AMC PAMPHLET

AMCP 706-196

ADA027370

ENGINEERING DESIGN HANDBOOK.

DEVELOPMENT GUIDE FOR RELIABILITY. PART TWO. DESIGN FOR RELIABILITY.

DDC
RECEIVED
JUL 27 1976
A

242p.

HEADQUARTERS, US ARMY MATERIEL COMMAND

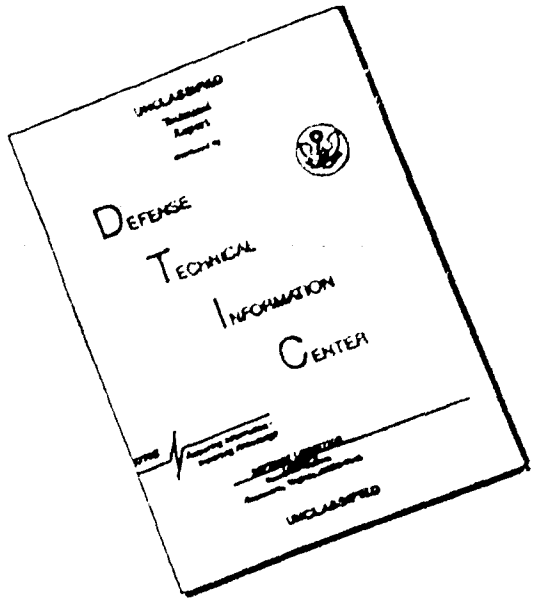
JANUARY 1976

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

039150

-196 DEVELOPMENT GUIDE FOR RELIABILITY, PART TWO JANUARY 1976

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

DEPARTMENT OF THE ARMY
HEADQUARTERS US ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333

AMC PAMPHLET
NO. 706-196

5 January 1976

ENGINEERING DESIGN HANDBOOK

DESIGN FOR RELIABILITY

ACCESSION for
White Section
Buff Section
UNANNOUNCED
JUSTIFICATION
DISTRIBUTION/AVAILABILITY CODES
A

TABLE OF CONTENTS

Paragraph		Page
	LIST OF ILLUSTRATIONS	vi
	LIST OF TABLES	viii
	PREFACE	ix
	CHAPTER 1. INTRODUCTION	
1-0	List of Symbols	1-1
1-1	General	1-1
1-2	System Engineering	1-2
1-3	System Effectiveness	1-4
1-4	The Role of Reliability	1-7
1-5	The Role of Maintainability	1-9
1-5.1	Relationship to Reliability	1-10
1-5.2	Design Guidelines	1-10
1-5.3	Prediction	1-12
1-5.4	Design Review	1-12
1-5.5	Availability	1-13
1-6	The Role of Safety	1-13
1-6.1	Relationships to Reliability	1-14
1-6.2	System Hazard Analysis	1-14
1-6.3	Trade-offs	1-15
1-7	Summary	1-16
	CHAPTER 2. THE ENVIRONMENT	
2-1	Introduction	2-1
2-1.1	Military Operations	2-1
2-1.2	Predicting Environmental Conditions	2-1
2-2	Effects of the Environment	2-3
2-2.1	General Categories	2-3
2-2.2	Combinations of Natural Environmental Factors	2-3
2-2.2.1	Evaluation of Environmental Characteristics	2-3
2-2.2.2	Combinations	2-3
2-2.2.3	Practical Combinations	2-7

TABLE OF CONTENTS

Paragraph		Page
2-2.3	Combinations of Induced Environmental Factors	2-8
2-2.4	Environmental Analysis	2-8
2-3	Designing for the Environment	2-8
2-3.1	Temperature Protection	2-14
2-3.2	Shock and Vibration Protection	2-15
2-3.3	Moisture Protection	2-17
2-3.4	Sand and Dust Protection	2-17
2-3.5	Explosion Proofing	2-18
2-3.6	Electromagnetic-Radiation Protection	2-19
2-4	Operations Research Methods	2-19

CHAPTER 3. MEASURES OF RELIABILITY

3-0	List of Symbols	3-1
3-1	Introduction	3-1
3-2	Probabilities of Success and Failure	3-1
3-3	Failure Distributions	3-2
3-4	Failure Rate	3-3
3-5	Time-to-Failure	3-5
3-6	Time Between Failures	3-5
3-7	Fraction Defective	3-6

CHAPTER 4. MODEL BUILDING AND ANALYSIS

4-0	List of Symbols	4-1
4-1	Introduction	4-1
4-2	Model Building	4-2
4-3	Analysis	4-9
4-4	Simulation	4-9
4-4.1	General Description of a Simulation Program	4-9
4-5	Computer Programs	4-16

CHAPTER 5. ALLOCATION OF RELIABILITY REQUIREMENTS

5-0	List of Symbols	5-1
5-1	Introduction	5-1
5-2	Systems Without Repair	5-2
5-2.1	Equal Allocation	5-3
5-2.2	Proportional Complexity	5-3
5-2.3	Simple-Modular Complexity	5-3
5-2.4	Detailed Complexity	5-8
5-2.5	Feasibility-of-Objectives Allocations	5-9
5-2.6	Redundant Systems	5-13
5-2.7	Redundant Systems with Constraints	5-13
5-2.7.1	Simple Redundancy Allocation with a Single Constraint	5-20
5-2.7.2	Dynamic Programming Allocation	5-20
5-2.7.3	Minimization of Effort Algorithm	5-20
5-3	Systems with Repair	5-23

TABLE OF CONTENTS

Paragraph		Page
5-3.1	An Elementary Approach to Steady-State Availability	5-23
5-3.2	Failure Rate and Repair Rate Allocation for Series Systems	5-25
5-3.3	A Simple Technique for Allocating Steady-State Availability to Series Systems	5-26
5-3.4	Failure and Repair Rate Allocations for Redundant Systems	5-26
5-3.5	Reliability with Repair and Instantaneous Availability	5-32

CHAPTER 6. HUMAN FACTORS

6-0	List of Symbols	6-1
6-1	Introduction	6-1
6-2	Design and Production	6-1
6-3	Human Engineering	6-2
6-4	Human Performance Reliability	6-3
6-4.1	The Relationship Between Human Factors and Reliability	6-4
6-4.2	Human Factors Theory	6-4
6-4.3	Man/Machine Allocation and Reliability	6-5
6-4.4	Interactions and Trade-Offs	6-8
6-4.5	THERP (Technique for Human Error Rate Prediction)	6-9

CHAPTER 7. CAUSE-CONSEQUENCE CHARTS

7-1	Introduction	7-1
7-2	Generation	7-2
7-2.1	System Definition	7-6
7-2.2	Fault Tree Construction	7-6
7-3	Minimal Cut Sets	7-7
7-3.1	Finding the Minimal Cut Sets	7-7
7-3.2	Modifications for Mutually Exclusive Events	7-12
7-4	Failure Probability	7-15

CHAPTER 8. FAILURE MODES AND EFFECTS ANALYSIS

8-0	List of Symbols	8-1
8-1	Introduction	8-1
8-2	Phase 1	8-2
8-3	Phase 2	8-2
8-4	Computer Analysis	8-13

CHAPTER 9. MODELS FOR FAILURE

9-0	List of Symbols	9-1
9-1	Introduction	9-1

TABLE OF CONTENTS

Paragraph		Page
9-2	Deterministic Stress-Strength	9-2
9-2.1	Tensile Strength	9-2
9-2.2	Safety Factors, Load Factors, and Margin of Safety	9-5
9-3	Probabilistic Stress-Strength	9-6
9-3.1	Computing Probability of Failure	9-8
9-3.2	Probabilistic Safety Margin	9-11
9-4	Simple Cumulative Damage	9-12
9-5	Severity Levels for Electronic Equipment	9-12
9-6	Other Models	9-18

CHAPTER 10. PARAMETER VARIATION ANALYSIS

10-0	List of Symbols	10-1
10-1	Introduction	10-1
10-2	Descriptions of Variability	10-2
10-3	Sources of Variability	10-5
10-4	Effects of Variability	10-6
10-5	Worst-Case Method	10-8
10-6	Moment Method	10-9
10-7	Monte Carlo Method	10-15
10-8	Method Selection	10-17
10-9	Computer Programs	10-17
10-9.1	A General Program	10-17
10-9.2	ECAP and NASAP	10-17

CHAPTER 11. DESIGN AND PRODUCTION REVIEWS

11-1	Introduction	11-1
11-2	Organizing for the Reviews	11-2
11-2.1	Review Board Chairman	11-2
11-2.2	Design Group	11-4
11-2.3	Other Review Team Members	11-4
11-2.4	Followup System	11-4
11-3	Review Cycles	11-5
11-3.1	Technical Exchange Phase	11-5
11-3.2	Internal Design Review Meeting/Agreement Phase	11-5
11-3.3	Army Involvement in Internal Design Review	11-5
11-3.4	Design Data Package Phase	11-5
11-3.5	Change Data Package	11-5
11-3.6	Performance Specification Changes	11-5
11-3.7	Government Response	11-6
11-3.8	Unsatisfactory Design Data	11-6
11-3.9	Army/Contractor Review Meeting	11-6
11-3.10	Standard Review	11-6
11-3.11	Subcontractor Design Review	11-6
11-4	Minimum Requirements in Conceptual-Phase Review	11-6
11-5	Minimum Requirements for Developmental-Phase Review	11-7
11-6	Checklists	11-8

TABLE OF CONTENTS

Paragraph		Page
	APPENDIX A. DESIGN DETAIL CHECKLISTS	
A-1	Introduction	A-1
A-2	Propulsion Systems	A-1
A-3	Fuel/Propellant System	A-1
A-4	Hydraulic Systems	A-2
A-5	Pressurization and Pneumatic Systems	A-3
A-6	Electrical/Electronic Systems	A-3
A-7	Vehicle Control Systems	A-5
A-8	Guidance and Navigation Systems	A-6
A-9	Communication Systems	A-7
A-10	Protection Systems	A-7
A-11	Fire Extinguishing and Suppression System	A-8
A-12	Crew Station Systems	A-9
A-13	Ordnance and Explosive Systems	A-11
	APPENDIX B. RELIABILITY DATA SOURCES	
B-1	Introduction	B-1
B-2	GIDEP, Government-Industry Data Exchange Program	B-1
B-2.1	Introduction	B-1
B-2.2	Functions	B-2
B-2.2.1	Engineering Data Bank	B-2
B-2.2.2	Failure Experience Data Bank	B-2
B-2.2.3	Failure Rate Data Bank (FARADA)	B-2
B-2.2.4	Metrology Data Bank	B-3
B-2.3	Operations	B-3
B-2.4	Cost Savings	B-4
B-3	Reliability Analysis Center--A DOD Electronics Information Center	B-4
B-4	Army Systems	B-5
B-4.1	The Army Equipment Record System (TAERS)	B-5
B-4.2	The Army Maintenance Management System (TAMMS) Including Sample Data Collection	B-5
B-5	Precautions in Use	B-6
B-6	Partial Listing of Data Banks in Operation	B-7
B-7	Discontinued or Transferred Activities	B-15
	APPENDIX C. ANNOTATED BIBLIOGRAPHY ON HUMAN FACTORS (from NTIS Government Reports Announcement)	

LIST OF ILLUSTRATIONS

Figure		Page
1-1	System Management Activities	1-3
1-2	Fundamental System Engineering Process Cycle	1-4
1-3	Flow Diagram for a General Optimization Process	1-6
1-4	Reliability/Maintainability Relationships	1-11
2-1	Latitudinal Distribution of Environmental Extremes	2-6
2-2	Semispatial Distribution of Environmental Extremes	2-7
2-3	Comparison Between Temperature and Other Environmental Factors	2-7
2-4	Comparison of Heat Removal Methods	2-15
2-5	Environmental Situation Diagram	2-20
2-6	Algorithm for Program Performance	2-21
2-7	Matrix of Interrelationships of Tasks	2-22
4-1	Example of Reliability Block Diagrams and Up-state Rules	4-4
4-2	ILS Localizer Functional Block Diagram	4-5
4-3	ILS Localizer Reliability Block Diagram	4-6
4-4	Progressive Expansion of Reliability Block Diagram	4-7
4-5	Sampling from a Distribution	4-8
5-1	Steady-state Availability vs the Ratio of Failure Rate to Repair Rate	5-25
5-2	Repair Rate to Failure Rate Ratio vs Unavailability ($n = 2$)	5-29
5-3	Repair Rate to Failure Rate Ratio vs Unavailability ($n = 3$)	5-29
5-4	Repair Rate to Failure Rate Ratio vs Unavailability ($n = 4$)	5-30
5-5	Repair Rate of Failure Rate Ratio vs Unavailability ($n = 5$)	5-30
6-1	The Man/Machine Interaction	6-5
6-2	Predicting Man/Machine Reliability	6-8
7-1	Fault Tree Logic Symbols	7-4
7-2	Fault Tree Event Symbols	7-5
7-3	Sample System	7-7
7-4	First Treetop System Boundary Condition for Sample System	7-7
7-5	First Fault Tree for Sample System 1	7-8
7-6	Second Treetop System Boundary Condition for Sample System	7-9
7-7	Second Fault Tree for Sample System	7-10
7-8	Sample System 2	7-13
7-9	Fault Tree for Sample System 2	7-14
7-10	Sample Fault Tree for Probability Evaluation	7-16
7-11	Boolean Equivalent of Sample Fault Tree Shown in Fig. 7-10	7-17
7-12	Sample Fault Tree with Time-Dependent Probabilities	7-18
8-1	Typical System Symbolic Logic Block Diagram	8-3
8-2	Typical Unit Symbolic Logic Block Diagram	8-4
8-3	Failure Effects Analysis Form	8-7
8-4	Symbolic Logic Block Diagram of Radar Example	8-10
8-5	Determination of Preamplifier Criticality	8-11
9-1	Typical Tensile-test Diagrams	9-4
9-2	Aluminum Simple Uniaxial Tension	9-8
9-3	Typical Probability Density Function g of Stress f and Strength F	9-9
9-4	Simply Supported Rectangular Plate Subject to Uniform Load P	9-16

LIST OF ILLUSTRATIONS

Figure		Page
9-5	Determination of Failure Rate λ_B as Related to Stress Ratio S for MIL-R-11/4E Resistors, RC-22	9-21
9-6	Determination of Longevity Factor π_L for MIL-R-11 Resistors, All Styles	9-21
9-7	Determination of Resistor Longevity as Related to Body Temperature, for MIL-R-11 Resistors, All Styles	9-21
10-1	Performance Variability	10-3
10-2	Performance Variability of a System as a Function of the Variability of Three Parameters	10-4
10-3	Frequency Histogram and Cumulative Polygon for a Typical Frequency Distribution	10-5
10-4	Moments of a Distribution	10-5
10-5	Worst-case Method	10-8
10-6	Moment Method	10-12
10-7	The Monte Carlo Method	10-15
10-8	Flow Diagram for General PVA Program	10-19

LIST OF TABLES

Table		Page
1-1	Partial List of Optimization Techniques	1-7
2-1	Major Environmental Factors	2-2
2-2	Environmental Effects	2-4
2-3	Analysis of Paired Environmental Factors	2-9
2-4	Environmental Analysis	2-10
2-5	Various Environmental Pairs	2-11
2-6	Low Temperature Protection Methods	2-16
3-1	General Application of Common Distributions	3-3
3-2	Behavior of the Failure Rate	3-4
4-1	Failure and Repair Distribution for Elements A and B in the Example	4-11
4-2	List of Pseudo-Random Numbers from the Uniform Distribution	4-12
4-3	Up/Down Time Pairs for the Example	4-12
4-4	Summary of Programs in the Reliability Area	4-13
5-1	Failure Rates for Old and New Hydraulic Systems	5-8
5-2	Example Radar System Description	5-8
5-3	Bombsight-System Description	5-12
5-4	Mechanical-Electrical System	5-15
5-5	Comparison of Improvement Strategies	5-19
5-6	Cost and Reliability Data Associated with Example Problem No. 7	5-23
6-1	List of Predictive Methods	6-3
6-2	Characteristics of Human and Machines	6-7
7-1	Minimal Cut Sets for Sample System as Determined by Conventional Means	7-15
8-1	Part Failure Modes	8-5
8-2	Column Descriptions for Figure 8-3	8-8
9-1	Comparison of the Chebyshev-Limit, the s-Normal Distribution and the Reasonable-Engineering-Guess (REG)	9-13
9-2	Resistance Factor Π_R for RC-22 Resistors	9-16
9-3	Environment Factors, Π_E, Σ_E, and Longevity, L, for MIL-R-11 Resistors	9-17
9-4	Constants for Use in Computing λ_B	9-18
10-1	Programs for PVA	10-18
11-1	Design Review Group, Responsibilities and Membership Schedule	11-3
11-2	Reliability Actions Checklist	11-9

PREFACE

This handbook, *Design for Reliability* is the first in a series of five on reliability. The series is directed largely toward the working engineers who have the responsibility for creating and producing equipment and systems which can be relied upon by the users in the field.

The five handbooks are:

1. *Design for Reliability*, AMCP 706-196
2. *Reliability Prediction*, AMCP 706-197
3. *Reliability Measurement*, AMCP 706-198
4. *Contracting for Reliability*, AMCP 706-199
5. *Mathematical Appendix and Glossary*, AMCP 706-200.

This handbook is directed toward reliability engineers who need to be familiar with the mathematical-probabilistic-statistical techniques for predicting the reliability of various configurations of hardware. The material in standard textbooks is not repeated here; the important points are summarized, and references are given to the standard works.

The majority of the handbook content was obtained from many individuals, reports, journals, books, and other literature. It is impractical here to acknowledge the assistance of everyone who made a contribution.

The original volume was prepared by Tracor Jitco, Inc. The revision was prepared by Dr. Ralph A. Evans of Evans Associates, Durham, N.C., for the Engineering Handbook Office of the Research Triangle Institute, prime contractor to the US Army Materiel Command. Technical guidance and coordination on the original draft were provided by a committee under the direction of Mr. O. P. Bruno, US Army Materiel Systems Analysis Agency, US Army Materiel Command.

The Engineering Design Handbooks fall into two basic categories, those approved for release and sale, and those classified for security reasons. The US Army Materiel Command policy is to release these Engineering Design handbooks in accordance with current DOD Directive 7230.7, dated 18 September 1973. All unclassified handbooks can be obtained from the National Technical Information Service (NTIS). Procedures for acquiring these handbooks follow:

a. All Department of Army activities having need for the handbooks must submit their request on an official requisition form (DA Form 17, dated Jan 70) directly to:

Commander
Letterkenny Army Depot
ATTN: AMXLE—ATD
Chambersburg, PA 17201

(Requests for classified documents must be submitted, with appropriate "Need to Know" justification, to Letterkenny Army Depot.) DA activities will not requisition handbooks for further free distribution.

b. All other requestors, DOD, Navy, Air Force, Marine Corps, non-military Government agencies, contractors, private industry, individuals, universities, and others must purchase these handbooks from:

National Technical Information Service
Department of Commerce
Springfield, VA 22151

Classified documents may be released on a "Need to Know" basis verified by an official Department of Army representative and processed from Defense Documentation Center (DDC), ATTN: DDC-TSR, Cameron Station, Alexandria, VA 22314.

Comments and suggestions on this handbook are welcome and should be addressed to:

Commander
US Army Materiel Development and Readiness Command
Alexandria, VA 22333

(DA Forms 2028, Recommended Changes to Publications, which are available through normal publications supply channels, may be used for comments/suggestions.)

b. All other requestors, DOD, Navy, Air Force, Marine Corps, non-military Government agencies, contractors, private industry, individuals, universities, and others must purchase these handbooks from:

National Technical Information Service
Department of Commerce
Springfield, VA 22151

Classified documents may be released on a "Need to Know" basis verified by an official Department of Army representative and processed from Defense Documentation Center (DDC), ATTN: DDC-TSR, Cameron Station, Alexandria, VA 22314.

Comments and suggestions on this handbook are welcome and should be addressed to:

Commander
US Army Materiel Development and Readiness Command
Alexandria, VA 22333

(DA Forms 2028, Recommended Changes to Publications, which are available through normal publications supply channels, may be used for comments/suggestions.)

CHAPTER 1 INTRODUCTION

1-0 LIST OF SYMBOLS

A = availability
$MTBF$ = mean time between failures, time^{-1}
$MTTR$ = mean time to repair, time^{-1}
I, II = subscripts to indicate systems I, II

1-1 GENERAL

Reliability engineering is the doing of those things which insure that an item will perform its mission successfully. The pressures and constraints on engineers to produce equipment and systems at minimum cost with maximum utility in minimum time have been very severe. Thus arose the original discipline of reliability which has two parts:

(1) Paying attention to detail
(2) Handling uncertainties.

As engineers and administrators became more adept at quantifying the effort to produce equipment and systems that could be relied upon, classification schemes for this effort were developed. Under such schemes, the word "reliability" has several meanings, all related to the dictionary, but some of them rather narrow and specific.

The traditional narrow definition of *s*-reliability (Ref. 3, Version A) is "the probability that an item will perform its intended function for a specific interval under stated conditions". In reliability calculations, the following extended definition is more often actually used:

> *s*-Reliability is the probability that the item successfully completes its mission, given that the item was in proper condition at the mission beginning.

The convention adopted in all Parts of this series is to use "*s*-" followed by the word when the term is used in a specially defined statistical sense—e.g., *s*-reliability, *s*-normal, *s*-availability, *s*-confidence.

This concept of *s*-reliability is applicable largely to items which have simple missions, e.g., equipment, simple vehicles, or components of systems. For large complex systems—e.g., an antiaircraft system (including the radars and weapons), a squadron of tanks, or a large communication network—it is more appropriate to use more sophisticated concepts such as system effectiveness to describe the worth of a system.

The reliability engineer must do more than merely collect data and perform actuarial services during the design, development, and field use of equipment. He must be sensitive to the countless decisions made during the evolution of a product, and he must assist in making these decisions. The reliability engineer has a responsibility to build specific amounts of longevity into equipment. He must be able to trade off the reliability parameters against the many other important parameters such as cost, weight, size, and scheduling. Great emphasis is placed on failures whose cause can be eliminated. Reliability mathematics must reflect the engineering search for causes of failure and the adequacy of their elimination. It must permit *s*-reliability prediction from the planning phase through the field-use phase to assure that failure probability does not exceed a permissible bound. *s*-Reliability is a quantitative probabilistic factor, which must be predictable in design, measurable in tests, assurable in production, and maintainable in the field. In short, it must be controllable throughout the life cycle of the product. Other system characteristics, such as maintainability and safety, also affect the mission-performing equipment and its related subsystems, including maintenance and support equipment, checkout and servicing, repair parts provisioning, and actual repair functions. Thus, reliability and other design considerations provide the basis for developing adequate systems which conform to mission objectives and requirements. This overall program is called system engineering. The purpose of this chapter is to provide a general understanding of system engineering and of reliability trade-offs with maintainability, safety, and performance.

1-2 SYSTEM ENGINEERING

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.

Specifically, a system is defined (Ref. 1, Version A) as: "A composite, at any level of complexity, of operational and support equipment, personnel, facilities, and software which are used together as an entity and capable of performing and supporting an operational role".

System engineering (Ref. 2) 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 the initial, conceptual phase through the subsequent contract definition, engineering development, production, and operational phases. These five activities (procurement and production, program control, configuration management, system engineering, and test and deployment management), their general functions within each of the system evolutionary phases, and their relationships to one another are summarized in Fig. 1-1. More details on system management are given in Ref. 8.

System engineering consists of four steps in an interacting cycle (Fig. 1-2). Step 1 considers threat forecast studies, doctrinal studies, probable Army 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 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.

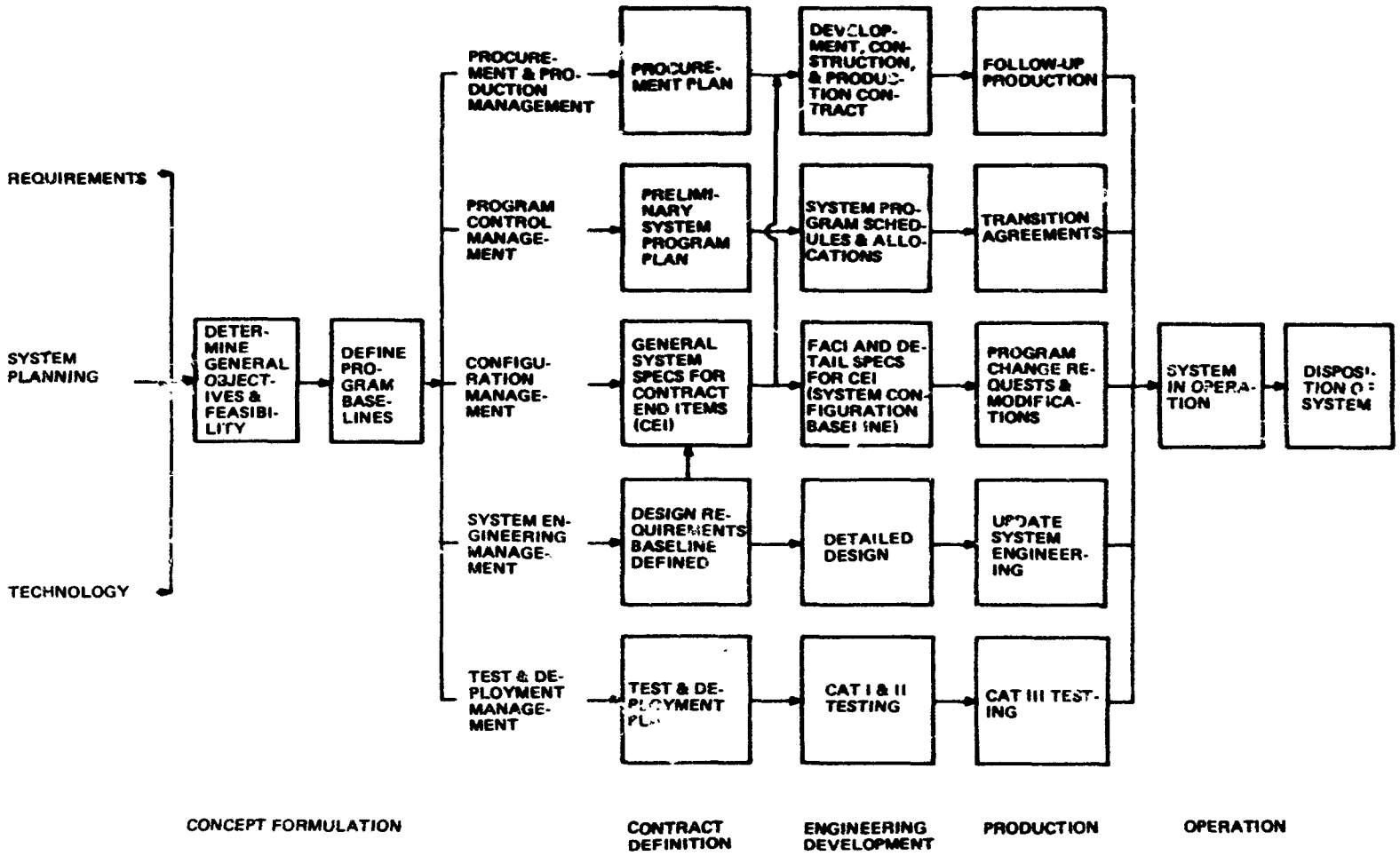


FIGURE 1-1. System Management Activities

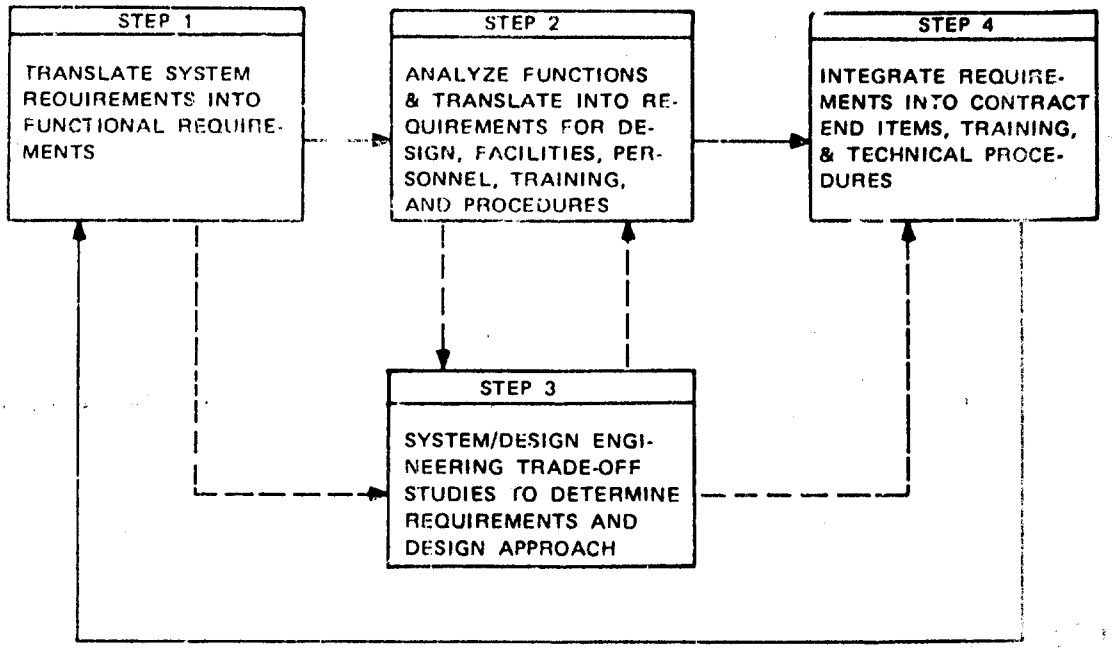


FIGURE 1-2. Fundamental System Engineering Process Cycle

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.

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.

1-3 SYSTEM EFFECTIVENESS

System effectiveness is defined (Ref. 3, Version B) as: "a measure of the degree to which an item can be expected to achieve a set of specific mission requirements, and which may be expressed as a function of availability, dependability, and capability". 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.

The 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, dependability, and capability included in the definition of system effectiveness illustrate these influences and their relationships to system effectiveness. MIL-STD-721 (Ref. 3, Version B) provides the following 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) point in time.

(2) Dependability. A measure of the item operating condition at one or more points during the mission, including the effects of reliability, maintainability, and survivability, given the item condition(s) at the start of the mission. It may be stated as the probability that an item will: (a) enter or occupy any one of its required operational modes during a specified mission, and (b) perform the functions associated with these operational modes.

(3) Capability. A measure of the ability of an item to achieve mission objectives, given the conditions during the mission.

Dependability is related to reliability; the intention was that dependability would be a more general concept than reliability. No designer should become bogged down in semantic discussions when intent is clear.

As an example, consider the use of machine guns against attacking aircraft. Since the design intent was to provide increased firepower and area coverage for ground support combat, the effectiveness of this "system" (machine gun) will be very low. The machine gun does not have an intended capability for antiaircraft use. This fact, however, has little to do with the availability or dependability of the machine gun. That particular application by the user/operator is simply a misuse. As another example (adapted from Ref. 4, par. 2.7.3), consider a previously serviceable vehicle tire that has a blowout at 90 mph on a hot day (110°F) due to impact with a jagged hole in the pavement. If most tires of this type survive high-speed, high-temperature operation under high impact loads, then the blowout (failure) is due to lack of reliability, since such severe environments (90 mph, 110°F, jagged hole) are within the capability of the tire type. If, however, the design requirements specified less severe environments (60 mph, 80°F, no jagged holes), then the failure was due to a lack of capability. Thus, in the first case, the system (tire) had adequate capability, but its reliability was low. In the second case, the reliability may have been high, but the capability (for that particular usage) was inadequate. In both cases, however, the system effectiveness for the applied usage was low.

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, 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 Fig. 1-3 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, of putting into precise, quantifiable terms the rules 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

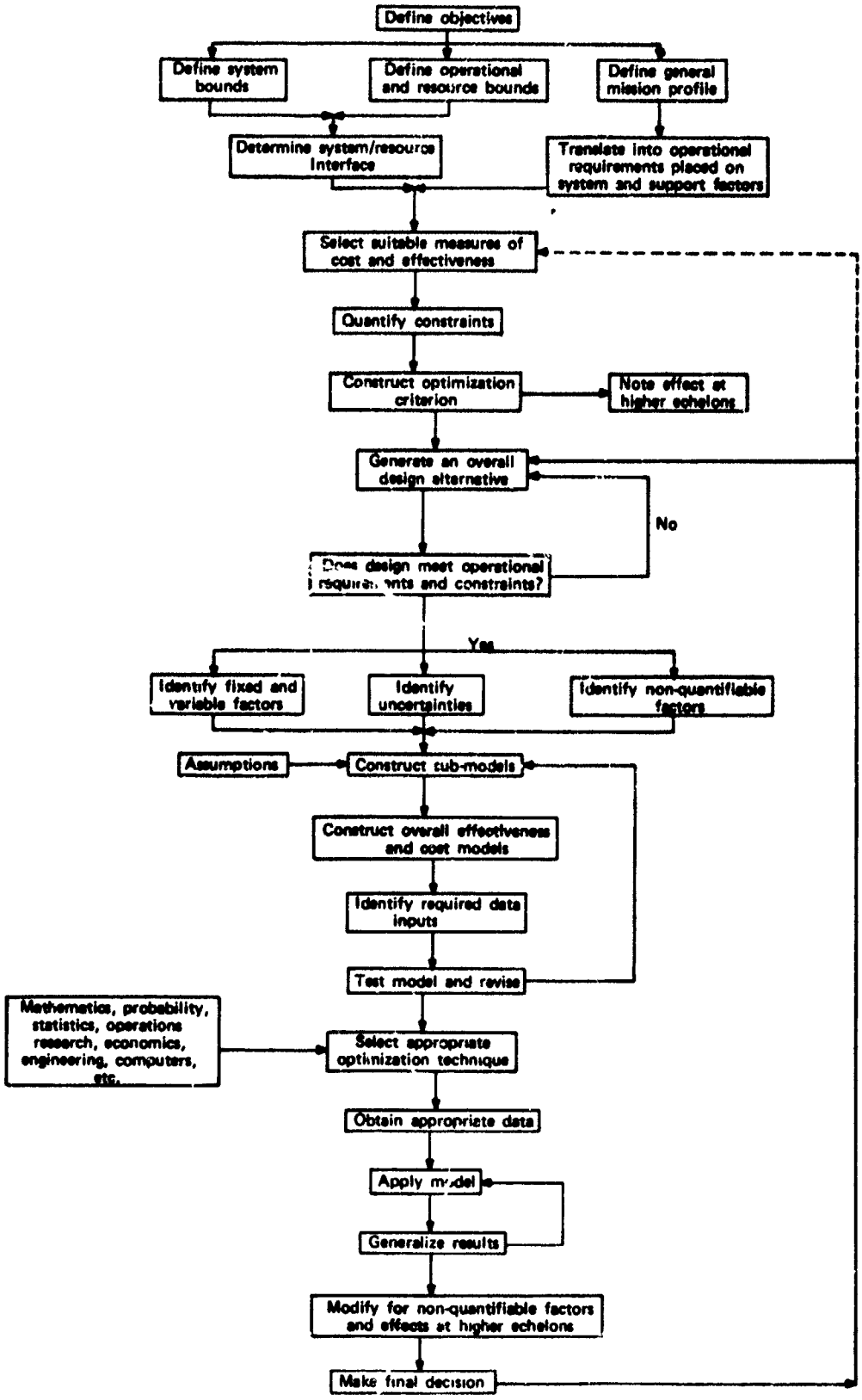


FIGURE 1-3. Flow Diagram for a General Optimization Process

most cars of a particular class (low-price sedans, sports models, etc.). Thus, the selection criteria essentially reduce 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.

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 actual techniques used to optimize system effectiveness are beyond the scope of this chapter. Table 1-1 (Ref. 4), for example, lists only some of the more commonly used techniques. Specific details are contained in the references already mentioned and in Ref. 26. Ref. 4, for example, contains methods and examples of basic mathematical and statistical concepts, simulation, queuing theory, sequencing and Markov processes, game theory, linear and dynamic programming, information theory, and others. These techniques are not peculiar to system effectiveness optimization nor are they limited to system engineering.

TABLE 1-1.

PARTIAL LIST OF OPTIMIZATION TECHNIQUES[4]

I. Mathematical Techniques

- 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

II. Statistical Techniques

- Bayesian analysis
- Decision theory
- Experimental design
- Information theory
- Method of steepest ascent
- Stochastic processes

III. Programming Techniques

- Dynamic programming
- Linear programming
- Nonlinear programming

IV. Other

- Gaming theory
- Monte Carlo techniques
- Queuing theory
- Renewal theory
- Search theory
- Signal flow graphs
- Simulation
- Value theory

1-4 THE ROLE OF RELIABILITY

The reliability effort includes not only the hardware but also the actions, procedures, software, and operators that use the hardware. The reliability depends on the reliability requirements, the testing, and the emphasis placed on reliability by management (both Government and contractor) throughout the life cycle of the equipment. Often as deadlines approach, something must be sacrificed (cost, schedule, performance, reliability);

management decides what it will be; e.g., will management decide that a paper "demonstration" be substituted for a physical demonstration of reliability?

It is much easier to talk about optimizing reliability and to analyze ways of doing it than it is to get a physical system which is optimized. Achieving high reliability is an engineering problem, not a statistical one.

Before reliability can be optimized, one needs to look at ways reliability can be changed and the kinds of constraints that can be imposed upon efforts to change it. These classifications are convenient for discussion. They do not in themselves limit anyone's activities. Not all changes which are made with the intention of improving reliability actually do improve it—especially when there is insufficient information about the mission.

Reliability can be modified by changing:

(1) The overall approach to the problem (e.g., wire lines or a microwave link for a communication system)

(2) The configuration of the system (e.g., an aircraft can have propeller or jet engines, wings over or under the fuselage, and the mounting and number of engines are adjustable)

(3) Some of the modules or subsystems (e.g., motor functions can be performed electrically, hydraulically, or by mechanical levers and gears)

(4) Some components (e.g., use high reliability parts or commercial ones)

(5) Details of manufacture (e.g., holes in steel can be punched, drilled, reamed, and/or burned)

(6) Materials (e.g., wood, plastics, metal alloys)

(7) Method of operation (e.g., the operator of a radio-receiver can be required to tune each stage separately or it can all be done with one switch)

(8) Definition of mission success (e.g., range and resolution of a radar)

(9) Amount of attention to detail (e.g., an alloy can simply be selected from a handbook table, or many tests can be run on many alloys to find the one which holds up best in service).

Efforts to improve reliability are constrained by:

(1) Cost of design effort
(2) Cost of parts manufacture
(3) Calendar time schedules
(4) Manpower available to do the job
(5) Availability of purchased components or materials
(6) Volume or weight of finished product
(7) Operator training limitations
(8) Uncertainty about actual use conditions
(9) Maintenance philosophy, and logistics
(10) Logical consequences of various user regulations
(11) User resistance to some configurations
(12) Management refusal to effect administrative changes
(13) Lack of knowledge about material or component properties or about the way a part will be made.

Other techniques and constraints are likely to be important in any particular job. Some of the changes and constraints are not easily quantifiable, and the ones listed are certainly not mutually exclusive. All of this makes a complete mathematical analysis virtually impossible.

It is worthwhile to have many of the critical failure modes such that the equipment fails gracefully; viz., there is a very degraded mode of operation which is still feasible after the major failure. For example, if the power steering on a vehicle fails, it may still be possible for it to limp to safety if the vehicle can be steered by hand.

The repair philosophy during a mission must be stated explicitly. Standby redundancy often can be considered a special case of repair—it is just a question of how the changeover is effected in case of failure. In some situations, the mission will not be a failure if the equipment is down for only a very short time. In what state will a repair leave the system? Is the entire system to be restored to a like-new condition after each failure? Will only a subsystem be restored to like-new or perhaps the equipment will be

returned to the statistical condition it had just before failure? In general, the exact situation will not be known, and it is a matter of engineering judgment to pick tractable assumptions that are reasonably realistic.

The design approaches and requirements are investigated by the system reliability engineer. They include the following:

(1) The definitions of (a) the mission, (b) successful completion, and (c) proper condition (at mission beginning) must be sufficiently explicit to make the reliability calculations.

(2) Relationships and interactions between reliability and each of the other system parameters (maintainability, etc.) must be carefully analyzed.

(3) A method of estimating reliability must be selected to permit quantitative description of the consequences of each design.

(4) Reliability objectives must be matched to the system mission.

(5) System reliability levels must be related to overall program resource allocations.

These and others are discussed in this handbook and Parts Three, Four, and Five.

The techniques used in this analysis include development of a model that considers:

(1) Required functions for each mission phase

(2) Identification of critical time periods for each function

(3) Establishment of external and internal environmental stresses for each functional element

(4) Operational and maintenance concepts

(5) Hardware and software system elements for each function

(6) Determination of any required functional redundancies.

Specific design techniques, such as stress derating, redundancy, stress/strength analysis, apportionment of reliability requirements, prediction, design of experiments and tests, parameter variation analysis, failure mode and effect analysis, and worst case analysis, are the "tools of the trade" for reliability engineers. Additionally, the reliability engineer must:

(1) Actively participate in selecting preferred parts having established reliabilities, and thus promote standardization within military systems.

(2) Participate in design reviews at appropriate stages to evaluate reliability objectives and achievement thereof.

(3) Monitor attainment of reliability requirements throughout the entire program.

(4) Work with other members of the system engineering team to integrate reliability with other engineering areas.

Thus, the reliability engineer performs system engineering from the reliability viewpoint. These methods and techniques are discussed in greater detail in later chapters and other Parts. Additional information is provided in the references at the end of this chapter; e.g., MIL-STD-785 (Ref. 1) specifies the requirements for system reliability programs, MIL-STD-721 (Ref. 3) defines terms for reliability and related disciplines, and AR 702-3 (Ref. 5) establishes Army requirements for reliability and maintainability.

1-5 THE ROLE OF MAINTAINABILITY

Maintainability is a characteristic of design and installation of equipment. s-Maintainability is defined (Ref. 3) as the probability that an item will be retained in a specified condition, or restored to that condition within a given time period, when maintenance is performed according to prescribed procedures and resources. Maintenance consists of those actions needed to retain the designed-in characteristics throughout the system lifetime. Maintainability, like reliability, must be designed into the equipment.

Maintainability engineering is similar to other engineering practices, but it emphasizes recovery of the equipment after a failure and reductions in upkeep costs. Maintainability engineers consider the purpose, type, use, and limitations of the product, all of which influence the ease, rapidity, economy, accuracy of its service and repair, effects of installation, environment, support equipment, personnel, and operational policies on the item geometry, size, and weight. Thus, maintainability studies assist in the development of a product which can be maintained by personnel of

ordinary skill under the environmental conditions in which it will operate.

1-5.1 RELATIONSHIP TO RELIABILITY

Reliability is related to the effectiveness of the maintenance performed on a system. If this maintenance is incorrect or not timely, the system may fail. Maintainability, on the other hand, can provide designed-in ease of maintenance and, thereby, increase the maintenance 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, as required by Ref. 5, then 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 then merely from the standpoint of initial acquisition. The overall cost of ownership has been estimated to be from three to twenty times the original acquisition cost. An effective design approach to reliability and maintainability can reduce this cost of upkeep.

The reliability and maintainability characteristics of an item are relatively fixed and difficult to change in the field. Thus, the soldier/user finds himself faced with accepting the item reliability as a determination of whether the item will function correctly or not; as long as it functions, he can use it. Consequently, reliability data do not greatly concern him (Ref. 7). Maintainability, on the other hand, provides the soldier/user with his only means of returning the equipment to a serviceable condition. A tank, for example, that has a nonrepairable weapon system becomes, on breakdown of the weapon, an immensely heavy mobile radio from the viewpoint of its users.

The primary objectives of the Army reliability, availability, and maintainability (RAM) programs are to assure that Army materiel will:

(1) Be ready for use when needed

(2) Be capable of successfully completing its mission and

(3) Fulfill all required maintenance objectives throughout its life cycle.

Ref. 8 provides guidance on management of reliability and maintainability programs, and Ref. 5 delineates concepts, objectives, responsibilities, and general policies for Army reliability and maintainability programs.

Policies and guidance on life cycles of Army equipment are provided by Refs. 6 and 9. Amplification of Army reliability and maintainability policies can be found in the references at the end of this chapter. Fig. 1-4 illustrates some of the fundamental relationships between reliability and maintainability.

1-5.2 DESIGN GUIDELINES

System maintainability goals must be apportioned among three major categories: (1) equipment design, (2) personnel, and (3) support. To accomplish this, a maintenance concept must be selected, and a mathematical model developed to describe the concept. Initially, the goals can be apportioned based upon past experience with similar systems, and upon general guidelines presented here and in the references for this chapter. As the design progresses, the initial apportionment can be changed by trade-offs among these three categories. The design goals can be further apportioned to the subsystem and component levels. Allocating maintainability for subsystems and components of a complex system can be difficult due to the mathematical/statistical complexity of the model. Some of the problems associated with combining or apportioning downtime and suggested approaches to their solution are covered in Refs. 7, 10, 11, and 12.

The design category covers the physical

aspects of the equipment, including the requirements for test equipment, tools repair parts, training, and maintenance skill levels. Equipment design, packaging, test points, accessibility, and other factors directly influence these requirements. The personnel category considers the actual skill levels of the maintenance technicians, their job attitudes and motivations, experience, technical knowledge, and other personnel characteristics associated with equipment maintenance. The support category encompasses the logistic and maintenance organizations associated with system support. Some of the areas included in support are: tools, test equipment, and repair parts stocked at specific locations; the availability of equipment technical publications; supply problems characteristic of, or peculiar to, particular maintenance sites; allocation of authorized maintenance levels; and establishment of maintenance organizational structures.

Some guidelines for engineers designing and developing Army equipment are:

(1) Reduce maintenance needs by designing reliability into equipment to insure desired performance over the intended life cycle.

(2) Use reliability improvements to save time and manpower by reducing preventive maintenance requirements and, thereby, provide more operational time for components.

(3) Reduce downtime by improving maintainability through simplification of test and repair procedures to reduce troubleshooting and correction time; for example, provide easy access and simple adjustments.

(4) Decrease the logistic burden (particularly in combat areas) by using standard parts, tools, test equipment, and components, and by planning for interchangeability of parts, components, and assemblies.

(5) Simplify equipment operation and maintenance requirements so that highly trained maintenance specialists will not be needed.

