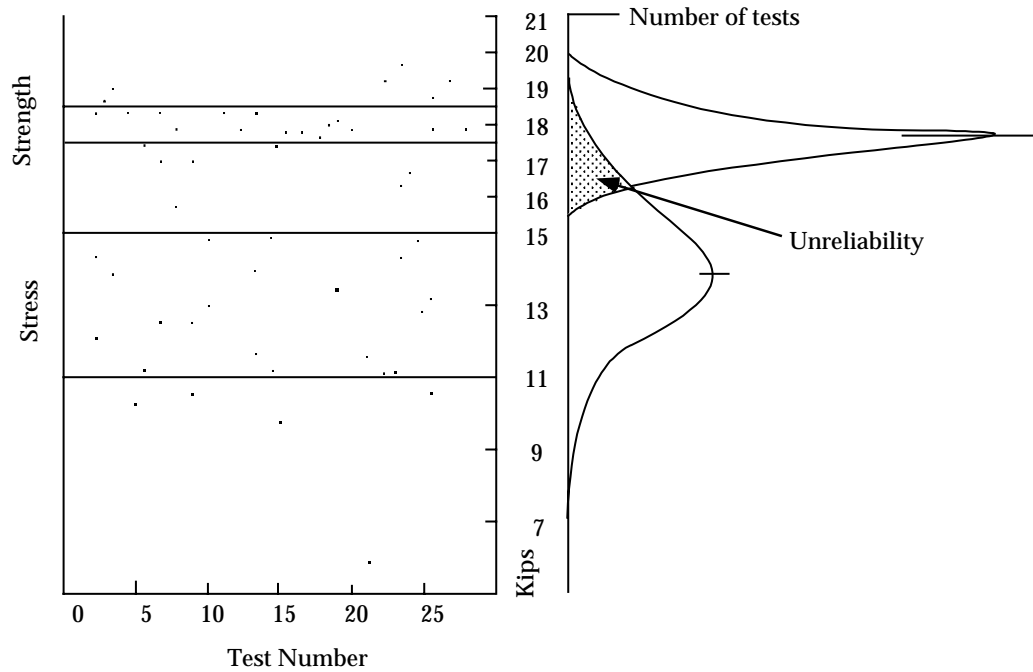
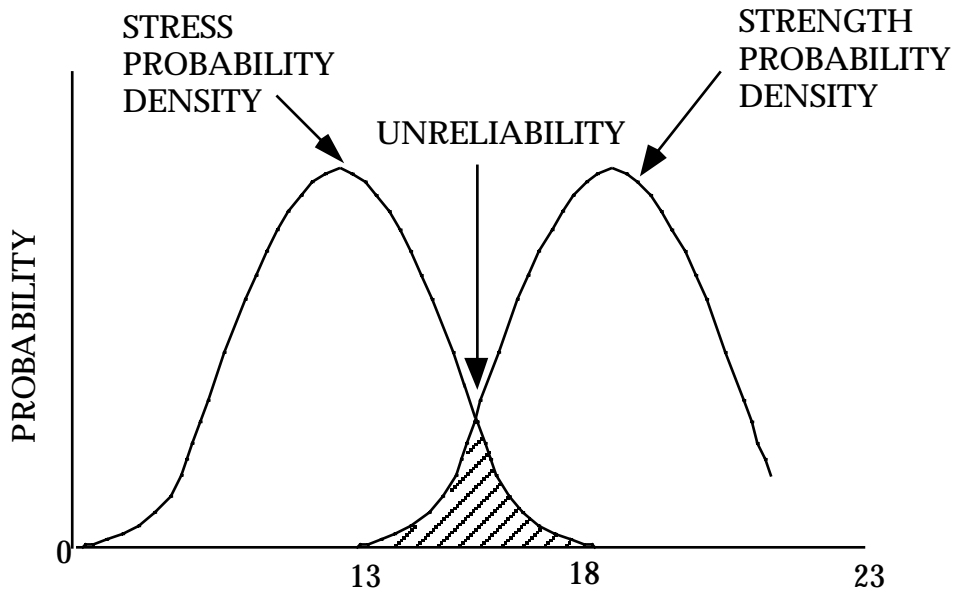
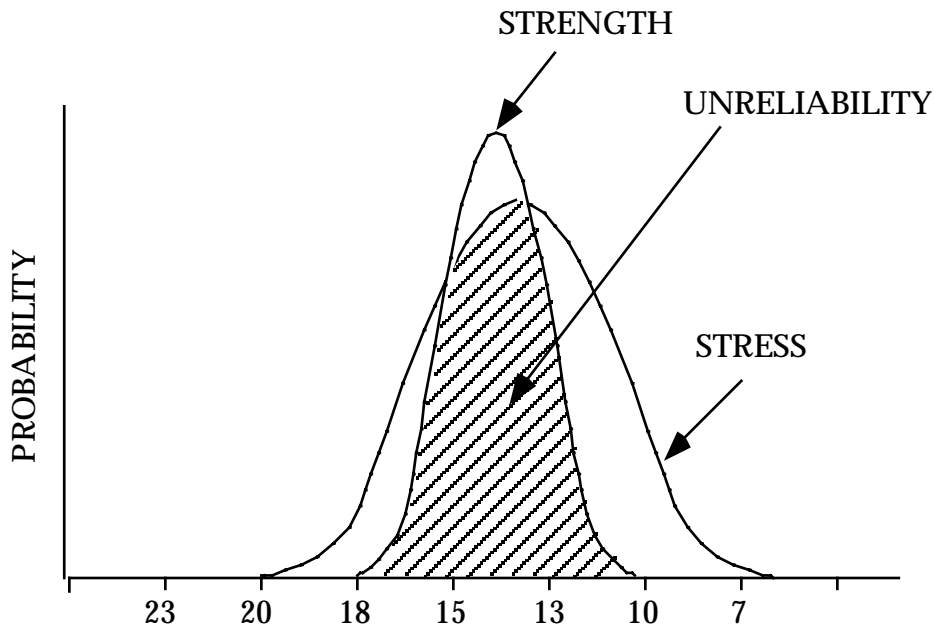


FIGURE 7.3-2: NORMAL (GAUSSIAN) STRESS-STRENGTH DISTRIBUTIONS AND UNRELIABILITY IN DESIGN

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



(a) Result of Increase of Variance in Strength with Time & Stress



(b) Result in Decrease in Strength with Time & Stress

FIGURE 7.3-3: FACTORS AFFECTING UNRELIABILITY

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

### 7.4 Reliable Circuit Design

This section cannot possibly cover all of the aspects of circuit design. In addition to a number of design textbooks, there are handbooks available (e.g., References [15] and [16]) which can be used to solve almost any circuit design problem.