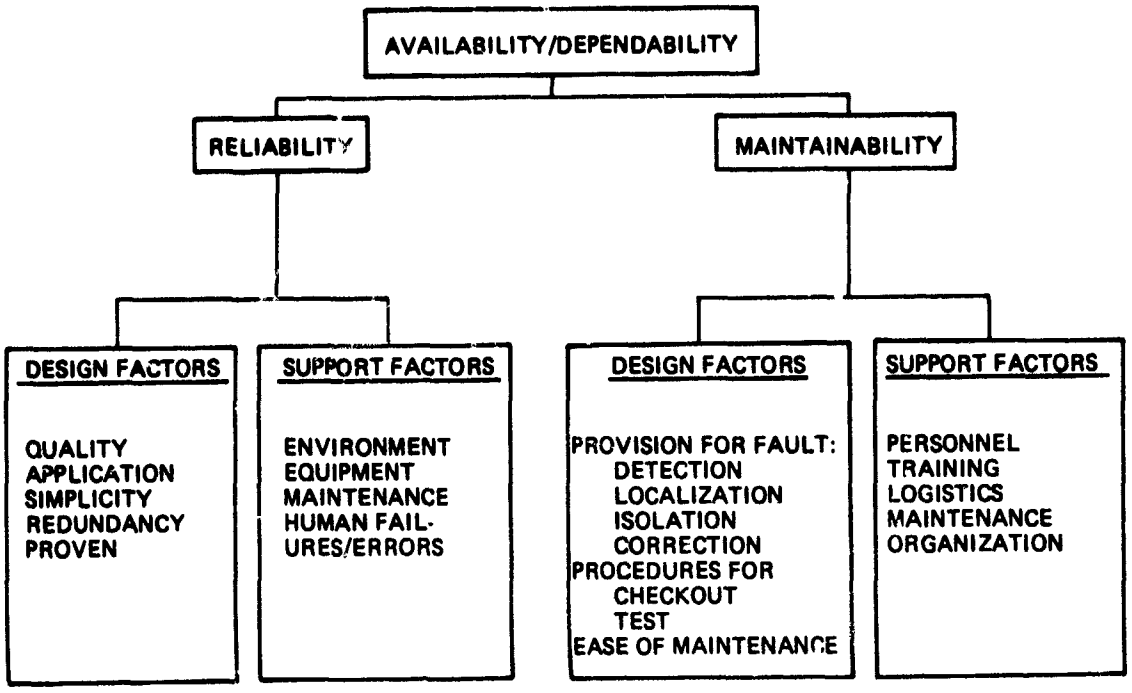


FIGURE 1-4. Reliability/Maintainability Relationships[7]

1-5.3 PREDICTION

Military specifications and contractual requirements incorporate maintenance time restrictions that must be met by the designer. Thus, predictions are needed to establish how close the equipment will be to these requirements during its development cycle and in its end-use phase. Similarly, a prediction of how long an item will be inoperative during maintenance is important to the user, because the user is deprived of the equipment contribution to his mission performance. This prediction must be quantitative and be capable of being updated as the item progresses through successive development phases. Two advantages of predicting maintainability are that:

(1) It identifies areas of poor maintainability which must be improved.

(2) An early assessment can be made of the adequacy of predicted downtime, quality and quantity of maintenance and support personnel, and tools and test equipment.

Most maintainability prediction methods use recorded reliability and maintainability experience obtained from comparable systems and components under similar conditions of use and operation. Thus, it is common to assume that the principle-of-transferability is applicable. Basically, this principle is that data from a system can be transferred and used to predict the maintainability of a comparable system that is in the design, development, or evaluation phase. Obviously, this approach depends upon establishing some commonality between systems. Usually this commonality can be inferred on a broad basis during the early design phase; but as the design is refined, the commonality must be established more exactly for equipment functions, maintenance task times, and levels of maintenance.

The data used in maintainability predictions depend on specific applications, but, in general, prediction methods use at least the following two parameters:

(1) Failure rates of components at the specific level of interest

(2) The amount of repair time required at each maintenance level.

Repair times are obtained from prior experience, simulation of repair tasks, or data from similar applications on other systems. Component failure rates, however, have been recorded by many sources as a function of use and environment. Some of these sources are listed in Refs. 13-17, and in Appendix B. Actual prediction techniques are covered in detail in Refs. 7, 10, 11, and 12.

1-5.4 DESIGN REVIEW

The design review process originally was established to achieve reliability objectives, but has since been extended to include all system characteristics throughout the life cycle (see Chap. 11). Maintainability specifications require that a formal design review program be established and documented for each development.

A design review involves four major tasks: (1) assembling data, (2) actual review, (3) documentation, and (4) followup. For maintainability, the first task (assembling data) includes engineering drawings; mock-ups, breadboard assemblies, or prototypes; maintainability prediction data; maintainability test data; and a description of the maintenance concept.

The review ought to be performed by people familiar with maintainability theory, maintenance processes, and human factors. The quantitative review techniques use prediction data to identify areas needing improvement, and the qualitative techniques use the experience and knowledge of the review board members, plus available reference material. The review ought to impartially analyze a design, isolate real or potential maintainability difficulties, propose solutions, and document the proceedings so that the designer can incorporate any needed changes. Thus, the designer benefits from the experience of other technical disciplines, and the equipment is improved. Design review meetings must be held at each stage during the equipment development to exercise control over the design, and to allow easier incorporation of changes. Further discussion of reviews is in Chapter 11.

1-5.5 AVAILABILITY

Maintainability trade-off techniques are used by designers to weigh the potential advantages of a maintainability design change against possible disadvantages. If mission requirements allow it, trade-offs can be made between maintainability and other parameters, such as reliability, or among the three categories of maintainability equipment—i.e., design, personnel, and support.

Availability is one of the important characteristics of equipment and systems. Generally speaking, *s*-availability is said to be the probability that, at any instant, an item is in proper condition to begin a mission (see the second definition of *s*-reliability in par. 1-1). There are many variations for an exact definition (see Ref. 10); they usually explicitly state what kinds of downtime are to be excluded or included in the calculation. Ref. 10 ought to be consulted for formal definitions of *s*-availability; for the purposes of this paragraph *s*-availability will be taken as

$$A = 1/[1 + (MTTR/MTBF)] \qquad (1\text{-}1)$$

where

A = availability calculated without considering downtime for scheduled or preventive maintenance, or logistic support. Ready time, supply downtime, waiting or administrative downtime, and preventive maintenance downtime are all excluded (see Ref. 10 for definitions).

$MTBF$ = Mean Time Between Failures, ignoring downtime.

$MTTR$ = Mean Time To Repair, viz., the average time required to detect and isolate a malfunction, make repairs, and restore the system to satisfactory performance (see the definition of A for other conditions).

s-Availability can be improved by reducing $MTTR$ and by increasing $MTBF$. Either $MTTR = 0$ or $MTBF \to \infty$ would provide perfect *s*-availability but, of course, neither is possible.

As examples, consider systems I and II with

$$MTTR_I = 0.1 \text{ hr}$$
$$MTBF_I = 2 \text{ hr}$$
$$MTTR_{II} = 10 \text{ hr}$$
$$MTBF_{II} = 200 \text{ hr}$$

Then the *s*-availability is

$$A_I = 1/[1 + (0.1/2)] = 0.952 \qquad (1\text{-}2a)$$
$$A_{II} = 1/[1 + (10/200)] = 0.952 \qquad (1\text{-}2b)$$

Both systems have the same *s*-availability, but they are not equally desirable. A 10-hr $MTTP$ might be too long for some systems whereas a 2-hr $MTBF$ might be too short for some systems.

Even though reliability and maintainability individually can be increased or decreased in combinations giving the same system availability, care must be taken to insure that reliability does not fall below its specified minimum, or that individually acceptable values of reliability and maintainability are not combined to produce an unacceptable level of system availability.

Other trade-off techniques involve:

(1) Increasing system availability by improving maintainability through trade-offs between design and support parameters, for example, by using sophisticated maintenance equipment to reduce maintainability requirements. This method, however, may increase overall program costs.

(2) Comparing costs versus availability for a basic system, a redundant system, a basic system plus sophisticated support equipment, etc., to determine which approach provides the highest availability for the least cost.

(3) Extending system-level techniques to subsystem or component levels and then working upward to the overall system level.

Refs. 7, 10, 11, and others at the end of this chapter provide additional discussions of trade-off techniques.

1-6 THE ROLE OF SAFETY

A safety program, one of the basic elements of the system engineering effort, has the following objectives:

(1) System design must include a level of safety consistent with mission requirements.

(2) Hazards associated with each system, subsystem, and equipment must be identified, evaluated, and eliminated or controlled to an acceptable level.

(3) Hazards that cannot be eliminated must be controlled to protect personnel, equipment, and property.

(4) Minimum risk levels must be determined and applied in the acceptance and use of new materials, and new production and testing techniques.

(5) Retrofit actions required to improve safety must be minimized by conservative design during the acquisition of a system.

(6) Historical safety data generated by similar system programs must be considered and used where appropriate (Ref. 18).

The purpose of safety analysis is to identify hazards and minimize or eliminate risks. Statistical and analytic techniques, however, are not a replacement for common sense. Sometimes, establishment of an acceptable risk level can result in unnecessary hazards when a change with a slight, acceptable increase in cost or decrease in effectiveness would eliminate the risk entirely. This reasoning is particularly pertinent when the event, even though its probability of occurrence is relatively low, might cause system failure.

1-6.1 RELATIONSHIPS TO RELIABILITY

Safety, like reliability and other system parameters, can be expressed as a probability, as, for example, the probability that no unsafe event will happen under specified operating conditions for a given time period. Thus, safety-analysis techniques closely parallel and, in some cases, actually use methods commonly associated with reliability. The Failure Mode and Effect Analysis (FMEA) and Cause-Consequence chart, for example, are reliability and safety tools. They are discussed in detail in Chapters 7 and 8. In general, safety is a specialized form of reliability study. This does not imply, however, that safety is a subordinate activity or derived discipline of reliability, but only that the activities of safety and reliability are closely related, both in concepts and in techniques. A system that is unreliable, for example, also may be unsafe, because system failures may cause injuries or loss of life of operators or users.

People are a more important part of safety than of reliability, because of possible injury to users or bystanders even when the mission is not imperiled. The human subsystem is discussed further in Chapter 6.

Just as a reliability/maintainability guideline requires that components that are difficult to maintain should be made more reliable, a reliability/safety guideline requires increased reliability of components that are unsafe to repair or replace. Some additional safety guidelines and techniques are discussed in the paragraphs that follow. Their relationships to reliability and to system engineering produce data that are useful to these other disciplines and, similarly, allow use of information generated by studies performed by other technical fields.

1-6.2 SYSTEM HAZARD ANALYSIS

As shown in Fig. 1-1, system lifetime is divided into five phases: (1) concept formulation, (2) contract definition, (3) engineering development, (4) production, and (5) operation. During the concept formulation phase, a preliminary hazard analysis identifies potential hazards associated with each design and must be reviewed and revised as the system progresses through subsequent phases. This analysis is qualitative and develops safety criteria for inclusion in the performance and design specifications formulated in Step 2 of the system engineering process (par. 1-2). The preliminary hazard analysis also must consider solutions to safety problems, outline inadequately defined conditions for additional study, and consider specific technical risks in the proposed design.

The subsystem hazard analysis is basically an expansion of the preliminary hazard analysis and usually occurs in the contract definition phase. Its purpose is to analyze the functional relationships between components of each subsystem and identify potential hazards due to component malfunctions or failures. Thus, the subsystem hazard analysis is similar to Step 3 of the system engineering process (par. 1-2) and, in fact, provides inputs to Step

3. An FMEA and Cause-Consequence chart, adapted to the safety viewpoint, are included to evaluate individual component failures and their influences on safety within each subsystem.

The contract definition phase also includes the system hazard analysis, which is basically an extension of the subsystem analysis in that the system hazard analysis treats safety integration and subsystem interfaces on an overall system basis. Trade-off and interaction studies during this phase must interlock with the system hazard analysis to obtain maximum system effectiveness and balanced apportionment among the various contributing disciplines (safety, reliability, etc.).

The operating hazard analysis encompasses safety requirements for personnel, procedures, and equipment in such functional areas as installation, maintenance, support, testing, storage, transportation, operation, training, and related activities. This study, like the previous ones, must be continued by reviews and revisions throughout the system life cycle, and involves having other disciplines (reliability, human factors, etc.) work with the safety engineers.

Thus, hazard analysis, through a comprehensive safety program, provides many useful inputs to the system engineering process and to other system parameters. These inputs—if effectively developed and intelligently used—can reduce overall program costs, contribute to economical scheduling, and make the task of interaction and trade-off studies much easier, since safety analysis techniques parallel or duplicate studies in reliability, maintainability, human factors, and other system disciplines.

1-6.3 TRADE-OFFS

Some trade-offs have been mentioned previously. The increase in reliability of parts that are relatively unsafe to repair or replace represents one such consideration. Trade-offs must be treated in the initial design phases, so that changes can be made early to preclude later problems in costs and scheduling or barely adequate fixes.

The selection of trade-off alternatives basically involves an analysis of all possible methods to improve safety, and a determination of the degree to which each method should be used. The analysis involves the investigation of safety hazards due to poor design, assembly errors, incorrect materials, improper test procedures, inadequate maintenance practices, careless handling during transportation, system malfunctions or failures that create unsafe conditions, and similar sources. Reliability and maintainability trade-offs, in conjunction with safety analysis, can reduce such hazards by use of standard components having proven reliability; ease of maintenance; and familiarity to operator/users, maintenance technicians, and production and test personnel. Similarly, reliability techniques such as redundancy, derating, and stress/strength analysis can be used to provide higher reliability and lower the probability of unsafe conditions. Safety/maintainability considerations, in addition to standardizing parts, can improve safety by reducing or eliminating hazards during maintenance through such methods as reducing weight and/or size to prevent personal strain or dropping hazards, eliminating sharp edges or projections, considering proximity of parts or subassemblies to dangerous items or conditions (high temperatures, moving machinery, etc.). One trade-off, which must be carefully evaluated for its effect on reliability or maintainability, is the use of remote control devices to isolate operators from safety hazards. These devices may, themselves, create reliability or maintainability difficulties, or may increase system engineering efforts unacceptably, or decrease system effectiveness through influences on reliability and/or maintainability. In almost all cases, remote control devices will increase system costs and development time. Remote control devices also will create their own unique problems of component, subassembly, or subsystem interfaces and interactions.

The references at the end of this chapter discuss in greater detail the design objectives, interactions, and trade-offs associated with safety. Safety terms, for example, are defined in Ref. 3, while Refs. 18 and 19 give military policies, guidelines, and objectives for system safety. Other approaches to safety are discussed in Refs. 20-25. Ref. 22

in particular treats the subject of safety/reliability relationships and trade-offs, and provides additional information on analytic methods, including FMEA and Fault Trees.

1-7 SUMMARY

Consideration of interactions and trade-offs must not be limited to the solution of problems that are easily identified or solved. Too often, a problem that is difficult to handle is simply ignored or treated with an expedient fix. Invariably, it is these fixes and ignored problems that reappear as major obstacles to schedule milestones and attainment of technical objectives, or contribute to cost overruns. Comprehensive trade-off and interaction studies must be made, therefore, in the initial design phases, so alternatives can be applied intelligently to preclude these downstream obstacles.

The heavy emphasis on trade-offs in this chapter does not mean that the designer is always faced with trade-off difficulties. In many situations, what is good for reliability is good for safety, maintainability, etc.; i.e., some things are just good all around.

As the gap between design drawings and actual hardware narrows in the engineering development phase, the importance of trade-offs, interactions, and thorough studies in each system discipline increases. Schedules and costs become critical restraints, and changes to the system must be made promptly and only when actually needed. Many programs have suffered schedule and cost overruns in production, for example, because effective studies either were not made, or were not used intelligently to identify and correct difficulties. An error invariably costs more to correct during production (or later) phases than it would if the same solution had been found and implemented during earlier phases. In some cases, tooling must be modified or even discarded and new tooling fabricated, parts must be scrapped or modified, engineering drawings must be changed, cost proposals must be prepared for changes, and new studies must be made to evaluate the impact and interactions created by these changes. These activities require the time and talents of the engineers and managers who otherwise could be concentrating on providing the Army with an effective system, rather than solving problems that should have been found and corrected earlier and with less effort. Thus, the importance of thorough, comprehensive trade-off and interaction studies cannot be overemphasized, although the cost for this extra effort must be provided for.

From the reliability viewpoint, the cost of designing to reduce the probability of an unwanted event is usually less than the subsequent cost to redesign and correct the resulting system problems. The loss created by the failure or malfunction, for example, must include system damage plus losses of time, mission objectives, and, perhaps, the lives of people associated with the correct functioning of the system. With this viewpoint, the reliability engineer must answer the following question: Does the initiation of a given corrective action sufficiently reduce the probability of an unwanted event to make the action worthwhile? This is a tough question to answer. Fortunately, the reliability engineer is aided in his decision by the other system engineering disciplines. The safety engineer, for example, can evaluate the risk to operators or other system personnel in the vicinity of the failure, and the human factors engineer can evaluate the responses of personnel to the failure to aid in predicting secondary accidents (injuries resulting from human reactions to the failure).

In designing for reliability, interactions and trade-offs should be applied to overall system objectives as they relate to future improvements in technology, expansions of system capabilities, and variations in predicted enemy actions and equipment. In other words, consideration should be given to designing some capacity into military systems to assimilate improvements throughout the life cycle. In the vehicle tire discussion of par. 1-3, for example, if technology did not permit fabrication of a tire capable of reliable operation in 90 mph, 110°F, and jagged surface environments, and if desired military objectives included these environments, then system design should plan for eventual development of such a tire. These plans would include increased braking capacity for the higher speeds, better suspensions for the jag-

ged surfaces, sturdier wheels and bearings, and other related aspects. Another approach to designing for the future involves the use of high reliability components in a system having components with relatively low reliability. The standard argument against this approach is that the low reliability components act as "weak links in the chain" and, thereby, negate the advantages of the high reliability items. If, however, these relatively unreliable parts subsequently are improved to higher reliabilities during the system lifetime, the overall system improvement cost is confined to replacing the low reliability items with their improved versions, rather than having a complete system overhaul or redesign to upgrade all components. The technique of designing for the future, however, must be evaluated carefully against actual needs. There are cases where such design measures are not appropriate. If the system lifetime is short compared with the anticipated development time of better components, planning for subsequent incorporation of these more reliable parts would not be practical. Similarly, if the system reliability is already at or above the actual requirement for its application, then a reliability "overkill" might be wasteful.

This chapter has presented the elements of system engineering and their relationships to one another and to reliability. The intent has been to provide an overall perspective of system engineering and the role of reliability in this system development process. Other disciplines such as quality assurance, value engineering, logistic engineering, manufacturing, and production engineering also contribute to system development, interact with reliability studies, and create their own unique tradeoffs with system parameters.

REFERENCES

1. MIL-STD-785, *Reliability Program for Systems and Equipment Development and Production.*
2. MIL-STD-499, *System Engineering Management.*
3. MIL-STD-721, *Definitions of Effectiveness Terms for Reliability, Maintainability, Human Factors, and Safety.*
4. AMCP 706-191, Engineering Design Handbook, *System Analysis and Cost-Effectiveness.*
5. AR 702-3, *Army Materiel Reliability, Availability and Maintainability (RAM).*
6. AMCP 11-6, *Program Evaluation and Review (PERT).*
7. C. D. Cox, Ed., *Maintainability Engineering Guide*, Report No. RC-S-65-2, U.S. Army Missile Command, Redstone Arsenal, Ala., April 1967.
8. AR 70-1, *Army Research, Development, and Acquisition.*
9. DA PAM 11-25, *Life Cycle Management Model for Army Systems.*
10. AMCP 706-134, Engineering Design Handbook, *Maintainability Guide for Design.*
11. E. J. Nucci, "Maintainability Design and Maintainability-Reliability-Maintenance Interrelations", *DoD Logistic Research Conference*, 1965.
12. MIL-HDBK-472, *Maintainability Prediction.*
13. *Bureau of Ships Reliability and Maintainability Training Handbook*, General Dynamics/Astronautics, San Diego, Calif., 1964.
14. NAVSHIPS 94501, *Bureau of Ships Reliability Design Handbook*, Federal Electric Corp., Paramus, N.J., 1968.
15. NAVWEPS 00-65-502, *Reliability Engineering Handbook*, 15 March 1968.
16. MIL-HDBK-217, *Reliability Stress and Failure Rate Data for Electronic Equipment.*
17. *Reliability and Maintainability Data-Source Guide*, U.S. Naval Applied Science Lab, N.Y., 1967.
18. MIL-STD-882, *System Safety Program for Systems and Associated Subsystems and Equipment.*
19. AR 385-16, *System Safety.*
20. A. J. Bonis, "Practical Aids on Reliability Safety Margins", Industrial Quality Control 21, 645-649 (June 1965).
21. A. Bulfinch, *Safety Margins and Ultimate Reliability*, Picatinny Arsenal, Dover, N.J., 1960.
22. R. F. Johnson, "System Safety-Implementation in the Reliability Program", *9th Annual West Coast Reliability Symposium*, 105-125 (1968). (Available

from Western Periodicals Co.; 13000 Raymer St.; North Hollywood, Calif.)

23. AFSC DH 1-6, *System Safety*, 2nd Ed., 20 January 1970.
24. *USAF-Industry System Safety Conference*, Directorate of Aerospace Safety, Norton AFB, Calif., 1969.
25. J. R. Jordan and R. L. Buchanan, "System Safety—A Quantitative Fallout from Reliability Analysis", 1967 Annals of Reliability and Maintainability 6, 653-660 (1967). (Available from SAE, 485 Lexington Ave., New York, N.Y. 10017.)
26. H. S. Balaban and D. L. Costello, *System Effectiveness: Concepts and Analytical Techniques*, No. 267-01-7-419, ARINC Research Corp., Washington, D.C., for Aeronautical Systems Div., USAF, January 1964.

CHAPTER 2 THE ENVIRONMENT

2-1 INTRODUCTION

A series of the Engineering Design Handbooks deals explicitly and in detail with environmental problems: Refs. 1, 10, 17, 18, and 19. This chapter gives a brief summary of some of the elements of the environment. Those Handbooks should be consulted for specific information.

Some miscellaneous aspects of environment vs reliability are covered in Refs. 11—16.

2-1.1 MILITARY OPERATIONS

Practically all military operations require information about the environment. In addition, the materiel and equipment used during these operations must provide satisfactory performance in the environment. Consequently, design and development engineers must be familiar with the reliability aspects of environmental influences and with methods used to prevent or reduce significant adverse effects due to the environment. Some generalization is possible for both the influences and the methods used to compensate for the effects, but the limits established for each must be reasonable. Unless design, test, and evaluation criteria are based upon a realistic model, the results will show only that the design operates satisfactorily within the artificial conditions of the environmental model. Whether designing equipment or devising environmental tests, there are two basic considerations:

(1) Decide which environmental factors are important because their effects might be adverse to military operations.

(2) Determine which of these conditions are most likely to occur.

Both considerations require knowledge of environmental elements and factors, but the first also involves a study of military activities and equipment that may be affected by the environment.

2-1.2 PREDICTING ENVIRONMENTAL CONDITIONS

Basically, there are two parts of the environmental problem:

(1) A consideration of the properties or characteristics of the environment.

(2) An analysis of the effects caused by the environment.

The first part leads to a division of the environment into three broad categories: (1) man-independent, (2) man-made, and (3) man-altered. Man-independent environment is an ambient condition and consists of climate, terrain, vegetation, and other elements existing at or near the surface of the earth. Man-made environment involves conditions such as radioactivity and shock waves from nuclear explosions, air pollution from fuel combustion, and interference from electromagnetic wave generation. Man-altered environment results from the interaction between man-independent conditions and man's activities; for example, increased ground and air temperatures caused by cities, erosion and decreased ground moisture levels due to removal of vegetation, and ecology modification by chemicals and pesticides. Since Categories 2 and 3 pertain to conditions caused by man, they usually are combined into one category called induced environment.

AMCP 706-115 (Ref. 1) divides environmental characteristics into elements and factors, which are defined as:

(1) Element: a broad and qualitative term such as climate, terrain, etc.

(2) Factor: a constituent of an element which can be measured quantitatively. Factors of the weather, for example, are temperature, wind, rain, etc.; factors of terrain are elevation, soil, soil moisture, etc.

Thus, there are three basic environmental elements: (1) climatic, (2) terrestrial, and (3) induced. Environmental factors associated with each of these three elements are shown

TABLE 2-1 MAJOR ENVIRONMENTAL FACTORS[1]

CLIMATIC	TERRESTRIAL	INDUCED
Temperature	Elevation	Shock
Solar Radiation	Surface Contour	Vibration
Atmospheric Pressure	Soil	Acceleration
Precipitation	Subsoil	Nuclear Radiation
Humidity	Surface Water	Electromagnetic Radiation
Ozone	Subsurface Water	Airborne Contaminants
Salt Spray	Vegetation	Acoustic Noise
Wind	Animals, Insects	Thermal Energy
Blowing Sand and Dust	Microbiological	Modified Ecology
Ice or Frost Formation		
Fog		

in Table 2-1 (adapted from Ref. 1). Specific combinations of individual factors and the frequency and intensity with which each factor occurs in the combination are associated with geographical environmental classifications such as arctic, desert, tropic, and temperate. The tropic, for example, has temperatures ranging from moderate to high, heavy rainfall and high humidity, dense vegetation, many animals and insects, many microbiological factors, and moderate to high levels of solar radiation. From a design standpoint, these factors are important. High ambient temperatures, for example, increase the operating temperatures in heat-sensitive equipment. Similarly, high humidity and microbiological factors encourage corrosion and fungus. Dense vegetation requires that protrusions, such as an antenna, either be mechanically protected or made sufficiently flexible to preclude breaking. If a piece of equipment, a jeep for example, must function in arctic and tropical environments, the design problems would include protection against freezing, etc., along with the protective measures included for tropic operation.

Inherent in the prediction of environmental conditions is the implication that frequency, duration, intensity, and interactions among factors also will be considered. For example, wind causes blowing sand and dust in the desert, salt spray on the ocean, and lower effective temperatures (due to the windchill factor) in the arctic. Conversely, the manner and rate of the reactions of the item to the effects of environmental factors may change with the intensity, duration, or frequency of the factors. An air filter on a jeep may function satisfactorily in a desert environment, even though above average amounts of dust and sand are present. But if this jeep were involved in a dust or sand storm, the increased intensity and duration of blowing sand and dust might cause the filter to become clogged and inoperative.

Environmental prediction methods require some numerical means of expressing intensities, frequencies, etc., hence, the effectiveness of the prediction will depend upon the quantification techniques and how they are applied to the relationships among contributing factors and between individual factors and their effects. Usually, environmental specialists deal with environmental factors in a form suitable for numerical measuring and recording, while military users commonly express environmental conditions in terms of geographical environmental features, or as combinations of factors.

Thus, the problem of designing, testing, and evaluating for environmental conditions becomes one of determining the most probable operating extremes and evaluating the

effects on the design within these extremes. To this end, several approaches have been developed, including an operational analysis (Ref. 2), a map-type presentation showing geographical (environmental) areas where environmental design limits would be exceeded for specific types of equipment (Ref. 3), and the use of computers to analyze data on environmental conditions.

2-2 EFFECTS OF THE ENVIRONMENT

2-2.1 GENERAL CATEGORIES

System failures due to environmental influences can be divided into two kinds of effects: (1) mechanical and (2) functional. Although both effects prevent the system from satisfactorily performing its intended mission, only mechanical effects represent an actual defect or failure of one or more components. The functional effects encompass system functions that have been altered adversely or impeded by environmental influences. The jeep filter mentioned in par. 2-1.2, for example, was clogged and rendered inoperative by sand and dust. The sand and dust environment caused the filter to fail and, therefore, is a mechanical effect. On the other hand, blowing sand and dust would have a functional effect on an optical rangefinder, since the visibility would be reduced and the otherwise functional rangefinder rendered unable to perform its intended function. Table 2-2 (Ref. 4) shows some principal effects and typical induced failures caused by environmental factors.

2-2.2 COMBINATIONS OF NATURAL ENVIRONMENTAL FACTORS

2-2.2.1 Evaluation of Environmental Characteristics

The characteristics of an environment are determined by which environmental factors are present and how these factors combine. Each of these two areas must be considered when evaluating environmental characteristics. The first one, which factors are present, is the easier to handle and usually involves listing of all pertinent environmental factors that may adversely affect the proposed design and the significant properties of each factor, such as amount, frequency, duration, and force; these data have been used for some time, and are reasonably available for many geographical areas. How environmental factors combine, however, is more difficult since one factor may cause another factor to occur (wind, for example, causing blowing sand or dust), or may intensify other factors (rain causing increased humidity), or may even decrease the effects of another factor (solar radiation causing a decrease or even elimination of fungous or microbiological effects). Thus, each factor and its associated properties must be compared with all other possible factors to identify and evaluate possible adverse combinations.

2-2.2.2 Combinations

Environmental conditions always occur as combinations of factors. For any given situation, there always will be such factors as pressure, temperature, and humidity, even though the values of each factor may be considered normal for the situation. Usually, specific environmental combinations are identified by the factors that deviate significantly from their normal values. Thus, the duration, frequency, and intensity with which each factor occurs are the important consideration, rather than the actual combination of factors, because these abnormal factors are usually the ones that cause poor reliability. For example, even though the humidity is zero, the humidity factor is still present, and the reliability difficulty for zero humidity is desiccation, as shown in Table 2-2. Of course, the situation could exist where zero humidity is desirable. In this case, even though zero humidity is not a difficulty, it still represents an important design consideration in the sense that devices to reduce the humidity may not be required.

In most combinations, extreme values of environmental factors occur individually, although, as pointed out in par. 2-2.2.1, the interrelationships between combined factors significantly can affect the expected values of individual factors. In some cases, however, because of their combining relationships, an extreme of one factor may intensify another

TABLE 2-2. ENVIRONMENTAL EFFECTS

FACTOR	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED (SEE NOTE 2)
High temperature	Thermal aging: Oxidation Structural change Chemical reaction Softening, melting, and sublimation Viscosity reduction, and evaporation Physical expansion	Insulation failure Alteration of electrical properties Structural failure Loss of lubricating properties Structural failure, increased mechanical stress, and increased wear on moving parts
Low temperature	Increased viscosity and solidification Ice formation Embrittlement Physical contraction	Loss of lubricating properties Alteration of electrical or mechanical functioning Loss of mechanical strength (see note 1), cracking, fracturing Structural failure, increased wear on moving parts
High relative humidity	Moisture absorption Chemical reaction: Corrosion Electrolysis	Swelling, rupture of container, physical breakdown, loss of electrical strength Loss of mechanical strength Interference with function, loss of electrical properties, increased conductivity of insulators
Low relative humidity	Dislocation: Embrittlement Granulation	Loss of mechanical strength Structural collapse Alteration of electrical properties, "dusting"
High pressure	Compression	Structural collapse Penetration of sealing Interference with function
Low pressure	Expansion Outgassing Reduced dielectric strength of air	Fracture of container, explosive expansion Alteration of electrical properties, loss of mechanical strength Insulation breakdown and arcing, corona and ozone formation
Solar radiation	Actinic and physicochemical reactions: Embrittlement	Surface deterioration, alteration of electrical properties Discoloration of materials, ozone formation
Sand and dust	Abrasion Clogging	Increased wear Interference with function, alteration of electrical properties

TABLE 2-2. ENVIRONMENTAL EFFECTS (cont'd)

FACTOR	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED (SEE NOTE 2)
Salt spray	Chemical reactions: Corrosion Electrolysis	Increased wear, loss of mechanical strength Alteration of electrical properties, interference with function Surface deterioration, structural weakening, increased conductivity
Wind	Force application Deposition of materials Heat loss (low velocity wind) Heat gain (high velocity wind)	Structural collapse, interference with function, loss of mechanical strength Mechanical interference and clogging, accelerated abrasion Accelerated low-temperature effects Accelerated high-temperature effects
Rain	Physical stress Water absorption and immersion Erosion Corrosion	Structural collapse Increase in weight, increased heat removal, electrical failure, structural weakening Removal of protective coatings, structural weakening, surface deterioration Enhanced chemical reactions
Blowing snow	Abrasion Clogging	Increased wear Interference with function
Temperature shock	Mechanical stress	Structural collapse or weakening, seal damage
High speed particles (nuclear irradiation)	Heating Transmutation and ionization	Thermal aging, oxidation Alteration of chemical, physical, and electrical properties; production of gases and secondary particles
Zero gravity	Mechanical stress Absence of convection cooling	Interruption of gravity-dependent functions Aggravation of high-temperature effects
Ozone	Chemical reactions: Crazing, cracking Embrittlement Granulation Reduced dielectric strength of air	Rapid oxidation Alteration of electrical or mechanical properties Loss of mechanical strength Interference with function Insulation breakdown and arcing
Explosive decompression	Severe mechanical stress	Rupture and cracking, structural collapse
Dissociated gases	Chemical reactions: Contamination Reduced dielectric strength	Alteration of physical and electrical properties Insulation breakdown and arcing
Acceleration	Mechanical stress	Structural collapse

TABLE 2-2. ENVIRONMENTAL EFFECTS (cont'd)

FACTOR	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED (SEE NOTE 2)
Vibration	Mechanical stress	Loss of mechanical strength, interference with function, increased wear
	Fatigue	Structural collapse
Magnetic fields	Induced magnetization	Interference with function, alteration of electrical properties, induced heating

1. This is not necessarily true for metals. Low temperature raises tensile strength and stiffness but reduces deformation and toughness for metals. Metals have many different failure mechanisms; a metallurgist ought to be consulted.
2. In general, the following terms may be applied to semiconductors and dielectrics:
   a. Alteration of electrical properties: increase or decrease of dielectric constant.
   b. Loss of electrical properties: decrease of dielectric constant to the extent that the material fails to serve its design function.
   c. Loss of electrical strength: breakdown of arc-resistance.

factor until it, too, may approach an extreme value. Heavy rainfall, for example, will cause the relative humidity to reach an extreme value. Similarly, solar radiation and temperature also may exist simultaneously as extreme values.

AR 70-38 (Ref. 5) discusses climatic environmental factors and their extremes from the viewpoint of military importance and relationship to research, development, test, and evaluation of materiel. Fig. 2-1 (Ref. 6) illustrates the environmental extremes and how they vary relative to latitude at the surface of the earth. Similarly, Fig. 2-2 (Ref. 6) shows the distribution of extremes at these latitudes for various altitudes above the surface of the earth. Both figures are very qualitative and do not represent actual values (no vertical scale is shown). Additionally, since the extremes do not occur all at the same time, these figures do not represent realistic combinations.

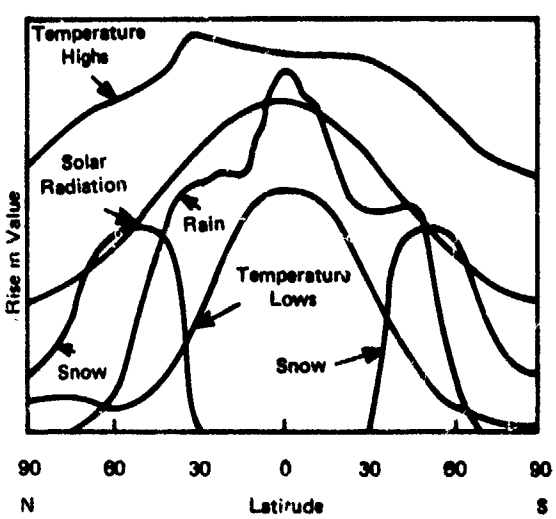


FIGURE 2-1. Latitudinal Distribution of Environmental Extremes[6]

Thus, it is necessary to consider environ-

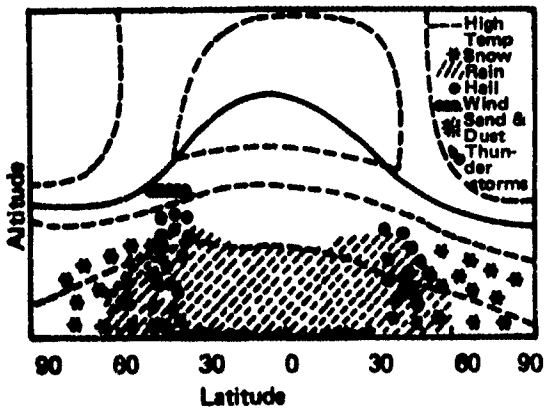


FIGURE 2-2. Semispatial Distribution of Environmental Extremes[6]

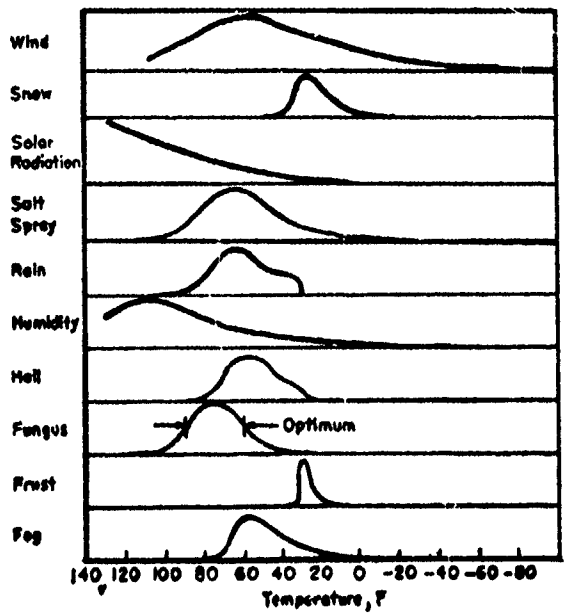


FIGURE 2-3. Comparison Between Temperature and Other Environmental Factors[6]

mental combinations of factors at values somewhat below their extremes. One method is to select the most significant environmental factor and establish its probable extreme value. Next, determine the second most significant factor and assign it the highest value that occurs naturally with the first factor. Then, the third most significant factor is identified, and its highest value occurring with the values of the first two factors is determined. This relative ranking system is continued in descending order of significance and values until the last pertinent factor has been considered. Obviously, this method can result in an extremely large number of possible combinations, since the number of combinations increases as the factorial of the number of factors involved. Ten factors, for example, provide 10! = 3,628,800 possible combinations. Thus, a more reasonable approach is needed. Since a possible combination may not be a practical combination from a reliability viewpoint, a study of practical combinations will be more useful.

2-2.2.3 Practical Combinations

A comparison of temperature with every other pertinent factor is a reasonable beginning in analyzing multiple combinations. One approach is to compare temperature to other factors graphically as shown in Fig. 2-3 (Ref. 6). Since Fig. 2-3 is intended only to illustrate a technique, no vertical scales are shown for the environmental factors, and hypothetical variations are indicated versus temperature (hot to the left, cold to the right). Depending upon the specific analytic requirements, wind, for example, could be expressed as speed in miles-per-hour, pressure in pounds per square inch, etc. Similarly, snow could be denoted as depth in inches, load bearing on a structure in pounds per square inch, etc. After completing the initial graphical analysis, a third factor can be included. For example, an evaluation could be made in which the occurrence of temperature, wind, and blowing snow is considered as a possible combination. Meteorological data for each factor then can be compared statistically with the values for the other factors, and probabilities determined and compared. Thus, the probability that "specific values (or ranges) for each factor occur with specific values (or ranges) of the other factors" will provide a weighting or relative ranking sequence for evaluating the selected combination. Since some combinations, although environmentally practical, will only occur in specific geographical areas, they can be eliminated from the analysis if the equipment will not be used in these areas. On the other hand, local environmental peculiarities must be con-

sidered carefully in any study, since they may create effects that otherwise would go undetected in a generalized analysis over a large area. Furthermore, many optimistic predictions of the future are wrong; "if the worst can happen, it will happen."

In addition to the graphical approach, environmental factors may be combined in pairs and analyzed by a chart similar to Table 2-3 (Ref. 7). The techniques involved in developing a chart are similar to those for the graphical method, and the same general comments apply to both approaches.

2-2-3 COMBINATIONS OF INDUCED ENVIRONMENTAL FACTORS

All environmental conditions are influenced to some extent by the presence of man or man's products. The basic act of breathing, for example, consumes oxygen and releases carbon dioxide and water vapor into the atmosphere. While the breathing of one man in the middle of a forest will not cause a noticeable change in the concentrations of oxygen, water vapor, or carbon dioxide, the change is extremely important in the closed atmosphere of a spacecraft life-support system. Similarly, the motion of a hydraulic piston causes shock and vibration, and the piston operating pressure and friction create heat. If the piston intake stroke allows moisture to enter the cylinder, the moisture may cause corrosion which, in turn, could lead to increased friction, greater wear, and additional heat. Any contaminants, such as sand or dust, that enter the cylinder with the moisture will also contribute to increased friction, wear, and heat. Even the color of paint used on equipment can affect reliability, since optically light colors such as white or silver also reflect significant amounts of infrared, while optically dark colors such as black or olive-drab will cause higher internal temperatures by absorbing infrared. These examples illustrate that induced environmental factors, either singly or in combination, represent the major environmental problems from a reliability viewpoint.

2-2.4 ENVIRONMENTAL ANALYSIS

After establishing the desired equipment parameters and roughing out the initial design, the designer ought to analyze the probable operating environment. The results can then be applied to system components to determine the environments experienced by individual components and how these individual environments will affect component operation and reliability. Thus, individual part specifications can be selected to compensate for environmental influences, rather than having to add environmental compensating methods after the design has progressed to more advanced stages. The environmental analysis must consider all phases of the mission profile, i.e., the equipment stockpile-to-target sequence. Some of the distinct phases that must be evaluated are transportation, handling, storage, standby-idle time, standby-active time, use or operational time, and maintenance. Each phase creates its own peculiar influences on equipment reliability. The circulation of air during operation, for example, may prevent the accumulation of moisture or dust, while the same item in storage may not have this circulation and may corrode or grow fungus. Table 2-4 (adapted from Ref 6) shows some effects of natural and induced environments during the various phases of the lifetime of an item. Table 2-5 (adapted from Ref. 6) provides reliability considerations for pairs of environmental factors. Ref. 7 gives more information on combinations of environments.

2-3 DESIGNING FOR THE ENVIRONMENT

Equipment failures have three convenient classifications:

(1) Poor design or incorrect choice of materials or components

(2) Inadequate quality control which permits deviations from design specifications

(3) Deterioration caused by environmental effects or influences.

The perceptive reader, at this point, will have observed that the first and third classes are related. Specifically, the careful selection of design and materials can extend item reliability by reducing or eliminating adverse environmental effects. Needless to say, this is not a profound thought, but merely one that is

TABLE 2-3. ANALYSIS OF PAIRED ENVIRONMENTAL FACTORS[7]

1 Combine to intensify mechanical deterioration.

2 Combine to intensify operational deterioration.

3 Both 1 and 2 apply:

4 Interdependent, or one element requires the other.

5 One element influences the intensity of the other.

6 Coexist with no important combined intensification.

W Weakened effect (Effects of combination are less than sum of effects of individual elements.)

X Incompatible

(Blank) Combination not considered.

A minus sign following the number expresses weak or doubtful intensification.

		Clouds	Fog	Frost	Fungus	Geomagnetism	Hail	Humidity	Lightning	Pollution, Air	Rain	Rain, Freezing	Salt Spray	Sand and Dust	Sleet	Snow	Solar Radiation	Temperature, High	Temperature, Low	Wind	Gravity, Low	Ionized Gases	Meteoroids	Pressure, Low	Radiation, Cosmic	Radiation, Electromag.	Radiation, Van Allen	Acceleration	Explosion	Icing	Radiation, Electromag.	Radiation, Nuclear	Shock	Temperature, High	Temperature, Low	Turbulence	Vibration, Acoustic	Vibration, Mechanical
Man-independent	Earth's Surface & Troposphere	Clouds																																				
		Fog	W																																			
		Frost	W																																			
		Fungus																																				
		Geomagnetism																																				
		Hail	3	X																																		
		Humidity	4	4	4	4		5																														
		Lightning	4	X			2-	3	5																													
		Pollution, Air	5-	1					1																													
		Rain	4	2	X	4		3	4	5	5																											
		Rain, Freezing	4						4																													
		Salt Spray		1-	W				W			W	W																									
		Sand and Dust		1-					1-		1-			1-																								
		Sleet	4					X	4	X		2	2																									
		Snow	4						4	X		2-																										
		Solar Radiation	5	W	W	W			1-			X		1	1-																							
		Temperature, High	W	W	X	4			1				X	1	W	X	X	1																				
		Temperature, Low			4	W			1				4	W	1	4	4	W	X																			
		Wind	2-	W	W			3		3	5	3		1	3	3	3	1	1-	3																		
Hyper & Space		Gravity, Low																6	6	6																		
		Ionized Gases				W												1	1	W		6																
		Meteoroids																																				
		Pressure, Low					2-		1									1-	1	1	W	5	5															
		Radiation, Cosmic					5											5					1-		3-													
		Radiation, Electromag					5																1-		3-													
		Radiation, Van Allen					4											4				6			3-	5												
		Acceleration																		1					2-													
Induced		Explosion							1-																1-													
		Icing	5	3-					4			1-	3	W				W	X	4	2-																	
		Radiation, Electromag					2-																2-		2-													
		Radiation, Nuclear																1-	1-				1		3-													
		Shock																		1					1-													
		Temperature, High																		X										X	3-		1					
		Temperature, Low																	X						3-							1-	1	X				
		Turbulence	2-	X				3		3		2							5		3									3								
		Vibration, Acoustic																							1-							W		1	1-			
		Vibration, Mechanical							1-					1-	1-			1	1	1					1				1			W		1	1	1	1	

Earth's Surface and Troposphere — Hyper & Space — Man-independent — Induced

TABLE 2-4. ENVIRONMENTAL ANALYSIS[6]

	MISSION REGIME	STORAGE	TRANSPORTATION	STAND-BY (IDLE)	STAND-BY (ACTIVE)	USE	MAINTENANCE
MAN-INDEPENDENT ENVIRONMENTS	Albedo					O	
	Aridity	X					
	Asteroids						
	Birds	O				⊠	⊠
	Clouds				O	O	
	Cosmic Radiation					X	
	Density, Air					O	
	Dust, Interplanetary						
	Dust, Lunar						
	Dust, Terrestrial	⊠	X	X	O		⊠
	Electricity, Atmospheric					⊠	
	Fog	X		X	O		O
	Frost	X		X	O		X
	Fungi	X					X
	Geomagnetism					O	
	Gravity					O	
	Hail	X	X	X	⊠	⊠	X
	Humidity	X	X	X	⊠	⊠	X
	Icing	X	X	⊠	⊠	⊠	⊠
	Ionized Gases					⊠	
	Insects	⊠	⊠	⊠	⊠	⊠	⊠
	Lightning	X	X	X	⊠	⊠	⊠
	Meteoroids						
	Ozone					X	
	Pollution, Air	X	X	X			⊠
	Pressure, Air				O	⊠	O
	Rain	X	X	X	⊠	⊠	⊠
	Salt Atmosphere	X	X	⊠	⊠		⊠
	Snow and Sleet	X	X	⊠	⊠	⊠	⊠
	Solar Flares						
	Solar Radiation	X					X
	Temperature	X	X	X	O	O	⊠
	Temperature Shock		X		X	X	X
	Terrain		X				⊠
	Trapped Radiation (Van Allen)						
	Turbulence				⊠	⊠	⊠
	Wind, Gusts, Shear	X	X	X	⊠	⊠	⊠
INDUCED ENVIRONMENTS	Acceleration				⊠	⊠	
	Acoustic Vibration			⊠	⊠	⊠	
	Countermeasures					⊠	
	Enemy Action	X	X	X	⊠	⊠	
	Explosive Atmosphere						
	Flutter					⊠	
	Ionized Gases					X	
	Magnetic Fields				O	O	O
	Moisture	X			⊠	⊠	⊠
	Nuclear Radiation				X	⊠	⊠
	Pressure					⊠	
	Shock		X		X	⊠	X
	Temperature			⊠	⊠	⊠	
	Temperature Shock			⊠	⊠	⊠	
	Vibration		X		X	X	X

EFFECTS:

O = Operational — Operational effect: Function, mission, etc., influenced, rather than direct physical alteration of item. Example: Reduced visibility caused by fog.

X = Mechanical/Physical — Mechanical/Physical effect: Direct physical alteration of item. Examples: Corrosion, fracture, puncture, melting.

⊠ = Either or both

TABLE 2-5. VARIOUS ENVIRONMENTAL PAIRS[6]

High Temperature and Humidity High Temperature tends to increase the rate of moisture penetration. The general deterioration effects of humidity are increased by high temperatures.	*High Temperature and Low Pressure* Each of these environments depends on the other. For example, as pressure decreases, outgassing of constituents of materials increases; and as temperature increases, the rate of outgassing increases. Hence, each tends to intensify the effects of the other.	*High Temperature and Salt Spray* High temperature tends to increase the rate of corrosion caused by salt spray.
High Temperature and Solar Radiation This is a man-independent combination that causes increasing effects on organic materials.	*High Temperature and Fungus* A certain degree of high temperature is necessary to permit fungus and microorganisms to grow. But, above 160°F (71°C) fungus and microorganisms cannot develop.	*High Temperature and Sand and Dust* The erosion rate of sand may be accelerated by high temperature. However, high temperatures reduce sand and dust penetration.
High Temperature and Shock and Vibration Since both of these environments affect common material properties, they will intensify each other's effects. The amount that the effects are intensified depends on the magnitude of each environment in the combination. Plastics and polymers are more susceptible to this combination than metals, unless extremely high temperatures are involved.	*High Temperature and Acceleration* This combination produces the same effect as high temperature and shock and vibration.	*High Temperature and Explosive Atmosphere* Temperature has very little effect on the ignition of an explosive atmosphere, but it does effect the air-vapor ratio which is an important consideration.
Low Temperature and Humidity Humidity decreases with temperature; but low temperature induces moisture condensation, and, if the temperature is low enough, frost or ice.	*High Temperature and Ozone* Starting at about 300°F (150°C), temperature starts to reduce ozone. Above about 520°F (270°C) ozone cannot exist at pressures normally encountered.	
Low Temperature and Solar Radiation Low temperature tends to reduce the effects of solar radiation, and vice versa.	*Low Temperature and Low Pressure* This combination can accelerate leakage through seals, etc.	*Low Temperature and Salt Spray* Low temperature reduces the corrosion rate of salt spray.
	Low Temperature and Sand and Dust Low temperature increases dust penetration.	*Low Temperature and Fungus* Low temperature reduces fungus growth. At sub-zero temperatures, fungi remain in suspended animation.

TABLE 2-5. VARIOUS ENVIRONMENTAL PAIRS[6] (cont'd)

Low Temperature and Shock and Vibration Low temperature tends to intensify the effects of shock and vibration. It is however, a consideration only at very low temperatures.	*Low Temperature and Acceleration* This combination produces the same effect as low temperature and shock and vibration.	*Low Temperature and Explosive Atmosphere* Temperature has very little effect on the ignition of an explosive atmosphere. It does however, affect the air-vapor ratio which is an important consideration.
Low Temperature and Ozone Ozone effects are reduced at lower temperatures, but ozone concentration increases with lower temperatures.	*Humidity and Low Pressure* Humidity increases the effects of low pressure, particularly in relation to electronic or electrical equipment. However, the actual effectiveness of this combination is determined largely by the temperature.	*Humidity and Salt Spray* High humidity may dilute the salt concentration, but it has no bearing on the corrosive action of the salt.
Humidity and Fungus Humidity helps the growth of fungus and microorganisms but adds nothing to their effects.	*Humidity and Sand and Dust* Sand and dust have a natural affinity for water and this combination increases deterioration.	*Humidity and Solar Radiation* Humidity intensifies the deteriorating effects of solar radiation on organic materials.
Humidity and Vibration This combination tends to increase the rate of breakdown of electrical material.	*Humidity and Shock and Acceleration* The periods of shock and acceleration are considered too short for these environments to be affected by humidity.	*Humidity and Explosive Atmosphere* Humidity has no effect on the ignition of an explosive atmosphere, but a high humidity will reduce the pressure of an explosion.
Humidity and Ozone Ozone reacts with moisture to form hydrogen peroxide, which has a greater deteriorating effect on plastics and elastomers than the additive effects of moisture and ozone.	*Low Pressure and Salt Spray* This combination is not expected to occur.	*Low Pressure and Solar Radiation* This combination adds nothing to the overall effects.
	Low Pressure and Fungus This combination adds nothing to the overall effects.	
Low Pressure and Sand and Dust This combination only occurs in extreme storms during which small dust particles are carried to high altitudes.	*Low Pressure and Vibration* This combination intensifies effects in all equipment categories, but mostly with electronic and electrical equipment.	*Low Pressure and Shock or Acceleration* These combinations only become important at the hyperenvironmental levels, in combination with high temperature.

TABLE 2-5. VARIOUS ENVIRONMENTAL PAIRS[6] (cont'd)

Low Pressure and Explosive Atmosphere At low pressures, an electrical discharge is easier to develop, but the explosive atmosphere is harder to ignite.	***Salt Spray and Fungus*** This is considered an incompatible combination.	***Salt Spray and Sand and Dust*** This will have the same combined effect as humidity and sand and dust.
Salt Spray and Vibration This will have the same combined effect as humidity and vibration.	***Salt Spray and Shock or Acceleration*** These combinations will produce no added effects.	***Salt Spray and Explosive Atmosphere*** This is considered an incompatible combination.
Salt Spray and Ozone These environments have the same combined effect as humidity and ozone.	***Solar Radiation and Fungus*** Because of the resulting heat from solar radiation, this combination probably produces the same combined effect as high temperature and fungus. Further, the ultraviolet in unfiltered radiation is an effective fungicide.	***Solar Radiation and Sand and Dust*** It is suspected that this combination will produce high temperatures.
Solar Radiation and Ozone This combination increases the rate of oxidation of materials.	***Fungus and Ozone*** Fungus is destroyed by ozone.	***Solar Radiation and Shock or Acceleration*** These combinations produce no additional effects.
Solar Radiation and Vibration Under vibration conditions, solar radiation deteriorates plastics, elastomers, oils, etc.; at a higher rate.		***Sand and Dust and Vibration*** Vibration might possibly increase the wearing effects of sand and dust.
Shock and Vibration This combination produces no added effect.	***Vibration and Acceleration*** This combination produces increased effects when encountered with high temperatures and low pressures in the hyperenvironmental ranges.	
Solar Radiation and Explosive Atmosphere This combination produces no added effects.		

sometimes forgotten or perhaps relegated to mental footnotes. The environment is neither forgiving nor understanding; it methodically surrounds and attacks every component of a system, and when a weak point exists, the equipment reliability suffers. Design and reliability engineers, therefore, must understand the environment and its potential effects, and then must select designs or materials that counteract these effects or must provide methods to alter or control the environment within acceptable limits. Selecting designs or materials that withstand the environment has the advantage of not requiring extra components that also require environmental protection and add weight and costs.

In addition to the obvious environments of temperature, humidity, shock, and vibration, the design engineer will create environments by his choice of designs and materials. A gasket or seal, for example, under elevated temperatures or reduced pressures may release corrosive or degrading volatiles into the system. Teflon may release fluorine, and polyvinylchloride (PVC) may release chlorine. Certain solid rocket fuels are degraded into a jelly-like mass when exposed to aldehydes or ammonia, either of which can come from a phenolic nozzle cone. These examples illustrate that internal environments designed into the system can seriously affect reliability.

Many aids are available to design and reliability engineers in selecting materials and components, e.g., the text, *Deterioration of Materials, Causes and Preventive Techniques*, by Glenn A. Greathouse and Carl J. Wessel (Ref. 8). In addition, military specifications, standards, and handbooks provide both general and specific guidance on this subject. Appendix B lists data banks that consolidate and evaluate materials and components from the reliability viewpoint.

2-3.1 TEMPERATURE PROTECTION

Heat and cold are powerful agents of chemical and physical deterioration for two very simple, basic reasons:

(1) The physical properties of almost all known materials are modified greatly by changes in temperature.

(2) The rate of almost all chemical reactions is influenced markedly by the temperature of the reactants. A familiar rule-of-thumb for chemical reactions is that the rate of many reactions doubles for every rise in temperature of 10 deg C (Ref. 8); this is equivalent to an activation energy of about 0.6 eV.

Basically, heat is transferred by three methods: (1) radiation, (2) conduction, and (3) convection. One, or a combination of these three methods, therefore, is used to protect against temperature degradation. High temperature degradation can be minimized by passive or active techniques. Passive techniques use natural heat sinks to remove heat, while active techniques use devices such as heat pumps or refrigeration units to create heat sinks. Such design measures as compartmentation, insulation of compartment walls, and intercompartment and intrawall air flow can be applied independently or in combination. Every system component should be studied from two viewpoints:

(1) Is a substitute available that will generate less heat?

(2) Can the component be located and positioned so that its heat has minimum effect on other components?

For a steady temperature, heat must be removed at the same rate at which it is generated. Thermal systems such as conduction cooling, forced convection, blowers, direct or indirect liquid cooling, direct vaporization or evaporation cooling, and radiation cooling must be capable of handling both natural and induced heat sources. Fig. 2-4 compares the effectiveness of several such methods.

Passive sinks require some means of progressive heat transfer from intermediate sinks to ultimate sinks until the desired heat extraction has been achieved. Thus, when heat sources have been identified, and heat removal elements selected, they must be integrated into an overall heat removal system, so that heat is not merely redistributed within the system. Efficiently integrated heat removal techniques can significantly improve item reliability.

Besides the out-gassing of corrosive volatiles when subjected to heat, almost all known

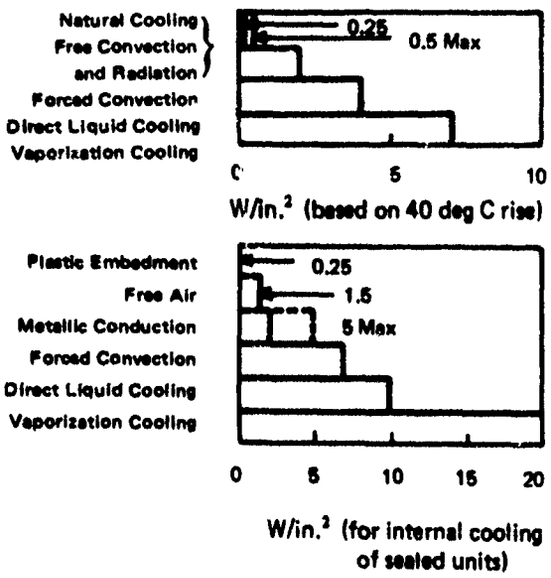


FIGURE 2-4. Comparison of Heat Removal Methods[6]

materials will expand or contract when their temperature is changed. This expansion and contraction causes problems with fit between parts, sealing, and internal stresses. Local stress concentrations due to nonuniform temperature are especially damaging, because they can be so high. A familiar example is a hot water-glass that shatters when immersed in cold water. Metal structures, when subjected to cyclic heating and cooling, may ultimately collapse due to the induced stresses and fatigue caused by flexing. The thermocouple effect between the juncture of two dissimilar metals causes an electric current that may induce electrolytic corrosion. Plastics, natural fibers, leather, and both natural and synthetic rubber are all particularly sensitive to temperature extremes as evidenced by their brittleness at low temperatures and high degradation rates at high temperatures. Table 2-6 summarizes some of the basic precautions for reliability at low temperatures. An always present danger is that in compensating for one failure mode, the change will aggravate another failure mode.

2-3.2 SHOCK AND VIBRATION PROTECTION

Basic structural design techniques, such as proper component location and selection of suitable materials, can aid in protecting an item against failure caused by severe environmental stresses from shock or vibration. One factor, however, which is not often considered, is that the vibration of two adjacent components or separately insulated subsystems can cause a collision between them if maximum excursions and sympathetically induced vibrations are not evaluated by the designer. Another failure mode, fatigue (the tendency for a metal to break under cyclic stressing loads considerably below its tensile strength) is an area of reliability concern due to shock or vibration. This includes low cycle fatigue, acoustic fatigue, and fatigue under combined stresses. The interaction between multiaxial fatigue and other environmental factors such as temperature extremes, temperature fluctuations, and corrosion requires careful study. Stress-strength analysis of components and parameter variation analysis are particularly suited to these effects. Destructive testing methods are also very useful in this area. For one-shot devices, several efficient nondestructive evaluation (NDE) methods are available—such as X ray, neutron radiography, and dye-penetrant—which can be used to locate fatigue cracks. Developing a simple design that is reliable is much better than elaborate fixes and subsequent testing to redesign for reliability.

In addition to using proper materials and configuration, the shock and vibration experienced by the equipment ought to be controlled. In some cases, however, even though an item is properly insulated and isolated against shock and vibration damage, repetitive forces may loosen the fastening devices. Obviously, if the fastening devices loosen enough to permit additional movement, the device will be subjected to increased forces and may fail. Many specialized self-locking fasteners are commercially available, and fastener manufacturers usually will provide valuable assistance in selecting the best fastening methods.

An isolation system can be used at the source of the shock or vibration, in addition to isolating the protected component. The best results are obtained by using both methods. Damping devices are used to reduce peak oscillations, and special stabilizers

TABLE 2-6. LOW TEMPERATURE PROTECTION METHODS[6]

EFFECT	PREVENTIVE MEASURES
Differential contraction	Careful selection of materials Provision of proper clearance between moving parts Use of spring tensioners and deeper pulleys for control cables Use of heavier material for skins.
Lubrication stiffening	Proper choice of lubricants: Use greases compounded from silicones, diesters or silicone-diesters thickened with lithium stearate Eliminate liquid lubricants wherever possible.
Leaks in hydraulic systems	Use of low-temperature sealing and packing compounds, such as silicone rubbers.
Stiffening of hydraulic systems	Use of proper low-temperature hydraulic fluids.
Ice damage caused by freezing of collected water	Elimination of moisture by: Provision of vents Ample draining facilities Eliminating moisture pockets Suitable heating Sealing Desiccation of air.
Degradation of material properties and component reliability	Careful selection of materials and components with satisfactory low-temperature capabilities.

employed when unstable configurations are involved. Typical examples of dampeners are viscous hysteresis, friction, and air damping. Vibration isolators commonly are identified by their construction and material used for the resilient element (rubber, coil spring, woven metal mesh, etc.). Shock isolators differ from vibration isolators in that shock requires stiffer springs and a higher natural frequency for the resilient element. Some of the types of isolation mounting systems are underneath, over-and-under, and inclined isolators.

A specific component may initially appear to be sufficiently durable to withstand the anticipated shock or vibration forces without requiring isolation or insulation. However, this observation can be misleading since the attitude in which a part is mounted, its location relative to other parts, its position within the system, and the possibility of its fasteners or another component fasteners coming loose can alter significantly the imposed forces. Another component, for example, could come loose and strike it or alter the forces acting on it to the extent that failure results.

The following basic considerations must be included in designing for shock and vibration:

(1) The location of the component relative to the supporting structure (i.e., at the edge, corner, or center of the supporting structure)

(2) The orientation of the part with respect to the anticipated direction of the shock or vibration forces

(3) The method used to mount the part.

2-3.3 MOISTURE PROTECTION

Moisture is a chemical and, considering its abundance and availability in almost all environments, is probably the most important chemical deteriorative factor of all. Moisture is not simply H_2O, but usually is a solution of many impurities; these impurities cause many of the chemical difficulties. In addition to its chemical effects, such as the corrosion of many metals, condensed moisture also acts as a physical agent. An example of the physical effects of moisture is the damage done in the locking together of mating parts when moisture condenses on them and then freezes. Similarly, many materials that are normally pliable at low temperatures will become hard and perhaps brittle if moisture has been absorbed and subsequently freezes. Condensed moisture acts as a medium for the interaction between many, otherwise relatively inert, materials. Most gases readily dissolve in moisture. The chlorine released by PVC plastic, for example, forms hydrochloric acid when combined with moisture.

Although the presence of moisture may cause deterioration, the absence of moisture also may cause reliability problems. The useful properties of many nonmetallic materials, for example, depend upon an optimum level of moisture. Leather and paper become brittle and crack when they are very dry. Similarly, fabrics wear out at an increasing rate as moisture levels are lowered and fibers become dry and brittle. Dusting is encountered in dry environments and can cause increased wear, friction, and clogged filters.

Moisture, in conjunction with other environmental factors, creates difficulties that may not be characteristic of the factors acting alone. For example, abrasive dust and grit, which would otherwise escape, are trapped by moisture. The permeability (to water vapor) of some plastics (PVC, polystyrene, polyethylene, etc.) is related directly to their temperature. The growth of fungus is enhanced by moisture, as is the galvanic corrosion between dissimilar metals.

Some design techniques that can be used singly or combined to counteract the effects of moisture are: elimination of moisture traps by providing drainage or air circulation; using desiccant devices to remove moisture when air circulation or drainage is not possible; applying protective coatings; providing rounded edges to allow uniform coating of protective material; using materials resistant to moisture effects, fungus, corrosion, etc.; hermetically sealing components; gaskets and other sealing devices; impregnating or encapsulating materials with moisture resistant waxes, plastics, or varnishes; and separation of dissimilar metals, or materials that might combine or react in the presence of moisture, or of components that might damage protective coatings. The designer also must consider possible adverse effects caused by specific methods of protection. Hermetic sealing, gaskets, protective coatings, etc., may, for example, aggravate moisture difficulties by sealing moisture inside or contributing to condensation. The gasket materials must be evaluated carefully for out-gassing of corrosive volatiles or for incompatibility with adjoining surfaces or protective coatings.

2-3.4 SAND AND DUST PROTECTION

In addition to the obvious effect of reduced visibility, sand and dust primarily degrade equipment by:

(1) Abrasion leading to increased wear

(2) Friction causing both increased wear and heat

(3) Clogging of filters, small apertures, and delicate equipment.

Thus, equipment having moving parts requires particular care when designing for sand and dust protection. Sand and dust will abrade optical surfaces, either by impact when being carried by air, or by physical abrasion when the surfaces are improperly wiped during cleaning. Dust accumulations have an affinity for moisture and, when combined, may lead to corrosion or the growth of fungus

In the relatively dry regions, such as deserts, fine particles of dust and sand readily are agitated into suspension in the air, where they may persist for many hours, sometimes reaching heights of several thousand feet. Thus, even though there is virtually no wind present, the speeds of vehicles or vehicle-transported equipment through these dust clouds can cause surface abrasion by impact, in addition to the other adverse effects of the sand or dust.

Although dust commonly is considered to be fine, dry particles of earth, it also may include minute particles of metals, combustion products, solid chemical contaminants, etc. These other forms may provide direct corrosion or fungicidal effects on equipment, since this dust may be alkaline, acidic, or microbiological.

Since most equipment requires air circulation for cooling, removing moisture, or simply functioning, the question is not whether to allow dust to enter, but, rather, how much or what size dust can be tolerated. The problem becomes one of filtering the air to remove dust particles above a specific nominal size. The nature of filters, however, is such that for a given working filter area, as the ability of the filter to stop increasingly smaller dust particles is increased, the flow of air or other fluid through the filter is decreased. Therefore, the filter surface area either must be increased, the flow of fluid through the filter decreased, or the allowable particle size increased; i.e., invariably, there must be a compromise. Interestingly enough, a study by R. V. Pavia (Ref. 9) showed that, for aircraft engines, the amount of wear was proportional to the weight of ingested dust, but that the wear produced by 100-μm dust was approximately half that caused by 15-μm dust. The 15-μm dust was the most destructive of all sizes tried.

Sand and dust protection, therefore, must be planned in conjunction with protective measures against other environmental factors. It is not practical, for example, to specify a protective coating against moisture if sand and dust will be present, unless the coating is carefully chosen to resist abrasion and erosion or is self-healing.

2-3.5 EXPLOSION PROOFING

Protection against explosion is both a safety and reliability problem. An item that randomly exhibits explosive tendencies is one that has undesirable design characteristics and spectacular failure modes. This type of functional termination, therefore, requires extreme care in design and reliability analyses.

Explosion protection planning must be directed to three categories (not necessarily mutually exclusive) of equipment:

(1) Items containing materials susceptible to explosion

(2) Components located near enough to cause the explosive items to explode

(3) Equipment that might be damaged or rendered temporarily inoperative by overpressure, flying debris, or heat from an explosion.

The first category includes devices containing flammable gases or liquids, suspensions of dust in the air, hypergolic materials, compounds which spontaneously decompose in certain environments, equipment containing or subjected to high or low extremes of pressure (includes implosions), or any other systems capable of creating an explosive reaction. The second category is fairly obvious and includes many variations on methods for providing an energy pulse, a catalyst, or a specific condition that might trigger an explosion. A nonexplosive component, for example, could create a corrosive atmosphere, mechanical puncture, or frictional wear on the side of a vessel containing high-pressure air and thereby cause the air container to explode. The third category encompasses practically everything, including items in the first two categories, since a potentially explosive device (such as a high-pressure air tank) can be damaged or made to explode by the overpressure, etc. from another explosion. Thus, some reasoning must be applied when considering devices not defined by the first two categories. From a practical standpoint, explosion protection for items in the third category ought to be directed to equipment that might possibly be near explosions. The sides of a maintenance van, for example, will be subjected to overpressures from exploding

enemy artillery rounds. If designed for protection against anything but a direct hit, the van would be extremely difficult to transport. Thus, mobility (and size) and protections against blast are traded off. On the other end of the compromise scale, however, is the bad effect on the reliability of internal equipment when explosion protection is minimal or nonexistent.

The possibility of an explosive atmosphere leaking or circulating into other equipment compartments must be recognized. Lead-acid batteries, for example, create hydrogen gas that, if confined or leaked into a small enclosure, could be exploded by electrical arcing from motor brushes, by sparks from metallic impacts, or by exhaust gases. Explosive environments, such as dust-laden air, might be circulated by air distribution systems.

Explosion protection and safety are very important for design and reliability evaluations, and must be closely coordinated and controlled. Just as safe equipment is not necessarily reliable, neither is reliable equipment necessarily safe; but the two can be compatible, and often are.

2-3.6 ELECTROMAGNETIC-RADIATION PROTECTION

The electromagnetic spectrum is divided conveniently into several categories ranging from gamma rays at the short-wavelength end through X rays, ultraviolet, visible, infrared, and radio, to the long-wavelength radiation from power lines. Solar radiation is the principal reliability concern. Damage near the surface of the earth is caused by the electromagnetic radiation in the wavelength range from approximately 0.15 to 5μm. This range includes the longer ultraviolet rays, visible light, and up to about midpoint in the infrared band. Visible light accounts for roughly one-third of the solar energy falling on the earth, with the rest being in the invisible ultraviolet and infrared ranges. The solar constant (the quantity of radiant solar heat received normally at the outer layer of the atmosphere of the earth) is, very roughly, about 1 kilowatt per square meter or 1 horsepower per square yard. In some parts of the world, almost this much can fall on a horizontal surface on the ground at noon (Ref. 10).

Solar radiation principally causes physical or chemical deterioration of materials. Examples are the effects due to increased temperature and deterioration of natural and synthetic rubber. As defined in par. 2-2.1, these are mechanical effects. Radiation also can cause functional effects, such as the temporary electrical breakdown of semiconductor devices exposed to ionizing radiation. Considerations to include in a radiation protection analysis are the type of irradiated material and its characteristics of absorption and sensitivity to specific wavelengths and energy levels, ambient temperature, and proximity of reactive substances such as moisture, ozone, and oxygen. Some specific protection techniques are shielding, exterior surface finishes that will absorb less heat and are less reactive to radiation effects of deterioration, minimizing exposure time to radiation, and removing possibly reactive materials by circulation of air or other fluids or by careful location of system components. More extensive information is given in Ref. 10.

2-4 OPERATIONS RESEARCH METHODS

Par. 2-2 discussed the complexity of describing the effects of the complete environment.

Operations analysis, the system concept of input-transform-output, provides a powerful tool for dealing with this complex situation and allows relationships between several inputs, between inputs and outputs, and between the transformation function and effectiveness of output.

Problem solving is always helped by diagramming the conditions. Fig. 2-5 provides a picture of the overall environmental situation. A climate consists of an envelope of natural environmental factors of natural ambient conditions. A generic classification of the environmental factors contains temperature, humidity, radiation, precipitation, contamination, and wind.

A systematic procedure is also valuable for handling technical review and technical review reporting and evaluation, and is partic-

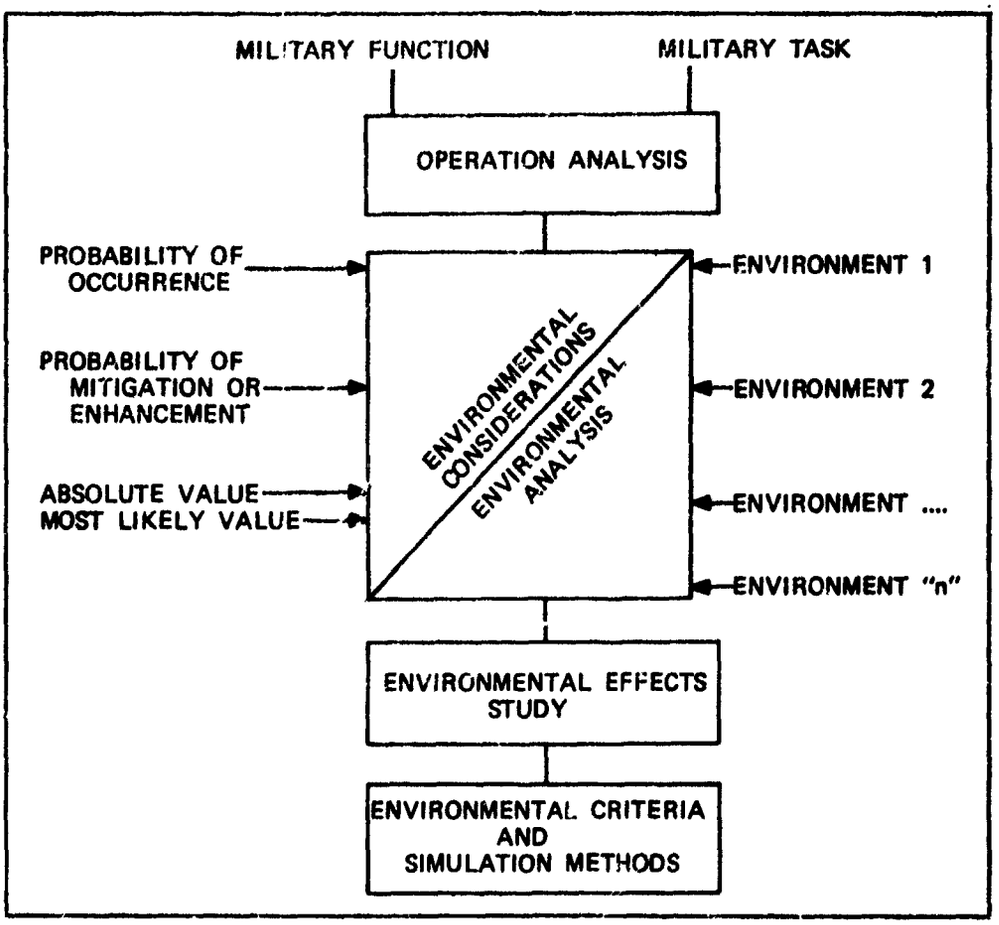


FIGURE 2-5. Environmental Situation Diagram[2]

ularly applicable to PERT methodology. Accordingly, the algorithm in Fig. 2-6 was designed to encompass the performance of each task and of the total program. Thus, performance at both levels will have several points of contact and will overlap.

The matrix in Fig. 2-7 shows these interwoven and interrelated points of contact. Tasks are grouped as follows: the left column contains environments consisting of all relevant environmental factors; the columns to the right are either factors of a subset of one or more environments, or are operations on the set and subset. Performance procedures are located in the horizontal rows.

By using the concept in Fig. 2-7, the progress and status of performance can be recorded, reported upon, and evaluated at each block and each row. Interrelationships are included in the blocks, and modes provided by the rows. Thus, blocks and rows represent checkpoints, and the figure becomes heuristic and modus operandi for both management and technical performance. More details of these methods can be found in Refs. 2 and 6.

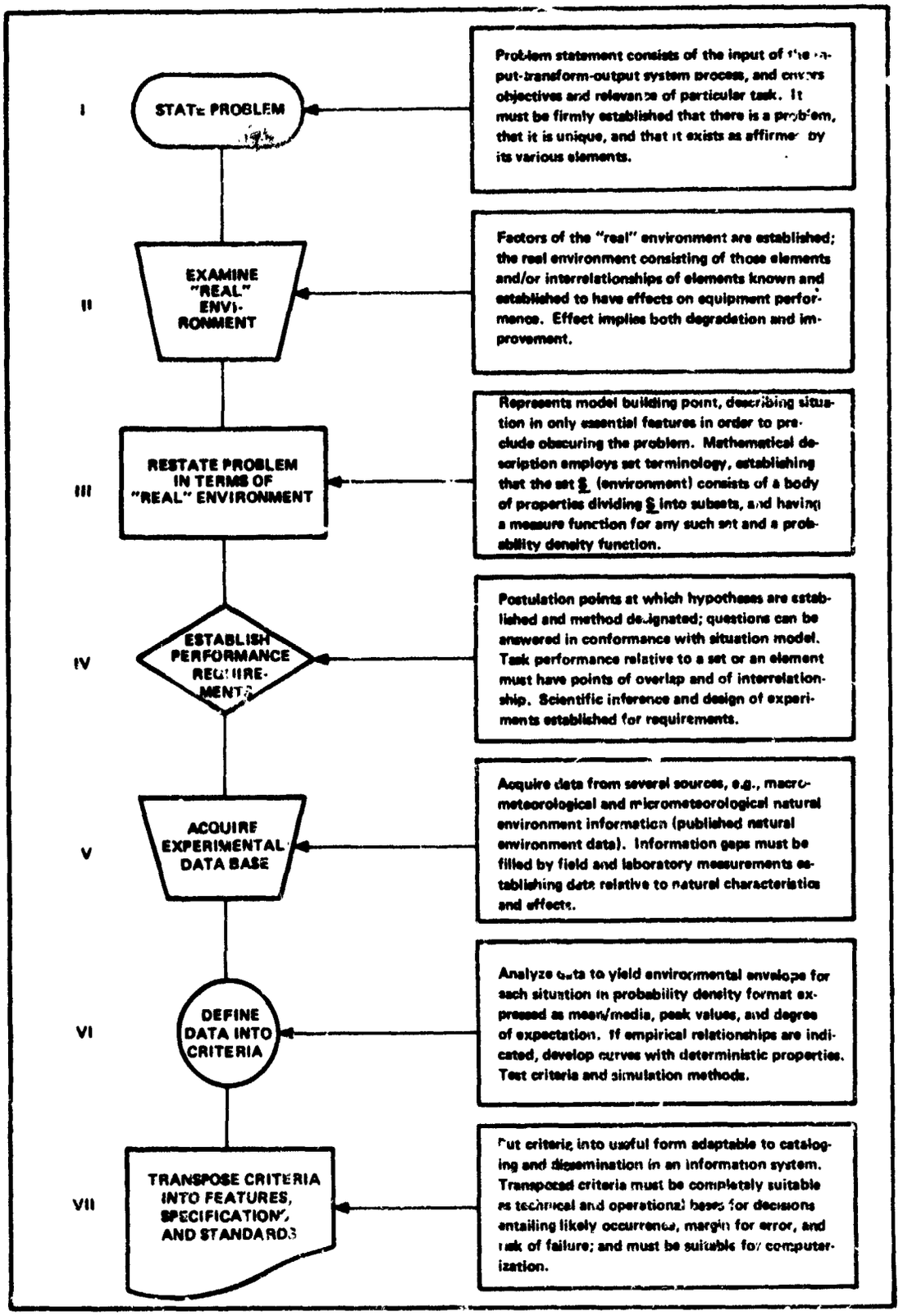


FIGURE 2-6. Algorithm for Program Performance

TASK	PERFORMANCE	TASK						
		OZONE	SUNSHINE	RAIN	SAND & DUST	COMBINED & SEQUENTIAL	INFORMATION SYSTEM	ARMY HAND-BOOK SERIES
POLAR & ARTIC	I. STATE PROBLEM			X	X			X
	II. EXAMINE "REAL" ENVIRONMENT			X	X			X
	III. RESTATE PROBLEM IN TERMS OF "REAL" ENVIRONMENT			X	X			X
	IV. ESTABLISH PERFORMANCE REQUIREMENTS			X	X			X
	V. ACQUIRE EXPERIMENTAL DATA BASE			X	X			X
	VI. REFINE DATA INTO CRITERIA			X	X			
	VII. TRANSPOSE CRITERIA INTO FEATURES, PROCEDURES, SPECIFICATIONS, AND STANDARDS			X	X			
TROPICAL	I. STATE PROBLEM				X			X
	II. EXAMINE "REAL" ENVIRONMENT				X			X
	III. RESTATE PROBLEM IN TERMS OF "REAL" ENVIRONMENT				X			X
	IV. ESTABLISH PERFORMANCE REQUIREMENTS				X			X
	V. ACQUIRE EXPERIMENTAL DATA BASE				X			X
	VI. REFINE DATA INTO CRITERIA				X			
	VII. TRANSPOSE CRITERIA INTO FEATURES, PROCEDURES, SPECIFICATIONS, AND STANDARDS				X			
ARID-DESERT	I. STATE PROBLEM			X				X
	II. EXAMINE "REAL" ENVIRONMENT			X				X
	III. RESTATE PROBLEM IN TERMS OF "REAL" ENVIRONMENT			X				X
	IV. ESTABLISH PERFORMANCE REQUIREMENTS			X				X
	V. ACQUIRE EXPERIMENTAL DATA BASE			X				X
	VI. REFINE DATA INTO CRITERIA			X				
	VII. TRANSPOSE CRITERIA INTO FEATURES, PROCEDURES, SPECIFICATIONS, AND STANDARDS			X				

NOTE: "X" = INCONSEQUENTIAL SEVERITY OF EFFECTS; NOT APPLICABLE.

FIGURE 2-7. Matrix of Interrelationships of Tasks[6]

REFERENCES

1. AMCP 706-115, Engineering Design Handbook, *Environmental Series, Part One, Basic Environmental Concepts.*
2. M. H. Simpson, *A Numerical Taxonomy Method to Evaluate and Predict Equipment Performance from Environmental Engineering Data*, FA Report No. R-1847, Frankford Arsenal, Philadelphia, Pa., April 1967.
3. C. G. Robinson and H. M. Bunch, *A Study of the Feasibility of Developing Overlay Maps to Indicate Performance Capabilities of Ordnance Equipment in Selected World Environments*, Southwest Research Institute, San Antonio, Texas, 1962.
4. John McGee and Chester Polak, *The Development of Standard Environmental Test Specimens*, WADC TR 59-697, Inland Testing Laboratories Division, Wright-Patterson AFB, Ohio, 1959.
5. AR 70-38, *Research, Development, Test, and Evaluation of Materiel for Extreme Climatic Conditions.*
6. E. C. Theiss et al., *Handbook of Environmental Engineering*, ASD Technical Report No. TR 61-363, Air Force Systems Command, Wright-Patterson AFB, Ohio, Technical Writing Service Division, McGraw-Hill Book Co., Inc., N.Y., 1961.
7. G. F. Arthur, *An Investigation of the Concurrence of Environmental Elements*, WADC Technical Note 60-162, Wright-Patterson AFB, Ohio, 1960.
8. G. A. Greathouse and C. J. Wessel, *Deterioration of Materials, Causes and Preventive Techniques*, Reinhold Publishing Corp., N.Y., 1954.
9. R. V. Pavia, *An Investigation into Engine Wear Caused by Dust*, Austral, Aeronautical Research Committee Report ACA-50, July 1950.
10. AMCP 706-116, Engineering Design Handbook, *Environmental Series, Part Two, Natural Environmental Factors.*
11. R. P. Haviland, *Engineering Reliability and Long Life Design*, D. Van Nostrand Co., Inc., N.J., 1964.
12. J. W. Christopher, "Man as a Part of the Design Environment", *Proceedings of the 1970 Annual Symposium on Reliability* 114-119 (1970).
13. S. Cherkasky, "Long-Term Storage and System Reliability", *Proceedings of the 1970 Annual Symposium on Reliability* 120-127 (1970).
14. G. Coren, W. Cotliar, and D. Conroe, "Predicting Environmental Interaction", 1967 Annals of Reliability and Maintainability 6, 12-19 (1967). (Available from SAE, 485 Lexington Ave., New York, N.Y. 10017)
15. H. A. Van Dine, Jr., "Environmental Stress Analysis", *ASOC Annual Technical Conference Transactions*, 109 (1968).
16. K. A. Chandler, "Paint Failures Due To Inadequate Specifications", Methods and Materials 16, No. 10, 22 (October 1969).
17. AMCP 706-117, Engineering Design Handbook, *Environmental Series, Part Three, Induced Environmental Factors.*
18. AMCP 706-118, Engineering Design Handbook, *Environmental Series, Part Four, Life Cycle Environments.*
19. AMCP 706-119, Engineering Design Handbook, *Environmental Series, Part Five, Glossary of Environmental Terms.*

CHAPTER 3 MEASURES OF RELIABILITY

3-0 LIST OF SYMBOLS

Cdf = Cumulative distribution function
MTBF = mean time between failures
MTTF = mean time to failure
pdf = probability density function
Sf = Survivor function, $Sf = 1 - Cdf$
t = time to failure (for nonrepairable items) time between failures (for repairable items)

3-1 INTRODUCTION

Engineers face tremendous difficulties in attempting to measure reliability, maintainability, safety, or other product characteristics precisely with a single number. The reason for the difficulty is that products are usually complex, are made up of many different parts, serve many different uses, and operate under many different conditions. The question "how good is a jeep?" might well take 50 pages of explanation and great detail to arrive at a plethora of answers. How then is it possible to measure the reliability of a jeep with a single number?

By using a single number to measure reliability, some information is lost. But the convenience of one number—or perhaps a few numbers—makes up for the lost information. All the measures given in this chapter are related to probabilities. The methods for calculating (predicting) reliability are given in *Part Three, Reliability Prediction*. A discussion of many concepts in probability and statistics together with information about specific probability distributions are given in *Part Six, Mathematical Appendix and Glossary*. Techniques involved in estimating and measuring reliability by means of test results on existing items are given in *Part Four, Reliability Measurement*.

The process of designing, creating, and producing reliable hardware is an engineering one, not a statistical one. But the measures of reliability are statistical; so the engineer does need to be familiar with probability and statistics.

Reliability is a measure of the ability of an item to complete its mission successfully, given that the item was in proper condition (available) at the mission beginning. Sometimes, quantitative reliability measures are assigned as a goal in the conceptual stage, before any design or hardware has been fabricated. In this case, the system must be designed and the subsystems and parts selected to preserve the desired reliability. At each decision point in the concept, design, or fabrication phase, the system reliability must be predicted. In these cases, the predicted reliability is compared with the required reliability, and such changes and trade-offs made as are necessary. This reliability constraint imposed upon designers and developers of equipment is not different in spirit from the cost constraints imposed on an architect. He wishes to create as distinguished a building as possible within the limits of his allowed costs. Nor is it different in spirit from the weight constraints imposed on an aircraft designer who must consider engine, equipment, and fuel requirements against the weight of the payload. The difference with the constraint on reliability is that it has been more recently recognized. Reliability, like cost and weight, must be specified in advance; the quantitative measures of reliability make it possible to do this.

Of the several measures of reliability, it is a matter of engineering judgment to decide which to use. Many times it will make little difference, but sometimes it will. A supplier, once given the measure as a specification, might well try to maximize his gains by changing anything but the specified measure. See *Part Five, Contracting for Reliability*.

3-2 PROBABILITIES OF SUCCESS AND FAILURE

The traditional narrow definition of reliability as a probability of success is repeated here from par. 1-1:

> "s-Reliability is the probability that an item will perform its intended function for a specific interval under stated conditions."

This definition has two major shortcomings:

PRECEDING PAGE BLANK-NOT FILMED

(1) It does not cover one-shot items like ammunition.

(2) It does not explicitly consider the condition of the item at the beginning of the mission, whereas virtually all calculations and predictions of *s*-reliability do consider it.

Most of the theoretical analyses of reliability which appear in the literature and those in *Part Three, Reliability Prediction* use the following definition which alleviates those two shortcomings:

> "*s*-Reliability is the probability that an item successfully completes its mission, given that the item was in proper condition at the beginning of the mission."

In a practical situation, the four elements of the definition must be carefully explained, defined, and delineated.

(1) The item

(2) The mission (especially any limitations on repair during the mission)

(3) Successful completion

(4) Proper condition (especially the manner in which it is assured).

For a theoretical analysis one usually specifies the repair philosophy for the components during the mission, and in what conditions the components may appear during the mission. Proper-condition almost always is assumed to be "every component is good", not merely that the item is functioning.

One-shot items are covered in par. 3-7.

The probability of failure often is calculated, rather than probability of success, because of the significant-figure difficulty with probabilities near 1 and because of the easy approximations for small probabilities. Failure and success are complementary events; the sum of their probabilities is 1.

3-3 FAILURE DISTRIBUTIONS

A failure distribution gives all the information about times to failure, not just a single number. (This paragraph is written as if the variable of interest is failure-time, but the variable could easily be strength, damage, etc.) In the usual application of failure distributions it is presumed that no failure/repair pairs are allowed, although preventive maintenance is considered occasionally. The statistical concepts of failure distributions are explained in *Part Six, Mathematical Appendix and Glossary*. The probability density function (*pdf*) is the description of a distribution most often used in discussions. It historically has been used, it has mathematical convenience, and its shape is usually quite characteristic of the distribution (whereas all cumulative distribution functions tend to look alike). It will be used in this paragraph. The uses of failure distributions are classified conveniently into interpolation, extrapolation, and calculations of moments and percentiles.

Interpolation (usually a smoothing type) means calculating a value of the *pdf* for a failure time that is within the region where data are available, but for which there was no test result or for which some smoothing of data was needed. The choice of failure distribution is not critical in interpolation. Many distributions will give equally good results, especially when goodness is evaluated with respect to the usual tremendous uncertainty in the data.

Extrapolation means calculating a value of the *pdf* for a failure time that is outside the region where data are available. This is the most popular and the most misleading use of distributions. It is misleading because the user forgets that he doesn't know the behavior in this region; he then confuses "numerical precision in calculation" with "accuracy of describing the real behavior". One method of avoiding this trap is to use two regions of failure time: internal and external. The internal region is essentially the one where interpolation, or very mild extrapolation, is possible. The external region is the one where gross extrapolation would have to be used. Very often it will be in two parts, one on either side of the internal region. One then estimates the fraction of the population which lies within these two subregions. In any subsequent calculation, a further assumption might have to be made about where in the subregion the values might be; but then the user is on guard that he is guessing and that he should see what happens for several different guesses. There is absolutely no law of nature that says

pdf's must be smooth tractable curves. The use of the external region is illustrated in Chapter 10, "Parameter Variation Analysis".

Calculation of moments and percentiles is done conveniently from the distributions using existing formulas and tables. But it is not necessary that the distribution be known before moments and percentiles can be estimated. Moments can be directly estimated from the data—indeed, equating sample moments to population moments is a well-known technique for parameter estimation. The usual moments are the mean and variance. Percentiles can be estimated directly from the data only in the interior region. If percentiles must be calculated in the exterior region, then guesses (possibly implicit) must be made about the failure-time behavior in that region.

Four of the common distributions and their traditional applications are given in Table 3-1. The table illustrates tradition more than it describes the real world.

3-4 FAILURE RATE

The term "failure rate" is defined several ways in the literature. But its use in the following way is so entrenched that it is not feasible to use another term. Other names for failure rate are conditional failure rate, instantaneous failure rate, hazard rate, and force of mortality.

"Failure rate (for continuous variables) is the ratio of the probability density function to the survivor function."

The probability density function *(pdf)* and survivor function *(Sf)* are discussed in *Pa. Six, Mathematical Appendix and Glossary*. The survivor function is sometimes called the reliability function; $Sf \equiv 1 - Cdf$ where Cdf is

TABLE 3-1

GENERAL APPLICATION OF COMMON DISTRIBUTIONS

Distribution	Typical Applications	Comments
Exponential	Large, often-repaired systems. Failure due to occasional, unpredictable environmental extremes.	Often used when insufficient data exist to show the form of the distribution.
Weibull	Mechanical and electronic components. Fatigue life. Antifriction-Bearing life.	Often used in any situation where the data do not rule it out. It is mathematically tractable.
Lognormal	Time to repair. Life of semiconductors. Fatigue life. Antifriction-Bearing life.	Often used where the log transform is easy for the data. Very similar shape, in its central region, to the Weibull.
s-Normal (Gaussian)	Life, where limited by physical wear. Wearout life. Describe relatively small variability in any characteristic of anything	Often used where insufficient data exist to show the exact form of the distribution, but when the exponential is clearly not applicable

the cumulative distribution function (for continuous variables). A longer way of saying it is—Failure rate is the rate of failure, at a time instant, given that the item was not failed at the beginning of that instant.

The formula for failure rate is

$$\text{failure rate} = \frac{pdf\{t\}}{Sf\{t\}} \qquad (3\text{-}1)$$

The difference between failure rate and the probability density function is that the *pdf* is a prediction made at time = 0 about the future; whereas the failure rate is a prediction about only the next instant. Both have the same units: reciprocal time.

Occasionally someone in the literature distinguishes between the failure of nonrepairable items and the failure rate of repairable items. This is a worthwhile endeavor, but the distinction, for simple systems, is not likely to find its way into the literature. If the system is not simple and if the repair strategy is complicated—i.e., if there are many conditions (states) of the system that must be distinguished—then failure rate is an ambiguous ill-defined term. Instead, transition rates between conditions are given for all possible transitions.