The only thing that this section can accomplish in the limited space available is to outline some of the circuit design methods available to ensure high reliability. They are by no means comprehensive; circuit designers should consult their own organizations' design rules, component application notes, the cited references and other relevant sources. The methods outlined in this section are intended as a guide to the points which reliability engineers and circuit designers need to consider.

In order to produce a reliable circuit design, the designer must consider the following reliability design criteria:

- (1) Component derating (discussed in the previous section)
- (2) Proper use of parts (discussed in 7.2)
- (3) Transient and overstress protection
- (4) Parameter degradation and analysis
- (5) Fundamental design limitations

Except for component derating, which was discussed in the previous section and parts use, which was discussed in 7.2, the following paragraphs discuss each of the listed criteria.

#### 7.4.1 Transient and Overstress Protection

Electronic components are often prone to damage by short-duration voltage transients, caused by switching of loads, capacitive or inductive effects, static electricity, power supply ripple, testing, etc. Small semiconductor components are particularly vulnerable, owing to the very low thermal inertia of their wire bonds. MOS devices are very vulnerable to static electricity, and require special protection.

The subject of electrostatic discharge (ESD) is treated very thoroughly in other sources, and will only be summarized here. It is becoming an increasingly important and recognizable problem with the trend toward the development of integrated circuits of greater complexity and higher component densities. Some of today's microcircuits can be damaged by ESD voltages as low as 20 volts. The smaller the part, the less power it can dissipate or the lower the breakdown voltage, and the more likely it is to be damaged by an electrostatic discharge (ESD). Certain parts are considered highly susceptible and their chances for damage are great. These include

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

metal oxide semiconductor (MOS) parts with a direct access to the MOS junction, high frequency parts produced by the Schottky barrier process, many bipolar and field-effect microcircuits like RAMs, ROMs, and PROMs utilizing small active area junctions, thin dielectrics, metallization crossovers, and N+ guard ring structures, precision film resistors and similar parts. A detailed list of electrostatic discharge sensitive (ESDS) parts and their voltage sensitivity ranges are provided in MIL-STD-1686 and MIL-HDBK-263. They also describe control programs that can be applied to minimize component failures due to ESD.

In addition to ESD, the designer must cope with the other causes of transient generation described in the first paragraph.

Semiconductor device circuit malfunctions can arise from two general sources: (1) transient circuit disturbances and (2) component burnout. Generally, transient upsets are the controlling factors, because they can occur at much lower energy levels.

Transients in circuits can prove troublesome in many ways. Flip-flop and Schmitt triggers can be inadvertently triggered, counters can change count, memory can be altered due to driving current or direct magnetic field effect, one-shot multivibrators can pulse, the transient can be amplified and interpreted as a control signal, switches can change state, semiconductors can latch-up, requiring reset, etc. The effect can be caused by transients at the input terminals, output terminals, on the supply terminals, or on combinations of these. Transient upset effects can be generally characterized as follows:

- (1) Circuit threshold regions for upset are very narrow. That is, there is a very small voltage amplitude difference between signals which have no probability of causing upset and signals which will certainly cause upset.
- (2) The dc threshold for response to a very slow input swing is calculable from the basic circuit schematic. This can establish an accurate bound for transients that exceed the dc threshold for times longer than the circuit propagation delay (a manufacturer's specification).
- (3) Transient upsets are remarkably independent of the exact waveshape, and depend largely on the peak value of the transient and the time duration over which the transient exceeds the dc threshold. This waveform independence allows relatively easy experimental determination of circuit behavior with simple waveforms (square pulse).
- (4) The input leads (or signal reference leads) are generally the ones most susceptible to transient upset.

Logic devices which interface with inductive or capacitive loads, or which "see" test connections, require transient voltage protection. This can be provided by a capacitor between the voltage line to be protected and ground to absorb high frequency transients, by diode protection to prevent

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

voltages from rising beyond a fixed value (clamping), or by series resistances to limit current values.

The transient voltage levels which can cause failure of semiconductor devices are referred to as VZAP. VZAP values depend upon transient duration. Passive devices can also be damaged by transient voltages, but the energy levels required are much higher than for small semiconductor devices. Therefore, passive devices do not normally need individual protection.

#### 7.4.1.1 On-Chip Protection Networks

On-chip protection networks for integrated circuits incorporate many of the principles that apply to equipment protection. It is appropriate therefore to discuss some of these principles before describing discrete devices that are used for protection from transients. The basic approach is to utilize clamps and attenuators that reduce current and voltage transients and protect internal components from excessive thermal dissipation or voltage levels capable of rupturing insulating layers.

A simple yet very effective protection network consists of a diode connected between an input terminal and ground. The diode is designed to clamp the input voltage to the gate to a level below the breakdown voltage for any input less than the design goal. Figure 7.4-1 shows the diagram and illustrates the voltage transfer function between the voltage source  $V_s$  and the internal gate being protected.

For negative values of input voltage  $V_s$  the voltage surge or ESD transient is conducted to ground with the gate voltage  $V_G$  increasing to one forward diode voltage drop. For positive voltages less than the diode breakdown voltage  $V_{BR}$  the protection diode is transparent and the gate voltage responds as it would to any signal voltage (note that any noise could be interpreted as a signal). If the transient exceeds  $V_{BR}$ , the diode goes into the reverse breakdown region, and further increases in the input voltage are attenuated by the voltage divider consisting of the diode incremental resistance and the source resistance  $R_s$ . The object is to prevent  $V_G$  from reaching the destructive level  $BV_{oxide}$  for any anticipated value of the input voltage  $V_s$ .

On-chip protection is the least expensive and best way to improve device and system level hardness and provide maximum customer satisfaction. Nevertheless, sensitive parts do exist, and their use compels the equipment designer to employ effective techniques for best performance and reliability.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