The reasons that failure rate is so popular a measure of reliability, as opposed to the *pdf*, are:

(1) Often one really is not interested in making predictions far into the future ("If it is operating now, will it still be operating a long time from now?"); rather one wishes to know only about the future itself ("For those which are still operating then, how likely are they to fail?").

(2) The assumption of constant failure rate is made so often, sometimes implicitly, that it is a common figure of merit for a component or system.

Whenever no time dependence is given for a failure rate, usually the failure rate is presumed to be constant.

Table 3-2 shows the failure rate characteristic for the four common distributions. The implications of failure rate behavior are:

TABLE 3-2

BEHAVIOR OF THE FAILURE RATE

Distribution	Failure-Rate Behavior
Exponential	Constant
Weibull	Monotonic. The direction depends on the shape parameter; can be always increasing (without bound), always decreasing (to zero "at infinity"), or constant. (See Part Six)
Lognormal	Increases to a maximum, then decreases to zero "at infinity"
s-Normal (Gaussian)	Always increases (without bound)

(1) Constant failure rate. An item of any age statistically has as long a life left as one of any other age. One should not replace good items when their hazard rate is constant.

(2) Increasing failure rate. Older items statistically have shorter lives left than newer items. Replacing old nonfailed items can be a good idea.

(3) Decreasing failure rate. Older items statistically have longer lives left than newer items. This is a case where the "bad die young".

These behaviors are statistical and mean only what they say—nothing more. An individual item with a decreasing failure rate might be wearing out, but could still live long because its initial strength was extremely high.

When the failure rate is increasing without bound ($\to\infty$), it is sometimes said to be in a wearout phase. Distributions with this property are then said to be wearout distributions.

The s-normal (Gaussian) and some Weibull distributions are wearout distributions. The exponential and lognormal distributions are not.

The parameter of a Poisson process is also a failure rate. See Refs. 1 or 2 for more details.

The failure rate of a system is often fairly high at the beginning when it is put into commission. This is largely due to human frailty in one form or another. Then, once the severe weaknesses have been removed (possibly even by redesign) the failure rate often settles down to a reasonably constant value (fluctuates within a factor of 2 or so). Some systems, if they are used long enough, have a rise in failure rate because many of the components seem to near the end of their useful lives. If this failure rate behavior is plotted as a function of time, it has the so-called bathtub shape. Many electronic systems become obsolete before their failure rate rises appreciably. Some systems are debugged thoroughly before being delivered. The bathtub curve is neither inevitable nor always desirable. It is better to avoid the term and separately discuss variations in failure rate if they will be important.

3-5 TIME-TO-FAILURE

This concept applies to nonrepairable items. It is sometimes called time-to-first-failure, but that concept usually is confusing since further failures are implied, but yet time-between-failures is obviously not meant. (One can, of course, calculate and use any figure he chooses, provided both he and the intended reader understand it.) In this paragraph, each item fails but once and so "failure" is "first failure". If the item is repaired and returned to a like-new condition, then it is considered a different, new item.

Not all failure-time distributions have a mean (i.e., the mean is "infinite"), but the usual ones do. The mean time-to-failure *MTTF* is

$$MTTF \equiv \int_0^\infty t\ pdf\{t\}\ dt = \int_0^\infty Sf\{t\}\ dt \qquad (3\text{-}2)$$

if the *MTTF* exists; where

t = time to failure
pdf = probability density function
Sf = survivor function

The *MTTF* is used because it is tractable and traditional. In some instances, the existence of many long-lived items inflates the *MTTF* so that it is not characteristic of lives actually observed in the field. Very often a median time-to-failure is more characteristic of the lives that will be observed in the field. For short times, failure rate is often a better, more useful reliability measure than *MTTF*; the early failures will hurt the system—no one cares about the exact life of the very long-lived systems.

The means and medians of the common distributions are given in *Part Six, Mathematical Appendix and Glossary*.

3-6 TIME BETWEEN FAILURES

This concept applies to repairable items. In any repair situation one must know the presumed condition of the item after repair in order to make calculations. There are two conventional tractable assumptions:

(1) A repaired item is "good as new". This means that, statistically, the repaired item is just like a new one.

(2) A repaired item is "bad as old". This means that, statistically, the repaired item is just as bad as it was before failure. An example is a jeep, just after a failed set of distributor points has been replaced; the overall condition of the jeep has not been significantly altered by the repair.

If the failure rate is constant, then the two assumptions are equivalent, since age is irrelevant in predicting future life.

When the repaired item is "good as new", the time-between-failures is the same as time-to-failure. If not, then the repair philosophy must be explicitly enumerated.

The mean time-between-failures (*MTBF*) appears often in the reliability literature; it is defined just as in Eq. 3-2. Unfortunately, the repair situation is rarely explained. In some

cases, the author may have been confused and, if it is a theory paper, the author may not even realize what his implicit assumptions are. Virtually always when *MTBF* is given a specific value (e.g., *MTBF* = 100 hr), the failure rate of the item is presumed constant (or reasonably so). When failure rate is constant, the *MTBF* is just the reciprocal of the failure rate.

For large complex repairable systems where no few components are responsible for many of the failures, and where the system has had many failures already, the failure rate is reasonably constant and *MTBF* is a reasonable concept.

Theoreticians have to be more wary of this concept than do engineers.

3-7 FRACTION DEFECTIVE

For one-shot items, such as ammunition, the time concept in reliability is not appropriate. They either function, or they fail in some way. So the fraction defective (or fraction good) is a useful concept. One often wishes to classify failures into several categories. For ammunition, two common categories are duds and prematures; generally, the fraction of prematures should be much less than the fraction of duds.

Another case where fraction defective is appropriate is where a distribution of strength of an item is reasonably known between some limits; e.g., the strength has an *s*-normal distribution with mean 10,000 lb and standard deviation of 1000 lb, in the range 7000 to 13000 lb. On the weak side, the actual strength is not known, the items are just considered defective and the fraction defective is estimated, say 0.5%. One rarely will care if a small fraction has strengths above 13000 lb because they will not affect appreciably the reliability.

Another use for fraction defective is where one doesn't care how good an item is, or how long it lasts, just as long as it is good enough. Then those which are good enough constitute the fraction good; the others are the fraction defective.

REFERENCES

1. W. Feller, *An Introduction to Probability Theory and its Applications*, John Wiley and Sons, Inc., N.Y., 1966.
2. M. L. Shooman, *Probabilistic Reliability: An Engineering Approach*, McGraw-Hill Book Co., N.Y., 1968.

CHAPTER 4 MODEL BUILDING AND ANALYSIS

4-0 LIST OF SYMBOLS

Cdf	=	Cumulative distribution function
$f(t)$	=	$pdf\{t\}$
$f(x)$	=	$pdf\{x\}$
$F(x)$	=	$Cdf\{x\}$
$g(y)$	=	$pdf\{y\}$
$G(y)$	=	$Cdf\{y\}$
pdf	=	probability density function
$R(t)$	=	$Sf\{t\}$
Sf	=	Survivor function, $Sf = 1 - Cdf$
t	=	a random variable, time
x	=	any random variable
y	=	$F(x)$
α	=	scale parameter, see Table 4-1
β	=	shape parameter, see Table 4-1
λ	=	a failure rate

4-1 INTRODUCTION

No one can analyze the real world situation or the real hardware; he can only analyze his mental picture of the situation or hardware. This mental picture is called a conceptual model (often shortened just to "model").

The idea of a conceptual model is adapted from the idea of a physical model such as a model car. In a physical model, the characteristics of importance are reproduced quite well. In a model car these might be proportions, shape, and color. The characteristics of little or no importance are not usually reproduced at all; e.g., there may be no motive power and the tires may not be pneumatic. The "inbetweens" receive indifferent treatment. The physical model is an abstracting of something important from the physical world; it is an imitation.

A conceptual model is analogous to a physical model. Since everything in the universe affects everything else to some degree, however slightly, any exact treatment would be hopelessly complicated. Therefore the engineer decides how he will look at the situation and makes a set of assumptions (both explicit and implicit) about what he will ignore and what he will include in the conceptual model. By its very nature, a conceptual model is incomplete: it ignores some things and describes others in an approximate fashion.

After having made a set of assumptions for a conceptual model, the engineer then operates on those assumptions with mathematics and logic; he analyzes them by any means at his disposal. While developing the logical implications of a set of assumptions, he often doesn't like the results: they don't seem to fit; they appear to be inconsistent with his beliefs, etc. Then he has two rational choices:

(1) Change his beliefs about the way the world is, if he is convinced that the set of assumptions is very realistic; and/or

(2) Go back and modify the assumptions, so that their logical implications do in fact fit his beliefs about the world.

The creation of a conceptual model is a circular, often haphazard, process wherein ideas come from everywhere and get analyzed, tested, compared, junked, and accepted.

A conceptual model is often mathematical in nature and the same formalism will describe several different situations. It is important to keep the distinction between the mathematics itself (which is quite general, completely impersonal, and always "true") and what it represents in an engineering sense.

All reliability analyses and optimizations are made on conceptual models of equipment, not on the equipment itself. The engineer forgets this at the peril of the person in the field who uses, not the engineer's conceptual model, but the real hardware.

This chapter describes the procedure used to create mathematical models of systems. The models can then be analyzed by the methods in *Part Three, Reliability Prediction*.

For systems with (a) repair, and (b) many elements that are treated separately, a more complicated description is needed than for simple nonrepairable systems. The possible states (conditions) of each element are defined, and the state (condition) of the system is the set of states of the elements. This

approach is sometimes called the state-matrix approach because the state of the system is described, not by a single number, but by a matrix of numbers. The approach is discussed more fully in par. 4-2.

Some terms that will be used are defined:

(1) Element. An element of a system is an item whose failure and repair characteristics are considered as a unit and not as a collection of items.

(2) Up. An item is up if it is capable of performing its function; i.e., it is available. There might be various degrees of being up, each with different failure behavior.

(3) Down. An item is down if it is not up.

(4) On. An item is on if it is both up and operating.

(5) Idle. An item is idle if it is up and not operating; i.e., it is being held in standby.

(6) State. The state of an item is a statement of its condition, as measured by its characteristics which are considered important. The states are often given names such as Up, In Repair, Degraded, Standby, or Failed.

(7) State-matrix. The state-matrix of an item is the matrix of the states of the elements of the item.

(8) Series. Elements of a subsystem are in series if they all must be up for the subsystem to be up.

4-2 MODEL BUILDING

To compute the reliability and maintainability measures of a system, there must be a mathematical model of the system. The appropriate mathematical model is a reliability model which consists of a reliability block diagram or a Cause-Consequence chart; all equipment failure time and repair time distributions; a definition of the states of each element and of the item; and a statement of maintenance, spares, and repair strategies.

A reliability block diagram is obtained from a careful analysis of the manner in which the system operates—i.e., the effects of failures on overall system performance of the various parts that make up the system; the support environment and constraints including such factors as the number and assignment of spare parts and repairmen; and finally, a consideration of the mission to be performed by the system. Careful consideration of these aspects yields a set of rules (which will be referred to as up-state rules) which define satisfactory operation of the system (system up) and unsatisfactory operation (system down), as well as the various ways in which these can be achieved. If a system operates in more than one mode, a separate reliability diagram must be developed for each.

For complicated systems, a Cause-Consequence chart might be more appropriate than a reliability diagram. See Chapter 7 for a discussion of Cause-Consequence charts and fault trees. Regardless of which is used, the model building is similar. This chapter uses reliability diagrams because the discussion is simpler that way.

A considerable amount of engineering analysis must be performed in order to develop a reliability model. The engineering analysis proceeds as follows:

(1) The engineer develops a functional block diagram of the system based on his knowledge of the physical principles governing system operation.

(2) The engineer uses the results of performance evaluation studies to determine to what extent the system can operate in a degraded state. This information can be provided by outside sources.

(3) Based on the functional block diagram, and the amount of acceptable performance degradation, the engineer develops the reliability block diagram, and the up-state rules.

(4) The reliability block diagram and the up-state rules are used as inputs to the equations for system behavior and for calculating various measures of reliability and maintainability (including availability). The actual analyses are described in *Part Three, Reliability Prediction.*

The reliability diagram is a pictorial way of showing all the success or failure combinations of the blocks in the system. Those combinations must be known before the reliability diagram can be drawn; one does not "derive" the combinations from the diagram for the first time; rather, they are implicit in

it since they were put there by the originator of the diagram. The rules for drawing the diagram are:

(1) A group of elements that are essential to performing the mission are drawn in series (Fig. 4-1(B)).

(2) Elements that can substitute for other elements are drawn in parallel (Fig. 4-1(C)).

(3) Each block in the diagram is like a switch. The switch is closed when the element it represents is good; it is open when the element is failed. Any closed path through the diagram is a success path.

(4) Elements shown in parallel are sometimes ambiguous. The usual convention is that if any one is good, the subsystem is good (see Rule 3). But some subsystems might require, for example, that 2 out of 5 are good, for the subsystem to be good. These combinations are difficult to draw in the simple way; so the techniques of Fig. 4-1(F) sometimes are used.

The failure behavior of each redundant element must be specified. Some common assumptions and terminologies are:

(1) Hot standby (active redundancy). The standby element has the same failure rate as if it were operating in the system.

(2) Cold standby (passive redundancy, spares). The standby element cannot fail. This often is assumed for spares on a shelf, or spares that are not electrically connected; but the assumption may well not be true.

(3) Warm standby. The standby element has a lower failure rate than an operating element. This is usually a realistic assumption, but often is not a tractable one.

It is possible for standby elements to have higher failure rates than operating elements. In those cases an attempt ought to be made to have the standbys in operation at all times—e.g., (1) an electronic system which is powered can stay warm and thus not be damaged by moisture, (2) ball or roller bearings can Brinell when they are not rotating, and (3) seals can deteriorate when not splashed by fluid.

The state-matrix approach does not use a reliability diagram because of the limitations of such diagrams. Rather, the states (conditions) in which each element can be found are listed; examples are Good, Degraded, Waiting for Preventive Maintenance, Waiting for Repair, and Failed. Some of the element states might also be grouped—e.g., operating might include Good, Degraded, or Waiting for Preventive Maintenance. Then the possible system states are listed and are grouped conveniently. Very often, Up or Down are sufficient descriptions of the system, but anything the designer and users agree on can be used—e.g., a communications receiver which is not Down more than 5 min might not be considered Failed. Next, the transition rate between each pair of states is specified. The usual assumption (Markov Chain) is made that the transition behavior depends only on the two states involved, not on any other past history. If the transition rates are not constant, the problem will be intractable for all but the simplest of systems. If there are many elements, each with several states, the problem can easily be intractable. More details on this approach can be found in Ref. 1 and *Part Three, Reliability Prediction.*

The reliability block diagram is basically a graphical, logical presentation of successful system operation. A functional block diagram and its associated reliability block diagram are illustrated in Figs. 4-2 and 4-3.

As the system design proceeds, a series of reliability block diagrams must be developed to progressively greater levels of detail (Fig. 4-4). The same level of detail ought to be maintained in a given block diagram. A documentation and numbering system should be instituted so that the family of reliability models developed for the system can be organized for ready use.

The elements of the overall reliability diagram ought to be as comprehensive as feasible in order to reduce the complexity of analysis.

Fig. 4-5 depicts a number of illustrative reliability block diagrams together with their up-state rules; they vary in complexity starting with the simplest (a single item) and progressing to levels of increasing complexity. An example of specifying the support subsystem would be the system described by (E) of Fig. 4-5; it has two repairmen, one of whom is assigned to items A and E, and the other is assigned to the remaining items; items A and

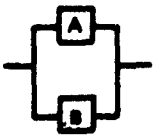
(A)

System is up if item A is up

(B)

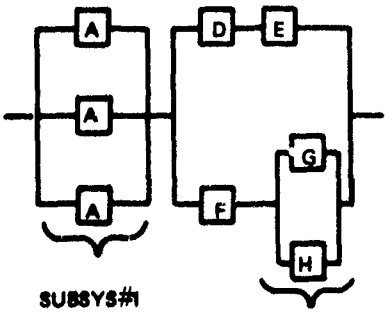
System is up if:
A is up AND
B is up AND
C is up

(C)



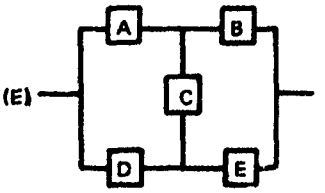
System is up if:
A is up OR
B is up

(D)



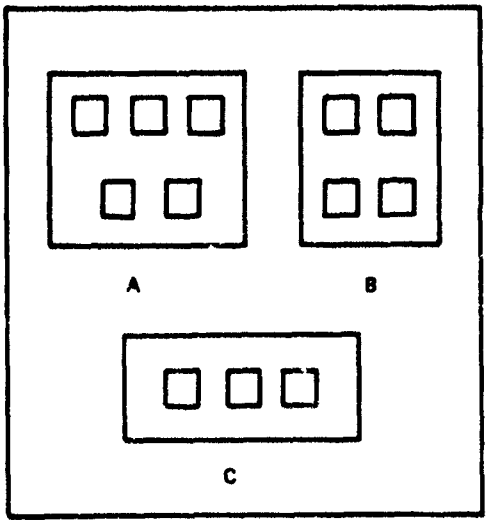
System is up if:
SUBSYS #1 is up AND
SUBSYS #2 is up.
SUBSYS #1 is up if:
at least 2 A's are up.
SUBSYS #2 is up if:
(D AND E) are up OR
[F AND (G OR H)] are up.

(E)



System is up if:
(A AND B) are up OR
(A AND C AND E) are up OR
(D AND E) are up OR
(D AND C AND B) are up

(F)



System is up if:
at least 3 A's are up AND
at least 2 B's are up AND
at least 1 C is up AND
the number of (A's + B's + C's) up is
at least 10

Note: AND means both/and
OR means and/or

FIGURE 4-1. Example of Reliability Block Diagrams and Up-state Rules[1]

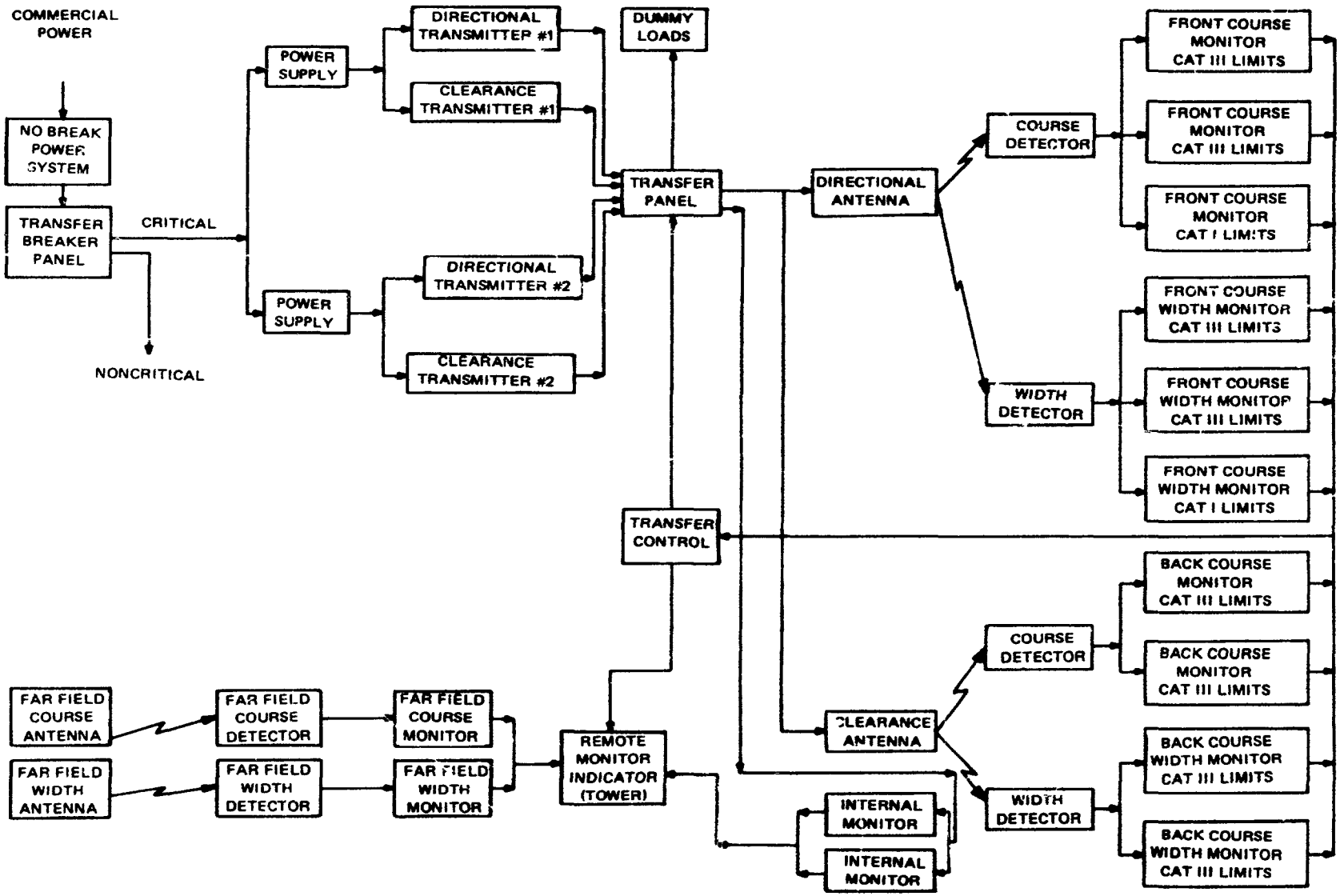


FIGURE 4-2. ILS Localizer Functional Block Diagram

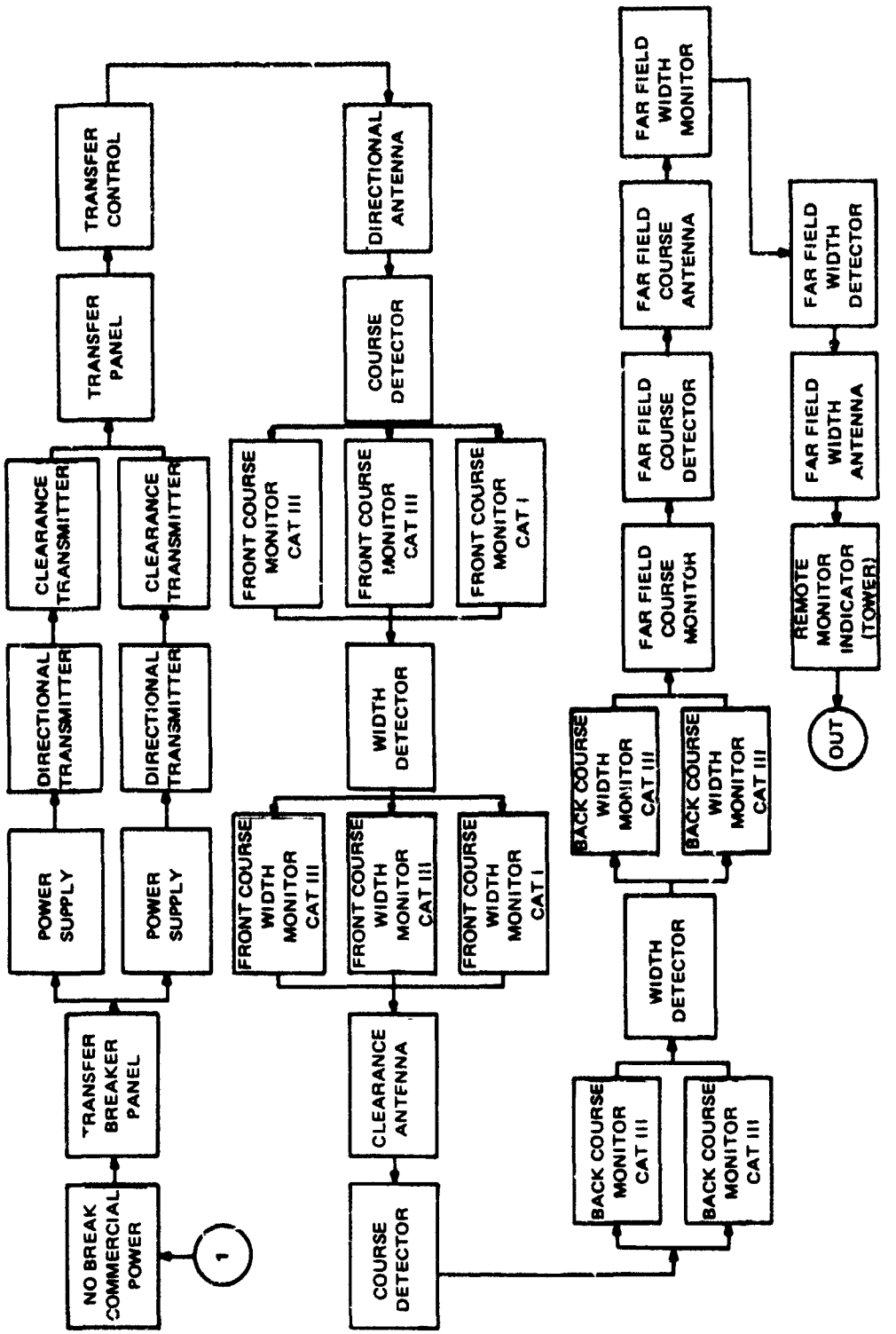


FIGURE 4-3. ILS Localizer Reliability Block Diagram

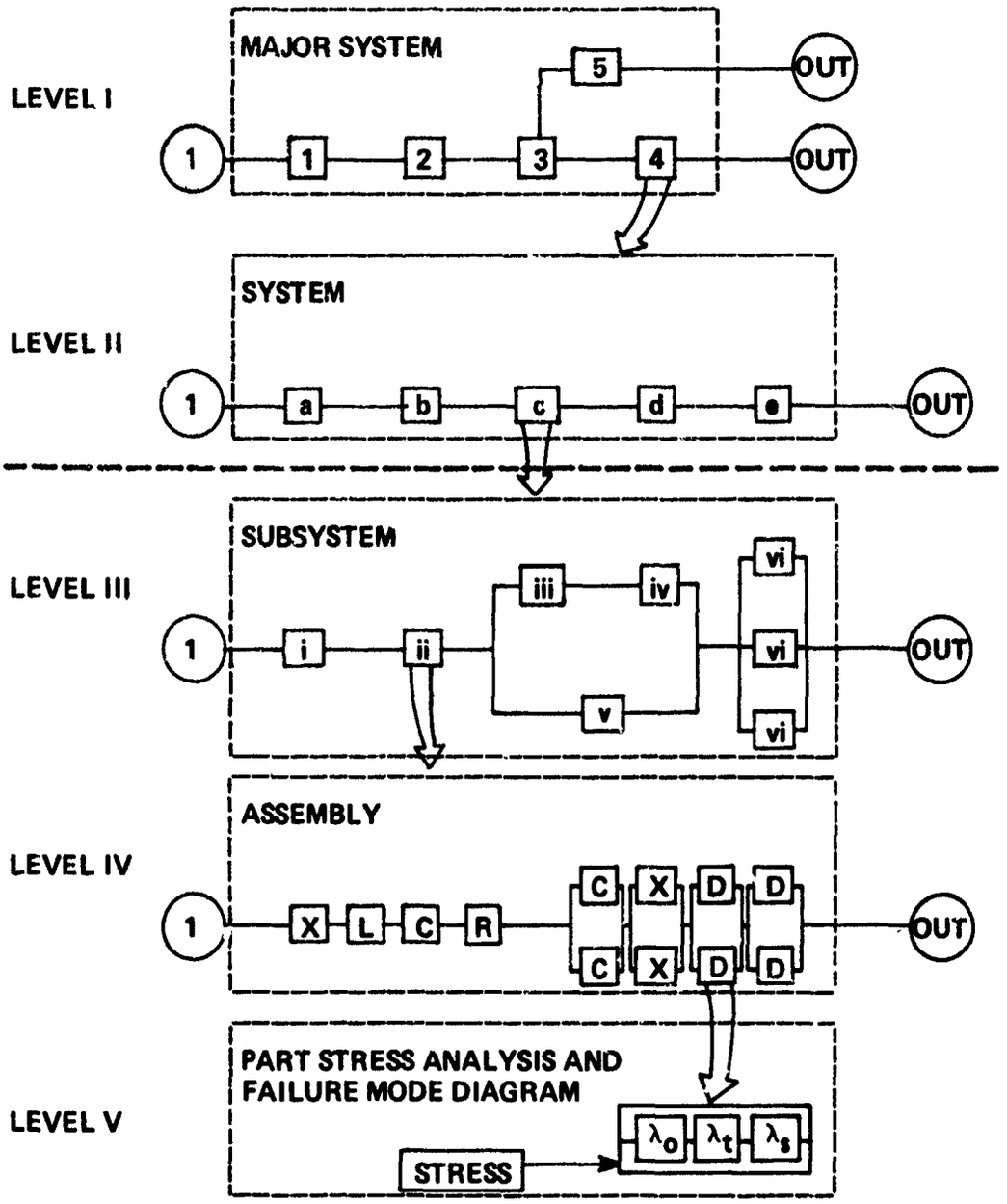


FIGURE 4-4. Progressive Expansion of Reliability Block Diagram

D require a spare part which is taken from a pool of five spares; item B requires no spares for its repair; item C is not repairable; and in the case of conflicting demands on repairmen and/or spares, the order of priorities to be followed is D, A, B, E.

The up-state rules are in addition to the diagram and define what combinations of elements must be up for the system to be up. A set of rules must be defined for each block or section in the reliability block diagram.

The failure and repair distributions of each equipment must be defined. The most common failure distributions are exponential, lognormal, and Weibull; and the most common repair distributions are exponential and

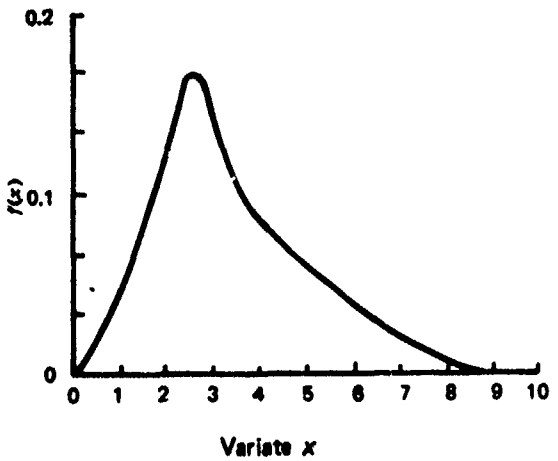


FIGURE 4-5(A). Probability Density Function f(x)

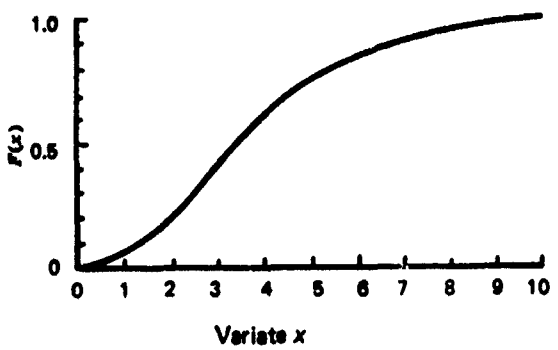


FIGURE 4-5(B). Cumulative Distribution Function F(x)

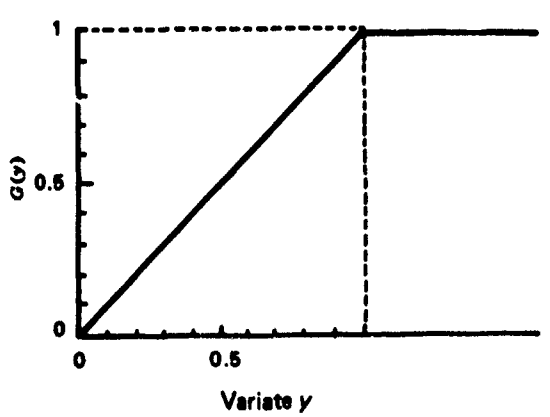


FIGURE 4-5(C). Cumulative Distribution Function G(y)

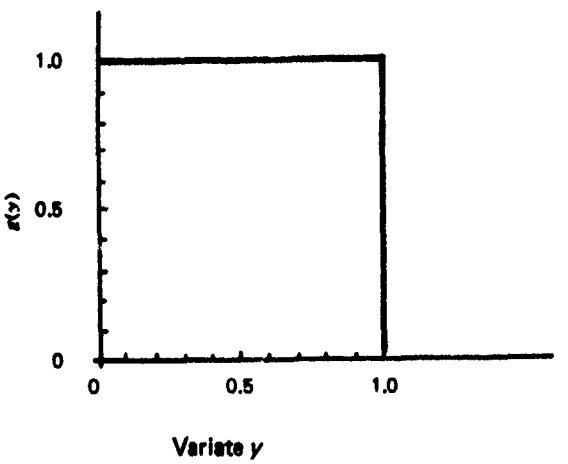


FIGURE 4-5 (D). Probability Density Function g(y)

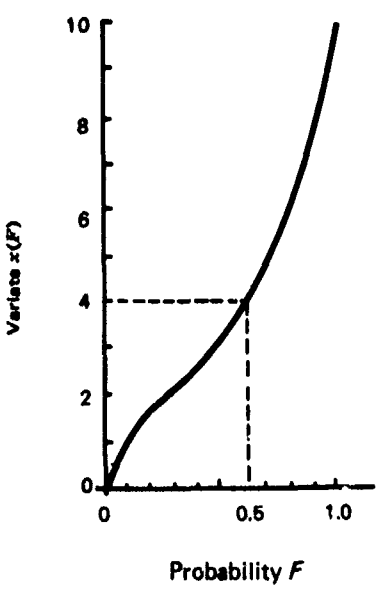


FIGURE 4-5 (E). Inverse Cumulative Distribution Function

FIGURE 4-5. Sampling from a Distribution[8]

lognormal. Great care must be taken when selecting repair and failure distributions; they need to be reasonably tractable and reasonably accurate. For complicated systems, nonconstant transition rates present an almost hopeless analytic difficulty.

Other factors that must be defined are the repair and maintenance strategies and spares allocation. The maintenance strategies define the number of repairmen assigned to each section. The repair strategies define the order in which equipments are repaired if more than one equipment is down. The spares allocation defines the number of spare equipments assigned to each section.

4-3 ANALYSIS

Figures-of-merit can in principle be computed for any electrical or mechanical system if a reliability model can be developed. A variety of techniques is available for computing the figures-of-merit. The specific techniques to be used on a problem depend on the parameter to be computed, the complexity and type of system, the type of failure and repair distributions, and the nature of the logistic system. All of these factors must be considered in detail. Simulation techniques and computer programs for reliability prediction often are used. Because of their complexity, detailed discussions of drift failure and stress/strength analysis are reserved for later chapters. Stress/strength analysis is discussed in Chapter 9, and drift failure is discussed in Chapter 10. *Part Three, Reliability Prediction* discusses the analysis of the mathematical model, once it has been developed. For a system of any complexity, it is likely that the analysis will not be feasible until many simplifying assumptions have been made in the original model. Ref. 1 is a good textbook on analytic methods.

4-4 SIMULATION

Simulation techniques (Ref. 2) can be used to determine the appropriate reliability and maintainability measures (r & m measures) for complex systems. This approach is also very useful for evaluating systems whose elements have nonexponential failure and repair distributions, redundant sections, and can operate in a degraded mode. Frequently, systems of this kind cannot be evaluated by ordinary analytic methods. Another advantage of using simulation is that the effect of the logistic system on the r & m measure can be explored in detail, e.g., the effect of administrative downtime on availability.

4-4.1 GENERAL DESCRIPTION OF A SIMULATION PROGRAM

Simulation of a complex system for the estimation of r & m measures is best accomplished by means of a computer program because of the large number of calculations that are required to estimate the r & m measures to an adequate level of s-confidence. Simulation is the direct observation of the system model "in action". It's a "try it and see" approach. The name Monte Carlo (from the gambling city) often is used when the simulation is probabilistic and repetitive. Monte Carlo simulation always is implied (in this chapter) by the word simulation.

The input data consist of:

(1) A list of elements in each section

(2) The failure, repair, and other event distributions of each element

(3) System failure criteria, which can include allowable downtime

(4) If the system operates in more than one mode, the input data must define the equipment list and failure criteria for each mode and the fraction of time the system operates in each mode.

The logic of such a program follows (Ref. 3):

(1) Select an operating mode.

(2) Generate time to failure for all elements by random sampling from the failure distributions.

(3) Search for the element with earliest time to failure.

(4) Check element reliability configuration and failure criteria to determine if such failure results in system failure. Check operating procedure to determine when the element failure will be discovered.

(5) Proceed to the next event. Generate a new time for that event. There may be

several competing events to be considered.

(6) If system failure occurs, record this along with the reason for failure and the time at which failure occurred.

(7) Repeat Steps (1)-(6) until the desired number of events have occurred.

(8) Print out results.

There are many simulation programs and languages in existence. It rarely will pay to write one from scratch. The best procedure is to contact the people who run the computer and see what is available for that computer.

A considerable amount of information can be obtained from this program. For example, the distribution of downtimes and times to failure, availability, and reliability for each element and for the system can be obtained to any desired level of s-confidence. The s-confidence level is determined by the number of runs made on the computer.

The basic principle of Monte Carlo simulation is sampling from statistical distributions. This sampling process must be random, so that a source of randomness is required. The most appropriate source of such randomness is a sequence of random numbers. When a deterministic algorithm is used to generate a sequence of "random" numbers, they are called pseudo-random numbers. Choosing an adequate set of pseudo-random numbers is an art in itself and must be considered seriously in any large scale Monte Carlo simulation (Ref. 4). When the simulation is being performed by hand calculation, a published table of pseudo-random numbers can be used (Ref. 4). For a large scale simulation performed on a computer, a subroutine called a pseudo-random number generator generates the pseudo-random numbers.

The distribution of a variable can be described by its cumulative distribution function (*Cdf*). The basis for Monte Carlo simulation is the fact that the distribution function of any *Cdf* is uniform between the values of 0 and 1.

Fig. 4-5 illustrates why a random number from the uniform distribution (on the interval 0 to 1) can be used to generate a random variable which has any desired distribution.

Let

$$
\begin{aligned}
f(x) &\equiv pdf\{x\}, \text{ Fig. 4-6(A)} \\
F(x) &\equiv Cdf\{x\}, \text{ Fig. 4-6(B)} \\
y &\equiv F(x) \\
G(y) &\equiv Cdf\{y\}, \text{ Fig. 4-6(C)} \\
g(y) &\equiv pdf\{y\}, \text{ Fig. 4-6(D)}
\end{aligned}
$$

where x = any random variable.

By studying the Figs. 4-5(A) through 4-5(D), one can convince himself that y does have the uniform distribution over the interval 0 to 1. Fig. 4-5(E) is just Fig. 4-5(A) redrawn with the axes reversed. By choosing (with uniform *pdf*) a number between 0 and 1, a value of F is obtained. By entering the F-axis in Fig. 4-5(E) (say $F = 0.6$), then going up to the curve, one finds the value of x to be 4. One can as easily use the survivor function *Sf* as the *Cdf* since it involves only a reversing of the horizontal scale in Fig. 4-5(E). In practice, the calculations of x's from the F's can be done in several different ways. Ref. 4 discusses several of them. Rarely will the design engineer be concerned about the details of such calculations. He needs only enough understanding to talk intelligently to a computer programmer or to use an existing simulation routine.

In practice, this process can be mechanized by using a table to represent the graphs in Fig. 4-5. Analytic methods also can be used. The analytic methods include:

(1) Analytic inversion of the cumulative distribution function and the calculation of the value of this function for the value of a selected uniform random variable

(2) Numerical inverse interpolation in the distribution function determined analytically

(3) A process of numerical inverse interpolation in a numerical approximation to the cumulative distribution function

(4) The numerical approximation to the inverse cumulative distribution function itself.

The analytic method of inversion is illustrated for the exponential distribution, which is so important in reliability engineering.

The *pdf* of time to failure is

$$f(t) = \lambda \exp(-ht) \qquad (4\text{-}1)$$

The *Sf* is

$$R(t) = \exp(-\lambda t) \qquad (4\text{-}2)$$

The inverse of the *Sf* is

$$t = -[\ln R(t)]/\lambda \qquad (4\text{-}3)$$

For example, let $\lambda = 5.0 \times 10^{-6}$/hr and let 3 values of R—from the uniform distribution over [0,1]—be 0.723, 0.032, 0.247. Then the 3 corresponding values of t are

$$t = [(\ln 0.723)/(5.0 \times 10^{-6}/\text{hr})]$$
$$= [(-0.3243)/(5.0 \times 10^{-6}/\text{hr})]$$
$$= 6.49 \times 10^{4} \text{ hr} \qquad (4\text{-}4)$$
$$t = -[(\ln 0.032)/(5.0 \times 10^{-6}/\text{hr})]$$
$$= 6.88 \times 10^{5} \text{ hr} \qquad (4\text{-}5)$$
$$t = -[(\ln 0.247)/(5.0 \times 10^{-6}/\text{hr})]$$
$$= 2.80 \times 10^{5} \text{ hr} \qquad (4\text{-}6)$$

The simulation procedure is illustrated by the very simple example that follows; any practical system will have many more complications. The system has the following properties:

(1) There are 2 elements, A and B. The system fails if either A or B fails.

(2) Upon the failure of A or B, the failed element is repaired. Then both are given preventive maintenance to restore them to like-new condition.

(3) All failures and repairs are *s*-independent.

(4) All failure and repair times have Weibull distributions. (*Part Six, Mathematical Appendix and Glossary* gives details on this and many other distributions.) The details of the distributions are given in Table 4-1.

(5) Preventive maintenance requires 2.0 hr.

Find the up-down time behavior of the system by simulation.

The program steps are as follows:

(1) Prepare the simulation program for this specific problem, including details of the distributions. This means that the program must "know" the 5 properties of the system previously listed. The exact form of inputing the information depends on the simulation program being used. All pseudo-random numbers are from the [0,1) uniform distribution.

TABLE 4-1

FAILURE AND REPAIR DISTRIBUTION FOR ELEMENTS A AND B IN THE EXAMPLE

The Weibull survival function is $Sf\{t\} = \exp[-(t/\alpha)^{\beta}]$; the value of t corresponding to Sf is $t = \alpha(-\ln Sf)^{1/\beta}$.

	α, hr	β, dimensionless	points for the Sf*, hr 50%	36.8%
Failure time, A	1200	1.4	920	1200
Failure time, B	1600	1.8	1310	1600
Repair time, A	3.1	3.4	2.8	3.1
Repair time, B	7.4	4.6	6.8	7.4

* The times shown are those which are exceeded by 50% and 36.8% of the occasions: they give an idea of the typical times associated with the distribution. The 50% point is the median; the 36.8% point is $1/e$ and is shown because it is easy to calculate, viz., $t = \alpha$. The value of t for the 50% point is calculated by setting the Sf to 50%. The times are rounded to 2 significant figures.

(2) Choose 2 pseudo-random numbers. Assign #1 to element A, #2 to element B; this is arbitrary, but makes no difference since the numbers are random enough. Calculate the corresponding failure times for A and B; the one with the shortest failure time is the one that fails.

(3) Choose a pseudo-random number. From Step 2, the identity of the failed element is known. Calculate the repair time.

(4) Add the preventive maintenance time.

(5) Record the duration of the up and down times. This life-cycle is finished. If more are to be run, go to Step 2.

(6) The simulations are finished, the distributions of up and down times are reasonably well known. Calculate the quantities of interest, e.g., *s*-availability, and print them out.

Three life-cycles will be examined. Table 4-2 lists the pseudo-random numbers that will be used; they were taken from Ref. 4, Table 26.11, but they could have come from any

TABLE 4-2

LIST OF PSEUDO-RANDOM NUMBERS FROM THE UNIFORM DISTRIBUTION

Cycle 1	Cycle 2	Cycle 3
.38856	.20431	.96806
.43328	.01169	.99605
.37729	.61815	.95317

generator of random numbers. The bunching effect in cycles 1 and 3 is just the "luck of the draw"; that's the way it happens sometimes.

CYCLE 1

Step 2. The 2 pseudo-random numbers are 0.38856 and 0.43328; they are the *Sf* for A and B, respectively. (Failure times are calculated from the formula in Table 4-2.)

The failure time for A is (1200 hr) × $(-\ln 0.38856)^{1/1.4}$

The failure time for B is (1600 hr) × $(-\ln 0.43328)^{1/1.8}$ = 1449 hr. A fails first; so the system was up for 1153 hr.

Step 3. The pseudo-random number is 0.37729. A is being repaired. The repair time for A is (3.1 hr) × $(-\ln 0.37729)^{1/3.4}$ = 3.08 hr.

Step 4. The preventive maintenance time for A is 2.0 hr; so the down time is (3.08 + 2.0) hr = 5.08 hr.

CYCLE 2

Step 2. The 2 pseudo-random numbers are 0.20431 and 0.01169; they are the *Sf* for A and B, respectively.

The failure time for A is (1200 hr) × $(-\ln 0.20431)^{1/1.4}$ = 1670 hr.

The failure time for B is (1600 hr) × $(-\ln 0.01169)^{1/1.8}$ = 3667 hr. A fails first; so the system was up for 1670 hr.

Step 3. The pseudo-random number is 0.61815. A is being repaired. The repair time for A is (3.1 hr) × $(-\ln 0.61815)^{1/3.4}$ = 2.50 hr.

Step 4. The preventive maintenance time for A is 2.0 hr; so the down time is (2.50 + 2.0) hr = 4.50 hr.

Step 5. Up time = 1153 hr. Down time = 5.08 hr.

Step 5. Up time is 1670 hr. Down time is 4.50 hr.

CYCLE 3

Step 2. The 2 pseudo-random numbers are 0.96806 and 0.99605; they are the *Sf* for A and B, respectively.

The failure time for A is (1200 hr) × $(-\ln 0.96806)^{1/1.4}$ = 103.7 hr.

The failure time for B is (1600 hr) × $(-\ln 0.99605)^{1/1.8}$ = 74.02 hr. B fails first; so the system was up for 74.0 hours.

Step 3. The pseudo-random number is 0.95317. B is being repaired. The repair time for B is (7.4 hr) × $(-\ln 0.95317)^{1/4.6}$ = 3.82 hr.

Step 4. The preventive maintenance time for B is 2.0 hr; so the down time is (3.82 + 2.0) hr = 5.82 hr.

Step 5. Up time = 74 hr. Down time = 5.82 hr.

Step 6. The up/down time pairs are shown in Table 4-3.

An estimate of the *s*-unavailability (poor though it is from only 3 cycles) is "total down time"/"total up and down time" = (15.40 hr)/ (2897 hr + 15.40 hr) = 0.0053. *s*-Availability = 1 − *s*-unavailability = 1 − 0.0053 = 0.9947.

Packaged simulation programs can estimate the uncertainty in that value. Other reliabil-

TABLE 4-3

UP/DOWN TIME PAIRS FOR THE EXAMPLE

	Up, hr	Down, hr
	1153	5.08
	1670	4.50
	74	5.82
Total	2897	15.40

TABLE 4-4. SUMMARY OF PROGRAMS IN THE RELIABILITY AREA

Program Description	Organizations (Originator or User/Sponsor)	References
Computerized Reliability Assessment Method	ARINC/NASA	5
RESCRIPT (Not a specific program but a reliability-oriented programming language for prediction)	Computer Concepts, Inc.	6
Automated Reliability Trade-Off Program for balancing cost vs predicted reliability	Collins Radio	7
Reliability Prediction of majority voter logic by Monte Carlo methods	IBM	8
Reliability Prediction of systems by combining failure rates	Radiation Inc.	9
Reliability Prediction of systems by combining failure rates	Lockheed-Georgia	10
Reliability Prediction of systems by programmed prediction equation	Marine Engineering Lab.	11
Reliability Prediction and crew safety analysis for complex aerospace systems from input logic models	Grumman/NASA	12
Reliability Prediction program for computing mission success and crew safety for Gemini Launch Vehicle; prediction equations required	Martin-Baltimore	13
Reliability Prediction by simulation	Air Force Institute of Technology	14
Special purpose program for prediction of Appollo mission success by simulation	GE-Tempo/NASA	15
Reliability Analysis and Prediction Independent of Distributions	Lear Siegler/NASA	16
Automatic Reliability Mathematical Model	NAA	17
Reliability Prediction of power systems	Westinghouse	18
Reliability Prediction of space vehicle by Monte Carlo simulation	NAA/NASA	19

TABLE 4-4. SUMMARY OF PROGRAMS IN THE RELIABILITY AREA (cont'd)

Program Description	Organizations (Originator or User/Sponsor)	References
Simulation of Failure-Responsive Systems	Westinghouse/NASA	20
Weibull Analysis Program - Conducts Weibull Reliability Analysis	Motorola	20
Reliability program; computer success probability; several components; different distributions; includes correlation between lifetimes	Service Bureau Corp.	21
Reliability program; computer system reliability estimates of components	Service Bureau Corp.	22
Mathematical Automated Reliability and Safety Evaluation Program	Mathematica/Sandia	22, 23
A simulation program for availability analysis using minimal cuts	RTI/NASL	24
Launch vehicle availability for the Saturn V	Boeing/NASA MSC	25
Availability and support, used on Minuteman	STL/AF	26
Availability re Monte Carlo (MORL)	Douglas/NASA	27
Availability re Monte Carlo, used on BMEWS	PRC	28
Investigation of the difficulties in existing program languages for availability and related problems	Cook Electric/AFSC RADC	29
Availability of aircraft, used on B58, F111	General Dynamics, F.W.	30
Effectiveness portion of a family of programs for early weapon system planning (UNILOG)	Martin, Orlando	30
Operational analysis and availability, used on Atlas and Centaur	General Dynamics, F.W.	31
Support-availability multi-systems operations model (SAMSOM)	RAND/AF	32

TABLE 4-4. SUMMARY OF PROGRAMS IN THE RELIABILITY AREA (cont'd)

Program Description	Organizations (Originator or User/Sponsor)	References
Efficient availability evaluation as changes are made	ARINC/NASL	15
Effectiveness and design adequacy simulation and evaluation of aircraft	ARINC/AF ASD	15
WSEIAC model, which combines availability, dependability, and capability	ARINC In-House	15
System effectiveness analyzer (SEA) for prediction and optimization	Computer Applications/NASL	15
Steady-state effectiveness, called system effectiveness evaluation analyzer (SEE/AN)	Auerbach/DCA	15
System simulation (SEE/SIM)	Auerbach/BuShips	15
ASW mission effectiveness in support of advanced ASW ship	ARMA/BuWps	15
Effectiveness of multi-mode systems, for the E2A/ATDS	ARINC/BuWps	15
Cost Reduction Early Decision Information Techniques (Oct 73)	Hughes Aircraft Co. Culver City, Calif.	15
Routine Reliability and Maintainability Prediction and Analysis	unknown	33
PREDICTORS	R/M Systems, Inc.	34
RELCOMP: A Computer Program for Calculating System Reliability and MTBF	Interstate Electronics Co.	35
BIAS: A Network Analysis Computer Program	Lawrence Radiation Laboratory	36
CROS: Computer Reliability Optimization System	Hoffman Electronics Co.	37
OLSASS: On-Line System Availability and Service Simulation	Aerojet ElectroSystems Co.	38
PATREC: PATtern RECognition Analysis of Fault Trees	Centre d'Etude Nucleaires de Saclay	39
STM: Synthetic Tree Model and DRAFT for automatic generation of Fault Trees	Aerojet Nuclear Co.	40
Computer Program for Approximating System Reliability	Research Triangle Institute	41

ity-maintainability measures can be calculated as desired. Two big advantages of a simulation exercise are:

(1) It forces the designer to consider all aspects of the failure-repair behavior of every element of the system in all possible situations.

(2) It graphically shows the designer the kinds of failure-repair behavior the system typically exhibits.

The simulation example took about 1 man-hour including the calculations with an engineering electronic calculator. Large systems can require man-months of time to set up and hours of run time on large computer installations.

4-5 COMPUTER PROGRAMS

Reliability predictions for complex systems frequently require a large amount of tedious computation. A number of computer programs have been developed for performing reliability predictions. A detailed listing of programs is presented in Table 4-4. Some of them may be proprietary. A check should be made at one's computer installation to determine what programs are available and what ones can be obtained.

REFERENCES

1. M. L. Shooman, *Probabilistic Reliability: An Engineering Approach*, McGraw-Hill Book Co., N.Y., 1968.
2. K. D. Tocher, *The Art of Simulation*, The English Universities Press Ltd., London, 1963.
3. S. J. Ganop, *NASLSIM-3 An Availability Reliability Simulation Program for Scenario Type Missions*, Lab Project 920-72-18, Progress Report 2, U S Naval Applied Science Laboratory, 1968.
4. Abramowitz and Stegun, Eds., *Handbook of Mathematical Functions*, AMS 55, National Bureau of Standards, U S Govt. Printing Office (1972).
5. D. E. Van Tijn, *Description of the Computerized Reliability Analysis Method (CRAM)*, Monograph 11, ARINC Research Corp., Washington, D.C., 1964.
6. I. R. Whiteman, *RESCRIPT — A Computer Programming Language for Reliability*, Presented at Fifth Annual West Coast Reliability Symposium, Los Angeles, California, 1964.
7. Van B. Parr, "Automated Reliability Trade-Off Program — ARTOP II", *Proceedings of the 1967 Annual Symposium on Reliability*, 847-857 (1967).
8. R. B. Coffelt, "Automated System Reliability Prediction", *Proceedings of the 1967 Annual Symposium on Reliability*, 302-4 (1967)
9. J. F. House and John LaCapra, *Systems Reliability Analysis and Prediction Through the Application of a Digital Computer*, Presented at National Symposium on Space Electronics and Telemetry, Miami Beach, Florida, 1962.
10. B. F. Shelley and D. O. Hamilton, "A Mechanized Aircraft Reliability Analysis Model", *Proceedings of the Tenth National Symposium on Reliability and Quality Control*. 560-6 (1964).
11. Charlotte McFaul, *Deep Submergence Rescue Vessel Reliability Prediction*, Technical Memo 415/65, U S Navy MEL, Annapolis, Maryland, 1965.
12. S. A. Weisburg and J. H. Schmidt, "Computer Technique for Estimating System Reliability", *Proceedings of the 1966 Annual Symposium on Reliability*, 87-97 (1966).
13. F. P. Kiefer, et al., "Man-rating the Gemini Launch Vehicle (Crew Hazard and Mission Analysis)", *Proceedings of the 1966 Annual Symposium on Reliability*, 260-8 (1966).
14. R. E. Finch, *An SPS Subroutine as a Simulation Aid*, School of Engineering, Air University, Wright-Patterson AFB. 1963, AD-425 237.
15. *Survey of Studies and Computer Programming Efforts for Reliability, Maintainability, and System Effectiveness*, Report OEM 1, Office of the Director of Defense Research and Engineering, September 1965, AD-622 676.
16. R. O'Bryant, "Variability Prediction — A New Method", *Proceedings of the 1967 Annual Symposium on Reliability*, 181-188 (1967).

17. C. W. McKnight, et al., "An Automatic Reliability Mathematical Model", *Proceedings of the Eleventh National Symposium on Reliability and Quality Control*, 518-32 (1965).
18. A. D. Patton, et al., "Power System Reliability II — Applications and a Computer Program", IEEE Transactions on Power Apparatus and Systems PAS-84, 636 (July 1965).
19. B. H. Hershkowitz, et al., "Reliability Simulation Model", *Proceedings of the Tenth National Symposium on Reliability and Quality Control*, 186-200 (1964).
20. J. M. Hannigan, *A Computer Program for the Simulation of Failure-Responsive Systems*, Technical Report No. 6, Westinghouse Defense and Space Center, 1966, N66-26880.
21. *Reliability Engineering at SBC*, Service Bureau Corporation, Computing Sciences Division, Palo Alto, California, 1966.
22. *A Description of the MARSEP Program — A Mathematica Report*, Mathematica, Inc., Princeton, N.J., July 1969.
23. A. M. Breipohl and R. A. Hernquist, *A Computer Program for Performing Reliability Analyses*, Report SC-TM-65-523, Sandia Laboratory, Albuquerque, New Mexico, December 1965.
24. *Evaluation of Computer Programs for System Performance Effectiveness, Volume II*, RTI Project SU-285, Research Triangle Institute, Research Triangle Park, North Carolina 27709, August 1967.
25. "Computer Tells Launch Vehicle Readiness", *Technology Week* (April 1967).
26. J. Dresner and K. H. Borchers, "Maintenance, Maintainability and System Requirements Engineering", *Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference* (1964).
27. A. M. Economos, "A Monte Carlo Simulation for Maintenance and Reliability", *Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference* (1964).
28. W. E. Faragher and H. S. Watson, "Availability Analyses — A Realistic Methodology", *Proceedings of the Tenth National Symposium on Reliability and Quality Control*, 365-78 (1964).
29. T. J. Horrigan, *Development of Techniques for Prediction of System Effectiveness*, RADC TDR-63-407, Cook Electric Company, February 1964, AD-432 844.
30. "Maintainability Trade-Off Techniques", *Maintainability Bulletin No. 8*, Electronic Industries Association, July 1966.
31. R. K. Ruhe, "Logic Simulation for System Integration and Design Assurance", *Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference* (1964).
32. T. C. Smith, "The Support-Availability Multi-System Operations Model", *Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference* (1964).
33. A. C. Spann, "A Synergistic Reliability and Maintainability Prediction Package", *Proceedings of the 1973 Annual Reliability and Maintainability Symposium*, 542-549 (1973).
34. K. G. Blemel, "Computer Software Synergism Integrates R/M Design", *Proceedings of the 1974 Annual Reliability and Maintainability Symposium*, 68-72 (1974).
35. J. L. Fleming, "Relcomp: A Computer Program for Calculating System Reliability and MTBF", IEEE Trans. Reliability R-20, 102-107 (August 1971).
36. J. L. Willows and W. G. Magnuson, Jr., "Bias: A Network Analysis Computer Program Useful to the Reliability Engineer", IEEE Trans. Reliability R-20, 108-116 (August 1971).
37. A. S. Cici and V. O. Muglia, "Computer Reliability Optimization System", IEEE Trans. Reliability R-20, 110-116 (August 1971).
38. Irving Doshay, "On-Line System Availability and Service Simulation (OL-SASS)", IEEE Trans. Reliability R-20, 142-147 (August 1974).
39. B. V. Koen and A. Camino, "Reliability Calculations with a List Processing Technique", IEEE Trans. Reliability R-23 (April 1974).
40. J. B. Fussell, *Synthetic Tree Models: A Formal Methodology for Fault Tree*

Construction, ANCR-1098, UC-32, Aeroject Nuclear Co., Idaho Falls, Idaho 83401, March 1973.

41. A. C. Nelson, J. R. Batts, R. L. Beadles, "A Computer Program for Approximating System Reliability", IEEE Trans. Reliability R-19, 61-65 (May 1970) and R-20, 88-90 (May 1971).

CHAPTER 5 ALLOCATION OF RELIABILITY REQUIREMENTS

5-0 LIST OF SYMBOLS

AEG = Active Element Group
A_i = availability of a subsystem
A_s = availability of system
C_c = cost constraint (par. 5-2.7.1)
C_k = cost of each unit in stage k $0 < C_k \leq 1$ (Dimensionless)
C'_k = complexity factor for (par. 5-2.5) for subsystem k
g = an effort function (par. 5-2.7.3)
M = number of modules in system
m = minimum number of units to be up for system to be up (par. 5-3.4)
m_k = number of modules or AEG types in subsystem k
N = number of subsystems
n = number of subsystems in series (par. 5-3.2)
$\bar{n}$ = constraint allocation vector (par. 5-2.7.1)
$\bar{n}_{ik}$ = number of type i AEG's in subsystem k
$\bar{n}_k$ = number of extra redundant units in stage k (par. 5-2.7.1)
old = subscript, implies the old system; as opposed to the new system about which calculations are being made.
Q = $1 - R$ (may have same subscript on both R and Q) implies a quantity which is allocated, e.g., see $\bar{\lambda}_k$ and $\bar{R}_k$.
q_k = unreliability for each unit in stage k
r = number of repairment for system (par. 5-3.2)
R_A, R_B, R_{Bi} = s-Reliability of subsystem A or B or of element Bi
r_i = relative failure rate of type i AEG
r'_{ik} = rating (par. 5-2.5) for factor i of subsystem k
$\bar{R}_k$ = s-Reliability allocated to subsystem k
r_{kl} = cost for stage k ($1000)
R_s = system s-reliability requirement
T = mission duration
T_i = defined by Eq. 5-72 (par. 5-2.7.1)
t_k = operating time for subsystem k, $0 < t_k \leq T$
U = $1 - A$ (also used with subscripts)
u_k = utility assigned to subsystem k, $0 < u_k \leq 1$ (dimensionless)
W = relative failure rate of system
W_j = defined by Eq. 5-117
w_k = relative failure rate of subsystem k
w'_k = rating (par. 5-1.2.5) for subsystem k
γ_j = λ_j/μ_j
γ_s = λ/μ for the system
$\bar{\lambda}_k$ = failure rate allocated to subsystem k
λ_s = required system failure rate
μ = repair rate (constant)
ρ = a ratio of new to old failure rates, (see Eq. 5-56)
^ = "hat", used on R (par. 5-2.7.3) to imply state-of-the-art value

5-1 INTRODUCTION

Allocation techniques permit the engineer to assign various effectiveness parameters to individual subsystems by knowing the overall system effectiveness requirement and system design. Several allocation procedures are available for situations such as reliability without repair $R(t)$, reliability with repair $RR(t)$, instantaneous availability $A(t)$, and steady-state availability A_s. The procedure used depends on the effectiveness measure, the extent of knowledge of system design, and whether constraints on cost or other parameters must be considered at the same time.

If the measure selected for the system is reliability without repair, subsystem reliability or failure rate can be assigned directly from the system requirement.

When reliability with repair or instantaneous availability is chosen as the measure of system effectiveness, the allocation procedure depends on the system configuration. For a simple series system with the proper servicing configuration, the system effectiveness measures can be expressed directly as the product of the subsystem measures and the subsystem measures can, in turn, be expressed as a function of subsystem failure and repair rates. For configurations with redundant subsystems, the system level effectiveness measure usually must be computed as a function of subsystem failure and repair rates, using the transition matrix technique described in Chapter 4. In either case the allocation procedures are more complex than those used for allocating reliability without repair.

The allocation process is approximate. The effectiveness parameters apportioned to the subsystems are used as guidelines to determine design feasibility. If the allocated effectiveness parameters 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 and all constraints, and results in subsystems that can be designed within the state of the art.

Of course, sometimes the system goals will have been too optimistic; however, that is a contractual problem—see *Part Five, Contracting for Reliability*—not an allocation problem. Also, another management problem, actually meeting the assigned goals, is not discussed. Some managers assign a small extra reduction to everyone and save the "surplus" to give to those who cannot meet their assigned goals.

5-2 SYSTEMS WITHOUT REPAIR

This situation is reasonably straightforward. The basic idea is to allocate reliability goals to each subsystem so that each subsystem will be equally difficult to design and develop. The following assumptions are made:

(1) All failure rates are constant. Rarely is any other assumption justified this early in the design. If it is, just interpret the failure rate as "mean failure rate for the mission".

(2) Each subsystem is operating, i.e., has a nonzero failure rate, for a time which can be less than the mission duration. No subsystem operates for zero time.

(3) Each subsystem contribution to system failure is weighted by its utility. This implies that the system does not always fail if the subsystem fails. Utility can be considered in two ways:

(a) The mission is composed of tasks. The utility of a subsystem is then the fraction of the mission that is not performed if only that subsystem is not working.

(b) There are varied missions. The utility of a subsystem is then the fraction of missions that fail if only that subsystem is not working. No subsystem has zero utility.

(4) The system complexity is allocated to subsystems on an additive basis. System complexity is normalized to 1, and the sum of the subsystem complexities is the system complexity. Complexity is related to estimated failure proneness of the elements composing a subsystem. Allocation methods differ on their bases of assigning complexity to each subsystem.

(5) System failure rate is a weighted sum of the subsystem failure rates.

These assumptions are consistent with the formula:

$$\lambda_s T = \sum_{k=1}^{N} u_k \bar{\lambda}_k t_k \qquad (5\text{-}1)$$

where

λ_s = required system failure rate, time^{-1}
T = mission duration, time
N = number of subsystems
u_k = utility assigned to subsystem k, $0 < u_k \leq 1$, dimensionless
$\bar{\lambda}_k$ = failure rate allocated to subsystem k, time^{-1}
t_k = operating time of subsystem k, $0 < t_k \leq T$, time

Eq. 5-1 is conventional for s-independent, series systems except for the utility.

The following allocation of failure rate is consistent with Eq. 5-1.

$$\bar{\lambda}_k = \frac{C_k}{(t_k/T)\,u_k}\,\lambda_s \qquad (5\text{-}2)$$

where

C_k = complexity factor of subsystem k,

$$0 < C_k \leq 1, \sum_{k=1}^{N} C_k = 1, \text{ dimensionless}$$

If $\bar{\lambda}_k$ in Eq. 5-2 is substituted in Eq. 5-1, an identity results, which demonstrates that Eq. 5-2 is indeed a solution to Eq. 5-1.

5-2.1 EQUAL ALLOCATION

This is the simplest situation. It arises under the following additional assumptions about the system:

(1) All utilities are 1: $u_k = 1$ for all k
(2) All subsystems operate for the entire mission: $t_k = T$ for all k
(3) Each subsystem is of equal complexity: $C_k = 1/N$ for all k.

Eq. 5-2 becomes

$$\bar{\lambda}_k = (1/N)\lambda_s. \qquad (5\text{-}3)$$

Eq. 5-3 is equivalent to

$$\bar{R}_k = R_s^{\,1/N} \qquad (5\text{-}4)$$

where

$\bar{R}_k$ = s-Reliability allocated to each subsystem
R_s = system s-reliability requirement

When the s-reliability R is near 1, it is often desirable to calculate the s-unreliability Q.

$$Q \equiv 1 - R \qquad (5\text{-}5)$$

It is easier to understand, because it is the probability of failure. Example Problem No. 1 illustrates the application of reliability goals.

5-2.2 PROPORTIONAL COMPLEXITY

When a new system is very similar to an old one, with the exception of a new reliability requirement, Eq. 5-2 can be simplified. The basic assumption is that

$$\frac{C_k}{(t_k/T)u_k} = \frac{\lambda_{k,old}}{\lambda_{s,old}} \qquad (5\text{-}8)$$

where

old = subscript denoting the old system.

Eq. 5-2, when combined with Eq. 5-8, simplifies to

$$\bar{\lambda}_k = \lambda_{k,old}\,\frac{\lambda_s}{\lambda_{s,old}} \qquad (5\text{-}9)$$

Example Problem No. 2 illustrates the procedure.

5-2.3 SIMPLE-MODULAR COMPLEXITY

Each subsystem is presumed to be composed of s-independent modules in series, each of which has the same failure rate. Complexity is taken to be the fraction of modules in the subsystem

$$C_k = m_k/M \qquad (5\text{-}15)$$

where

m_k = number of modules in subsystem k
M = number of modules in the system

Then Eq. 5-2 becomes

$$\bar{\lambda}_k = \frac{(m_k/M)}{(t_k/T)u_k}\,\lambda_s \qquad (5\text{-}16)$$

Example Problem No. 3 illustrates the procedure.

It is possible to calculate subsystem s-reliability, but its meaning is distorted by the utility and operating time factors in Eq. 5-1. It is better not to make the calculation since the proper explanations will be lost too easily, and the results will appear erroneous without the explanations.

Example Problem No. 1

A group of 8 roller bearings is required to have an s-reliability of 0.99 and the conditions of Eqs. 5-3 and 5-4 are assumed to be satisfied. What s-reliability is to be allocated to each bearing?

Procedure	Example	
(1) Set R_s to the required system s-reliability, and N to the number of subsystems. Solve also for Q_s by Eq. 5-5.	$R_s = 0.99$ $N = 8$ $Q_s = 1 - 0.99 = 0.01$	(5-6)
(2) Solve for $\bar{R}_k$ by Eq. 5-4 and $\bar{Q}_k$ by Eq. 5-5.	$\bar{R}_k = (0.99)^{1/8} = 0.99874$ $\bar{Q}_k = 1 - 0.99874 = 0.00126$	(5-7)

Each bearing can have only about 1/8 the failure probability of the whole system. The application of the formulas presumes that bearing failures are s-independent of each other; e.g., failure is not due to a sudden stoppage of lubricating-oil flow to all bearings.

Example Problem No. 2

An old hydraulic power supply must be upgraded to a better failure rate. The characteristics of the old system are given in Columns 1, 2 of Table 5-1, and the conditions for Eq. 5-9 are assumed to be satisfied. The failure rate requirement for the new upgraded system is 200 per 10^6 hr. Allocate this requirement to the subsystems.

Procedure	Example	
(1) Set λ_s and $\lambda_{s,old}$ to the given values.	$\lambda_s = 200$ per 10^6 hr $\lambda_{s,old} = 256$ per 10^6 hr	(5-10)
(2) Calculate $\lambda_s/\lambda_{s,old}$.	$\frac{\lambda_s}{\lambda_{s,old}} = \frac{200 \text{ per } 10^6 \text{ hr}}{256 \text{ per } 10^6 \text{ hr}} = 0.78125$	(5-11)
(3) Fill in column 3, Table 5-1, by Eq. 5-9.	$\bar{\lambda}_1 = (3 \text{ per } 10^6 \text{ hr}) \times 0.78125 = 2.344 \text{ per } 10^6 \text{ hr}$ $\bar{\lambda}_2 = (1 \text{ per } 10^6 \text{ hr}) \times 0.78125 = 0.7813 \text{ per } 10^6 \text{ hr}$ . . . . . . $\bar{\lambda}_{10} = (67 \text{ per } 10^6 \text{ hr}) \times 0.78125 = 52.34 \text{ per } 10^6 \text{ hr}$	(5-12)
(4) Round off the $\bar{\lambda}_k$ to 2 significant figures for Table 5-1; so too much accuracy will not be implied.	$\bar{\lambda}_1 = 2.3$ per 10^6 hr $\bar{\lambda}_2 = 0.78$ per 10^6 hr . . . . . . $\bar{\lambda}_{10} = 52$ per 10^6 hr	(5-13)
(5) Confirm that the sum of allocated failure rates for the new system does not exceed the requirement, i.e., $\Sigma\bar{\lambda}_k \leq 200$. (Units are "per 10^6 hr".)	$\Sigma\bar{\lambda}_k = 2.3 + 0.78 + 59 + 36 + 23 + 20 + 3.1 + 0.78 + 2.3 + 52 = 199.26 \leq 200$	(5-14)

In practice, more attention would be devoted to the pump and starter which together account for over 50% of the system failures, and little if any to the reservoir, strainer, filter, flexible coupling, and manifold which together account for less than 5% of the system failures.

Example Problem No. 3

An early-warning radar has a reliability requirement of 0.90 for a 12-hr mission (Ref. 2). The system is described in Table 5-2, columns 1, 2, 4, and by the following information: if the moving-target indicator is failed (but the rest of the system is operating), then 25% of the targets will be lost in ground clutter. Other subsystems are essential. The mission value is presumed proportional to the number of targets. Allocate the failure rates to each subsystem.

Procedure	Example	
(1) Assign known values.	$R_s = 0.90$, $T = 12$ hr	(5-17)
(2) Determine total number of modules M in system, i.e., $M = \Sigma n_k$.	$M = 256$	(5-18)
(3) Calculate mission failure rate by Eq. 4-3, i.e., $\lambda_s = -(\ln R_s)/T$.	$\lambda_s = -\ln 0.90/12$ hr $= 0.10536/12$ hr $= 8.78/1000$ hr	(5-19)
(4) Fill in column 3, Table 5-2, by Eq. 5-15.	$C_1 = 35/533 = 0.0657$ $C_2 = 91/533 = 0.1707$ . . . . . . $C_5 = 88/533 = 0.1651$	(5-20)
(5) Fill in column 5, Table 5-2, i.e., t_k/T.	$t_1/T = 12/12 = 1.00$ . . . . . . $t_5/T = 6/12 = 0.50$	(5-21)
(6) Fill in column 6, Table 5-2, i.e., u_k. Essential subsystems have a utility of 1. Nonessential subsystems have a utility equal to the fraction of targets lost when that subsystem is failed.	$u_1 = u_2 = u_3 = u_4 = 1$ $u_5 = 0.25$	(5-22)
(7) Fill in column 7, Table 5-2, by Eq. 5-16.	$\bar{\lambda}_1 = \frac{0.0657}{1.00 \times 1.00} \times 8.78$ per 1000 hr $= 0.5769$ per 1000 hr $\bar{\lambda}_2 = \frac{0.1707}{1.00 \times 1.00} \times 8.78$ per 1000 hr $= 1.499$ per 1000 hr . . . . . . $\bar{\lambda}_5 = \frac{0.1651}{0.50 \times 0.25} \times 8.78$ per 1000 hr $= 11.60$ per 1000 hr	(5-23)

(8) Round off $\bar{\lambda}_k$ to 2 significant figures for Table 5-2, column 7; so too much accuracy will not be implied.

$$\left.\begin{array}{l}\bar{\lambda}_1 = 0.58 \text{ per 1000 hr} \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \bar{\lambda}_8 = 12 \text{ per 1000 hr}\end{array}\right\} \tag{5-24}$$

The failure rates in column 7, Table 5-2 do not sum to λ_s = 8.78 per 1000 hr (Eq. 5-19) because of the various weighting factors. To check the calculations, Eq. 5-1 has to be used.

(9) Fill in column 8, Table 5-2, i.e., $u_k \bar{\lambda}_k t_k$.

$$\begin{array}{l}1)\ 1.00 \times (0.58/1000 \text{ hr}) \times 12 \text{ hr} \\ \quad = 0.00696 \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ 5)\ 0.25 \times (12/1000 \text{ hr}) \times 6 \text{ hr} \\ \quad = 0.01800\end{array} \tag{5-25}$$

(10) Sum column 8 by Eq. 5-1.

$$\begin{aligned}\Sigma &= 0.00696 + 0.01800 + 0.1680 \\ &\quad + 0.04560 + 0.01800 \\ &= 0.1054\end{aligned} \tag{5-26}$$

(11) Compare with requirement $\lambda_s T = 8.78 \times 12 = 0.1054$

$$0.1054 < 0.1054 \tag{5-27}$$

The requirement is satisfied to within the accuracy of the problem statement.

TABLE 5-1

FAILURE RATES FOR OLD AND NEW HYDRAULIC SYSTEMS

(1) Subsystem	Failure Rate $\bar{\lambda}_j$, per 10^6 hr (2) Old System	(3) New System
1. Reservoir	3	2.3
2. Strainer	1	0.78
3. Pump	75	59.
4. Motor	46	36.
5. Check Valve	30	23.
6. Relief Valve	26	20.
7. Filter	4	3.1
8. Flexible coupling	1	0.78
9. Manifold	3	2.3
10. Starter	67	52.
Total (System)	256	199.28 < 200

5-2.4 DETAILED COMPLEXITY

Each subsystem is composed of Active Element Groups (AEG) as explained in Ref. 4. The complexity of each subsystem is proportional to the relative failure rate of its AEG's. The AEG's for each subsystem are presumed to be s-independent and in series. A table of relative failure rates is required. Some are given in Appendix A of Ref. 4. Failure rates in Ref. 1 can be adapted to this purpose, as can in-house data. All AEG failure rates must be relative to one reference, e.g., mechanical elements cannot have one reference and electronic parts another reference. In some older explanations of this procedure (Ref. 4), the data are presumed to have several references; all the data must then be normalized to one of the references.

TABLE 5-2. EXAMPLE RADAR SYSTEM DESCRIPTION

(1) Subsystem	(2) Number of Modules n_k	(3) Complexity C_k	(4) Operating Time, hr t_k	(5) Fraction of Operating Time t_k/T	(6) Utility u_k	(7) Allocated Failure Rate, per 1000 hr $\bar{\lambda}_k$	(8) $u_k\bar{\lambda}_k t_k$
1. Power Supply	35	.0657	12	1.00	1.00	0.58	0.00696
2. Transmitter	91	.1707	12	1.00	1.00	1.5	0.01800
3. Receiver	88	.1651	12	1.00	1.00	1.4	0.01680
4. Display and Control	231	.4334	12	1.00	1.00	3.8	0.04560
5. Moving-target Indicator	88	.1651	6	0.50	0.25	12.	0.01800
Total	533	1.0000					0.1054

Mission duration T = 12 hr
Mission s-reliability requirement 0.90

λ_s = 8.78 per 1000 hr
$\lambda_s T$ = 0.1054

The subsystem complexity is

$$C_k = w_k / W \tag{5-28}$$

$$w_k = \sum_{i=1}^{m_k} r_i \, n_{ik} \tag{5-29}$$

$$W = \sum_{k=1}^{N} w_k \tag{5-30}$$

where

n_{ik} = number of type i AEG's in subsystem k
r_i = relative failure rate of type i AEG
w_k = relative failure rate of subsystem k
W = relative failure rate of the system
m_k = number of AEG types in subsystem k

Example Problem No. 4 illustrates the procedure.

5-2.5 FEASIBILITY-OF-OBJECTIVES ALLOCATIONS

This technique adapted from Ref. 5 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 assigned 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 engineer using his engineering know-how and experience. 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 ratings can be selected by individual engineers, or through some form of voting technique among a group of design engineers.

The 4 ratings for each subsystem are multiplied together to give a rating for the subsystem; the subsystem rating will be between 1 and 10^4. The subsystem ratings are then normalized so that their sum is 1. The normalized subsystem rating C'_k is used in place of the factor $C_k/(t_k/T)$ in Eq. 5-2. The utility of each subsystem is considered to be 1. Eqs. 5-1 and 5-2 then become

$$\lambda_s T = \sum_{k=1}^{N} \bar{\lambda}_k T \tag{5-42}$$

$$\bar{\lambda}_k = C'_k \lambda_s \tag{5-43}$$

where

C'_k = complexity of subsystem k

$$C'_k \cong w'_k / W' \tag{5-44}$$

$$w'_k \cong r'_{1k} r'_{2k} \, r'_{3k} \, r'_{4k} \tag{5-45}$$

$$W \cong \sum_{k=1}^{N} w'_k \tag{5-46}$$

Example Problem No. 4

Consider a bombsight system comprising three subsystems: a power supply, navigation computer, and optical equipment. The power supply and the optical equipment are series elements in the reliability model; since both must work for the system to be up, the utility of these subsystems is 1. Since the optical equipment can be controlled manually in the event of navigation computer failure, the navigation computer utility is less than 1. Estimates made on the basis of performance of similar systems indicate that 57 mission failures occur for every 100 missions in which the navigation computer and nothing else failed. Therefore, the utility of the navigation computer is 0.57. The system reliability requirement R_s is 0.94 for 6 hr of system operation. The operating time of the power supply and optical equipment is also 6 hr; that for the navigation computer is 5 hr. Detailed steps for conducting the apportionment follow. The system data are given in Table 5-3, columns 1, 2, 3, 7a, 8.

Procedure	Example	
(1) Assign known values.	$R_s = 0.94$ $T = 6$ hr	(5-31)
(2) Calculate λ_s by Eq. 4-2, i.e., $\lambda_s = -(\ln R_s)/T$.	$\lambda_s = -\ln 0.94/6$ hr $= 10.31$ per 1000 hr	(5-32)
(3) Fill in column 4, Table 5-3, i.e., $r_i n_{ik}$. Round off to 1 decimal place, which is more than enough accuracy.	$r_1 n_{11} = 4.3 \times 40 = 172$ $r_2 n_{21} = 2.2 \times 3 = 6.6$ . . . . . . $r_5 n_{53} = 61 \times 1 = 61$ $r_6 n_{63} = 0.030 \times 3 = 0.1$	(5-33)
(4) Calculate column 5, Table 5-3, by Eq. 5-29.	$w_1 = 172 + 6.6 + 27$ $= 206.6$ $w_2 = 30 + 207 + 77 + 39 + 16 + 192 + 61 + 154 + 0.4$ $= 776.4$ $w_3 = 11 + 5.4 + 1.9 + 9.6 + 61 + 0.1$ $= 89.0$	(5-34)
(5) Calculate W by Eq. 5-30.	$W = 206 + 776 + 89$ $= 1071$	(5-35)
(6) Calculate C_k by Eq. 5-28.	$C_1 = 206/1071 = 0.192$ $C_2 = 776/1071 = 0.725$ $C_3 = 89/1071 = 0.083$	(5-36)
(7) Calculate column 7b, Table 5-3, i.e., t_k/T.	$t_1/T = 6$ hr$/6$ hr $= 1$ $t_2/T = 5$ hr$/6$ hr $= 0.833$ $t_3/T = 6$ hr$/6$ hr $= 1$	(5-37)

(8) Fill in column 8, Table 5-3, utility u_k, from statement of the problem.

$$\left.\begin{aligned} u_1 &= 1 \\ u_2 &= 0.57 \\ u_3 &= 1 \end{aligned}\right\} \qquad (5\text{-}38)$$

(9) Calculate the $\bar{\lambda}_k$ for column 9, Table 5-3, by Eq. 5-2. Round off to 2 significant figures in the table, so too much accuracy will not be implied. Place unrounded values in parentheses for calculating column 10, the check column.

$$\bar{\lambda}_1 = \frac{0.192}{1 \times 1} \times 10.31 \text{ per 1000 hr} = 1.980 \text{ per 1000 hr}$$

$$\bar{\lambda}_2 = \frac{0.725}{0.833 \times 0.57} \times 10.31 \text{ per 1000 hr} = 15.75 \text{ per 1000 hr} \qquad (5\text{-}39)$$

$$\bar{\lambda}_3 = \frac{0.083}{1 \times 1} \times 10.31 \text{ per 1000 hr} = 0.8559 \text{ per 1000 hr}$$

(10) Calculate column 10, Table 5-3, i.e., $u_k \bar{\lambda}_k t_k$.

$$\begin{aligned} u_1 \bar{\lambda}_1 t_1 &= 1 \times (1.980 \text{ per 1000 hr}) \times 6 \text{ hr} \\ &= 0.01188 \\ u_2 \bar{\lambda}_2 t_2 &= 0.57 \times (15.75 \text{ per 1000 hr}) \times 5 \text{ hr} \\ &= 0.04489 \\ u_3 \bar{\lambda}_3 t_3 &= 1 \times (0.8559 \text{ per 1000 hr}) \times 6 \text{ hr} \\ &= 0.00514 \end{aligned} \qquad (5\text{-}40)$$

(11) By Eq. 5-1, the sum of column 10, Table 5-3, ought to be equal to $\lambda_s T$.

$$\begin{aligned} \text{sum} &= 0.01188 + 0.04489 + 0.00514 \\ &= 0.06190 \\ \lambda_s T &= -\ln R_s \\ &= 0.06188 \end{aligned} \qquad (5\text{-}41)$$

The requirement is satisfied within the accuracy of the problem statement.
As in the previous example, in par. 5-2.4, the subsystem s-reliability is not calculated.

TABLE 5-3. BOMBSIGHT-SYSTEM DESCRIPTION

(1) Subsystem and AEG Name	(2) Relative failure rate of AEG r_i	(3a) Number of AEG's in subsystem n_{ik}	(3b) m_k	(4) $r_i n_{ik}$	(5) w_k	(6) C_k	(7a) (hrs) t_k	(7b) t_k/T	(8) u_k	(9) (per 1000 hrs) $\bar{\lambda}_k$	(10) $u_k\bar{\lambda}_k t_k$
1. Power Supply			3		206	0.192	6	1	1	2.0	
a. *Primary power	4.3	40		172						(1.980)	0.01188
b. Relay	2.2	3		6.6							
c. Relay, Stepping	27.	1		27							
2. Navigation Computer			9		776	0.725	5	0.833	0.57	16	
a. *Pulse, low power (tube)	3.0	10		30						(15.75)	0.04489
b. *Pulse, low power (transistor)	0.90	230		207							
c. Synchro. resolver	2.2	35		77							
d. Gyro	39.	1		39							
e. Thermostat	0.64	25		16							
f. Motor	4.8	40		192							
g. Dehydrator	61.	1		61							
h. Relay	2.2	70		154							
i. Counter	0.030	12		0.4							
3. Optical Equipment			6		89	0.083	6	1	1	0.86	
a. Synchro, resolver	2.2	5		11						(0.8559)	0.00514
b. Prism	1.8	3		5.4							
c. Thermostat	0.64	3		1.9							
d. Motor	4.8	2		9.6							
e. Dehydrator	61.	1		61							
f. Counter	0.030	3		0.1							
Total					1071	1.000					0.06190

Mission Reliability, $R_s = 0.94$

Mission Time, $T = 6$ hr

$\lambda_s T = 0.06188$

$\lambda_s = 10.31$ per 1000 hr

*Refers to Electronic Components

where

w'_k = subsystem rating
W = system rating
r'_{ik} = rating for factor i of subsystem k; i = 1 is intricacy, i = 2 is state of the art, i = 3 is performance time, i = 4 is environment.

Example Problem No. 5 illustrates the procedure.

5-2.6 REDUNDANT SYSTEMS

The technique described so far in par. 5-2 can be used to allocate reliability without repair for simple redundant systems consisting of two redundant units. Relationships have been developed for both active and standby redundancy by calculating an equivalent series failure index for the redundant subsystem. Ref. 6 describes the procedure and gives graphs for calculating some of the conversion factors. The Ref. 6 procedure is based on finding a common multiplier for all failure rates—even those in redundant systems. This procedure permits the use of the basic allocation formulas developed for series systems.

Before jumping into the allocation problem for systems that contain redundant elements, the designer must ask himself: "What criterion do I want to use in this allocation?". The allocation in par. 5-2.2, where previous failure rates are known or estimated, finds a common factor $(\lambda_s/\lambda_{s,old})$ with which to multiply all failure rates. If this factor is applied to all elements in a subsystem that contains redundancy, the system failure rate will be too low.

The Example Problem No. 6 and Table 5-5 illustrate the situation. The formulas for calculation, and the notation are:

$$R_s = R_A R_B \quad (5\text{-}52)$$
$$R_B = 1 - (1 - R_{Bi})^2 \quad (5\text{-}53)$$
$$R_{Bi} = 1 - (1 - R_B)^{1/2} \quad (5\text{-}54)$$
$$R = \exp(-\lambda T) \quad (5\text{-}55a)$$
$$\lambda T = -\ln R \quad (5\text{-}55b)$$
$$\rho = (\lambda T)_{new}/(\lambda T)_{old} \quad (5\text{-}56)$$

where

s = subscript denoting system
A,B = subscripts denoting subsystems A,B
Bi = subscript denoting elements Bi i = 1,2 (viz., $B1,B2$)
R = s-Reliability
λ = failure rate of an element, or mean failure rate for B and s (over mission time T)
T = mission time
λT = s-Expected number of failures during the mission; i.e., the fraction of times the item will fail, when a great many missions are considered.

Eqs. 5-52, 5-53, and 5-54, where subscripts are shown, are true only for those subscripts; Eqs. 5-55 and 5-56 are always true.

5-2.7 REDUNDANT SYSTEMS WITH CONSTRAINTS

A project engineer frequently must commit large sums of money for the development and procurement of large and complex weapon systems (Ref. 6). These procurements often must take place within severe time and budget limitations. Although the budget limitations may place very severe restrictions upon the final system configuration, the project engineer is under pressure to deliver a system that has high performance for a given cost and satisfies operational requirements. This paragraph considers several methods of achieving maximum system reliability for a given set of constraints. Since weapon systems are complex, the interrelationships among system design characteristics often are not obvious; therefore, a methodical approach to design optimization is required.

The allocation methods described in this paragraph offer the engineer a set of convenient tools that are relatively easy to apply. They are algebraic in nature and can be solved using a slide rule. However, these techniques cannot be applied to the more complex problem of designing an optimal system in the face of constraints.

Example Problem No. 5

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 hr 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 5-4, columns 1-5. Compute the allocated failure rate for each subsystem.

Procedure	Example	
(1) Compute the product of the ratings r'_j for each subsystem and their sums—i.e., fill in column 6, Table 5-4—by Eqs. 5-45 and 5-46.	$w'_1 = 5 \times 6 \times 5 \times 5$ $= 750$ . . . . . . $w'_6 = 6 \times 5 \times 5 \times 5$ $= 750$ $W' = 750 + 840 + 2500 + 2240$ $+ 640 + 750$ $= 7720$	(5-47)
(2) Compute the complexity factors C'_k for each subsystem—i.e., fill in column 7, Table 5-4—by Eq. 5-44.	$C'_1 = 750/7720$ $= 0.097$ . . . . . . $C'_6 = 750/7720$ $= 0.097$	(5-48)
(3) Compute system failure rate λ_s from system specifications by Eq. 4-3; $R_s = 0.90$ and $T = 120$ hr.	$\lambda_s = -\ln 0.90/120$ hr $= 878.0$ per 10^6 hr	(5-49)
(4) Compute the allocated subsystem failure rate $\bar{\lambda}_k$—i.e., fill in column 8, Table 5-4—by Eq. 5-43.	$\bar{\lambda}_1 = 0.097 \times (878.0$ per 10^6 hr$)$ $= 85.17$ per 10^6 hr $\bar{\lambda}_2 = 0.109 \times (878.0$ per 10^6 hr$)$ . . . . . . $\bar{\lambda}_6 = 0.097 \times (878.0$ per 10^6 hr$)$ $= 85.17$ per 10^6 hr	(5-50)
(5) Round off failure rates $\bar{\lambda}_k$ to 2 significant figures, so that too much accuracy will not be implied; sum and compare with λ_s Eq. 5-49.	$\Sigma = 85 + 96 + 280 + 250 + 73 + 85$ $= 869 < 878$	(5-51)

TABLE 5-4. MECHANICAL-ELECTRICAL SYSTEM

(1) Subsystem	(2) Intricacy r_1'	(3) State-of-the-art r_2'	(4) Performance time r_3'	(5) Environment r_4'	(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	280
4. Flight Control	8	8	5	7	2240	.290	250
5. Structure	4	2	10	8	640	.083	73
6. Auxiliary Power	6	5	5	5	750	.097	85
Total					7720	1.000	869

System s-reliability = 0.90

Mission Time = 120 hours

λ_s = 878 per 10^6 hours

Example Problem No. 6

SYSTEM: OLD

Procedure	Example	
(1) State the given quantities.	$(\lambda T)_A = 0.0500$ $(\lambda T)_B = 0.0500$	(5-57)
(2) Calculate the remainder of the columns of Table 5-5.		
Use Eq. 5-55a for R_A.	$R_A = \exp(-0.05) = 0.9512$	
Use Eq. 5-55a for R_B.	$R_B = \exp(-0.05) = 0.9512$	
Use Eq. 5-52 for R_s.	$R_s = 0.9512 \times 0.9512 = 0.9048$	
Use Eq. 5-54 for R_{Bi}.	$R_{Bi} = 1 - (1 - 0.9512)^{1/2} = 0.7792$	
Use Eq. 5-55b for $(\lambda T)_{Bi}$.	$(\lambda T)_{Bi} = -\ln 0.7792 = 0.2495$	
Use Eq. 5-55b for $(\lambda T)_s$.	$(\lambda T)_s = -\ln 0.9048 = 0.1000$	(5-58)

SYSTEM: NEW NO. 1

(1) State the given quantities.	$(\lambda T)_A = 0.0500/2 = 0.0250$ $(\lambda T)_{Bi} = 0.2495/2 = 0.1248$	(5-59)
(2) Calculate the remainder of the columns of Table 5-5.		
Use Eq. 5-55a for R_{Bi}.	$R_{Bi} = \exp(-0.1248) = 0.8827$	
Use Eq. 5-53 for R_B.	$R_B = 1 - (1 - 0.8827)^{1/2} = 0.9862$	
Use Eq. 5-55a for R_A.	$R_A = \exp(-0.025) = 0.9753$	
Use Eq. 5-52 for R_s.	$R_s = 0.9753 \times 0.9862 = 0.9618$	
Use Eq. 5-55b for $(\lambda T)_s$.	$(\lambda T)_{Bi} = -\ln 0.9618 = 0.0389$	(5-60)
Use Eq. 5-55b for $(\lambda T)_B$.	$(\lambda T)_B = -\ln 0.9862 = 0.0139$	
Use Eq. 5-56 for ρ and round off to 2 significant figures.	$\rho_s = 0.0389/0.1 = 0.39$ $\rho_{Bi} = 0.1248/0.2495 = 0.50$	

SYSTEM: NEW NO. 2

(1) State the given quantities.	$(\lambda T)_A = 0.0500/2 = 0.0250$ $(\lambda T)_B = 0.0500/2 = 0.0250$	(5-61)
(2) Calculate the remainder of the columns of Table 5-5.		
Use Eq. 5-55a for R_A.	$R_A = \exp(-0.0250) = 0.9753$	
Use Eq. 5-55a for R_B.	$R_B = \exp(-0.0250) = 0.9753$	
Use Eq. 5-52 for R_s.	$R_s = 0.9753 \times 0.9753 = 0.9512$	
Use Eq. 5-54 for R_{Bi}.	$R_{Bi} = 1 - (1 - 0.9753)^{1/2} = 0.8429$	
Use Eq. 5-55b for $(\lambda T)_s$.	$(\lambda T)_s = -\ln 0.9512 = 0.0500$	
Use Eq. 5-55b for $(\lambda T)_{Bi}$.	$(\lambda T)_{Bi} = -\ln 0.8429 = 0.1709$	(5-62)
Use Eq. 5-56 for ρ and round off to 2 significant figures.	$\rho_s = 0.0500/0.1 = 0.50$ . . . . . . $\rho_{Bi} = 0.1709/0.2495 = 0.68$	

The analysis that follows uses the tabulation in Table 5-5.