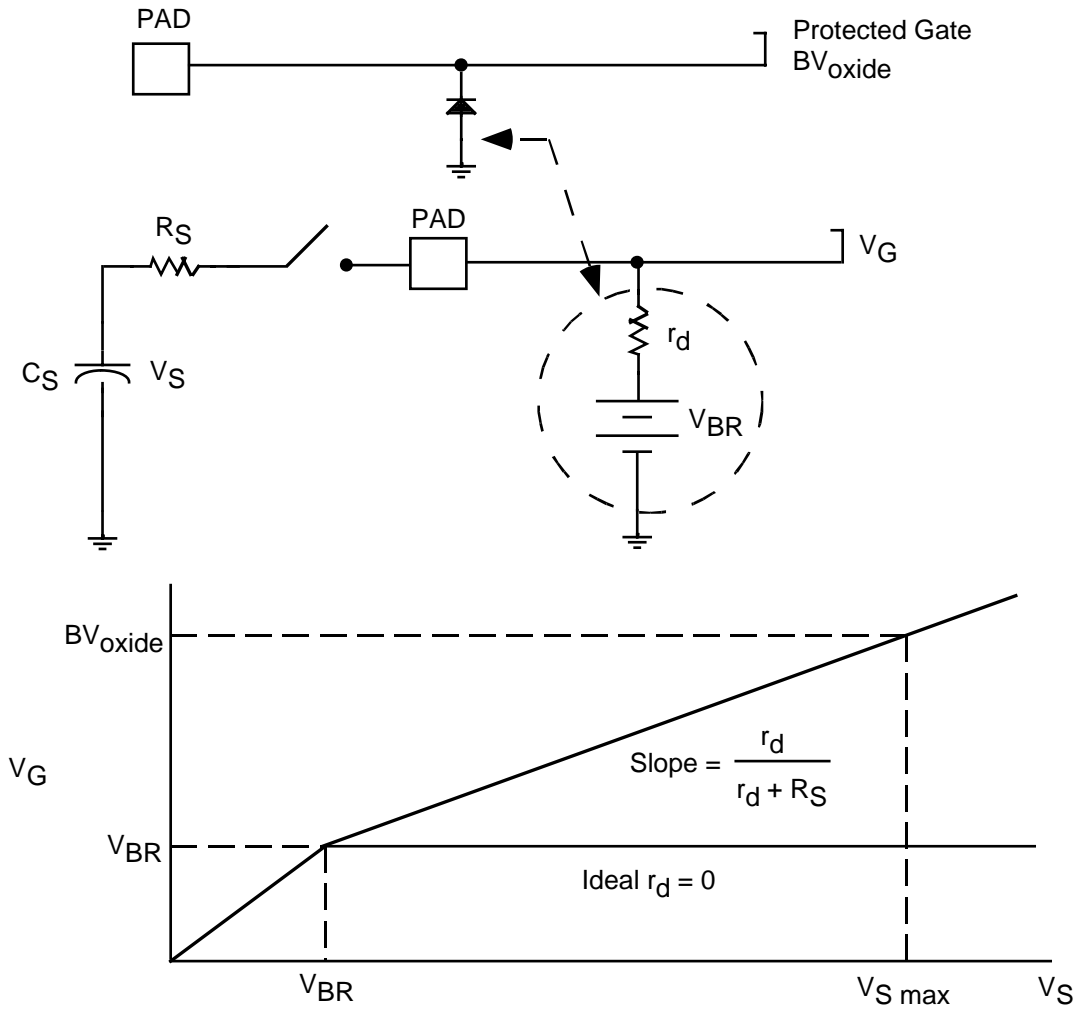


FIGURE 7.4-1: ON-CHIP DIODE PROTECTION CIRCUIT

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.4.1.2 Metal Oxide Varistors (MOVs)**

A varistor is a variable resistor whose value depends on the voltage (or current). It is, in other words, a non-linear resistive element that serves the dual function of clamping and energy absorption. Invented in Japan, it is a widely used, effective, and low cost solution to the problem of controlling voltage surges, especially on power lines.

The metal oxide varistor, or MOV, consists mostly of ZnO with a small amount of other oxide additives. The powdered material is pressed and sintered to form various shapes and sizes according to the intended application. ZnO is conductive, and the individual grains are separated by an insulating layer that produces a p-n junction-like characteristic. At about 3 volts across the insulating layer a tunneling mechanism provides electrons for carrying the current. The nominal “clamping” voltage is determined by the number of grain boundaries between the electrodes.

The conduction is highly non-linear and the current and voltage are related by the equation:

$$I = CV^\alpha$$

where C depends on the cross section area and thickness and  $\alpha$  is a constant between 20 and 50. A plot of this equation on a linear scale resembles the characteristics of a back-to-back diode configuration.

The current rating of an MOV depends on its area, and the energy absorbed depends on the volume. Since energy is absorbed uniformly throughout its volume, the energy rating can be substantial. The speed of these devices is excellent, limited primarily by the lead inductance. There is a small aging effect. MOVs generally have low leakage current, even at elevated temperatures, and good tolerance to radiation environments.

MOVs are available in many sizes, shapes, and ratings, for applications in both ac and dc systems ranging from several volts to several thousand volts. Peak current ratings range from a few tens of amperes to several tens of kiloamperes, with energy capabilities from fractions of a joule to 10 kilojoules. When one compares these energies with the millijoules in an ESD pulse capable of destroying an integrated circuit, it becomes clear that MOVs are not a good choice for protecting the inputs of integrated circuits from ESD. In addition, the capacitance of even the smallest MOVs is fractions of a nanofarad and would degrade the high frequency performance. Nevertheless, protection of power ICs or of circuit boards is a possible application, and MOVs are available as coaxial inserts for connector pins.

The largest application for MOV surge suppressors is protection against power line surges. Many computers, appliances, power cord extensions, etc., are equipped with MOVs for protection from routine power line transients.

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

**7.4.1.3 Protective Diodes**

Discrete diodes and diode networks can be used in a multitude of applications for protection in power lines, signal lines, and equipment from transients caused by lightning or lightning induced effects, power line surges, inductive switching, ESD, or EMP. The sophisticated processing technology of the silicon semiconductor industry makes possible such a wide variety of applications.

Turn-on time for silicon pn junctions is extremely short, claimed to be a picosecond or so in theory, with actual response time limited by lead inductance. The series resistance is very small, leading to a minimal increase in clamping voltage with current. Clamping voltage ranges from several volts to several hundred volts. Pulse power rating at 100 ns ranges from a few kilowatts to over 10 megawatts. From 100 ns to 10 ms the power rating follows the classical Wunsch-Bell model, decreasing as  $t^{-1/2}$ . Power is derated linearly above 25°C to zero at 175°C. Since the series resistance is so small virtually all of the power is dissipated in the depletion layer of the pn junction, which ranges from small fractions of a micron at lower voltage ratings to several tens of microns at 500 volts. Diode capacitance can be as low as several tens of picofarads for high voltage diodes, and an order of magnitude larger at lower voltages. Many different packaging styles are available, including arrays in ceramic dual-in-line packages, hermetically sealed.

**7.4.1.4 Silicon Controlled Rectifier Protection**

A silicon controlled rectifier (SCR) is a four-layer silicon device employing regenerative feedback to achieve a snap-back characteristic that offers excellent circuit protection and low power dissipation. High power devices have been in use for many years as a control device for lighting, motors, and voltage control. Their use in protection networks for integrated circuits is more recent.