The factor λT is the s-expected number of failures in a mission. In the old system, those failures are evenly split between A and B. The elements $B1$ and $B2$ have 5 times the failures that A has,

In New No. 1, the failure rates for the elements have been equally improved, by design. Now A has 2 times the failures of B, i.e., B has been improved more than A has.

In New No. 2, the failure rates for the subsystems have been equally improved, by design. The system failures are evenly split between A and B, as in the old system; however, $B1$, $B2$ only needed their failure rates reduced to 68% of the old value, while A needed its failure rate reduced to 50% of its old value.

The degree of imbalance depends on the kind of system and the numbers chosen for illustration, but the principle remains: there is no one "right" way to allocate reliability improvement to elements of redundant systems.

A quick-and-dirty method of allocating reliability improvement is to apply the system improvement factor to each element, as in par. 5-2.2. The new system will then be better than needed. Take this "bonus" and allocate it to the series subsystems that appear least capable of meeting the improvement goals. With the widespread use of engineering calculators for small systems and computerized calculations for large systems, the trial-and-error method proposed here is quick (no special formulas are needed) and is good enough.

The quick-and-dirty method will be illustrated for the system in Table 5-5. Suppose the system is to have its failure rate halved.

SYSTEM: NEW NO. 3 ("Quick and Dirty" Allocation)

(1) State system failure reduction.

$$\left.\begin{aligned} \rho_s &= 0.50 \\ (\lambda T)_s &= 0.1000 \times 0.50 \\ &= 0.0500 \end{aligned}\right\} \qquad (5\text{-}63)$$

(2) Apply the reduction factor to each element of the system as described in the steps that follow.

See, System: New No. 1

(3) Find the surplus failures, i.e.,

$$(\lambda T)_{new\ No.3} - (\lambda T)_{new\ No.1} \qquad (5\text{-}64)$$

$$0.0500 - 0.0389 = 0.0111 \qquad (5\text{-}64)$$

(4) Decide on the basis of difficulty of meeting goals, i.e., where to allocate the surplus failures. Assume the element $B1$ and $B2$ will be difficult to improve; accordingly, give B about 2/3 and A about 1/3.

$$\left.\begin{aligned} \text{extra for } B &= 0.0111 \times (2/3) \\ &= 0.0074 \\ \text{extra for } A &= 0.0111 \times (1/3) \\ &= 0.0037 \\ (\lambda T)_B &= 0.0139 + 0.0074 \\ &= 0.0213 \\ (\lambda T)_A &= 0.0250 + 0.0037 \\ &= 0.0287 \end{aligned}\right\} \qquad (5\text{-}65)$$

(5) Calculate the remainder of the columns in Table 5-5.

Use Eq. 5-55a for R_A.	$R_A = \exp(-0.0287) = 0.9717$	
Use Eq. 5-55a for R_B.	$R_B = \exp(-0.0213) = 0.9789$	
Use Eq. 5-52 for R_s.	$R_s = 0.9717 \times 0.9789 = 0.9512$	
Use Eq. 5-55b for $(\lambda T)_s$.	$(\lambda T)_s = -\ln 0.9512 = 0.0500$	
Use Eq. 5-54 for R_{Bi}.	$R_{Bi} = 1 - (1 - 0.9789)^{1/2} = 0.8548$	(5-66)
	$(\lambda T)_{Bi} = -\ln 0.8548 = 0.1569$	
Use Eq. 5-55b for $(\lambda T)_{Bi}$.	$\rho_s = 0.0500/0.1000 = 0.50$	
Use Eq. 5-58 for ρ and round off to 2 significant figures.	. .	
	. .	
	. .	
	$\rho_{Bi} = 0.1569/0.2495 = 0.63$	

The problem has been "solved"; no complicated charts or theory had to be used; and the results look reasonable. $B1$ and $B2$ require less improvement than does A, and the system goal of 50% reduction in λT was met.

Whenever redundancy is involved in a subsystem, that subsystem will not have a constant failure rate, nor will the system. The allocations of λT (or of λ) then depend somewhat on mission time. This is another reason why it rarely pays to use anything but quick-and-dirty methods of allocation. In very large system, the calculations will be long and tedious, but the principles on which the calculation are based ought to be simple.

TABLE 5-5. COMPARISON OF IMPROVEMENT STRATEGIES

NAME			OLD		NEW #1			NEW #2			NEW #3		
system s	sub-system	elements	λT	R	λT	R	ρ	λT	R	ρ	λT	R	ρ
			.1000	.9048	.0389	.9618	.39	.0500	.9512	.50	.0500	.9512	.50
	A	A	.0500	.9512	.0250	.9753	.50	.0250	.9753	.50	.0287	.9717	.57
	B		.0500	.9512	.0139	.9862	.28	.0250	.9753	.50	.0213	.9789	.43
		B1	.2495	.7792	.1248	.8827	.50	.1709	.8429	.68	.1569	.8548	.63
		B2	.2495	.7792	.1248	.8827	.50	.1709	.8429	.68	.1569	.8548	.63

New #1: $\lambda_{new} = \frac{1}{2}\lambda_{old}$ for the elements
New #2: $\lambda_{new} = \frac{1}{2}\lambda_{old}$ for the subsystems

System s has 2 subsystems A,B in series.
Subsystem B has 2 elements, B1, B2 in active (hot) parallel redundancy.
Subsystem A has 1 element, itself.

$R \equiv \exp(-\lambda T)$

where

$R \equiv$ reliability of the item
$\lambda T \equiv -\ln R$, the expected number of failures for the mission
$\lambda \equiv$ an equivalent failure rate for the mission time T
$\rho \equiv (\lambda T)_{new}/(\lambda T)_{old} = \lambda_{new}/\lambda_{old}$

A number of different optimization techniques are available that work well for many different types of problems. The methods are general; however, only a limited number of variables will be considered, permitting the use of simple examples. Also, from a practical point of view, limiting the analysis to a few variables results in mathematically tractable problems whose results can be visualized by the engineer.

An allocation of subsystem reliability with constraints requires the existence of data or formulas that relate the constrained variables to reliability, i.e., the cost (or weight, etc.) of system alternatives of different reliabilities must be computable. This is usually the area of greatest uncertainty in system design, and the cost data frequently are obtained by means of a rough guess. Although the techniques described are general, the engineer must keep in mind the fact that the results produced are very sensitive to the quality of the input data.

5-2.7.1 Simple Redundancy Allocation With a Single Constraint

As the complexity of weapon systems increases, their reliabilities tend to decrease. One method for coping with this problem is to design reliable systems using less reliable subsystems in redundant configurations.

The simple technique in this paragraph describes a method for maximizing system reliability subject to a single constraint such as cost; it also can be extended to multiple constraints. An abundant literature has been developed that describes the techniques used for redundancy allocation, such as Lagrange multipliers and dynamic programming.

Example Problem No. 7 illustrates the procedure (Refs. 7 to 23).

5-2.7.2 Dynamic Programming Allocation

Dynamic programming allocation (Ref. 10) is another useful procedure when system reliability must be allocated to the subsystems in the face of constraints on such factors as weight and cost. The dynamic programming approach can be most useful because it can be implemented with a simple algorithm that consists of only arithmetic operations. Some advantages of the dynamic programming approach are:

(1) Large problems can be solved with a minimum number of calculations (this "minimum" may be very large for a complex system).

(2) There is always a finite number of steps required in computing an optimum solution.

(3) There are no restrictions of any kind on the form of the functional expressions for computing reliability or the form of the cost estimating equations. Nonlinear functions can be used if required.

The dynamic programming algorithms provide a guide through the maze of possible alternate calculations that may arise when big systems are being analyzed. The dynamic programming approach also can be applied to the problem of reliability optimization of redundant systems with repair. The use of the dynamic programming algorithm does not in any way remove the requirement for computing the reliability and cost for each system configuration. However, it minimizes the total number of calculations by rejecting those configurations that would result in a decreasing reliability or in costs exceeding the cost constraints, etc.

Many algorithms can be developed to solve dynamic programming problems. Generally, the algorithm chosen should be the one that is more efficient, i.e., finds the solution with the least number of iterations. For any reasonably large system a large number of calculations are required; therefore, the engineer must consider using the computer and should consult the system programmers to find what programs are readily available.

5-2.7.3 Minimization of Effort Algorithm

The minimization of effort algorithm technique (Ref. 24) can be used to allocate reliability requirements to the subsystems in a way that minimizes the engineering design effort (cost, man-hours, etc.) required to achieve overall system reliability. We are not applying a constraint to cost by merely trying

Example Problem No. 7

A system consists of four subsystems (called stages) whose reliabilities and costs are known. The overall system reliability of 0.357 is completely unacceptable for a new application in which at least 0.99 is required. One approach to achieving the system requirement is to add active redundant units until the new reliability requirement is satisfied. Unfortunately, a cost constraint of $27,000 has been established. What system configuration maximizes system reliability and satisfies this constraint?

Procedure	Example	
(1) State the system reliability requirement.	$R_s = 0.99$	(5-67)
(2) State the cost restraint.	$C_c = \$27{,}000$	(5-68)
(3) Tabulate the predicted cost, reliability, and unreliability of each subsystem (stage).	See Table 5-6.	
(4) Define a vector $\vec{n} = (n_1, n_2, ..., n_n)$ which is called the constraint vector where n_i = number of (extra) redundant units in stage i.	$\vec{n} = (n_1, n_2, n_3, n_4)$	(5-69)
(5) Define the cheapest allocation vector, i.e., the one with no redundancy.	$\vec{n}_0 = (0, 0, 0, 0)$	(5-70)
(6) Add a single redundant unit to each stage in succession, generating four new systems each of which has a single redundant unit in one stage. Compute the allocation vector for each.	$\vec{n}_1 = (1, 0, 0, 0)$ $\vec{n}_2 = (0, 1, 0, 0)$ $\vec{n}_3 = (0, 0, 1, 0)$ $\vec{n}_4 = (0, 0, 0, 1)$	(5-71)
(7) For each new system compute the term: $T_i = \left(\frac{1}{C_{i1}}\right)\ln\left(\frac{1 - Q_i^{n+1}}{1 - Q_i}\right)$ (5-72)	$T_1 = \left(\frac{1}{1.2}\right)\ln\left(\frac{1 - 0.2^2}{1 - 0.2}\right) = 0.1494$ $T_2 = \left(\frac{1}{2.3}\right)\ln\left(\frac{1 - 0.3^2}{1 - 0.3}\right) = 0.1141$ $T_3 = \left(\frac{1}{3.4}\right)\ln\left(\frac{1 - 0.25^2}{1 - 0.25}\right) = 0.0656$ $T_4 = \left(\frac{1}{4.5}\right)\ln\left(\frac{1 - 0.15^2}{1 - 0.15}\right) = 0.0311$	(5-73)
(8) Since the first term T_1 is the largest, add a redundant unit in stage 1 and write the allocation vector.	$\vec{n} = (1, 0, 0, 0)$	(5-74)
(9) Compute the system reliability and cost for this new system: $R_s = (2R_1 - R_1^2)R_2 R_3 R_4$ (5-75)	$R_s = (2 \times 0.80 - 0.80^2) \times 0.7 \times 0.75 \times 0.85 = 0.428$	(5-77)
$C_s = 2C_1 + C_2 + C_3 + C_4$ (5-76)	$C_s = 2 \times 1200 + 2300 + 3400 + 4500 = \$12{,}600$	(5-78)

where

C_{i1} = cost of each unit in stage i
Q_i = unreliability of each unit in stage i
n = number of redundant units in stage i
$n + 1$ = total number of units in stage i.

(10) Repeat Steps (6) and (7) until a system that satisfies reliability requirement and cost restraint is obtained. If the cost restraint is exceeded at $R_s = 0.99$, then select the system that yields the highest R_s within the cost constraint. In this example, the computations are repeated until systems represented by the following redundancy allocation vectors are obtained:

$$\vec{n}_{s1} = (2, 2, 1, 1) \tag{5-79}$$

$$\vec{n}_{s2} = (2, 2, 2, 1) \tag{5-80}$$

(11) Compute system reliability and cost for each of these systems:

$$R_{s1} = [1 - (1 - R_1)^3][1 - (1 - R_2)^3] \times [1 - (1 - R_3)^2][1 - (1 - R_4)^2] \tag{5-81}$$

$$C_{s1} = 3C_1 + 3C_2 + 2C_3 + 2C_4 \tag{5-82}$$

$$R_{s2} = [1 - (1 - R_1)^3][1 - (1 - R_2)^3] \times [1 - (1 - R_3)^2][1 - (1 - R_4)^2] \tag{5-83}$$

$$C_{s2} = 3C_1 + 3C_2 + 3C_3 + 2C_4 \tag{5-84}$$

$$R_{s1} = 0.8345 \tag{5-85}$$

$$C_{s1} = \$26,600 \tag{5-86}$$

$$R_{s2} = 0.9288 \tag{5-87}$$

$$C_{s2} = \$29,700 \tag{5-88}$$

The system represented by the redundancy allocation vector $\vec{n}_{s2} = (2, 2, 2, 1)$ exceeds the cost constraint. The system represented by the vector $\vec{n}_{s1}$ satisfies the cost constraint; however, the system reliability falls far short of the 0.99 required. The technique of redundancy allocation is not sufficient, and a reliability improvement program would be required.

TABLE 5-6

COST AND RELIABILITY DATA ASSOCIATED WITH EXAMPLE PROBLEM NO. 7

STAGE	Cost ($1000)	RELIABILITY	UNRELIABILITY
1	$C_{11} = 1.2$	0.80	$Q_1 = 0.20$
2	$C_{21} = 2.3$	0.70	$Q_2 = 0.30$
3	$C_{31} = 3.4$	0.75	$Q_3 = 0.25$
4	$C_{41} = 4.5$	0.85	$Q_4 = 0.15$

to minimize it. This technique is useful because the function that relates engineering effort in terms of man-hours or cost to reliability need not be known exactly—but it must obey certain basic assumptions. The technique is outlined in the paragraphs that follow.

A system consists of n subsystems, which are in series for reliability purposes. The state-of-the-art system reliability $\hat{R}_s(t)$ is

$$\hat{R}_s(t) = \hat{R}_1(t) \cdot \hat{R}_2(t) \cdots \cdot \hat{R}_n(t) \quad (5\text{-}89)$$

The system must be redesigned to satisfy a new reliability goal $R_s(t)$, where $R_s(t) < \hat{R}_s(t)$. What reliabilities must be allocated to the subsystems so that the new system reliability is achieved and the overall design effort is minimized?

The design effort is expressed in terms of an effort function $g_s(R_s, \hat{R}_s)$:

$$g_s(R_s, \hat{R}_s) = \sum_{i=1}^{n} g(\bar{R}_i, \hat{R}_i) \quad (5\text{-}90)$$

Where the super bar denotes "allocated value". Each individual subsystem effort function is a function of its state-of-the-art reliability $\hat{R}_i$ and allocated reliability $\bar{R}_i$. The required system reliability $R_s(t)$ is equal to the product of the allocated subsystem reliabilities $\bar{R}_i(t)$:

$$\bar{R}_1(t) \cdot \bar{R}_2(t) \cdot \bar{R}_3(t) \cdots \cdot \bar{R}_n(t) \geq R_s(t) \quad (5\text{-}91)$$

The effort function must obey the following assumptions:

(1) $g(\bar{R}_i, \hat{R}_i) \geq 0$ (5-92)

(2) $g(\bar{R}_i, \hat{R}_i)$ is nonincreasing in $\hat{R}_i$ for fixed $\bar{R}_i$ and nonincreasing in $\bar{R}_i$ for fixed $\hat{R}_i$.

(3) $g(\bar{R}_i, \bar{R}_i) + g(\bar{R}_i, \hat{R}'_i) = g(\bar{R}_i, \hat{R}'_i)$ (5-93) where $\bar{R}_i < \hat{R}_i < \hat{R}'_i$

(4) $g(0, \bar{R}_i)$ has a derivative $h(\bar{R}_i)$ such that $\bar{R}_i h(\bar{R}_i)$ is strictly increasing in the interval $0 < \bar{R}_i < 1$.

The procedure is illustrated by means of the Example Problem No. 8.

5-3 SYSTEMS WITH REPAIR

For repairable systems, the subsystems effectiveness parameters (reliability, availability, MTTF) cannot be derived directly from the system level parameters. Instead, a set of subsystem failure and repair rates is assumed, and the system level effectiveness parameter is computed. The computed result is compared with the requirement, and the subsystem failure and repair rates are modified. This process is repeated until the system requirement is satisfied.

The system effectiveness requirement can be satisfied with a large number of different sets of subsystem failure and repair rates (all transition rates are presumed to be constant). Therefore, engineering judgment must be used to narrow the choice of values. It is also possible to trade off failure rates, repair rates, maintenance strategies, and costs in achieving the system requirement. The problem of allocating subsystem parameters is really a problem of trade-offs.

5-3.1 AN ELEMENTARY APPROACH TO STEADY-STATE AVAILABILITY

The elementary problem discussed here illustrates the way in which subsystem failure and repair rates can be allocated to satisfy a system availability requirement. Consider a single unit whose required steady-state availability A_s is specified.

Example Problem No. 8

A system consists of three s-independent subsystems, A, B, C, all of which must function without failure in order to achieve system success. The predicted subsystem reliabilities are $R_A = 0.90$, $R_B = 0.80$, and $R_C = 0.85$, which results in a system reliability of 0.613. A system reliability requirement of 0.70 is established. Allocate reliability to each subsystem in a manner that minimizes the total engineering effort. For simplicity, assume identical effort functions for the three subsystems.

Procedure	Example	
(1) State the system reliability requirements and the number of subsystems.	$R_s(t) = 0.70$, $n = 3$	(5-94)
(2) Arrange the subsystem predicted reliabilities in ascending order.	$R_B(t) = 0.80$, $R_C(t) = 0.85$, $R_A(t) = 0.90$	(5-95)
(3) Allow the subscripts of the predicted reliabilities to take on the following values: B = 1, C = 2, A = 3 and rewrite the reliabilities.	$R_1(t) = 0.80$, $R_2(t) = 0.85$, $R_3(t) = 0.90$	(5-96)
(4) Compute the series of terms: $r_j(t) = \left[\dfrac{R_s(t)}{\prod_{i=j+1}^{n+1} \hat{R}_j(t)}\right]^{1/j}, j = 1, 2, 3$ (5-97)	$r_1(t) = \left(\dfrac{0.70}{0.85 \times 0.90 \times 1.0}\right)^1 = 0.915$; $r_2(t) = \left(\dfrac{0.70}{0.90 \times 1.0}\right)^{1/2} = 0.882$; $r_3(t) = \left(\dfrac{0.70}{1.0}\right)^{1/3} = 0.888$	(5-99)

where

$$R_{n+1}(t) = 1 \qquad (5\text{-}98)$$

(5) Compare the following pairs of values:		
$R_1(t), r_1(t)$	$0.80 < 0.915$	
$R_2(t), r_2(t)$	$0.85 < 0.882$	
$R_3(t), r_3(t)$	$0.90 > 0.888$	
(6) Define the largest subscript j such that: $\hat{R}_j(t) < r_j(t)$ (5-100)	$j = 2$, because 2 is the largest subscript for which $\hat{R}_j(t) < r_j(t)$.	
(7) The allocated subsystem reliabilities $\bar{R}_A(t)$, $\bar{R}_B(t)$, and $\bar{R}_C(t)$ are:		
$\bar{R}_A(t) = 0.90$ (unchanged), $\bar{R}_B(t) = \bar{R}_1(t) = r_2(t)$, $\bar{R}_C(t) = \bar{R}_2(t) = r_2(t)$	(5-101)	$\bar{R}_A(t) = 0.90$, $\bar{R}_B(t) = 0.882$, $\bar{R}_C(t) = 0.882$ (5-102)
(8) Check the allocation: $\bar{R}_s(t) = R_A(t) \cdot \bar{R}_B(t) \cdot \bar{R}_C(t)$ (5-103)		$\bar{R}_s(t) = 0.90 \times 0.882 \times 0.882 = 0.700$ (5-104)

$$A_s = \frac{\mu}{\mu + \lambda} = \frac{1}{1 + (\lambda/\mu)} \qquad (5\text{-}105)$$

where

λ = unit failure rate (constant), and
μ = unit repair rate (constant).

A given availability (Fig. 5-1) can be achieved by any combination of failure rate and repair rate that gives the same ratio, i.e., λ and μ can assume any value provided the ratio is fixed to give the required availability. Availability can be increased by decreasing the failure rate or increasing the repair rate. Constraints can be applied to λ, or μ, or both. If costs can be related to λ and μ, a relatively complex trade-off must be performed, even for a simple 1-unit system.

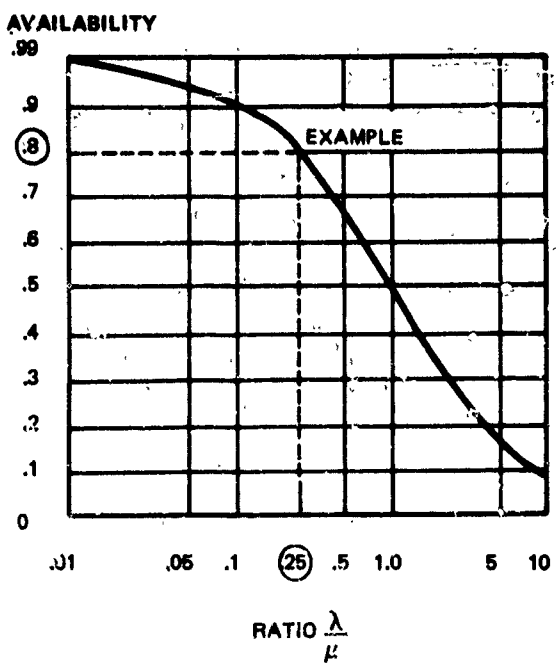


FIGURE 5-1. Steady-state Availability vs the Ratio of Failure Rate to Repair Rate[26]

5-3.2 FAILURE RATE AND REPAIR RATE ALLOCATION FOR SERIES SYSTEMS

Several cases can be considered:

(1) A single repairman must repair any one of n identical, s-independent subsystems in series. The ratio of failure rate to repair rate is such that there is a strong possibility that a second subsystem will fail while the first one is being repaired.

(2) Same as (1) except a repairman is assigned to each subsystem and can only work on that particular subsystem.

(3) Same as (1) except some intermediate number of repairmen r less than the number of subsystems is assigned. Any repairman can work on any system.

(4) Repeat cases (1)-(3) with nonidentical subsystems.

The steady-state availability in Case (1) is:

$$A_s = \frac{\left(\frac{\mu}{\lambda}\right)^n}{n! \sum_{j=0}^{n} \frac{\left(\frac{\mu}{\lambda}\right)^j}{j!}} \qquad (5\text{-}106)$$

where

μ = subsystem repair rate
λ = subsystem failure rate
n = number of subsystems in series.

For example, if $n = 4$ and $A_s = 0.90$, the allocation equation becomes:

$$0.90 = \frac{\left(\frac{\mu}{\lambda}\right)^4}{24\left[1 + \left(\frac{\mu}{\lambda}\right) + \frac{1}{2}\left(\frac{\mu}{\lambda}\right)^2 + \frac{1}{6}\left(\frac{\mu}{\lambda}\right)^3 + \frac{1}{24}\left(\frac{\mu}{\lambda}\right)^4\right]} \qquad (5\text{-}107)$$

$\mu/\lambda = 38.9$

The complexities of allocating failure and repair rates for even simple cases are apparent. If the subsystems are not identical, the allocation must be solved using the state matrix approach to compute availability.

Case (2) represents the situation in which a repairman is assigned to each subsystem. It is equivalent to the condition in which $\mu/\lambda >> 1$, i.e., failure rate is much smaller than repair rate. Since this is true of many systems, a wide variety of practical problems can be solved.

The steady-state availability of a series system of n identical, s-independent subsystems is

$$A_s = A_i^n = \left[\frac{1}{1+(\mu/\lambda)}\right]^n \qquad (5\text{-}108)$$

where

A_s = system steady-state availability
A_i = subsystem availability
n = number of subsystems

Example Problem No. 9 illustrates the procedure.

5-3.3 A SIMPLE TECHNIQUE FOR ALLOCATING STEADY-STATE AVAILABILITY TO SERIES SYSTEMS

A procedure similar to the method in par. 5-2.2 for allocating reliability without repair can be used when the ratio $\gamma_j \equiv \lambda_j/\mu_j < 0.1$ for subsystem j, for all j. The accuracy of the method increases as γ_j decreases. The availability of a series system with subsystems whose failures and repairs are all s-independent is:

$$A_s = \frac{1}{1+\sum_{j=1}^{N}\gamma_j} \qquad (5\text{-}115)$$

where

γ_j = ratio for subsystem j with all $\gamma_j < 0.1$
n = number of subsystems in series

The system γ_s:

$$\gamma_{s,old} = \gamma_1 + \gamma_2 + \cdots + \gamma_n \qquad (5\text{-}116)$$

A relative weighting factor W_j can be computed from:

$$W_j = \gamma_j/\gamma_{s,old} \qquad (5\text{-}117)$$

The new system is similar in design to the old, and the relative weighting factors are the same for each new subsystem.

Example Problem No. 10 illustrates the procedure.

5-3.4 FAILURE AND REPAIR RATE ALLOCATIONS FOR REDUNDANT SYSTEMS

A system comprising several stages of redundant subsystems whose λ/μ ratio is less than 0.1 can be treated as if the stages were s-independent. The system steady-state availability A_s is

$$A_s = A_1 \cdot A_2 \cdot A_3 \cdot \cdots \cdot A_n \qquad (5\text{-}131)$$

where

A_j = the availability of stage j.

This is equivalent to treating each stage as if it had a repairman assigned to it. It is also equivalent to saying that a single repairman is assigned to the system, but that the probability of a second failure occurring while the first is being repaired is very small. If the stages are not s-independent, the system availability must be computed by the state matrix approach. In either case, the system requirement can be obtained with a range of failure and repair rates. Trade-off procedures must be used to determine the best set of these parameters.

The availability of a system of n identical units where at least m of n must be operating for the system to be operating is:

$$A_s = \sum_{j=m}^{n}\binom{n}{j}\left(\frac{\mu}{\lambda+\mu}\right)^j\left(\frac{\mu}{\lambda+\mu}\right)^{n-j}$$

$$= \frac{1}{(\lambda+\mu)^n}\sum_{j=m}^{n}\binom{n}{j}\mu^j\lambda^{n-j} \qquad (5\text{-}132)$$

where

μ = unit repair rate (constant)
λ = unit failure rate (constant)
n = total number of units
m = minimum number of units which must be up for the system to be up.

Availabilities can be computed as a function of repair rate to failure rate ratios for systems of up to five redundant units in parallel using Figs. 5-2 through 5-5 (Ref. 25).

If the subsystems in the stage are not identical, state matrix techniques can be used to compute availability.

Example Problem No. 9

A system consists of three identical, s-independent subsystems connected in series. The availability requirement is 0.99, and the repair rate is limited to 0.3 per hr. What is the minimum failure rate which must be allocated to each subsystem to satisfy the system requirement? A repairman is assigned exclusively to each subsystem.

Procedure	Example	
(1) State the system availability requirement.	$A_s = 0.99$	(5-109)
(2) Compute the availability of each subsystem by $A_i = (A_s)^{1/n}$ (5-110)	$A_i = 0.99^{1/3} = 0.99666$	(5-111)
(3) For each subsystem compute the ratio λ/μ by: $\frac{\lambda}{\mu} = \frac{1}{A_i} - 1$ (5-112)	$\frac{\lambda}{\mu} = \frac{1}{0.99666} - 1 = 0.00336$	(5-113)
(4) Compute $\bar{\lambda}$ by Eq. 5-113 with $\mu = 0.3$ per hr. The final answer is rounded off to 2 significant figures to avoid implying too much accuracy.	$\bar{\lambda} = 0.00336 \times (0.3 \text{ per hr}) = 1.0 \text{ per } 1000 \text{ hr}$	(5-114)

Case (3) represents a much more complex problem. Availability must be computed using the state matrix approach. An optimum allocation requires the use of dynamic programming algorithms.

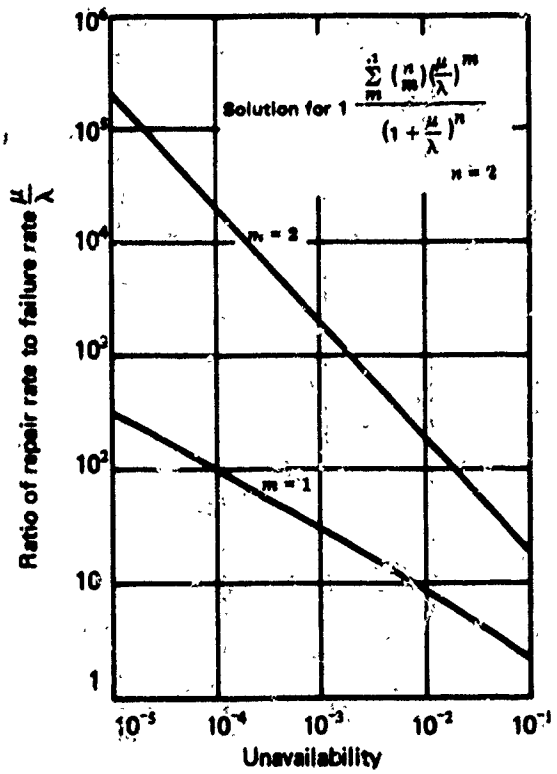
Example Problem No. 10

A system consisting of two s-independent subsystems has an availability of 0.90. Subsystem 1 has an availability of 0.97, and subsystem 2 has an availability of 0.93. A new system, similar in design to this one, must meet a required 0.95 availability. What are the new subsystem availabilities and ratios of failure-to-repair rate?

Procedure	Example	
(1) State the availability requirement A_s of the new system.	$A_s = 0.95$	(5-118)
(2) Compute the sum γ_s of the γ-ratios for the old system: $\gamma_{s,old} = \gamma_1 + \gamma_2$ (5-119)	$\gamma_{s,old} = 0.0309 + 0.0753 = 0.1062$	(5-120)
(3) Compute the relative weights W_j by Eq. 5-117.	$W_1 = \frac{0.0309}{0.1062} = 0.291$	(5-121)
	$W_2 = \frac{0.0753}{0.1062} = 0.709$	(5-122)
(4) Compute an overall γ_s for the new system by: $\gamma_s = \frac{1}{A_s} - 1$ (5-123)	$\gamma_s = \frac{1}{0.95} - 1 = 0.0526$	(5-124)
(5) Compute the allocated γ_j for each subsystem of the new design by: $\gamma_j = W_j \gamma_s$ (5-125)	$\bar{\gamma}_1 = 0.291 \times 0.0526 = 0.0153$; $\bar{\gamma}_2 = 0.709 \times 0.0526 = 0.0373$	(5-126)
(6) Compute the availabilities $\bar{A}_j$ allocated to each subsystem by: $\bar{A}_j = \frac{1}{1 + \bar{\gamma}_j}$ (5-127)	$\bar{A}_1 = \frac{1}{1 + 0.0153} = 0.985$; $\bar{A}_2 = \frac{1}{1 + 0.0373} = 0.964$	(5-128)
(7) Check the allocated availability A_s of the new system by: $A_s = \bar{A}_1 \cdot \bar{A}_2$ (5-129)	$A_s = 0.985 \times 0.964 = 0.950$	(5-130)

Since the allocated ratios are known, the trade-off studies can be performed.

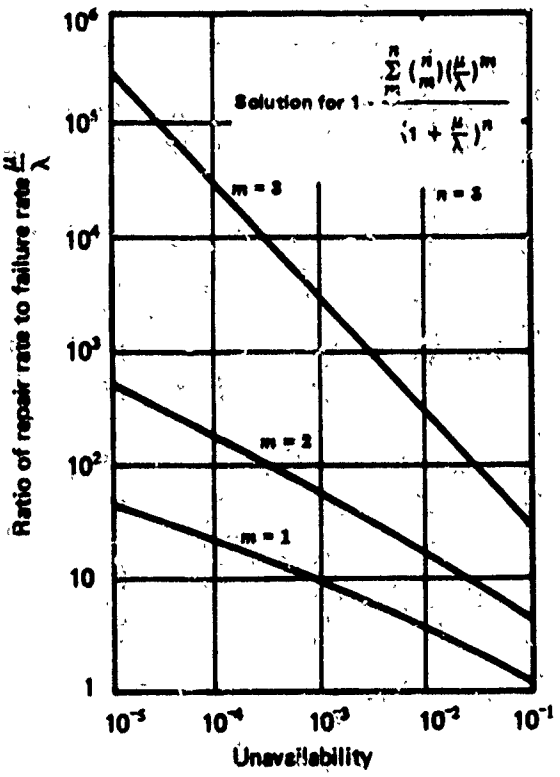
m = minimum number of units which must be up for the system to be up.
n = total number of units.



Copyrighted by Prentice-Hall, Englewood Cliffs, N.J., 1963. Reprinted from *System Reliability Engineering* by permission.

FIGURE 5-2. Repair Rate to Failure Rate Ratio vs Unavailability (n = 2)[25]

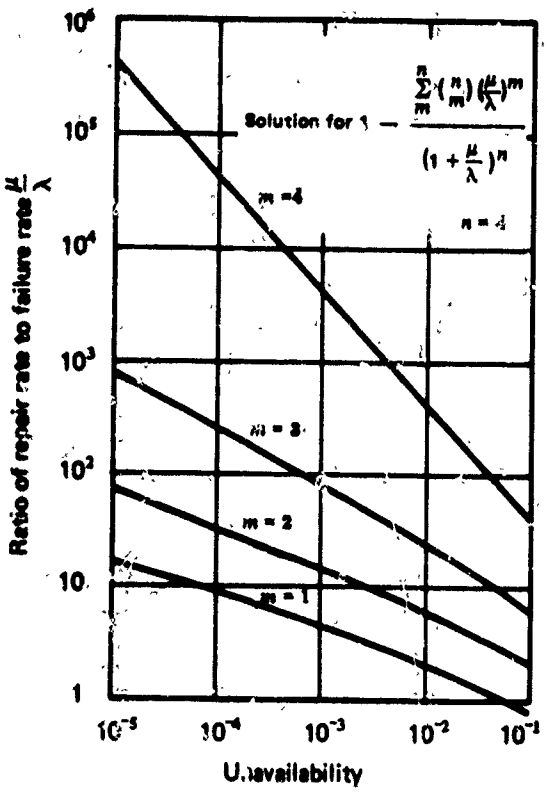
m = minimum number of units which must be up for the system to be up.
n = total number of units.



Copyrighted by Prentice-Hall, Englewood Cliffs, N.J., 1963. Reprinted from *System Reliability Engineering* by permission.

FIGURE 5-3. Repair Rate to Failure Rate Ratio vs Unavailability (n = 3)[25]

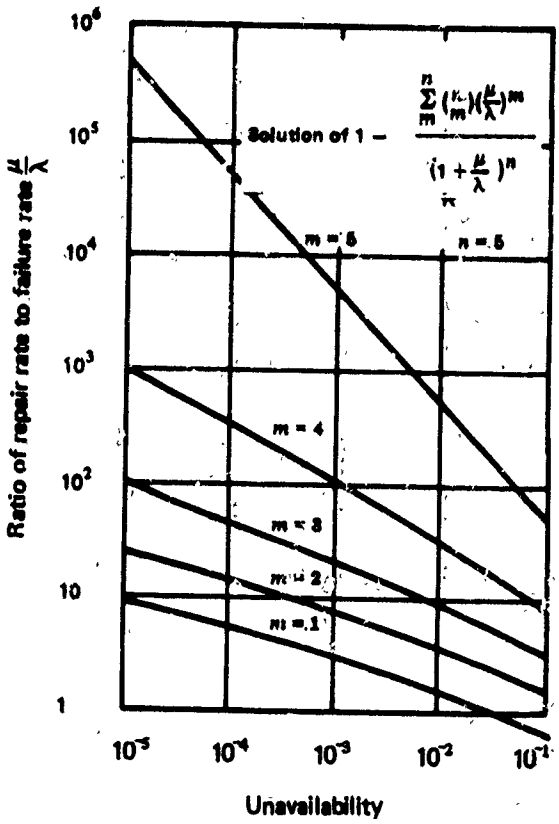
m = minimum number of units which must be up for the system to be up.
n = total number of units.



Copyrighted by Prentice-Hall, Englewood Cliffs, N.J., 1963. Reprinted from *System Reliability Engineering* by permission

FIGURE 5-4. Repair Rate to Failure Rate Ratio vs Unavailability (n = 4)[25]

m = minimum number of units which must be up for the system to be up.
n = total number of units.



Copyrighted by Prentice-Hall, Englewood Cliffs, N.J., 1963. Reprinted from *System Reliability Engineering* by permission.

FIGURE 5-5. Repair Rate of Failure Rate Ratio vs Unavailability (n = 5)[25]

Example Problem No. 11

A system consists of five identical, s-independent subsystems connected in an active redundant configuration. A system availability of 0.999 is required. Four out of five subsystems must be operating for the system to be up. What is the required μ/λ ratio?

Procedure		Example	
(1) State the system availability requirement A_s.		$A_s = 0.999$	(5-133)
(2) Compute the system unavailability U_s by:			
$U_s = 1 - A_s$	(5-134)	$U_s = 1 - 0.999 = 0.0010$	(5-135)
(3) Enter Fig. 5-5 for $m = 4$ and $U_s = 0.0010$, and determine μ/λ.		$\mu/\lambda = 100$	(5-136)

Example Problem No. 11 illustrates the procedure.

5-3.5 RELIABILITY WITH REPAIR AND INSTANTANEOUS AVAILABILITY

In general, reliability with repair and instantaneous availability only can be computed using the state matrix approach. Except for very simple systems, algebraic expressions that represent reliability without repair and instantaneous availability as functions of subsystems repair failure and repair rates are extremely cumbersome and cannot be manipulated readily. The engineer must define the transition matrix of the system in order to implement these procedures.

REFERENCES

1. MIL-HDBK-217, *Reliability Stress and Failure Rate Data for Electronic Equipment.*
2. W. H. Von Alven, Ed., *Reliability Engineering*, Prentice-Hall, Englewood Cliffs, N.J., 1964.
3. *Reliability of Military Electronic Equipment*, Advisory Group on Reliability of Electronic Equipment (AGREE), Office of the Assistant Secretary of Defense, U S Government Printing Office, Washington, D.C., June 1957.
4. H. S. Balaban, et al., *The Allocation of System Reliability. Vol. II. Step-by-Step Reliability Allocation Procedure*, ASD TDR 62-20, Aeronautical Systems Div., USAF, Wright-Patterson AFB, Ohio, June 1962.
5. F. E. Marsh, "Inherent Reliability Design Practices, Reliability Apportionment", *Reliability Control in Aerospace Equipment Development*, Society of Automotive Engineers, Technical Progress Series, SAE, N.Y., 38 (1963).
6. *Cost-Effectiveness Supplement, Vol. III*, AFSC-TR-65-4, Weapons System Effectiveness Industry Advisory Committee (WSEIAC), January 1965.
7. L. A. Aroian, *Maximization of the Reliability of a Complex System by the Use of Items in Sequence*, ST4TM/60-0000-00034, Space Technology Laboratories, Los Angeles, California.
8. R. E. Barlow and L. C. Hunter, "Criteria for Determining Optimum Redundancy", IRE Transactions on Reliability and Quality Control, RQC-9, 73-7 (April 1960).
9. R. E. Barlow and F. Proschan, *Mathematical Theory of Reliability*, John Wiley and Sons, N.Y., 1965.
10. R. Bellman and S. Dreyfus, "Dynamic Programming and the Reliability of Multicomponent Devices", *Operations Research*, 200-6 (April 1958).
11. G. Black and F. Proschan, "On Optimal Redundancy", *Operations Research*, 581-8 (1959).
12. H. Everett, "Generalized Lagrange Multiplier Method for Solving Problems of Optional Allocation of Resources", *Operations Research*, 399-417 (May 1963).
13. B. J. Flehinger, "Reliability Improvement Through Redundancy at Various System Levels", *IBM Journal* (April 1958).
14. R. Gordon, "Optimum Redundancy for Maximum System Reliability", *Operations Research*, 229-43 (April 1957).
15. J. D. Kettelle, Jr., "Least-Cost Allocations of Reliability Investment", *Operations Research*, (March 1962).
16. J. Luttschwager, "Dynamic Programming in the Solution of a Multistage Reliability Problem", *Journal of Industrial Engineering*, 69-175 (1964).
17. G. E. Neuner and R. N. Miller, "Resource Allocation for Maximum Reliability", *Proceedings of the 1966 Annual Symposium on Reliability*, 332-46 (1966).
18. F. Proschan and T. A. Bray, "Optimum Redundancy Under Multiple Constraints", *Operations Research*, 800-14 (September 1965).
19. G. Pugh, "Lagrange Multipliers and the Optimal Allocation of Defense Resources", *Operations Research*, 548-57 (July 1964).
20. M. Sasaki, "A Simplified Method of Obtaining Highest System Reliability",

Proceedings of the Eighth National Symposium on Reliability and Quality Control, 489-502 (January 1962).

21. M. Sasaki, "An Easy Allotment Method Achieving Maximum System Reliability", *Proceedings of the Ninth National Symposium on Reliability and Quality Control*, 109-24 (January 1963).
22. R. B. Thakkar and R. C. Hughes, "Aerospace Power Systems: Maximizing Reliability with Respect to Weight", *IEEE Transactions on Aerospace*, 528-34 (April 1964).
23. L. Webster, "Choosing Optimum System Configurations", *Proceedings of the Tenth National Symposium on Reliability and Quality Control*, 345-59 (January 1964).
24. A. Albert, *A Measure of the Effort Required to Increase Reliability*, Technical Report No. 43. Applied Mathematics and Statistics Laboratory, Stanford University, 1958.
25. G. H. Sandler, *System Reliability Engineering*, Prentice-Hall, Englewood Cliffs, N.J., 1963.
26. NAVWEPS 00-65-502, *Handbook of Reliability Engineering*, June 1964.
27. M. L. Shooman, *Probabilistic Reliability: An Engineering Approach*, McGraw-Hill Book Co., N.Y., 1968.

CHAPTER 6 HUMAN FACTORS

6-0 LIST OF SYMBOLS

Cdf = Cumulative distribution function
pdf = probability density function
$Pr\{\cdot\}$ = probability of . . .
$Pr\{\cdot|\cdot\}$ = conditional probability. The "|" is read as "given that".
Sf = Survivor function: $Sf \equiv 1 - Cdf$

6-1 INTRODUCTION

All systems of concern in this Handbook are of, by, and for humans. Analyses of the behavior and needs of humans are among the more controversial of the sciences; thus it is no surprise that there are several competing approaches to the handling and identification of people problems. Refs. 22 and 23 analyze some of these approaches; but even there, some disagreements exist about the comparisons themselves. It is convenient to classify four types of human interactions with a system; the classes are convenient, but not sharp and clear cut:

(1) Design and production of a system
(2) Operators and repairers as mechanical elements (human engineering)
(3) Operators and repairers as decision elements (human performance reliability)
(4) Bystanders (this classification is not considered further because it is largely a safety matter, not reliability).

An example of the fuzziness between classes is an operator's having to decide what to do, then doing it; there is considerable interaction between the two activities.

An initial appraisal of the man/machine system must consider such aspects as: allocation of functions (man vs machine), automation, accessibility, human tasks and their performance metrics, human stress characteristics, information presented to the human and the reliability of inferences coupled with the decisions on the basis of such information, and accessibility. The answers to these questions and the study of man/machine interactions and interfaces fall within the field variously called human factors, human engineering, or ergonomics (Ref. 28). This field is defined in MIL-STD-721 (Ref. 7) as: "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 area of human engineering, personnel selection, training, life support, job performance aids, and human performance evaluation."

Human factors engineering is applied to research, development, test, and evaluation of systems to insure efficient integration of man into the system environment. This integration is intended to increase and preserve human and machine performance in the system during operation, control, maintenance, and support activities. Human engineering, therefore, becomes an active participant in the system engineering process and, consequently, must be weighed against safety, reliability, maintainability, and other system parameters to obtain trade-offs providing increased system effectiveness. During the concept formulation phase, human factors data are used in predictions of system effectiveness and for initial function allocation studies. Human reliability studies during the contract definition phase are included in system reliability calculations, maintainability time and performance evaluations, system and subsystem safety analyses, and specific human engineering design criteria. The engineering development and production phases provide specific man/machine interactions for amplification of previous studies, isolate and define trade-off and interaction problems not previously identified, and allow verification of prior design decisions on reliability, maintainability, safety, and other system parameters which interact with human factors.

An annotated bibliography of 27 items taken from NTIS reports is listed in Appendix C.

6-2 DESIGN AND PRODUCTION

On the average, people are average. This truism is often forgotten by system designers, planners, and managers. Each wants to have well-above-average people in the tasks he is

PAGE BLANK-NOT FILMED

arranging. System designers do pay some attention to this problem when considering operators and repairers. But rarely is it considered in the design and manufacturing areas, although industrial and manufacturing engineers do deal with it as they are able in their constricted region of operation.

Beginning with the conception of a system, it is important to realize the limitations of the people involved all through the life cycle. Large organizations cannot and will not change rapidly, even though there is a management decree that the change will occur. People cannot adequately plan complete changes in a way of life or of work—there are too many unknown, unforeseen factors.

A system and its subsystems ought to be straightforward to design. Interfaces between subsystems ought to be as simple as possible. The more complexity, the more likely errors are to occur. Checklists are a valuable aid to designers. Design reviews and other product reviews (Chapter 11) help to overcome human limitations by putting some redundancy in the design system.

The designer of an equipment needs to consider how it will be produced; e.g., what kinds of quality control will be necessary, what machines/operators will actually perform a task. Reducing the occasion of very similar appearing parts, but which are different, can help avoid mistakes. A design that can accept looser tolerances might be better than one which requires tight tolerances, even though the latter would perform better if everything were right.

The designer needs to consider how the equipment actually will be repaired in the field. For example, if a repair when done right takes about 8 hr, and when done almost-right takes 1 hr, which way will it be done under the pressures of understaffed maintenance crews many of whom are inexperienced? One cannot expect that field service personnel will have the knowledge about the system that the designers have. Even where the situation is understood, the officer-in-charge under the pressures of command might well choose to have the almost-right repair that takes only 1 hr. The designer must always keep in mind that the equipment will be used and repaired by ordinary people who have other things in mind than "babying" the equipment. He must realize the difference between what people actually will do, and what he thinks they ought to do.

If the familiar production processes in a plant will have to change, then a quality assurance effort must be implemented to be sure the system does change and that it changes correctly.

A Cause-Consequence chart (Chapter 7) is a good tool for viewing the design-production process. It allows one to look at:

(1) What can go wrong (causes)
(2) How likely it is to go wrong
(3) What happens when it does go wrong (consequences)
(4) How to alleviate the severe consequences.

Anywhere people are involved in doing something, the Cause-Consequence chart—even a very simple one—can help locate potential people problems.

System planners should be aware of the impact of administrative policies on the reliability of systems. In Ref. 10 it is shown that many reported failures were not the result of either faulty design or human error (for the Air Force F-106 avionics systems), but were "required" by the procedural environment. Ref. 10 ought to be read by every system planner.

6-3 HUMAN ENGINEERING

This area deals largely with motor responses of operators and with varied human physical capabilities. Refs. 1-6 cover this area adequately. Typical constraints are that:

(1) An operation ought to be within the physical capabilities of the central 95% of the potential operators.

(2) A person is not required to do something that his coordination will not allow him to do, e.g., something akin to patting his head with the left hand while rubbing his chest with the right hand.

(3) Real people cannot easily use, read, and respond to controls and displays, especially in times of psychological stress.

Mock-ups under realistic conditions are very helpful in uncovering forgotten constraints. For example, if an equipment must be used at night in extremely cold weather, have a person try to use it in a freezing, poorly lit room for several hours.

Military standards, regulations, specifications, and other publications contain guidelines, policies, and requirements for human factors and human engineering. For example, Army requirements and policies for human engineering programs are presented in Refs. 8-10. MIL-STD-1472 (Ref. 1), the MIL-STD-803 series (Refs. 2-4), and MIL-H-46855 (Ref. 5) give design criteria, requirements, and definitions for human engineering in military systems. Standardization, automation, visual and auditory displays, controls, labeling, workspace design, maintainability, remote handling devices, safety hazards, and environmental requirements are some of the subjects treated in these sources (Refs. 1-5). Definitions of human factors terms are also found in MIL-STD-721 (Ref. 7).

6-4 HUMAN PERFORMANCE RELIABILITY

The analysis of human factors recognizes that both human and machine elements can fail, and that just as equipment failures vary in their effects on a system, human errors can also have varying effects on a system. In some cases, human errors result from an individual's action, while others are a consequence of system design or manner of use. Some human errors cause total system failure or increase the risk of such failure, while others merely create delays in reaching system objectives. Thus, as with other system parameters, human factors exert a strong influence on the design and ultimate reliability of all systems having a man/machine interface. A good summary and critical review of human performance reliability predictive methods is given in Ref. 22 which is a summary of Ref. 23. Both references contain excellent bibliographies. Table 6-1 is taken from Ref. 22 and lists the available predictive methods.

TABLE 6-1. LIST OF PRED IVE METHODS

OPERABILITY METHODS

A. Analytic

*1. American Institute for Research (AIR) Data Store
*2. THERP-Technique for Human Error Rate Prediction
*3. TEPPS-Technique for Establishing Personnel Performance Standards
4. Pickrel/McDonald Method
5. Berry-Wolff Method
6. Throughput Method
7. Askren/Regulinski Method
8. DEI-Display Evaluative Index
9. Personnel Performance Metric
10. Critical Human Performance and Evaluative Program (CHPAE)

B. Simulation

*1. Digital Simulation Method
2. TACDEN
3. Boolean Predictive Technique
*4. HOS-Human Operator Simulator
*5. ORACLE-Operations Research and Critical Link Evaluator

MAINTAINABILITY METHODS

1. ERUPT-Elementary Reliability Unit Parameter Technique
*2. Personnel Reliability Index
*3. MIL-HDBK 472 Prediction Methods

*Methods described in Ref. 22. References to all methods are given in Ref. 22.

In the initial evaluation of a design, the man/machine system can be put into clearer perspective by answering the following two questions:

(1) In the practical environment, which of the many characteristics that influence human performance are truly important; which must be included in the design; and under what circumstances is each characteristic important?

(2) What effect will including or excluding particular characteristics have on the design of the system?

6-4.1 THE RELATIONSHIP BETWEEN HUMAN FACTORS AND RELIABILITY

Both reliability and human factors are concerned with predicting, measuring, and improving system performance. System failures are caused by human or equipment malfunctions. Thus, system reliability must be evaluated from the viewpoint that the system consists not only of equipment and procedures, but also includes the people who use them. The reliability engineer must analyze and provide for reliability in the equipment and procedures, and also must work closely with the human factors engineer to identify and plan for human reliability factors and their effects on the overall system reliability. Similarly, the human factors engineer is concerned, from the reliability viewpoint, with the reliability of humans in performing or reacting to equipment and procedure activities, and the effect that system reliability will have on human activities. When the man/machine interface is complex, for example, the possibility of human error increases, with an accompanying increase in the probability of system failure due to human error. Of particular concern to the reliability and human factors engineers are the frequency and modes of human failures, and the degree of adverse effect of human failures on the system. One obvious approach to eliminating failures due to human error is to replace the human by a machine. This approach, however, must consider the complexity, reliability, interactions with other equipment, cost, weight, size, adaptability, maintainability, safety, and many more characteristics of a machine replacement for the human. An interesting facet of the human factors/reliability relationship (and which also concerns the maintainability engineer) is that the continuation of the system designed-in reliability depends upon the detection and correction of malfunctions. This task usually is assigned to humans. Thus, system performance can be enhanced or degraded, depending upon whether or not the malfunction information is presented so that it is understood readily. By studying human response to various stimuli (audio, visual, etc.), the human factors engineer provides valuable guidance in the design of system malfunction indicators. Ref. 11 contains additional information on human reliability and includes methods for collecting, analyzing, and using system failure data in quantitative approach to human reliability. A study of the feasibility of quantifying human reliability characteristics and subsequent development of a methodology for quantifying human performance, error prediction, control and measurement are discussed in Refs. 12-14, 30, 32-35. Ref. 31 is a comprehensive abstract of human performance measures.

6-4.2 HUMAN FACTORS THEORY

Basically, human behavior is a function of three parameters (Ref. 26):

(1) Stimulus-Input (S). any stimuli, such as audio or visual signals, failure indications, or out-of-sequence functions which act as sensory inputs to an operator.

(2) Internal Reaction (O). the operator's act of perceiving and interpreting the S and reaching a decision based upon these inputs.

(3) Output-Response (R), the operator's response to S based upon O. Talking, writing, positioning a switch, or other responses are examples of R.

All behavior is a combination of these three parameters, with complex behavior consisting of many S—O—R chains in series, parallel, or interwoven and proceeding concurrently. Each element in the S—O—R chain depends upon successfully completing the preceding element. Human errors occur when the chain is broken, as, for example, when a change in conditions occurs but is not perceived as an S; when several S's cannot be discriminated by the operator; when an S is perceived but not understood; when an S is correctly recognized and interpreted, but the correct R is unknown (i.e., operator cannot reach a decision, or complete O); when the correct R is known but is beyond the operator's capabilities (i.e., operator completes O but cannot accomplish R); or when the correct R is within the operator's capabilities but is incorrectly performed.

Human factors, reliability, safety, maintainability, and other system engineering elements must be directed to a system design that contributes to proper operator responses by creating perceivable and interpretable stimuli requiring reactions within the operator's capabilities. Feedback ought to be incorporated into the design to verify that operator responses are correct. In other words, equipment characteristics should serve as both input and feedback stimuli to the operator. These relationships between human and equipment elements are depicted in Fig. 6-1.

6-4.3 MAN/MACHINE ALLOCATION AND RELIABILITY

The functional block diagrams, allocation of task error rates, mathematical modeling of performance, prediction of performance reliability, and validation are applied to human subsystems in much the same manner as in the reliability of hardware subsystems. Stochastic modeling and quantification of human performance reliability can be done in either time-discrete or time-continuous domains. Particularly useful techniques are:

(1) Data generation and processing, including tests of randomness, stationarity, and ergodicity

(2) Failure modes and effects analysis (Chapter 8)

(3) Parameter variation analysis (Chapter 10)

(4) Cause-Consequence charts (Chapter 7)

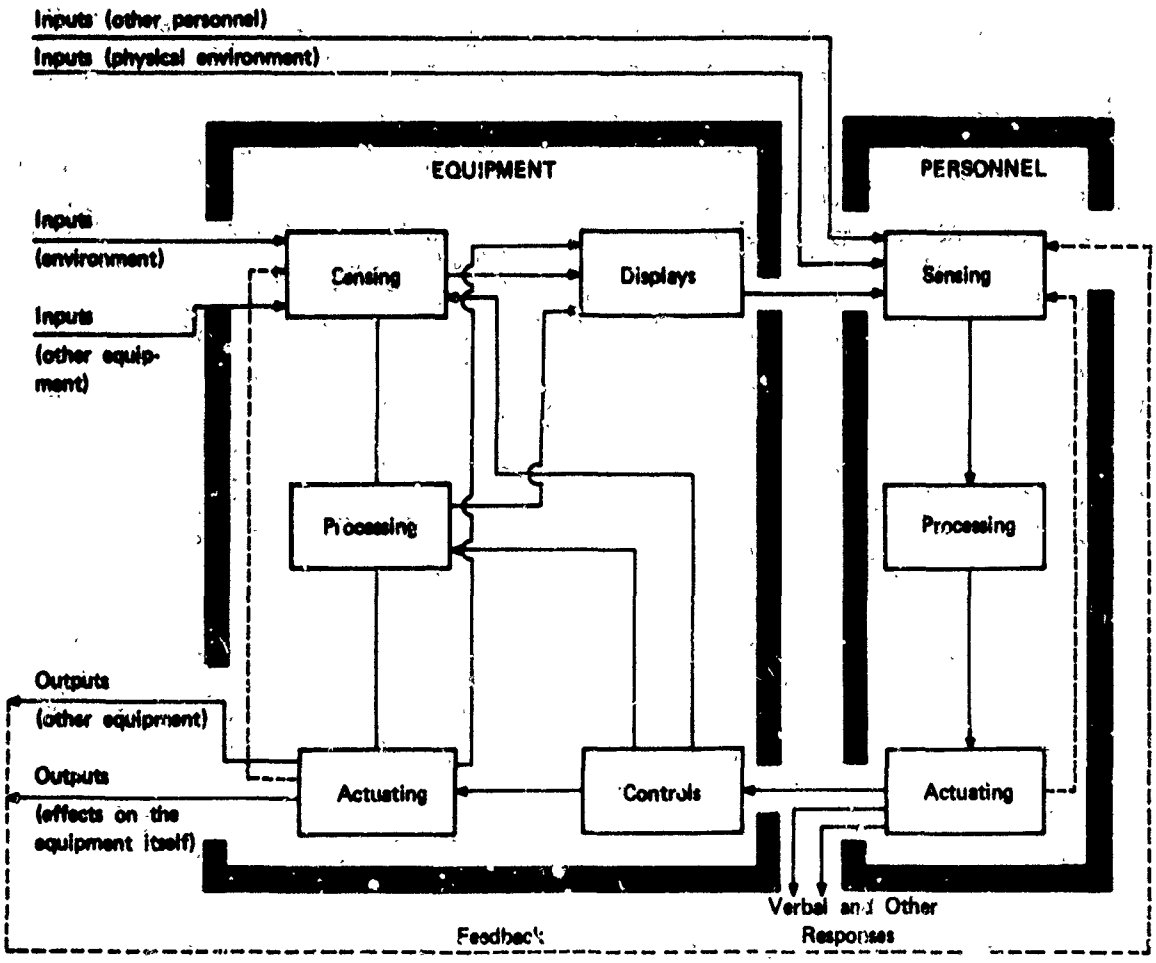


FIGURE 6-1. The Man/Machine Interaction.[8]

(5) Estimation of suitable distributions for random variables

(6) Decisionmaking methods such as hypothesis testing, multiple decision and sequential testing, and formulating rules for strategies.

Many of these techniques are discussed in greater detail in Refs. 25, 36-41.

Reliability of a system is affected by the allocation (not necessarily quantitative) of system functions to either the man, the machine, or both. Table 6-2 lists some of the salient characteristics of the humans and machines which are pertinent to the allocation choice. As is evident from studying Table 6-2, the prediction of human reliability is more difficult than the prediction of machine reliability. The machine's insensitivity to extraneous factors (Item 10 in Table 6-1) versus the human's sensitivity to these factors is one consideration, leading to human performance variability and the subsequent capability to predict machine reliability more precisely. In fact, a human's response can be sufficiently influenced to vary from 0.0001 to 0.9999 reliability within conditions that would not affect a machine. The machine, for example, does not react to environments of combat which could produce severe psychological stress and breakdown in a human. Since the trade-off depends partly on the nature of the system and human functions and partly on the way the allocation problem is approached, each design situation requires a separate human factors analysis. Such variables as cost, weight, size, hazard levels, adaptability, and state of technology must be considered for each system.

One approach to the choice between man and machine is to compare the predicted reliabilities of each. This approach, however, should not be based solely on failure rates, since humans are sufficiently adaptable to recover quickly and correct some human-induced malfunctions. Similarly, humans have the flexibility to handle unique situations that might cause system failure if an unadaptable machine were assigned the task. An approach based on reliability comparisons ought to use failure rates in conjunction with an analysis of man/machine characteristics and the desired task accomplishments.

Another approach to man/machine allocation is illustrated by Fig. 6-2. This approach has three general steps:

(1) Develop a prediction model.

(2) Generate Task Equipment Analysis (TEA) data.

(3) Predict man/machine reliability using the TEA data as inputs to the prediction model.

The predictive model can be developed in either the time-discrete or time-continuous domains, depending on the nature of the human task. The human performance reliability is defined as (Ref. 42):

(1) $Pr\{\text{task performance without error} \mid \text{stress}\}$ (discrete)

(2) $Pr\{\text{task performance without error in an increment of time} \mid \text{stress}\}$ (continuous).

Embodied in the stress is the totality of all factors—psychological, physiological, and environmental—which affect human performance.

For discrete tasks such as pushing a button or throwing a lever, the task random variable has only discrete values (often, the positive integers). The reliability of some discrete repetitive task (assuming that the trials are s-independent and have the same probability) can be estimated simply as the fraction of the trials which are a success. The discrete human performance unreliability sometimes can be approximated by the error-rate multiplied by the time-interval (Ref. 24).

The time-continuous quantification of human performance reliability is applied to such tasks as:

(1) Tracking a signal displayed on a screen

(2) Manually controlling the pitch, roll, and yaw of an aircraft

(3) Performing a vigilance task which might require, for example, the detection of the presence (or absence) of a specified event. In this type of task, the random variable is continuous in time over some domain.

The time-to-error has a random distribution, just as time-to-failure of hardware; this distribution will have a *pdf*, *Cdf*, *Sf*, and failure rate (error rate). Depending on the specific task, a measure of human perfor-

TABLE 6-2. CHARACTERISTICS OF HUMANS AND MACHINES[3]

Characteristics Tending to Favor Humans	Characteristics Tending to Favor Machines
1. Ability to detect certain forms of energy.	1. Monitoring men or other machines.
2. Sensitivity to a wide variety of stimuli within a restricted range.	2. Performance of routine, repetitive, precise tasks.
3. Ability to perceive patterns and generalize about them.	3. Responding quickly to control signals.
4. Ability to detect signals (including patterns) in high noise environments.	4. Exerting large amounts of force smoothly and precisely.
5. Ability to store large amounts of information for long periods and to remember relevant facts at the appropriate time.	5. Storing and recalling large amounts of precise data for short periods of time.
6. Ability to use judgment.	6. Computing ability.
7. Ability to improvise and adopt flexible procedures.	7. Range of sensitivity to stimuli.
8. Ability to handle low probability alternatives (i. e., unexpected events).	8. Handling of highly complex operations (i. e., doing many different things at once).
9. Ability to arrive at new and completely different solutions to problems.	9. Deductive reasoning ability.
10. Ability to profit from experience.	10. Insensitivity to extraneous factors.
11. Ability to track in a wide variety of situations.	
12. Ability to perform fine manipulations.	
13. Ability to perform when overloaded.	
14. Ability to reason inductively.	

mance reliability might be mean time-to-first-error, mean time-to-error, median time-between-errors, or something similar. Numerous other measures similarly can be formulated. For example, because of the capacity of the human to correct self-generated errors, it is germane to model some performance function related to error correction. In Ref. 24 such performance measure is formulated as correctability and defined as:

$Pr\{$Completion of task error correction in a certain time | stress$\}$. The time-to-task-error-correction is analogous to time-to-repair and has a random distribution (and of course, all the descriptions of such a distribution). Refs. 12, 23, 27 provide a comprehensive treatment of man-machine reliability modeling in this context.

Examples of numerical evaluation of these probabilities are:

(1) The human subsystem (operator) is required to interconnect two machines in a

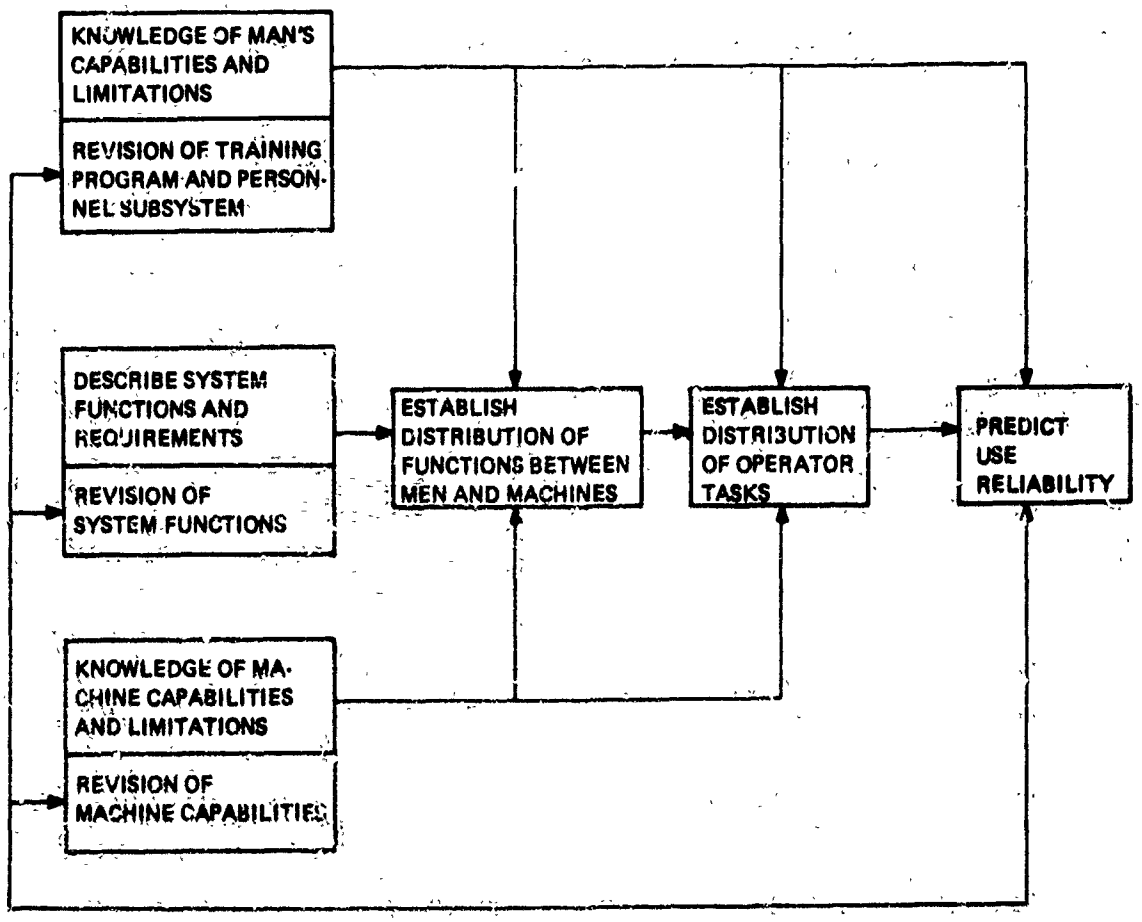


FIGURE 6-2. Predicting Man/Machine Reliability[12]

decision sense. From TEA data it is determined that the probability of a successful interconnection on a single trial is 10%—a very difficult task.

(2) Radar operators who are tracking multiple target signals have two types of errors: missing a target which is displayed, or false alarming. TEA data might show that the time-to-first-false-alarm is lognormally distributed. As shown in *Part Six, Mathematical Appendix and Glossary*, the parameters of the distribution could be estimated (along with their uncertainties) from some sample data. The median time-to-first-false-alarm could then be calculated, as could any other point on the distribution.

6-4.4 INTERACTIONS AND TRADE-OFFS

The principal determinant of man/machine performance is the complexity of human tasks within the system. A system design that requires frequent and precise adjustments by an operator may create reliability problems associated with wear-out or maladjustment of the control device, or maintainability problems from repeated replacement of the worn control. On the other hand, a design providing an automatic adjusting mechanism may cause problems of cost, weight, size, reliability, maintainability, or safety due to the control's complexity. Similarly, for the same level of effectiveness,

a system that through design, location, or environment is difficult to repair must necessarily be made more reliable than a system with a less complex man/machine interface. Thus, the man/machine interaction can contribute to, or detract from, the effectiveness of other disciplines depending upon trade-offs and interactions selected during the system engineering process.

Refs. 6, 18-21 give additional design guides and approaches for solving human factors problems and trade-offs with other disciplines. A valuable consideration, the use of human factors information by designers, is discussed and illustrated with tests and examples in Refs. 15-17.

6-4.5 THERP (TECHNIQUE FOR HUMAN ERROR RATE PREDICTION)

The human performance reliability model developed at Sandia Laboratories is defined as (Ref. 42):

> "THERP is a method to predict human error rates and to evaluate the degradation to a man-machine system likely to be caused by human errors in association with equipment functioning, operational procedures and practices, and other system and human characteristics which influence system behavior."

There are five steps in applying the model.

(1) Define the system failures (consequences). Work with the failures one at a time.

(2) List and analyze the human operations related to each failure (task analysis).

(3) Estimate the appropriate error probabilities.

(4) Estimate the effects of human errors on the system failure. Usually the hardware characteristics will have to be considered in the analysis.

(5) Recommend changes to the man/machine system and return to Step 2.

Ref. 42 summarizes and explains the THERP model (and extolls its virtues). Ref. 43 is an annotated bibliography of the Sandia Laboratories work in this area and will be very helpful to anyone trying to estimate the effects of human frailty on a system. It lists 44 sources of further information.

REFERENCES

1. MIL-STD-1472, *Human Engineering Design Criteria for Military Systems, Equipment and Facilities.*
2. MIL-STD-803A-1, *Human Engineering Design Criteria for Aerospace Systems and Equipment, Part 1: Aerospace System Ground Equipment*, 1964.
3. MIL-STD-803A-2, *Human Engineering Design Criteria for Aerospace Systems and Equipment, Part 2: Aerospace System Facilities and Facility Equipment*, 1964.
4. MIL-STD-803A-3, *Human Engineering Design Criteria for Aerospace Systems and Equipment, Part 3: Aerospace Vehicles and Vehicle Equipment*, 1967.
5. MIL-H-46855, *Human Engineering Requirements for Military Systems, Equipment, and Facilities.*
6. W. E. Woodson and D. W. Conover, *Human Engineering Guide for Equipment Designers*, Univ. of Calif. Press, Berkeley, Calif., 1966.
7. MIL-STD-721, *Definitions of Effectiveness Terms for Reliability, Maintainability, Human Factors, and Safety.*
8. AR 70-8, *Human Resources Research Program.*
9. Anon., "Description of Human Factors Reports by Sandia Laboratories", July 1973, Available from Sandia Laboratories, Albuquerque, New Mexico 87115.
10. H. R. Leuba, "The Impact of Policy on System Reliability", IEEE Trans. on Reliability R-18, 137-140 (August 1969).
11. B. P. Davis and C. N. Cordoni, "People Subsystem Measurement for Total Reliability", *Proceedings of the 1970 Annual Symposium on Reliability*, 394 (1970).
12. G. E. Miller et al., *Human Factors Aspects of Reliability*, Publication No. U2296, Philco Corp., Newport Beach, Calif., 1964.
13. J. A. Kraft, "Mitigation of Human Error through Human Factors Design Engi-

neering", *Annals of 7th Reliability and Maintainability Conference* 7 300 (1968).

14. K. Inaba and R. Matson, "Measurement of Human Errors with Existing Data", *Annals of 7th Reliability and Maintainability Conference* 7, 301 (1968).
15. D. Meister and D. E. Farr, *The Utilization of Human Factors Information by Designers*, System Effectiveness Laboratory, The Bunker-Ramo Corp., Calif., 1967.
16. D. Meister et al., *A Further Study of the Use of Human Factors Information by Designers*, System Effectiveness Laboratory, The Bunker-Ramo Corp., Calif., 1967.
17. R. W. Pew, *Human Information-Processing Concepts for System Engineers*, Univ. of Michigan, Mich., 1965.
18. G. Chaikin et al., *Engineering Practice Study-Human Engineering*, Report No. RC-S-65-1, US Army Missile Command, Redstone Arsenal, Ala., 1965.
19. Davis, Faulkner, and Miller, "Work Physiology", Human Factors 11, No. 2, 157 (April 1969).
20. Alan Swain, "The Human Element in System Development", *Proceedings of the 1970 Annual Symposium on Reliability*, 20-28 (1970).
21. James J. Keenan, "Interactionist Models of the Varieties of Human Performance", *Annals of 6th Reliability and Maintainability Conference* 6,76 (1967).
22. D. Meister, "A Critical Review of Human Performance Reliability Predictive Methods", IEEE Trans. Reliability R-22, 116-123 (Aug. 1973).
23. D. Meister, "Comparative Analysis of Human Reliability Models", Final Report Contract N00024-71-C-1257, Bunker-Ramo Corp., Nov. 1971, AD-734 432.
24. T. L. Regulinski and W. B. Askren, "Stochastic Modeling of Human Performance Effectiveness Functions", *Proceedings 1972 Annual Reliability and Maintainability Symposium*, 407-416 (1972).
25. T. L. Regulinski, "Systems Maintainability Modeling", *Proceedings 1970 Annual Reliability Symposium*, 449-457 (1970).
26. T. L. Regulinski, "Quantification of Human Performance Reliability—Research Method Rationale", *Proceedings of US Navy Human Reliability Workshop*, Report NAVSHIPS 0967-412-4010, Washington, D.C. (July 1971).
27. T. L. Regulinski, Ed., Special Issue on Human Performance Reliability: IEEE Transactions on Reliability R-22, No. 3, August 1973.
28. E. J. McCormis, *Human Engineering*, McGraw-Hill Publishing Co., New York, N.Y., 1967.
29. D. Meister, "Human Factors in Reliability", *Reliability Handbook*, W. G. Ireson, Ed., McGraw-Hill Publishing Co., New York, N.Y., 1966.
30. G. F. Rabideau, "Prediction of Personnel Subsystem Reliability Early in System Development Cycle", *Proceedings of the National Aerospace System Reliability Symposium*, Institute of Aerospace Sciences, New York, N.Y., 1962.
31. R. D. O'Connell, *Handbook of Human Performance Measures*, Space Biology Laboratory, University of California, Los Angeles, July 1972.
32. C. W. Simon, *Economical Multifactor Designs for Human Factors Engineering Experiments;* Hughes Aircraft Company Report No. HAC-P73-326, Culver City, Calif., June 1973.
33. G. Chaikin, *Human Factors/Human Engineering;* report of Ground Equipment and Materials Command, Army Missile Command, Redstone Arsenal, Alabama, June 1973, AD-763 168.
34. I. J. Little, *The Design of Analysis of a Human Body Motion Measurement System;* Report of Guidance and Control Directorate, Army Missile Command, Redstone Arsenal, Alabama, September 1972, AD-751 134.
35. A. Chapanis, *Relevance of Physiological and Psychological Criteria to Man-Machine Systems—The Present State of the Art;* Report TR-24, Dept. of Psychology, Johns Hopkins University, Md., 1970.
36. T. L. Regulinski and W. B. Askren, *Mathematical Modeling of Human Performance Errors for Reliability Analysis*

of Systems, Report of Aerospace Medical Research Laboratory No. AMRL-TR-68-93, Wright-Patterson AFB, Ohio 45433, January 1969.

37. D. Meister et al., *The Effect of Operator Performance Variables on Airborne Electronic Equipment Reliability*, Report RADC-TR-70-140, Rome Air Development Center, Griffis AFB, N.Y., July 1970.
38. D. T. Hanifa, *Human Performance Quantification in System Development:Recent Advances*, Report No. 70-M-0733 of Dunlap Associates, Inc., Santa Monica, Calif. July 1970.
39. A. I. Siegel and J. J. Wolf, *Man-Machine Simulation Models*, John Wiley and Sons Publishing Co., New York, N.Y., 1969.
40. A. I. Siegel and J. J. Wolf, "A Model for Digital Simulation of Two-Operator Man-Machine Systems", Ergonomics, 5:4 (1962).
41. A. I. Siegel and J. J. Wolf, "A Technique for Evaluating Man-Machine Systems Design", Human Factors, 3:1 (1961).
42. Alan D. Swain, "Shortcuts in Human Reliability Analysis", *NATO Advanced Study Institute on Generic Techniques in Systems Reliability Assessment*, Nordhoff Publishing Company, Holland (1974, in press).

CHAPTER 7 CAUSE-CONSEQUENCE CHARTS

7-1 INTRODUCTION

A Cause-Consequence chart shows the logical relationships between causes (events which are analyzed in no more detail) and consequences (events which are of concern only in themselves, not as they in turn affect other events). The chart usually is represented with consequences at the top and causes at the bottom; and the words Top and Bottom have come into common use to describe those portions of the chart. A Failure Modes and Effects Analysis (FMEA) deals largely with the bottom part of the chart. A fault tree is a part of a Cause-Consequence chart. It consists of only one consequence and all its associated branches. The remainder of this chapter deals mostly with fault trees. The Cause-Consequence chart is created by superimposing the separately created fault trees. The Cause-Consequence chart can be used to organize one's knowledge about any set of causes and their consequences; its use is not limited to hardware-oriented systems.

The principles of fault tree creation are straightforward, and easy to grasp. The notation to be used and the discipline to be followed ought to be learned before trying to create a fault tree for a system. The practice of Fault Tree Analysis is tedious, extremely time consuming, and most profitable. Ordinarily, it is done in conjunction with an FMEA (see Chapter 8) because both of the analyses deal with causes and consequences. The bookkeeping aspects—viz., the keeping track of each item, its states (conditions) which are to be considered, and its place in the hierarchy—are very important because mistakes are so easy to make. Unless a strict discipline of labeling items and their states is followed, it is easy to make errors in identifying items, e.g., two different codes might be assigned to one item.

A fault tree usually is constructed in parts because it takes so much room. Each page of the fault tree refers to other pages of the fault tree and has certain conditions that are true for that page. One must carefully keep track of all of these in order to keep errors out of the fault tree.

There is a set of conventions for constructing fault trees; it should be followed rigorously. The reason for following the conventions is to have a fault tree whose parts can be created by several people and which can be understood by many people. Since some set of rules must be followed, if utter chaos is to be avoided, one may as well choose the set in common use.

It is worthwhile keeping a file of general subtrees for common items (e.g., pumps and motors) to avoid having to create that subtree each time it is needed. In each application, the general subtree in the file can be pruned to fit the application.

Usually a fault tree is drawn with the same orientation as the Cause-Consequence chart: the trunk (representing the consequence) is at the top and the leaves (representing the causes) are at the bottom.

During the course of constructing the fault tree, there will be many false starts, blind alleys, system changes, and mistakes. The engineers will learn a great deal about the system; in fact, this scheme of knowledge organization is useful precisely because it does require that the engineers know and make explicit assumptions about the relationships of items in the system.

Fault trees can be used for a complete plant as well as any of the component systems and subsystems. Fault trees provide an objective basis for analyzing system design, performing trade-off studies, analyzing common mode failures, demonstrating compliance with safety requirements, and justifying system changes or additions.

The logic of the approach makes it a visibility tool for both engineering and management. Many reliability techniques are inductive and are concerned primarily with assuring that hardware will accomplish reliably its assigned functions. The fault tree method is concerned with assuring that all critical aspects of a system are identified and control-

PRECEDING PAGE BLANK-NOT FILMED

led. The fault tree itself is a graphical representation of Boolean logic associated with the development of a particular system failure (consequence), called the TOP event; to basic failures (causes), called primary events. For example, the TOP event could be the failure of a reactor scram system to operate during an excursion, with the primary events being failures of the individual scram-system components.

In 1961 the concept of fault tree analysis was originated by Bell Telephone Laboratories as a technique for safety evaluation of the MINUTEMAN Launch Control System (Ref. 1). At the 1965 Safety Symposium (Ref. 2) several papers expounded the virtues of fault tree analysis. They marked the beginning of a widespread interest in using fault tree analysis as a reliability tool in the nuclear reactor industry. In the early 1970's great strides were made in the solution of fault trees to obtain complete reliability information about relatively complex systems (Refs. 3-7). The collection and evaluation of failure data are still very important (Refs. 8-11).

Fault tree analysis is of major value in:

1. Directing the analyst to ferret out failures deductively
2. Pointing out the aspects of a system which are important with respect to the failure of interest
3. Providing a graphical aid for system management people who are removed from the system design changes
4. Providing options for qualitative or quantitative system reliability analysis
5. Allowing the analyst to concentrate on one particular system failure at a time
6. Providing the analyst with genuine insight into system behavior.

Fault tree models do have disadvantages. Probably the most outstanding is the cost of development in first-time application to a system. As in the development of engineering drawings, the cost is somewhat offset by future application of the models in accident prevention, maintenance scheduling, and system modifications. The additional expense is justified by the detail resulting from fault tree analysis. Another disadvantage is that not many engineers are familiar with it. A lesser disadvantage is that skilled personnel might develop a fault tree for a given system in different ways.

Although certain single failures that can result in several component failures simultaneously—called common mode failures*—can be pointed out by a detailed fault tree analysis, the analyst must be alert to include other common mode failures properly in the fault tree and to be aware that fault tree analysis does not inherently ferret out all common mode failures.

Most of this chapter is adapted from Ref. 17.

7-2 GENERATION

A system *component* is a basic constituent for which failures are considered primary failures during fault tree construction. Consequently, the components of a given system can change depending on the TOP event being studied or the detail the analyst wishes to include in the fault tree analysis. Some components have several operating states, none of which are necessarily failed states. For example, relay contacts can be open or closed. The description of these states is called the *component configuration*.

Fault tree construction is the logical development of the TOP event. As the construction proceeds, each fault event also is developed until primary failures are reached. A *fault event* is a failure situation resulting from the logical interaction of primary failures. The development of any fault event results in a *branch* of the fault tree. The event being developed is called the *base event* of the branch. The branch is complete only when all events in the branch are developed to the level of primary failures. Every event in a branch is in the *domain* of the base event. In addition, if the base event is an input to an AND gate, every event in the branch is in the domain of every input to that AND gate.

A fault tree *gate* is composed of two parts:

1. The Boolean logic symbol that relates the inputs of the gate to its output event
2. The output event description.

*This nomenclature has been changed in 1975 to "common cause" failure.

A gate is equivalent to another gate if and only if the logic symbol, the output event description, and the effective-boundary-conditions associated with the output event are identical. These effective-boundary-conditions modify an event and are imposed by the analyst or are generated by previously occurring fault events. A complete treatment of these effective boundary conditions is given in Ref. 12. The event description must have two parts: (1) the incident identification, and (2) the entity identification. The *incident identification* defines, as briefly as possible, the fault without indicating any hardware involved. The *entity identification* specifies the item involved.

Two kinds of symbols are used in a fault tree: logic symbols as shown in Fig. 7-1, and event symbols as shown in Fig. 7-2 (Refs. 1,8,13,17).

The logic symbols (gates) are used to interconnect the events that contribute to the specified main (TOP) event. The logic gates that are used most frequently to develop fault trees are the basic AND and OR Boolean expressions. The AND gate provides an output event only if all input events occur simultaneously. The OR gate provides an output event if one or more of the input events are present.

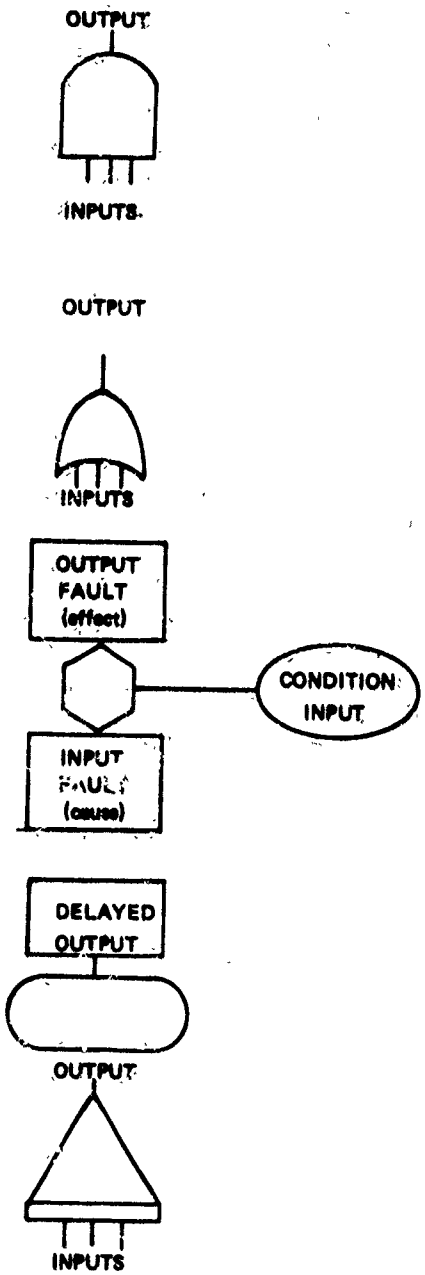
The usual event symbols are the rectangle, circle, and diamond. The rectangle represents a fault event resulting from the combination of more-basic faults acting through logic gates. The circle designates a basic system-component failure or fault input that is s-independent of all other events designated by circles and diamonds. The diamond symbol describes fault inputs that are considered basic in a given fault tree. However, the event is not basic in the sense that laboratory data are applicable. Rather, the fault tree is simply not developed further, either because the event is of insufficient consequence or the necessary information is unavailable. In order to solve a fault tree, both circles and diamonds must be used to represent events for which reliability information is necessary to the fault tree. Events that appear as circles or diamonds are treated as primary events.

The triangles shown in Fig. 7-2 strictly are not event-symbols although traditionally they have been classified as such. The triangle indicates a transfer from one part of the fault tree to another. A line from the side of the triangle (transfer-out triangle) denotes an event transfer out from the associated logic gate. A line from the apex of the triangle denotes an event transfer into the associated logic gate from the transfer-out triangle with the same identification number.

The other logic gates and events symbols are shown and explained in Figs. 7-1 and 7-2.

A *minimal cut set* is a smallest set of primary events, inhibit conditions, and/or undeveloped fault events which must all occur in order for the TOP event to occur. The primary events represent the resolution of the fault tree. The minimal cut sets represent the modes by which the TOP event can occur. For example, the minimal cut set $A_1 A_2$ means that both the primary events A_1 and A_2 must occur in order for the TOP event to occur. The occurrence of A_1 and A_2 is a mode by which the TOP event occurs. If either A_1 or A_2 does not occur, then the TOP event does not occur by this mode. The set of events $A_1 A_2 C$, where C is another primary event, is not a minimal cut set because C is redundant and is not necessary for the occurrence of the TOP event; C can either occur or not occur, and as long as A_1 and A_2 both occur, then the TOP event will occur. A minimal cut set is a collection of component failures all of which are necessary and sufficient to cause system failure by that minimal cut set. A complete set of minimal cut sets is all the failure modes for the given system-failure.

The minimal cut sets are important because they depict which failures must be repaired in order for the TOP failure to be removed from the failed state. The minimal cut sets point out the weakest links in the system. The primary events in the 1-event minimal cut sets usually are the most important. A 1-failure analysis is a fault tree drawn to obtain only the 1-event minimal cut sets (1-failure) for the TOP event. For a 1-failure analysis, the fault tree ends whenever an AND gate is reached that does not have deeper common causes (which effectively transform an AND gate to an OR gate).



AND Gate

Coexistence of all inputs required to produce output.

OR Gate

Output will exist if at least one input is present.

INHIBIT Gate

Input produces output directly when conditional input is satisfied.

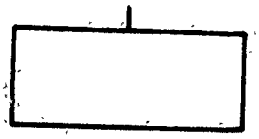
DELAY Gate

Output occurs after specified delay time has elapsed.

MATRIX Gate

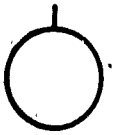
Output is related to one or more unspecified combinations of undeveloped inputs.

FIGURE 7-1. Fault Tree Logic Symbols[17]



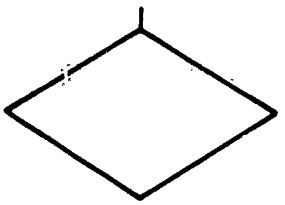
RECTANGLE

A fault event usually resulting from the combination of more-basic faults, which are acting through logic gates.



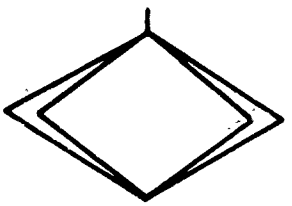
CIRCLE

A basic component-fault — an s-independent event.



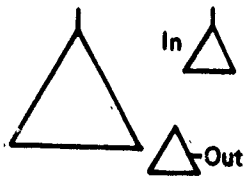
DIAMOND

A fault event not developed to its cause.



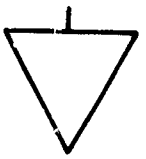
DOUBLE DIAMOND

An important undeveloped fault-event that requires further development to complete the fault tree.



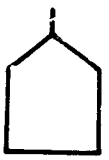
TRIANGLE

A connecting or transfer symbol.



UPSIDE DOWN TRIANGLE

A similarity transfer — the input is similar but not identical to the like identified input.



HOUSE

An event that usually occurs. Also, useful as a "trigger event" for logic structure change within the fault tree.

FIGURE 7-2. Fault Tree Event Symbols[17]

Fault trees are very flexible with regard to the degree of detail to be included. In the fault tree itself primary failures can be failures of the smallest mechanical linkage in a microswitch or failures of a power-generating station. The resolution of the analysis is determined by the needs of the analyst. Having determined the resolution, the analyst has options with regard to evaluating the fault tree. Indeed, the fault tree itself can be the final objective. In addition to the system visibility and understanding obtained by studying the fault tree, further qualitative analysis of the fault tree can produce all of the system modes of failure. Finally quantitative evaluation is possible, i.e., probabilistic failure information can be obtained about the TOP event and minimal cut sets from probabilistic failure information about the components.

Generation of fault trees has two steps: system definition and construction of the tree. Each step is discussed in the paragraphs that follow.

7-2.1 SYSTEM DEFINITION

System definition is often the most difficult task associated with fault tree analysis. Of primary importance is a functional layout diagram of the system showing all functional interconnections and identifying each system component. (For some systems that are not hardware oriented, such a diagram may not exist and, indeed, the Cause-Consequence chart itself might be the only feasible diagrammatic system representation.) An example might be a detailed electrical schematic. Physical system bounds are then established to focus the attention of the analyst on the precise area of interest. A common error is failure to establish realistic system bounds and thereby to initiate a diverging analysis.

Sufficient information must be available for each of the system components to allow the analyst to determine the necessary modes of failure of the components. This information can come from the experience of the analyst or from the technical specifications of the components.

Next, the system boundary conditions must be established. These boundary conditions are not to be confused with the physical bounds of the system. System boundary conditions define the situation for which the fault tree is to be drawn. A most important system boundary condition is the TOP event. For any given system, there is a multitude of possibilities for TOP events. Selecting an appropriate TOP event is sometimes difficult. The complete Cause-Consequence chart will have many TOP events. One of them is chosen for each fault tree. Choosing good, useful TOP events is not easy because one is rarely sure how high to go. The system initial configuration is described by additional system boundary conditions. This configuration must represent the system in the unfailed state. Consequently, these system boundary conditions depend on the TOP event. Initial conditions are then system boundary conditions that define the component configurations for which the TOP event is applicable. All components that have more than one operating state generate an initial condition. System boundary conditions also include any fault event declared to exist or to be not-allowed for the duration of the fault tree construction. These events are called *existing system boundary conditions* or *not-allowed system boundary conditions*. An existing system boundary condition is treated as certain to occur, and a not-allowed system boundary condition is treated as an event with no possibility of occurring. Neither existing nor not-allowed system boundary conditions appear as events in the final system fault tree. Finally, in certain cases, partial development of the TOP event, called the treetop, also is required as a system boundary condition. If the treetop system boundary condition is required, it is not considered as part of the fault tree construction process because it is obtained by inductive means.

7-2.2 FAULT TREE CONSTRUCTION

Published information dealing with generalized fault tree construction is quite limited. Haasl (Ref. 1) has described some general concepts, and Fussell (Ref. 12) has presented a construction methodology for electrical systems that is deductive and formal.

An example demonstrates some of the fundamental aspects of fault tree construction. A sample system schematic is shown in

Fig. 7-3. The system physical bounds include this entire system. The system boundary conditions are:

TOP Event ≡ Motor overheats
Initial Condition ≡ Switch closed
Not-allowed Events ≡ Failures due to effects external to system
Existing Events ≡ Switch closed
Treetop ≡ Shown in Fig. 7-4.

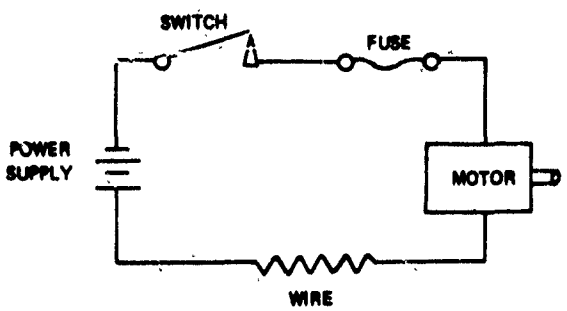


FIGURE 7-3. Sample System

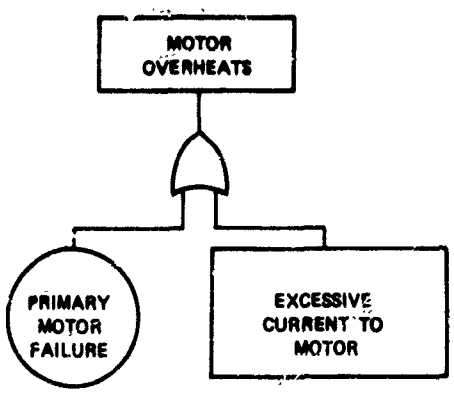


FIGURE 7-4. First Treetop System Boundary Condition for Sample System

7-3 MINIMAL CUT SETS

A minimal cut set is a collection of primary failures all of which are necessary and sufficient to cause the failure by that minimal cut set. A complete set of minimal cut sets is all the failure modes for a given system and TOP event. For the fault tree in Fig. 7-5, the minimal cut sets are, by inspection, the sets of primary events:

1. Motor Failure (overheated)
2. Fuse Failure (closed) Wiring Failure (shorted)
3. Fuse Failure (closed) Power Supply Failure (surge).