The four-layer structure of an SCR is shown in Figure 7.4-2 together with its current-voltage characteristic. For positive values of voltage a very small leakage current flows until the forward breakdown voltage  $V_{BF}$  is reached, whereupon the device switches into a low-voltage, high-current conduction state. It remains in this state until the transient surge decreases to a low value where the SCR current falls below the holding current  $I_H$ . The SCR then reverts to its normal blocking state.

In the blocking state the np junction is reverse biased and sustains the large voltage. Once triggering occurs the junction voltage collapses, and both transistors saturate. This leads to a small voltage across the device in the conducting state. By adjusting the doping levels the breakdown voltage can be varied over a wide range. In integrated circuit form there are large parasitic resistors that complicate the design; nevertheless the basic ideas are the same.

The holding current is a very important parameter in any SCR. The device cannot resume its non-conducting state unless the current falls below  $I_H$ . In an ac circuit this is accomplished by the normal reversal of voltage every half cycle. In surge suppression this requires that the



## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

transient be reduced to a level where the source resistance or other resistance be sufficient to limit the current to less than  $I_H$  when the transient has subsided, otherwise the continued dissipation may destroy the device (as in latch-up).

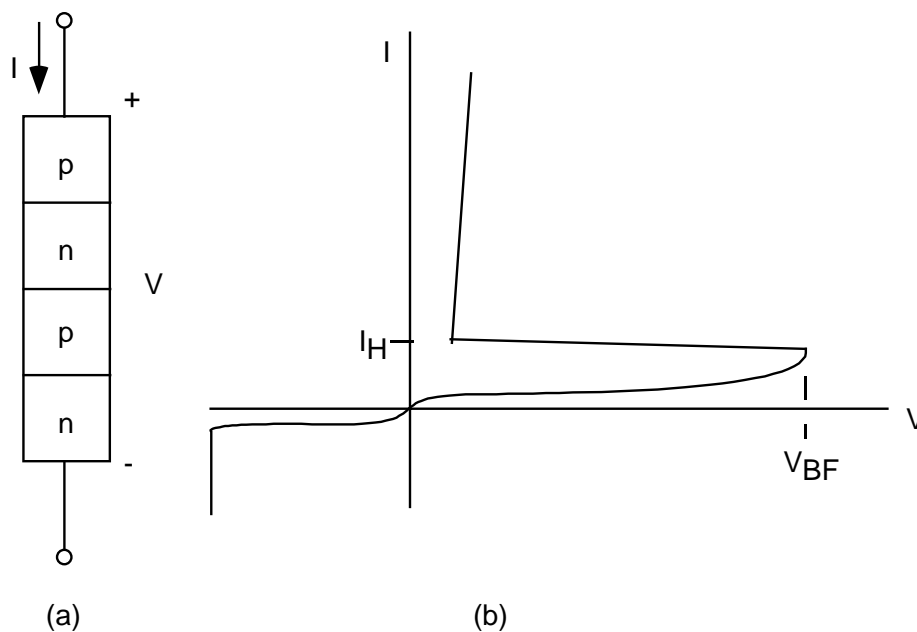


FIGURE 7.4-2: (A) FOUR-LAYER STRUCTURE OF AN SCR  
(B) CURRENT - VOLTAGE CHARACTERISTIC

The key that makes the SCR such an effective clamping device is its very low voltage in the conducting state, together with its very low incremental resistance. As a result it can conduct large currents with very little power dissipation. In effect, it is a “crowbar” device once triggered.

Besides its use in on-chip protection, discrete devices and arrays are available for a large variety of applications, from protecting integrated circuits and circuit boards to surge protection and control in high-voltage, high-current environments.

#### 7.4.1.5 Passive Component Protection

Discrete components can also be useful in reducing susceptibility to transient electrical overstress. To be effective, they must function in concert with other impedances. For example, a resistor in series with the input impedance to an integrated circuit can form a voltage divider network to attenuate the transient and absorb part of the energy. Similarly, a resistor across the line could act with the source resistance to attenuate a surge. On the other hand, if the source were a true voltage source, then shunt elements would have no effect. Furthermore, since a linear device affects desired signals as well as transients, it may not be feasible to use a purely linear network, especially if the frequency spectrum of the signals overlaps the spectrum of the

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

disturbance. Nevertheless, resistors, capacitors, and inductors can be an inexpensive means to achieve the desired result.

There are several types of resistors, the common ones being carbon composition resistors, film resistors, and wirewound resistors. The conducting element in a carbon composition resistor is made of a silica-loaded resin with dispersed carbon particles that is formed into a slug or pellet. Because the thermal mass of the slug is relatively large, it can absorb a considerable amount of energy. Experimental data show that a 100  $\Omega$ , 1/8 W carbon composition resistor can dissipate 1 Mw of power for 1 ms before exhibiting a resistance change greater than 5%. The damage threshold follows a  $t^{-1}$  dependence to 100 ms, where the threshold is about 10 watts. The energy absorbed in this range is several orders of magnitude greater than the threshold for integrated circuits.

Note that the power level in the preceding paragraph corresponds to a voltage of 10 kV across the 100 W resistor, far in excess of the rated value of 150 volts. Nevertheless, unless the power dissipation results in catastrophic thermal failure or flashover, the resistor will remain functional and continue to offer protection.

At high frequencies the capacitance and inductance of the resistor must be considered. A typical value for the parasitic capacitance is 1.6 pF. For a low value resistor, less than 100 ohms, the capacitive reactance is negligible below several hundred MHz. For higher values the upper cutoff frequency can be as low as 10 MHz. If the resistor is used in a shunt arrangement the capacitance would aid in transient suppression by blunting very fast wavefronts; on the other hand, in a series arrangement the capacitance would be deleterious, exposing a sensitive integrated circuit to the full leading edge spike.

The parasitic inductance of a carbon composition resistor depends on the size of the conducting slug and the length of the leads. In a practical sense the larger the conductor the lower the inductance, with hollow or square conductors the best shape. A typical measured value of inductance for carbon composition resistors is 20 nH, with leads adding to this by about 20 nH per inch. However, with short leads and except for very low values of resistance the capacitive reactance from the lead terminations and the capacitance between conducting particles dominates the high frequency performance and total impedance decreases at high frequencies faster than with film resistors.

Film resistors consist of evaporated films of thickness from 0.005 to 1 mm, or thicker films up to 100 mm deposited from a resistive ink, or, in the case of carbon film resistors, deposited from the pyrolytic decomposition of an organic gas. Sheet resistances for the different types vary from 10 to 10,000 ohms per square. The films are spiral-cut to trim the resistors to final value. The spiraling increases the total inductance; nevertheless, the high frequency performance is dominated by capacitance.

The ability to absorb energy from a transient pulse depends on the thermal mass of the resistive element and on the maximum temperature that can be tolerated before permanent damage occurs.

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

Film-type resistors, especially carbon film, have a much higher critical temperature than carbon composition resistors. However their much smaller thermal mass makes them inferior to carbon composition resistors for this application. In fact, ESD pulses are known to cause permanent damage to film resistors. The spiraling causes a non-uniform power dissipation in the film that can lead to thermal damage at the ends of the spiral cut, and high voltages can cause an arc across the spiral cuts. Both types of damage have been observed.

Wirewound resistors are made by winding a resistance wire on a substrate or bobbin. Although the thermal mass is large, and, in fact, pulse-handling capabilities compare to those of carbon composition resistors in some cases, the very large inductive property limits their suitability for fast transient suppression.

There are two main classes of capacitors, electrolytic and electrostatic. Electrolytic capacitors include aluminum and tantalum types, characterized by large capacitance values, up to 1 F, but limited to voltages below 600 volts. They are made of high purity aluminum foil or tantalum, anodized to form the dielectric layer. This layer has unidirectional properties similar to those of a diode. Unless both electrodes are anodized the capacitor is unipolar and the instantaneous voltage must always remain of one polarity. At voltages roughly 50% higher than the rated voltage additional electrode material is anodized and a substantial current can flow.

One of the principal applications of electrolytic capacitors is in power supply filtering, where they also perform the useful function of suppressing surges that are coupled through from power lines. They are also used on printed circuit boards to decouple circuits connected to power busses, or to shield sensitive ICs from noise generated on the board.

Electrolytic capacitors are limited by their poor frequency response. They have a large inductive component that limits the self resonant frequency to 10 kHz or so. For this reason electrolytics are often paralleled with a 0.1 or 0.01 mF electrostatic capacitor that acts as a low impedance to high-frequency signals.

The main electrostatic capacitor types include plastic, ceramic disk, ceramic multilayer chip capacitors, and glass and mica capacitors. Plastic capacitors are made by evaporating a thin layer of aluminum onto a thin plastic film of polyester, polystyrene, polycarbonate, or other plastic. They exhibit the interesting property of self-healing, whereby voltage breakdown at a site is cleared by the evaporation of the aluminum around that site, restoring operation to an equal or higher voltage capability.

Ceramic capacitors make use of the high dielectric constant of ferroelectric materials to achieve large capacitance values in a small package. For disk capacitors the appropriate combination of powders is mixed and pressed into the desired form. These are sintered at high temperature, then electrodes are screened on, and the device encapsulated. By forming a very thick disk, high voltage ratings can be achieved. Multilayer chip capacitors are made from a slurry containing the mix of dielectric powders, and cast onto a stainless steel or plastic belt. After drying, electrodes are screen printed, the layers are stacked, then cut apart into individual units. The capacitors are

---

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

---

then sintered, contacts attached, and encapsulated. Because of their extremely small size, these capacitors are especially useful in hybrid circuits or on printed circuit boards.

Glass and mica capacitors are used in tuned circuits and high frequency applications where their stability and accuracy are needed. They are made from alternate layers of the dielectric and metal foils, brought out at either end, where leads are attached. They are available in high voltage ratings but relatively low capacitance values.

Electrostatic capacitors are capable of withstanding surges several times their rated values. In smaller values, especially, the dielectric thickness may be increased to keep the area a manageable size, even though the voltage rating is listed the same as other capacitors of the same style. This makes them good candidates for transient suppression.

Inductors can serve useful purposes in filters or attenuators for transient electrical overstress. On the other hand, inductors can be the source of high voltage transients when high di/dt values are encountered, and the main design task then becomes one of *minimizing* parasitic inductance. The fact that inductance is a magnetic field phenomenon means that coupling from magnetic fields produced by arcs or conductors carrying discharge current needs to be minimized by good layout practices and shielding.

Inductors are not as widely used as resistors and capacitors because of their size, weight, cost, and dissipative property. Because discrete inductors are wound with wire of non-zero resistivity parasitic resistance is unavoidable and can limit the performance, especially at high frequencies where skin effect becomes important.

Ferrite beads are an interesting form of inductance often used to reduce high frequency noise. They consist of a ferrite material of high  $\mu$  that is lossless to a high frequency, even up to the gigahertz range. They are designed to be slipped over a wire, or multiple turns can be threaded through a single bead. They are transparent to dc or low frequencies, but introduce inductive reactance and then resistance at selected high frequencies. In combination with other circuit impedances they are widely used to reduce noise and system transients as a low-cost and convenient measure.

### 7.4.1.6 Protective Devices Summary

Surge suppressors such as gas tubes and air-gap arrestors for lightning protection have been omitted because they are used mainly in exterior locations or service entrances but seldom in electronic equipment. The characteristics of the protection devices discussed are summarized in Table 7.4-1, but the entries are for only those devices that are appropriate for use on printed circuit boards or within equipment enclosures. Very large diodes and SCRs are available but seldom used for circuit board applications. The following material illustrates how these protection devices can be used.

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.4.1.7 Protection Design For Parts, Assemblies and Equipment

The best way to build robust equipment is to use parts that are themselves robust. This is the most efficient, cost-effective, and practical approach. It protects integrated circuits during fabrication, testing, shipping, assembly, and equipment operation and repair. It requires no extra components or board space and imposes no degradation in frequency response. Nonetheless, sensitive parts do exist and at times must be used; in any event no matter how well a system performs it can always be improved by good design.

If an item of equipment were battery operated, shielded from electrical and magnetic fields and radiation, and had no input or output ports it might be impervious to anything except perhaps a direct lightning stroke. Realistically, equipment has a direct connection to power lines, signal ports, output ports, switches and other controls, apertures for cooling air, etc. The equipment will encounter transients at the inputs, radiated fields, both direct and indirect ESD discharges, handling by inexperienced personnel and repair persons, etc.

TABLE 7.4-1: COMPARISON OF PROTECTION DEVICES

	ADVANTAGES	DISADVANTAGES	RANGE OF MAXIMUM VALUES*	COMMENTS
MOV	low cost high energy capability low leakage current radiation hard	high capacitance aging effect	$E = 0.06J - 10kJ$ $I_{peak} = 25A - 100kA$ $V_{DC} = 3.5V - 6kV$ $C = 11pF - 11nF$	especially useful for power line transients, board protection
Diode	low series resistance low capacitance	higher cost	$P = 400 - 6500W$ $V = 5 - 270V$ $I_{peak} = 2 - 600A$ $C = 3 - 500pF$	fail short or open
SCR	nearly ideal characteristics low leakage current	higher cost limited availability turn-off requirements need to be addressed	$V = 30 - 270V$ $I_{peak} = 2 - 600A$ $C = 3 - 90pF$	fail short
R, L, C	low cost readily available	linear devices often not transparent to signals	$V = 100V - 10kV$ $p = 0.1 - 1mW$	often used in conjunction with other transient suppressor

\*Values in this column apply to specific transient waveforms or other special conditions. Consult specification sheets for details.

There are many anecdotes about computer malfunctions on cold winter days when the humidity is low: sensitive keyboards; equipment that is “dead on arrival;” costly repairs and retrofits; latent failures; etc. One expert in the discipline claims that computer upset can be caused by shaking coins in a plastic bag nearby. Upsets and failures are not only annoying, they can be very costly. Unless one is prepared to condition power and signal lines, prohibit static-prone materials

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

and furnishings, and thoroughly train all staff members in proper procedures, the best approach is to make the equipment fool-proof.

To protect against direct-discharge ESD, it is necessary either to insulate the equipment or to provide a safe alternative path for the discharge current. If the discharge is indirect, then the equipment must be properly shielded to prevent magnetic or electrostatic coupling to interior circuitry. Protection must also be provided for maintenance, upgrading, or repair operations. This requires on-board protection and good layout.

There are four categories of techniques for system hardening.

- (1) Board layout
- (2) Shielding and grounding
- (3) Use of transient protective devices
- (4) Use of passive components and filters

Because of the wide overlap between these categories it is not possible to treat them as entirely separate areas; however all of them will be covered in what follows.

#### 7.4.1.8 Printed Wiring Board Layout

Arrangement of parts on a printed wiring board should give priority to sensitive ICs. These should be placed near the center of the board where they are less likely to be contacted during handling. To further protect the components a guard ring should be in place around the periphery. The guard ring should be connected to the pull-out lever or board latch and to frame ground, but not directly to circuit ground. To prevent arc-over after the board has been installed the guard ring should be connected to circuit ground through a high resistance to bleed off static charges that might accumulate. To avoid electromagnetic interference (EMI), noisy circuitry should be segregated from sensitive circuits, and analog circuits segregated from digital. Edge-triggered logic should be avoided where possible. In extreme cases Faraday shields might be needed. To avoid coupling between an ESD discharge path (such as the guard ring) and sensitive inputs, parallel traces should be avoided. It is best to remember that any circuit that is a good radiator is also a good receiver for EMI. Whenever a trace becomes a significant fraction of a wavelength it has the potential of becoming a good antenna. Since light travels a foot per ns in free space (slower in materials), fast risetime transients can be efficiently radiated from short lines; therefore leads should be kept short, or shielded where necessary.

Inductive coupling is minimized by small loop areas. For example, power and ground traces should be close together. This can be accomplished by running multiple power and ground lines, on different layers, and transposing them at intervals. It is preferable to run each set of these multiple feeders back to a common point near the connector rather than form one long, continuous run. To maximize the capacitance between power and ground, a ground plane, and

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

ground fill, should be utilized - no area should be left unused. To minimize coupling between signal lines it is preferable to alternate them with ground or power buses, but this may not be feasible from a real estate and frequency performance point of view.

Power supply filtering and decoupling is such an important concern that many boards use several capacitors to reduce noise and glitches on the power bus caused by digital circuits. Clearly even a low magnitude transient is capable of causing upset. Even though the power supply itself has a very low output impedance, cabling within the cabinet and the impedance of interconnects provide opportunities for EMI. One recommendation is that each board use an electrolytic capacitor ( $> 50 \mu\text{F}$ ), a  $0.01 \mu\text{F}$  capacitor for high frequency suppression, and a ferrite bead on the power lead, all as close as possible to the connector. Also recommended is a  $0.01 \mu\text{F}$  capacitor for each IC. Such filtering will also help to attenuate surges on the power lines that couple through the power supply. At high frequencies the power supply busses are a significant fraction of a wavelength, and the characteristic impedance of the transmission line formed by the power supply trace and ground can contribute significantly to the noise. One way to lower the characteristic impedance is to use a power supply trace that is separated from the ground plane by a thin insulator. In lieu of this the inductance of the supply trace should be minimized by making the buss as wide as possible, and by providing multiple paths for the supply current.

#### 7.4.1.9 Shielding

Equipment enclosures rely on the reflection of incident electromagnetic waves or their absorption by  $I^2R$  losses in the material to prevent the transmission of electromagnetic energy, either into the equipment, or from the equipment. In the first case we wish to protect the interior circuits from radiation caused by indirect ESD, lightning, or EMI. In the second case we wish to prevent emission from the equipment itself in order to avoid adding to the EMI background, and to comply with regulatory requirements.

An electromagnetic wave incident on a conducting surface generates currents in the material that produce electromagnetic fields opposing the incident wave. The stimulated wave is observed as a reflection of the incident wave, and the stimulated current produces losses in the body of the material that represent an attenuation of the wave as it progresses through the conductor. If the illuminated body is a perfect conductor the wave is totally reflected; there is no penetration of the shield, which acts like a Faraday cage. When the conductor is less than ideal only a portion of the wave is reflected, and non-uniform conduction currents flow in a layer near the surface. This is the so-called skin effect. The skin depth is the distance in which the induced currents or fields decrease by a factor of  $1/e$ , to 37% of their original amplitude.

The shielding effectiveness due to absorption depends on the thickness of the material, and the decibel loss in any given material increases with the square root of frequency. (Ref. [101], RADC-TR-78-156, "Electromagnetic Properties and Effects of Advanced Composite Materials: Measurement and Modeling" and Ref. [102], RADC-TR-81-162, "Electromagnetic Shielding Effectiveness for Isotropic and Anisotropic Materials.")

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

The other component of shielding refers to the reflection of the electromagnetic wave at front and back surfaces of the shield. A plane wave or an electric field is reflected very effectively from the surface of a good conductor. A magnetic field tends to be reflected from the back surface of a shield as it re-enters the atmosphere. The magnetic field that is reflected is virtually 100% of the incident wave, *but is reflected in phase*, and adds to the incident wave, again producing a standing wave.

Shielding effectiveness must be re-examined when the incident wave is not a plane wave (far-field condition). When the source is close to the shield (near-field region) the wave impedance is not 377 ohms and important differences exist.

The transition between near-field and far-field regions occurs at a distance  $d = \lambda/2\pi$ . At greater distances the fields are plane waves, the wave impedance is 377 ohms, and both the E field and H field decrease with distance as  $1/r$ .

In the near-field region the reflection conditions are different because the wave impedance is different. For electric field sources the reflection losses are even greater than those with a plane wave. Consequently, shielding is not a problem. Even a thin, evaporated coating on a plastic layer is effective, although making a good electrical contact to ground the shield is problematic. (Grounding of any shield or conducting surface within the enclosure is necessary to prevent secondary arcs within the equipment.) When the source generates a primarily magnetic field, shielding is more of a challenge. Reflection losses are *smaller* than those of a plane wave, and *decrease* as the frequency decreases. Since absorption losses are small at low frequencies, it becomes a challenge to design shielding against low-frequency, near-field, magnetic sources.

The common methods of shielding against low-frequency magnetic fields are the use of ferromagnetic shields, such as “mumetal” and the use of the “shorted turn”. Some ferromagnetic materials have very high permeabilities below 1 kHz and are particularly effective in confining magnetic fields. The “shorted turn” method uses a closed, conducting loop perpendicular to the magnetic field to generate an opposing magnetic field within its area. It is useful in subduing emissions from motors, transformers, etc.

Indirect ESD sparks and other arcing sources are usually high impedance, high E field sources. Magnetic sources are those that involve large currents as in power lines, ground return wires, conductors carrying a discharge current, transformers, etc.

Once appropriate shielding material has been selected, any apertures must be given proper attention. These are required for input and output signals, power, switches and controls, ventilation, and access. The general rule is that the largest dimension of an aperture must be a small fraction of a wavelength at the highest harmonics present. Some experts recommend  $\lambda/10$ , others as small as  $\lambda/50$ . With digital clock frequencies at 100 MHz and harmonics approaching 1 GHz the appropriate size of apertures to limit emissions would be of the order of 3 cm. To shield from ESD arcs of 10 ns duration would likewise require an aperture of 3 cm. With microwave



## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

equipment even these dimensions are too large. Note that any aperture with a wire through it acts like a section of coaxial cable with good transmission.

The 3 cm limit refers to the largest dimension of the aperture. If an opening is long and narrow it acts as a slot antenna, receiving or emitting frequencies corresponding to its length. When a larger opening must be used it can be subdivided into smaller openings or covered with a wire mesh. Access panels and doors must have closure seams protected by gaskets or interrupted by screws at least every 3 cm.

All conductive surfaces within the equipment should be grounded. Otherwise a secondary arc between the surface and another part of the cabinet could occur, or, worse yet, to a sensitive part or a trace on the printed wiring board. An arc occurring within the cabinet is itself a source of close range EMI confined to the cabinet enclosure. Direct ESD injection to internal circuitry must be prevented. No parts of the internal circuitry should be accessible to hands or fingers, and any direct discharge must be confined to the cabinet or shielding only. There should be no accessibility through apertures; switches and other controls should have grounded cases or should be insulated and sufficiently separated from circuits to preclude the possibility of arcing.

7.4.1.10 Grounding

Grounding refers literally to the electrical connection between equipment and a conducting rod driven into the earth. Figure 7.4-3 shows how grounding is accomplished at the service entrance to a building.

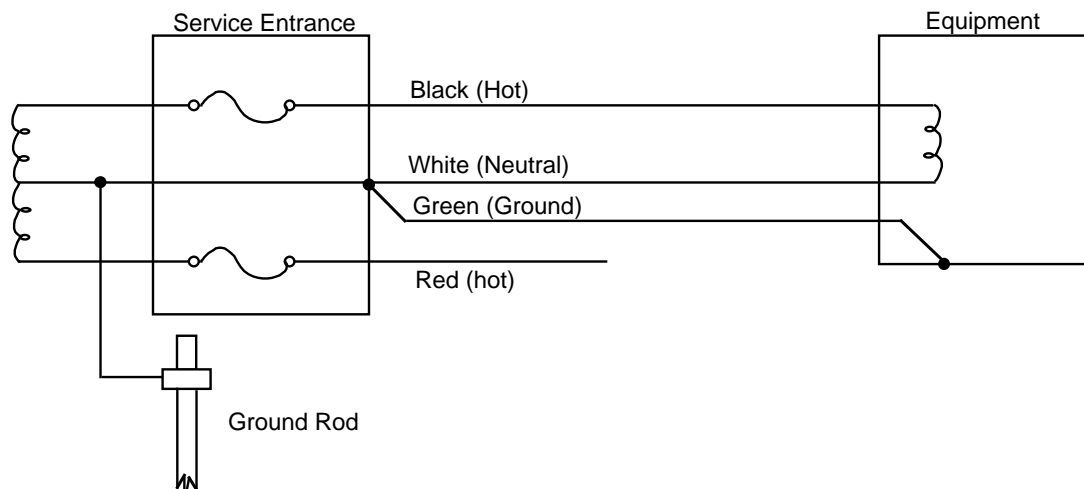


FIGURE 7.4-3: GROUNDING PRACTICE AT A SINGLE PHASE SERVICE ENTRANCE

If the “ground” for every circuit in every piece of equipment were at the same potential as the building earth ground, as intended, the circuit and systems designers’ jobs would be much easier. The reason this is not the case is because all ground conductors have impedance associated with

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

them that renders different parts of the ground system at different potentials whenever ground currents are present.

An extreme case is associated with a nearby lightning stroke. Even if the stroke is conducted harmlessly to “ground”, the flow of the extremely large currents through the finite resistance of the earth would cause one building ground to be at a different potential from another. If two items of equipment were located in two different buildings, connected by a shielded cable “grounded” at each end, a large current would flow through the shield and through the equipment.

One can immediately sense that grounding may be as much an art as a science; nevertheless there are important general principles that are effective in minimizing grounding problems. The overriding concern is to prevent large ground currents from flowing through impedances (especially inductive impedances) that raise parts of the system ground to higher voltages, the so-called “ground bounce” problem.

In Figure 7.4-4 several subsystems have their ground returns “daisy-chained”. This invites problems. The noisy currents from the block of digital circuits flow through  $Z_{G2}$  and  $Z_{G1}$  and together with the large and erratic currents from the power electronics block that flow through  $Z_{G1}$  raise the potential of the ground bus of the low level and sensitive analog block, raising the noise level in that system. It is far better to keep the grounds from each block separate, and connect them all at a common point. Figure 7.4-5 shows separate grounds returned to a common point.

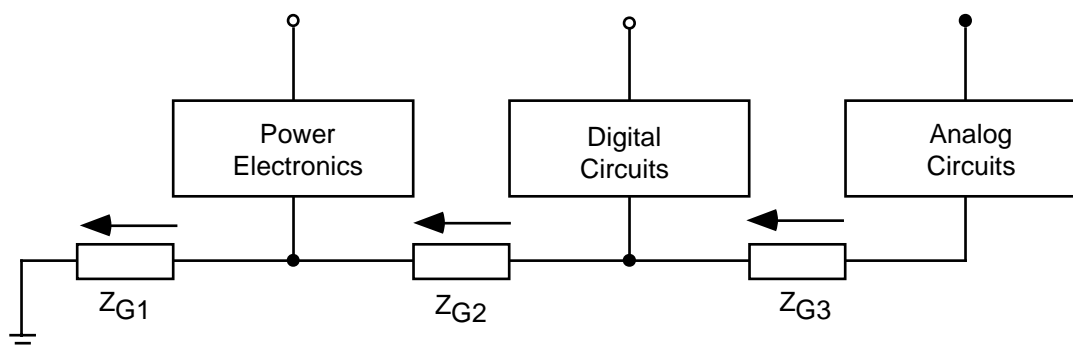


FIGURE 7.4-4: CIRCUIT SUBSYSTEMS WITH GROUND CONNECTIONS “DAISY-CHAINED” INVITES PROBLEMS

## SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

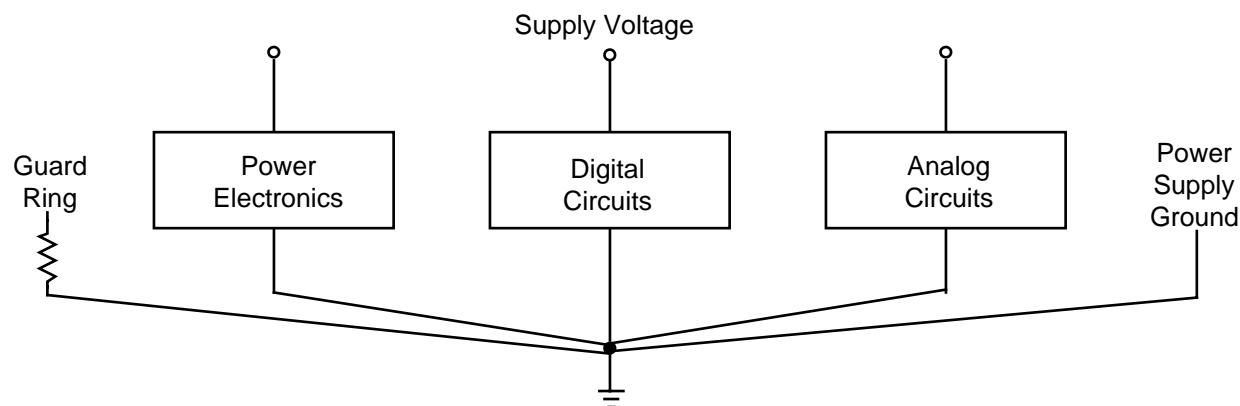


FIGURE 7.4-5: GROUND TRACES RETURNED TO A COMMON POINT

The question often arises, should the cabinet also be connected to the common ground point? Generally no. If the green safety wire enters the cabinet it is usually the best place for the common ground point, and the enclosure should be grounded there. This raises the possibility that a direct ESD discharge could cause an arc from the cabinet to a point on a printed wiring board. If the cabinet has a low impedance from the discharge site to the ground point this is unlikely. It may be necessary to keep the boards a sufficient distance from the cabinet, but to connect the ground of each board to the nearest cabinet point is not a good solution.

On the printed wiring board itself ground traces should be low impedance, with particular attention given to keep the inductance low. Ground planes, ground fill, and ground grids are effective ways to accomplish this. Several ground traces from the connector can be interspersed with signal lines to reduce crosstalk, and power supply filtering at the connector can be supplemented by running power and ground traces in such a manner as to maximize the capacitance between them.

Shielded cables should have their shields grounded at the point of entry with a 360° contact to the socket, rather than with a pigtail. Although shielded cables are usually grounded at both ends, this is not necessarily advisable, especially if the equipment is spaced some distance apart. The shield may be a better “ground” than the green safety wire between outlets, thus raising the possibility of large current flow in the shield. At high frequencies the stray capacitance of the shield negates the advantages of shielding connected at one end only, and both ends are usually grounded. Also, grounding the cable at both ends can produce a ground loop. Any nearby source of flux may introduce considerable current into this loop.

#### 7.4.1.11 Protection With MOVs

Metal oxide varistors, or MOVs, can be used in several ways to protect electronic equipment. They are *not* especially useful in protecting individual inputs to integrated circuits. The prospect of populating a printed circuit board with large numbers of extra devices is not appealing, and the capacitance of the low voltage types is excessive and would seriously degrade the speed of a

---

**SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES**

---

digital system. They are intended to absorb energy far in excess of the threshold energy for a typical IC. Because they are low cost and high speed they have proved to be useful in other ways.

In principle an MOV could be used to suppress transients on power supply buses. They are not appropriate for clamping supply voltages because the MOV tolerance is greater than that of many dc supply requirements. Nevertheless, they would be appropriate for suppressing large amplitude transients.

Transient protection on input and output signal lines is a possible application, especially if the lines are long and subjected to a noisy environment. Telephone lines are susceptible to power contact (when the line makes accidental contact with a power line), induction from power lines, and transients from lightning strokes. EMI and direct or indirect ESD are other sources. In any case the use of an MOV can limit the transients and is a viable option. MOVs are available as connector pin inserts for cable connectors. They are an integral part of the connector, cylindrical in shape, with a hollow core so that the pins of a standard connector can be inserted. They provide transient surge protection in voltage ratings from 6 to 150 volts dc with energy absorption from 0.5 to 1.5 joules. The capacitance ranges from 350 to 2750 pF, with the larger values in the lower voltages.

The main advantage of connector pin inserts over board-mounted suppressors is that they do not take up valuable board space. A second important advantage is that surge currents are diverted directly to ground through the connector itself rather than being conducted onto board traces. This concept has extended to other schemes that employ voltage-variable material as an add-on to standard connectors. The material has a clamping voltage of 100 volts, typical, when subjected to a 15 kV ESD transient, yet adds only 3 pF of shunt capacitance.

The most popular application of MOVs is in power line protection. Typically, an MOV is connected across the line at a point where the power line enters the equipment cabinet. A 0.01 to 0.1  $\mu$ F capacitor is placed in parallel to act as a low impedance shunt element for high frequency noise. The MOV has a good high frequency response as well, but the capacitor is effective at amplitudes below the clamping level of the MOV. Without the capacitor the high frequency transients would couple through the power supply and hence into the interior circuits.

The first step in selecting an MOV is to determine the steady-state working voltage. This is usually taken to be 10-25% above the nominal voltage of the circuit. For 120 volt ac application this implies an MOV with a maximum voltage rating of 132-150 volts rms.

The energy or surge power rating of the MOV is more difficult to specify. Clearly the larger the MOV the better, but this is unrealistic. Attempts to calculate power and energy absorption for a specific location are also unrealistic because the characteristics of the surge source are unknown, the impedance seen by the suppressor is unknown, and the presence of other equipment with non-linear loading is unknown. Rather than design to meet some proposed situation it is better to