Although these minimal cut sets were determined by examination of the fault tree, usually a more formal procedure is needed. One such approach has been suggested by Vesely and Narum (Ref. 14). The Boolean equation implied by the fault tree is constructed by a computer. The primary events are then "turned on" one at a time. Each time, a check is made to determine whether the equation is "true". Next, all possible combinations of two primary events are turned on and again the equation is checked each time to determine whether it is true. Each time the equation is true, the collection of primary events that were turned on is a cut set. After these cut sets are determined, all cut sets that are supersets of other cut sets are discarded so as to winnow the minimal cut sets. Vesely and Narum (Ref. 14) have suggested a Monte Carlo approach whereby appropriate weighting of the primary events is used to accelerate the process of determining the minimal cut sets. However, doubt that all the minimal cut sets have been found is always present when the Monte Carlo approach is used. In practice, both of the preceding methods generally require excessive computer time to obtain cut sets containing more than three primary events.

7-3.1 FINDING THE MINIMAL CUT SETS

This approach (Ref. 17) begins at the TOP event and proceeds to the primary events without simulation, Boolean manipulation, or Monte Carlo. Rather, the fault tree is resolved directly into the minimal cut sets. The execution time is, thereby, not an exponential function as it is with other methods, but is approximately a linear function of the average length of the cut sets. A key point of this method is that an AND gate alone always increases the size of a cut set while an OR gate alone always increases the number of cut sets. To obtain the minimal cut sets, this

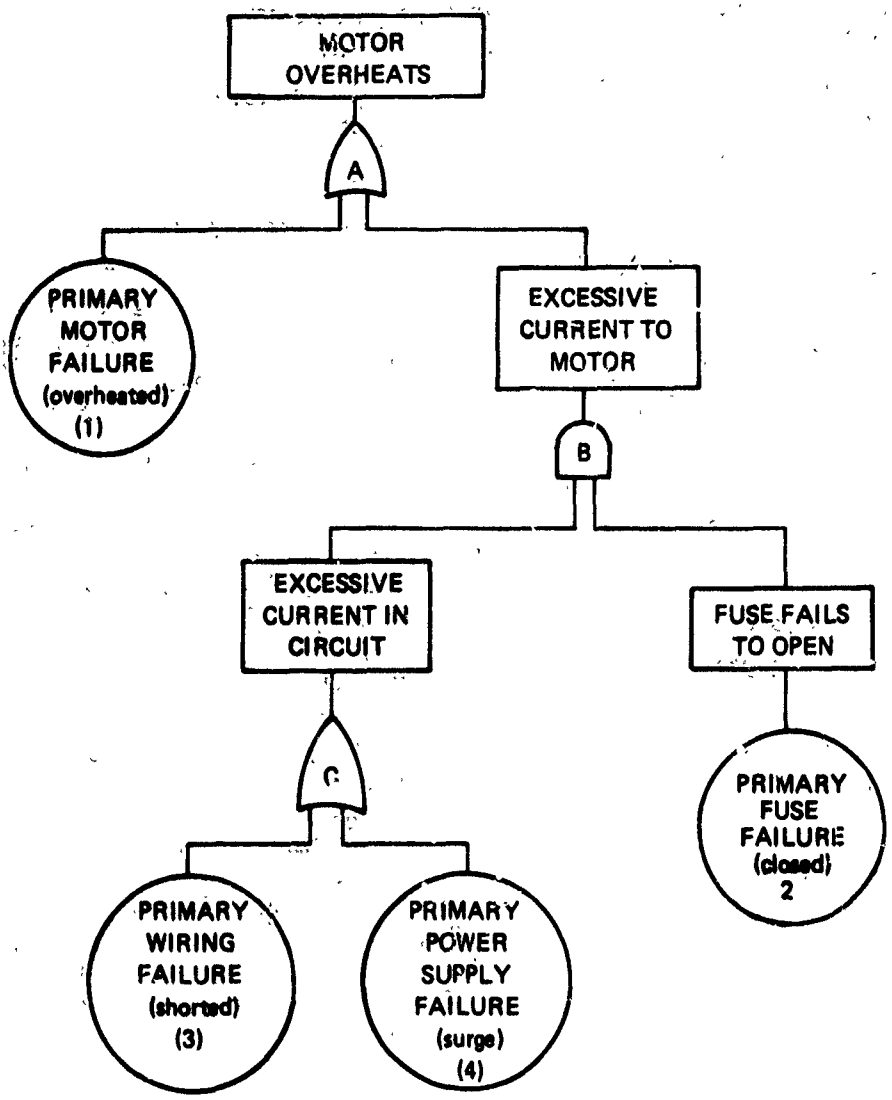


FIGURE 7-5. First Fault Tree for Sample System 1

method requires that the *Boolean indicated cut sets (BICS)* be obtained first. The BICS are defined such that, if all the primary events are different, the BICS will be precisely the minimal cut sets. This definition of the BICS does not mean that the method is limited to fault trees with primary events appearing only once in the fault tree.

Fig. 7-4 reflects the inductive reasoning that the motor overheats if an electrical overload is supplied to the motor or a primary failure within the motor causes the overheating; for example, bearings lose their lubrication or a wiring failure occurs within the motor.

From a knowledge of the components, the fault tree shown in Fig. 7-5 is constructed. The event "excessive current to motor" occurs if excessive current is present in the circuit and the fuse fails to open. The event "excessive current in circuit" occurs if the wire fails shorted or the power supply surges. The fault tree is now complete to the level of primary failures.

For the same sample system but with different system boundary conditions, a second example illustrates the treatment of secondary failures, i.e., failures possibly caused by failure feedback between components. For

this example, the system boundary conditions are:

TOP Event ≡ Motor does not operate
Initial Condition ≡ Switch closed
Not-allowed Events ≡ Failures due to effects external to system(operator failures not included)
Existing Events ≡ None
Treetop ≡ Shown in Fig. 7-6.

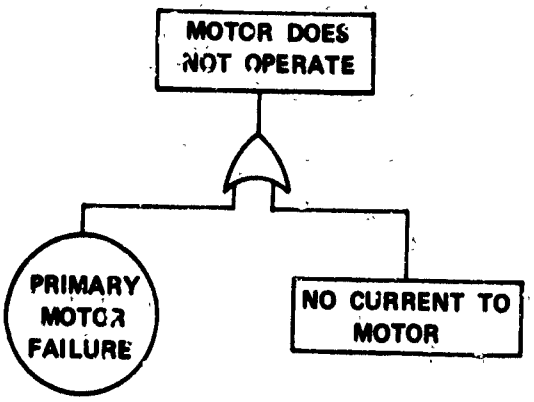


FIGURE 7-6. Second Treetop System Boundary Condition for Sample System[1]

The completed fault tree is shown in Fig. 7-7. Here the diamond symbol is used to indicate that the event "switch open" is not developed to its causes. The switch's being open is a failure external to the system bounds and, in this analysis, insufficient information is available for developing the event.

The event "fuse fails open" occurs if a primary or secondary fuse failure occurs. Secondary fuse failure can occur if an overload in the circuit occurs, because an overload can cause the fuse to open. The fuse does not open, however, every time an overload is present in the circuit, because all conditions of an overload do not result in sufficient overcurrent to open the fuse. The inhibit condition then is used as a weighting factor applied to all the fault events in the domain of the inhibit condition. Since the inhibit condition is treated as an AND logic gate in a probabilistic analysis, it is a probabilistic weighting factor. The inhibit condition has many variations in fault tree analysis, but in all cases it represents a probabilistic weighting factor.

Even though the generation and analysis of fault trees nominally are separate tasks, there is a great deal of interaction between the two. During the course of analysis, engineers become aware of things they had forgotten or not realized while the tree was being generated.

Trees can be evaluated qualitatively and quantitatively. Qualitative evaluation is very profitable because so much understanding of the system is developed during the evaluation. Both methods are discussed in the remainder of this chapter.

Each gate in the fault tree arbitrarily is named with a value ω and each primary event with a value ϕ. The following definitions apply to this approach:

$\rho_{\omega,i}$ ≡ input i to gate ω
λ_ω ≡ number of inputs to gate ω
x ≡ BICS x
y ≡ entry y in a BICS
$\Delta_{x,y}$ ≡ variable representing entry y in BICS x
$x$max ≡ largest value of x yet used
$y$max ≡ largest value of y yet used in BICS x.

The values ω, ϕ, $\rho_{\omega,i}$, λ_ω and the gate type (AND or OR) are assumed known, where values of $\rho_{\omega,i}$ are discernible values of ω or ϕ. $\Delta_{1,1}$ is the first set equal to the ω value representing the gate immediately under the TOP event. From this point on, the goal is to eliminate all ω values from the $\Delta_{x,y}$ matrix. When this elimination is complete, only ϕ values remain and the BICS are determined. To accomplish this elimination, an ω value is located in the $\Delta_{x,y}$ matrix, the values of x,y, and ω are noted and

$$\Delta_{x,y} = \rho_{\omega,1}. \qquad (7\text{-}1)$$

For ω an AND gate:

$$\Delta_{x,y\max+1} = \rho_{\omega,\pi}, \pi = 2,3,\ldots,\lambda\omega, \qquad (7\text{-}2)$$

where $y$max is incremented when π is incremented.

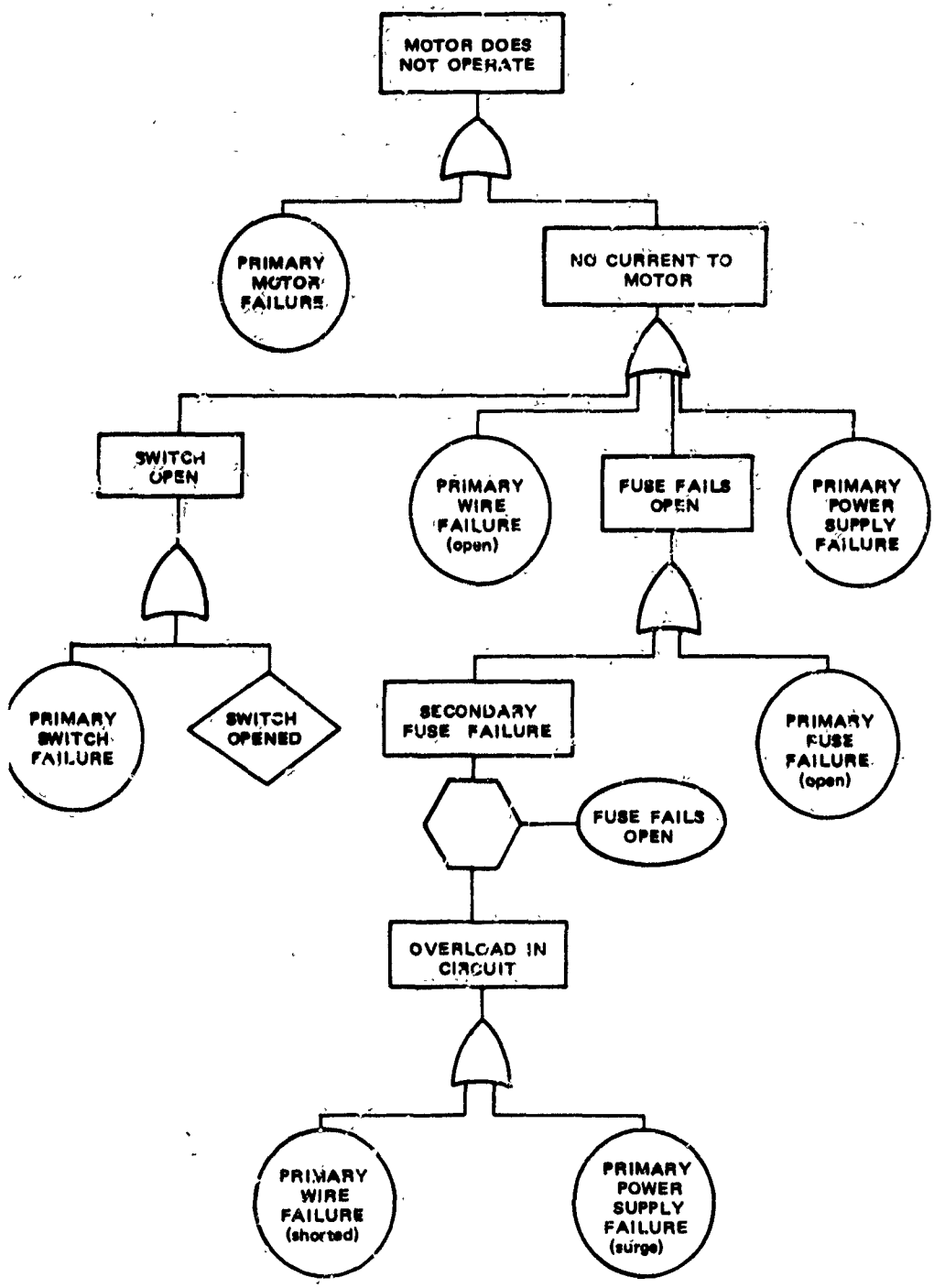


FIGURE 7-7. Second Fault Tree for Sample System[1]

For ω an OR gate:

$$\Delta_{x\max+1,n} = \begin{cases} \Delta_{x,n}, n = 1,2,\ldots,y\max; n \neq y \\ \rho_{\omega,\pi}, n = 2,3,\ldots,\lambda_\omega; n = y \end{cases} \quad (7\text{-}3)$$

where $x\max$ is incremented when π is incremented.

Eqs. 7-1 and 7-2 or 7-3 are repeated until all the entries in the $\Delta_{x,y}$ matrix become values of ϕ. The BICS are then determined. A simple search procedure is used to determine the minimal cut sets.

The number of BICS (the number of rows in the $\Delta_{x,y}$ matrix) for a fault tree generally can be determined in a reasonable time by hand. The number of BICS is an upper bound to the number of minimal cut sets. If $x_{i,j}$ is a parameter associated with input j to gate i, where $x_{i,j} = 1$ for all primary events, then

$$X_i = \begin{cases} x_{i,1} \cdot x_{i,2} \cdot x_{i,3} \cdot \cdots \cdot x_{i,j\max}, \text{ if } i \text{ is an AND gate} & (7\text{-}4) \\ x_{i,1} + x_{i,2} + x_{i,3} + \cdots + x_{i,j\max}, \text{ if } i \text{ is an OR gate} & (7\text{-}5) \end{cases}$$

$$x_{k,\ell} = X_i \quad (7\text{-}6)$$

where k is the gate into which Gate i is input ℓ. If logic gate i is directly under the TOP event then $X_i = X_{TOP}$ is the number of BICS for the fault tree. The value x_k is determined only when all its input parameters are determined; hence, gates that have only primary events ($x_{i,j} = 1$ for all j) as input are the beginning points.

The computation is simple, as can be seen from examining the fault tree in Fig. 7-5. From Eq. 7-5, $X_C = (1 + 1) = 2$ and then from Eq. 7-4,

$$X_B = (x_{B,1})(x_{B,2}) = (X_C)(x_{B,2}) = (2)(1) = 2 \quad (7\text{-}7)$$

and, finally, since A is an OR gate

$$X_A = X_{TOP} = (x_{A,1}) + (x_{A,2}) = (x_{A,1}) + X_B = 3. \quad (7\text{-}8)$$

Therefore, the $\Delta_{x,y}$ matrix contains three rows. The maximum number of primary events in any BICS for a fault tree also generally can be determined in a reasonable time by hand. This maximum is an upper bound to the maximum number of primary events in any minimal cut set for that fault tree. The determination is similar to that for the number of BICS. If $y_{i,j}$ is a parameter associated with input j to gate i where $y_{i,j} = 1$ for all primary events, then

$$Y_i = \begin{cases} y_{i,1} + y_{i,2} + y_{i,3} + \cdots + y_{i,j\max}, \text{ if } i \text{ is an AND gate} & (7\text{-}9) \\ \max\{y_{i,1}, y_{i,2}, y_{i,3}, \ldots, y_{i,j\max}\}, \text{ if } i \text{ is an OR gate} & (7\text{-}10) \end{cases}$$

$$y_{k,\ell} = Y_i \quad (7\text{-}11)$$

where k is the gate into which Gate i is input ℓ. If logic gate i is directly under the TOP event, then $Y_i = Y_{TOP}$ is the maximum number of primary events in any BICS for the given fault tree. Y_i is determined only when all its input parameters are determined; hence, the analyst must begin with gates that have only primary events ($y_{i,j} = 1$ for all j) as input.

For example, the fault tree in Fig. 7-5 is again considered. From Eq. 7-10, $Y_C = \max\{1,1\} = 1$ and from Eq. 7-9,

$$Y_B = Y_C + y_{B,2} \quad (7\text{-}12)$$

$$Y_A = Y_{TOP} = \max\{1,2\} = 2.$$

Therefore, the largest BICS contains two primary events. The $\Delta_{x,y}$ matrix for the fault tree of Fig. 7-5 is a 2×3 matrix. This method easily can be extended to determine the maximum number of 1-, 2-, 3-, ... event BICS, hence an upper bound on the 1-, 2-, 3-, ... event minimal cut sets, respectively, is determined.

The fault tree of Fig. 7-5 illustrates the method of determining minimal cut sets. Each gate has been labeled with a letter and each primary event with a number. The input is then

ω	Gate Type	λ_W	$\rho_{\omega,i}$	
A	OR	2	1	B
B	AND	2	C	2
C	OR	2	4	3

The solution is begun by preparing a $\Delta_{x,y}$ matrix:

$\Delta_{x,y}$

$x \backslash y$		
	A	

Since A is an OR gate, Eqs. 7-1 and 7-3 are used to give

$\Delta_{x,y}$

$x \backslash y$		
	1	
	B	

To eliminate B, Eqs. 7-1 and 7-2 are used to obtain

$\Delta_{x,y}$

$x \backslash y$		
	1	
	C	2

Finally, since C is an OR gate, Eqs. 7-1 and 7-3 are used again to obtain

$\Delta_{x,y}$

$x \backslash y$		
	1	
	4	2
	3	2

From the preceding matrix, the minimal cut sets are as follows:

Minimal Cut Set	Primary Events
1	1
2	4, 2
3	3, 2

The results agree precisely with the results obtained previously by inspection. Since all the primary events in the fault tree are different, the BICS in the preceding $\Delta_{x,y}$ matrix are the minimal cut sets. If some of the BICS contain duplicate events, this duplication is eliminated by discarding redundant events. Also, if some of the BICS are supersets of other BICS, all supersets are discarded. The minimal cut sets remain.

The advantage of the method lies in the speed with which it can determine large cut sets. As a typical example, for a fault tree with 2000 BICS, the smallest of which contains 20 primary events and the largest of which contains 25 primary events, the time required by the UNIVAC 1108 computer to locate all the BICS is less than 16 sec.

7-3.2 MODIFICATIONS FOR MUTUALLY EXCLUSIVE EVENTS

Most methods for obtaining minimal cut sets must be modified somewhat to handle mutually exclusive fault events that appear in the domain of the same AND logic gate. If this modification is not implemented, erroneous "minimal cut sets" result. The manner in which erroneous minimal cut sets appear is illustrated by the example in the system schematic in Fig. 7-8. The purpose of the system is to provide light from the bulb. When the switch is closed, the relay contacts close and the contacts of the circuit breaker, a normally closed relay, open. If the relay contacts open, the light will go out and the operator will immediately open the switch which in turn causes the circuit breaker contacts to close and restore the light. The system boundary conditions include:

TOP Event ≡	No light
Initial Conditions ≡	Switch closed Relay contacts closed Circuit breaker contacts open
Not-allowed Events ≡	Operator failures Wiring failures Secondary failures.

Operator failures, wiring failures, and secondary failures are neglected to simplify the fault tree (see Fig. 7-9).

Table 7-1 gives the primary events that are declared to be minimal cut sets by conventional methods of determining minimal cut sets for the system shown in Fig. 7-8. As can be reasoned from Fig. 7-8, sets (6), (8), (10), and (12) will not cause the TOP event. Only set (12), being logically impossible, could

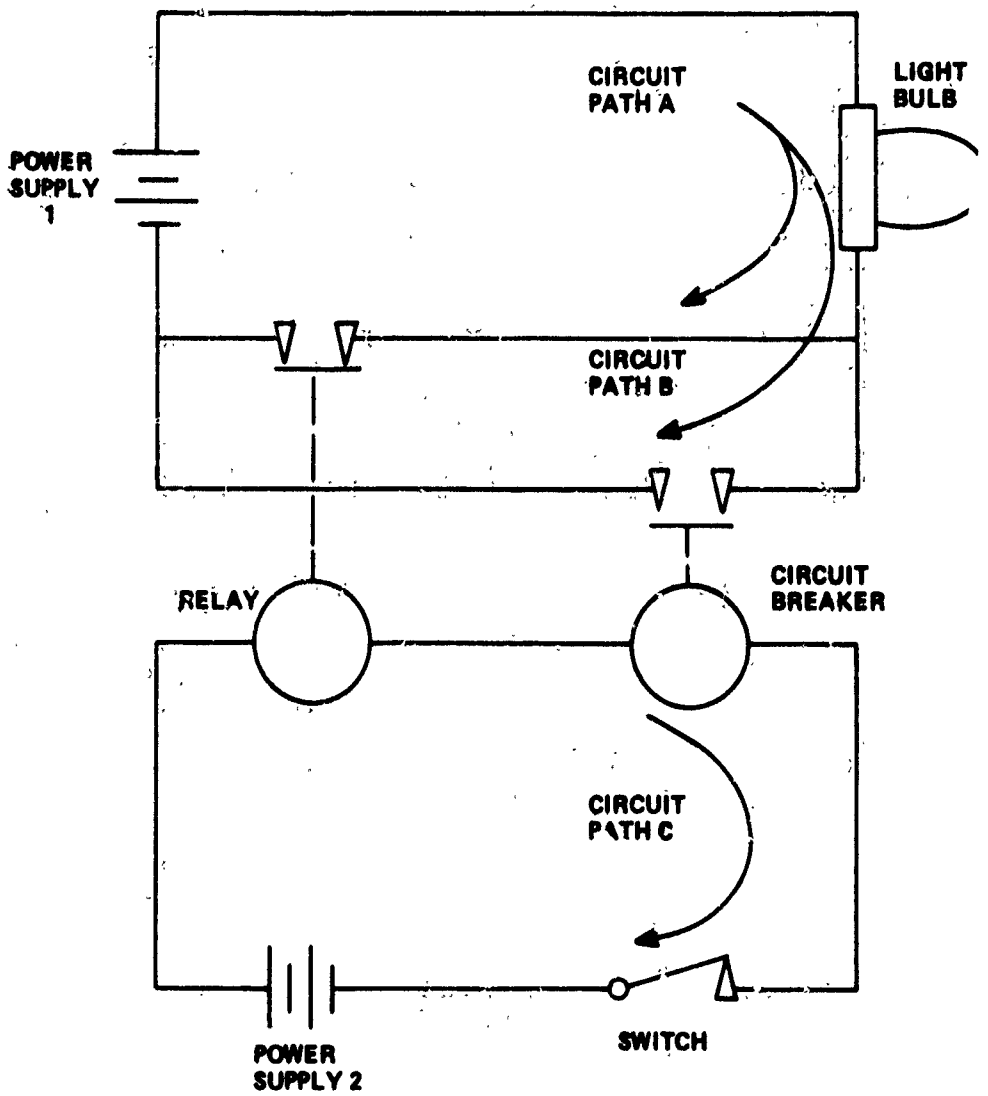


FIGURE 7-8. Sample System 2.

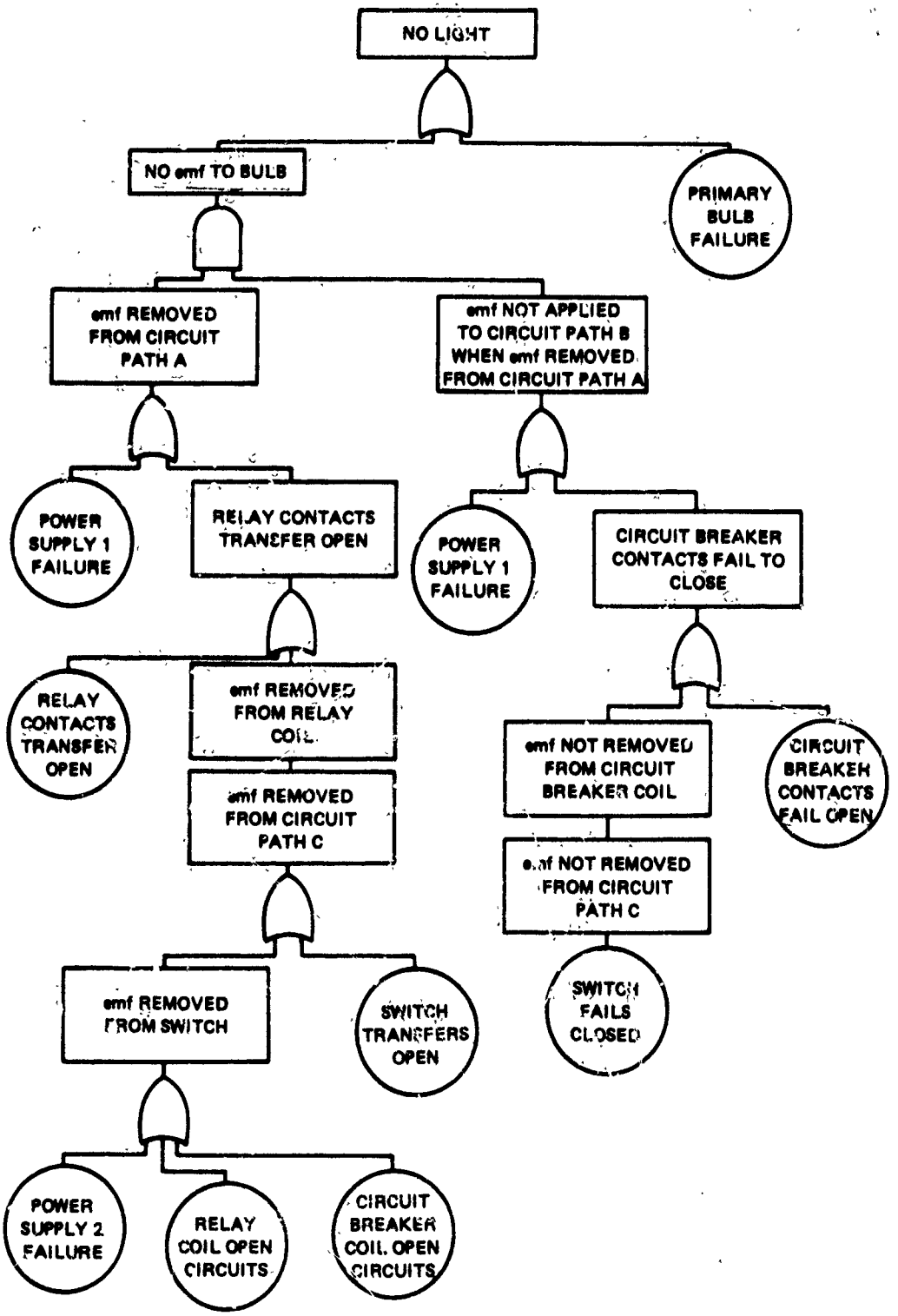


FIGURE 7-9. Fault Tree For Sample System 2

TABLE 7-1.
MINIMAL CUT SETS FOR SAMPLE SYSTEM AS DETERMINED BY CONVENTIONAL MEANS

(1)	Primary bulb failure
(2)	Primary Power Supply 1 failure
(3)	Relay contacts transfer open Circuit breaker contacts fail open
(4)	Relay contacts transfer open Switch fails closed
(5)	Power Supply 2 failure Circuit breaker contacts fail open
(6)	Power Supply 2 failure Switch fails closed
(7)	Relay coil open circuits Circuit breaker contacts fail
(8)	Relay coil open circuits Switch fails closed
(9)	Circuit breaker coil opens circuit Circuit breaker contacts fail open
(10)	Circuit breaker coil opens circuit Switch fails closed
(11)	Switch transfers open Circuit breaker contacts fail open
(12)	Switch transfers open Switch fails closed

have been detected as erroneous from the minimal cut sets themselves.

The reason for these erroneous minimal cut sets is that the fault event "power removed from Circuit Path C", hereafter called $\bar{X}$, and the fault event "power not removed from Circuit Path C", hereafter called $\bar{Y}$, are mutually exclusive fault events. Consequently, collections of component failures that reflect certain combinations of the primary events used to develop these events will not cause TOP failure. Since $\bar{X}$ and $\bar{Y}$ are both in the domain of an AND logic gate, they were combined in determining the minimal cut sets. Alleviating this difficulty in the method of par. 7—3.1 is easy. The mutually exclusive events are flagged. These events then never are combined; hence, erroneous minimal cut sets are not obtained. However, if these erroneous additional minimal cut sets are considered, the error is generally conservative; i.e., a higher system—failed probability is calculated.

Most methods for finding the minimal cut sets presume that the primary events are s-independent; correcting them for mutually exclusive events is more difficult.

7-4 FAILURE PROBABILITY

There are basically three methods for solving fault trees: (1) direct simulation (Ref. 15), (2) Monte Carlo (Ref. 7), and (3) direct analysis (Ref. 6).

Direct simulation basically uses Boolean logic hardware (similar to that in digital computers) in a one-to-one correspondence with the fault tree Boolean logic to form an analog circuit. This method usually is prohibitively expensive. A hybrid method obtains parts of the solution using the analog technique and parts from a digital calculation, in an effort to be cost competitive. Because of the expense involved, this method rarely is used.

Monte Carlo methods are perhaps the most simple in principle but in practice can be expensive. Since Monte Carlo is not practical without the use of a digital computer, it is discussed in that framework. The most easily understood Monte Carlo technique is called "direct simulation". The term "simulation" frequently is used in conjunction with Monte Carlo methods, because Monte Carlo is a form of mathematical simulation. (This simulation should not be confused with direct analog simulation.) Probability data are provided as input, and the simulation program represents the fault tree on a computer to provide quantitative results. In this manner, thousands or millions of trials can be simulated. A typical simulation program involves the following steps.

1. Assign failure data to input fault events within the tree and, if desired, repair data.

2. Represent the fault tree on a computer to provide quantitative results for the overall system performance, subsystem performance, and the basic input event performance.

3. List the failure that leads to the undesired event and identify minimal cut sets contributing to the failure.

4. Compute and rank basic input failure and availability performance results.

In performing these steps, the computer program simulates the fault tree and, using the input data, randomly selects the various parameter data from assigned statistical distributions; and then tests whether or not the TOP event occurred within the specified time period. Each test is a trial, and a sufficient number of trials is run to obtain the desired quantitative resolution. Each time the TOP event occurs, the contributing effects of input events and the logical gates causing the specified TOP event are stored and listed as computer output. The output provides a detailed perspective of the system under simulated operating conditions and provides a quantitative basis to support objective decisions.

To illustrate how direct analysis might be applied to a simple fault tree for static conditions, the fault tree shown in Fig. 7-10 is considered. It contains s-independent, primary events A, B, C, and D with constant probabilities of failure 0.1, 0.2, 0.3, and 0.4, respectively. This assumption of constant failure probabilities distinguishes this example from realistic fault tree evaluation. The fault tree, as shown in Fig. 7-10, is not in convenient form because Events X1 and X2 are not s-independent—they both are functions of Primary Event B. By Boolean manipulation the fault tree shown in Fig. 7-11 is equivalent to the one shown in Fig. 7-10; the minimal cut sets for both fault trees are identical. The fault tree shown in Fig. 7-11 is in convenient form for calculating the probability of the TOP event.

Two basic laws of probability are used in a fault tree evaluation.

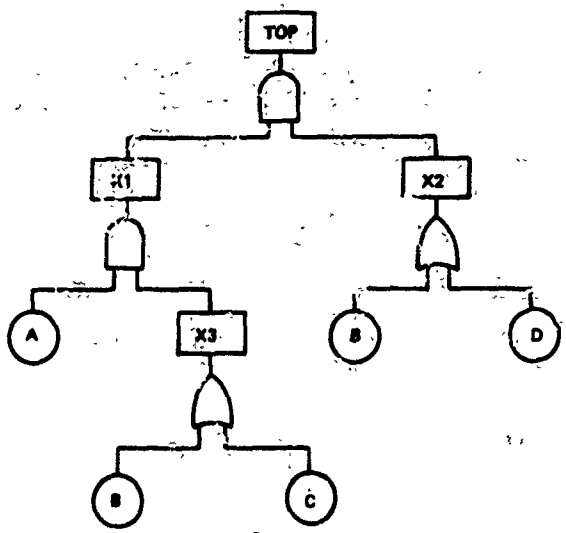


FIGURE 7-10. Sample Fault Tree for Probability Evaluation

$$Pr\{A1 \cup A2\} = Pr\{A1\} + Pr\{A2\} - Pr\{A1 \cap A2\} \quad (7\text{-}14)$$

$$Pr\{A1 \cap A2\} = Pr\{A1\}\, Pr\{A2|A1\} \quad (7\text{-}15)$$

where

$A1, A2$ = any two event

$\cup$ = logic symbol for union, and/or (often represented as addition)

$\cap$ = logic symbol for intersection, both/and (often represented as multiplication)

Eq. 7-14 simply states that the probability of a union is the sum of the probabilities of the individual events minus the probability of their intersection. In terms of the fault tree, the probability of a 2-event OR gate is the sum of probabilities of the two events attached to the gate minus the probability of the two events both occurring. Eq. 7-15 states that the probability of an intersection is the probability of one, $Pr\{A1\}$, times the probability of the other, given the occurrence of the first, $Pr\{A2|A1\}$. In terms of the fault tree in Fig. 7-11, the probability of a 2-event AND gate is the product of the probabilities of the two attached events, because primary events of a fault tree are s-independent; (if not, special precautions must be taken as mentioned in par. 7-3.2).

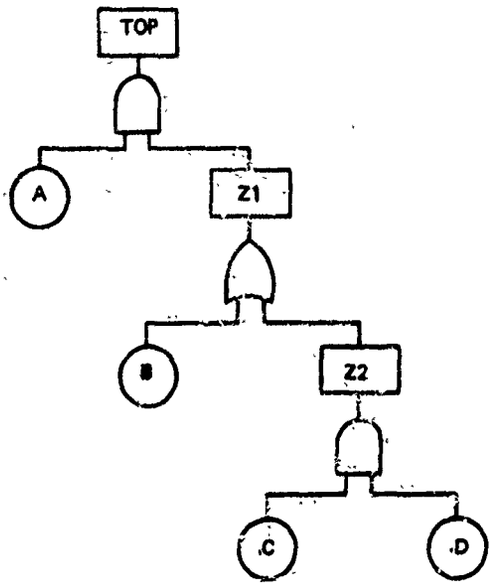


FIGURE 7-11. Boolean Equivalent of Sample Fault Tree Shown in Fig. 7-10.

Since all events are s-independent in the fault tree shown in Fig. 7-11, unlike the events of the tree shown in Fig. 7-10, the event probabilities are as follows:

$$Pr\{Z2\} = Pr\{C\}\ Pr\{D\}$$
$$Pr\{Z1\} = Pr\{B\} + Pr\{Z2\} - Pr\{B\}Pr\{Z2\}$$
$$Pr\{TOP\} = Pr\{Z1\}Pr\{A\}. \quad (7\text{-}16)$$

Upon substitution,

$$Pr\{TOP\} = Pr\{A\}Pr\{B\} + Pr\{A\}Pr\{C\}Pr\{D\} - Pr\{A\}Pr\{B\}Pr\{C\}Pr\{D\}$$
$$Pr\{TOP\} = 0.0236. \quad (7\text{-}17)$$

The probability of the system being in the failed state is 0.0236 for the given primary event failure probabilities. This fault tree has two minimal cut sets, AB and ACD. Primary Event A appears in both minimal cut sets and hence is most crucial to the system. If the $Pr\ \{A\}$ can be reduced to one-half of its original value, i.e., from 0.1 to 0.05, the system failure probability is reduced to 0.0118, or one-half its original value.

In spite of the seeming simplicity of this example, until recently, a practical method for solving complex fault trees analytically was not known for trees containing primary failures with time-dependent failure probabilities and repair possibilities. With the advent of Kinetic Tree Theory (Ref. 6) analytic solutions requiring only relatively small amounts of computer time were possible for complex trees. The fault tree itself is solved through a blend of probability theory and differential calculus. AND, OR, and INHIBIT gates, and general failure and repair distributions are allowed. Complete probabilistic information first is obtained for each primary failure of the fault tree, then for each minimal cut set, and finally for the TOP failure itself. The information is obtained as a function of time and, hence, with regard to reliability, complete kinetic behavior is obtained. The expressions are simple and yield numerical results efficiently, with an average computer time on the order of one minute on the IBM 360/75 computer for a 500 primary failure fault tree (Ref. 6).

An elementary example of a fault tree solution with failure and repair probabilities as functions of time is two identical, s-independent system units, A and B, operating such that the simultaneous failure of both is required to cause system failures (see Fig. 7-12). All failure and repair events are s-independent.

For Events A and B, $F(t)$ represents the time-to-failure *Cdf*, and $G(t)$ is time-to-repair *Cdf*. These functions are

$$F(t) = 1 - e^{-\lambda t}$$
$$G(t) = 1 - e^{-\mu t} \quad (7\text{-}18)$$

where

λ = constant failure rate for a primary failure

μ = constant repair rate.

If $q(t)$ is the probability of the primary failure existing at time t, then from Ref. 16, pp. 112-132,

$$q(t) = \frac{\lambda}{\lambda + \mu}(1 - e^{-(\lambda+\mu)t}). \quad (7\text{-}19)$$

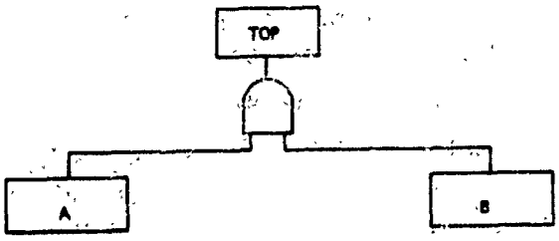


FIGURE 7-12. Sample Fault Tree with Time-Dependent Probabilities

Now $Q(t)$ is defined as the probability that the TOP event exists at time t. Since the TOP failure exists at time t if and only if all the primary failures exist at time t,

$$Q(t) = [q(t)]^2 . \qquad (7\text{-}20)$$

In practice, the methods used for fault tree analysis will depend on which ones are available for the computer being used. It will rarely, if ever, be worthwhile generating a computer program especially for a particular problem.

REFERENCES

1. D. F. Haasl, "Advanced Concepts in Fault Tree Analysis", *System Safety Symposium*, see Ref. 2.
2. *System Safety Symposium*, Proceedings of symposium sponsored by the University of Washington and the Boeing Company, Seattle, Washington, June 8-9, 1965. Available from the University of Washington Library, Seattle, Washington.
3. S. N. Semanderes, "ELRAFT A Computer Program for the Efficient Logic Reduction Analysis of Fault Trees", *IEEE Transactions on Nuclear Science*, November 1970 p. 79.
4. P. Nagel, "Importance Sampling in System Simulation", *IEEE Transactions on Nuclear Science*, November 1970, p. 101.
5. W. E. Vesely, *Analysis of Fault Trees by Kinetic Tree Theory*, IN-1330 (October 1969).
6. W. E. Vesely, "A Time-Dependent Methodology for Fault Tree Evaluation", Nuclear Engineering and Design 3, 2 (August 1970).
7. P. A. Crosetti, *Computer Program for Fault Tree Analysis*, DUN-5508 (April 1969).
8. P. A. Crosetti, "Fault Tree Analysis with Probability Evaluation", *IEEE Transactions on Nuclear Science*, 132 (November 1970).
9. G. E. Greger, D. A. Snyder, P. D. Gross, *Description and Uses of a Critical Systems Data File for Nuclear Plants*, The American Society of Mechanical Engineers, 345 East 47th Street, New York, New York 10017, January 9-12, 1972.
10. M. M. Yarosh, "Accident Analysis", Nuclear Safety, 3,4 (1962).
11. L. Leonardini, "The Third Reliability Meeting at Riso", Nuclear Safety 11, 4 (July-August 1970).
12. J. B. Fussell, *Synthetic Tree Model—A Formal Methodology for Fault Tree Construction*, ANCR-1098 (March 1973).
13. A. B. Mearns, "Fault Tree Analysis: The Study of Unlikely Events in Complex Systems', *System Safety Symposium*, See Ref. 2.
14. W. E. Vesely and R. E. Narum, *PREP and KITT: Computer Codes for the Automatic Evaluation of a Fault Tree*, IN-1349 (August 1970).
15. J. M. Michels, "Computer Evaluation of the Safety Fault Tree Model", *System Safety Symposium*, see Ref. 2.
16. G. H. Sandler, *System Reliability Engineering*, Prentice-Hall, Inc., Englewood Cliffs, N. J., 1963.
17. J. B. Fussell, "Fault Tree Analysis—Concepts and Techniques", *NATO Advanced Study Institute on Generic Techniques of System Reliability Assessment*, Nordhoff Publishing Company, Holland (1974, in press). (Work performed by Aerojet Nuclear Company under the auspices of the U S Atomic Energy Commission)

CHAPTER 8 FAILURE MODES AND EFFECTS ANALYSIS

8-0 LIST OF SYMBOLS

$(CR)_{ij}$ = CRiticality, viz, the portion of the system failure rate due to item i's failing in its mode j

$(CR)_s$ = system criticality, viz, failure rate

α_{ij} = failure mode frequency ratio of item i for the failure mode j

β_{ij} = loss probability of item i for failure mode j

λ_i = failure rate of item i

Σ_i, Σ_j = sum over all i or j

8-1 INTRODUCTION

Failure Modes and Effects Analysis (FMEA) (Ref. 1) is a technique for evaluating the reliability of a design by considering potential failures and their effect on the system. It is a systematic procedure for determining the cause of failures and defining actions to minimize their effects. It can be applied at any level from complete systems to parts. The basic approach is to describe or identify each failure mode of an item, i.e., each possible way it can fail to perform its function. The analysis consists of identifying and tabulating the failure modes of an item, along with the effects of a failure in each mode. Following this analysis, corrective action can be taken to improve the design by determining ways to eliminate or reduce the probability of occurrence of critical failure modes. This corrective action is performed by considering the relative seriousness of the effects of failures.

Criticality of an item is the degree to which satisfactory mission completion depends on the item. A mission usually has several tasks, e.g., a vehicle needs to provide prompt safe delivery of its cargo and safe delivery of its crew. A mission also is classified conveniently into several time phases. Some failure modes of an item will affect adversely some tasks and some phases of a mission, but not necessarily all of them. Some failure modes concerning crew and public safety are not failures in the ordinary sense; for example, sharp edges which can cut a vehicle operator do not "fail", they are just there.

The principles of FMEA are straightforward and easy to grasp. The practice of FMEA is tedious, time-consuming, and very profitable. It is best done in conjunction with Cause-Consequence charts and Fault Tree analysis; both are explained in Chapter 7. The bookkeeping aspects, namely, the keeping track of each item and its place in the hierarchy, are very important because mistakes are so easy to make.

An FMEA also can be used as a basis for evaluating redesign, substitution, or replacements proposed during manufacture, assembly, installation, and checkout phases.

The FMEA consists of two phases which provide a documented analysis for all critical components of a system. First, however, definitions of failure at the system, subsystem, and sometimes even part level must be established.

Phase 1 is performed in parallel with the start of detail design and updated periodically throughout the development program as dictated by design changes. Phase 2 is performed before, or concurrently with, the release of detail drawings.

The Phase 1 analysis consists of the following steps:

(1) Constructing a symbolic logic block diagram, viz., the reliability diagram mentioned in Chapter 4 or a Cause-Consequence chart mentioned in Chapter 6.
(2) Performing a failure effect analysis, taking into account modes of failure such as:
   (a) Open circuits
   (b) Short circuits
   (c) Dielectric breakdowns
   (d) Wear
   (e) Part-parameter shifts
(3) Proper system and item identification
(4) Preparation of a critical items list.

During Phase 2, the results of Phase 1 are revised and updated as required by design changes. In addition, all items in the system are analyzed to determine their criticality with respect to the system.

8-2 PHASE 1

During this phase the following detailed steps are performed:

(1) A Symbolic Logic Block Diagram is constructed. This diagram is developed for the entire system to indicate the functional dependencies among the elements of the system and to define and identify its subsystems. It is not a functional schematic or a signal flow diagram, but a model for use in the early analysis to point out weaknesses. Figs. 8-1 and 8-2 show typical symbolic logic diagrams. Fig. 8-1 illustrates the functional dependency among the subsystems, sets, groups, and units that make up the system. Fig. 8-2 illustrates the functional dependencies among assemblies, subassemblies, and parts that make up one of the units in Fig. 8-1.

(2) A failure effect analysis is performed for each block in the symbolic logic block diagram, indicating the effect of item failure on the performance of the next higher level on the block diagram. Table 8-1 (Ref. 1) shows a typical group of failure modes for various electronic and mechancial parts, representing equipment of the mid-1960's. The failure mode ratios are estimates and are to be revised on the basis of the user's experience. However, they can be used as a guide in performing a detailed failure effects analysis.

Fig. 8-3 illustrates a useful form for conducting a failure effect analysis. (See also Fig. 8-5 for an example of its use.) For each component in the system, appropriate information is entered in each column. Column descriptions are given in Table 8-2.

A numerical reference for all items in the symbolic logic block diagram must be provided by using a standard coding system, such as that specified in MIL-STD-16 (Ref. 2). All items below the set and group levels are identified using the scheme illustrated in Fig. 8-2. Items at and above the group and set levels are not subject to this standard nomenclature scheme. These items can be assigned a simple code such as that illustrated in Fig. 8-1. In this illustration, the system is assigned a letter; and the subsystems, sets, and groups are assigned numbers in a specifically ordered sequence. As an example, the code *S*-23-01 designates the first group of the third set in the second subsystem of system *S*. The exact coding system used is not as important as making sure that each block in the diagram has its own number. Identical items (same drawing numbers) in different systems, or in the same system but used in different applications, should not be assigned the same code number.

(3) During the failure effects analysis, a number of changes to the block diagrams may be required. Therefore, to minimize the number of changes in the coding system, it is recommended that the failure effects analysis be completed before assignment of code numbers is finalized.

(4) Based on the failure effects analysis, a list of critical items should be prepared. This list will contain those items whose failure results in a possible loss, probable loss, or certain loss of the next higher level in the symbolic logic block diagram. Items that can cause system loss should be identified clearly in the list.

8-3 PHASE 2

This phase is implemented by performing the following steps:

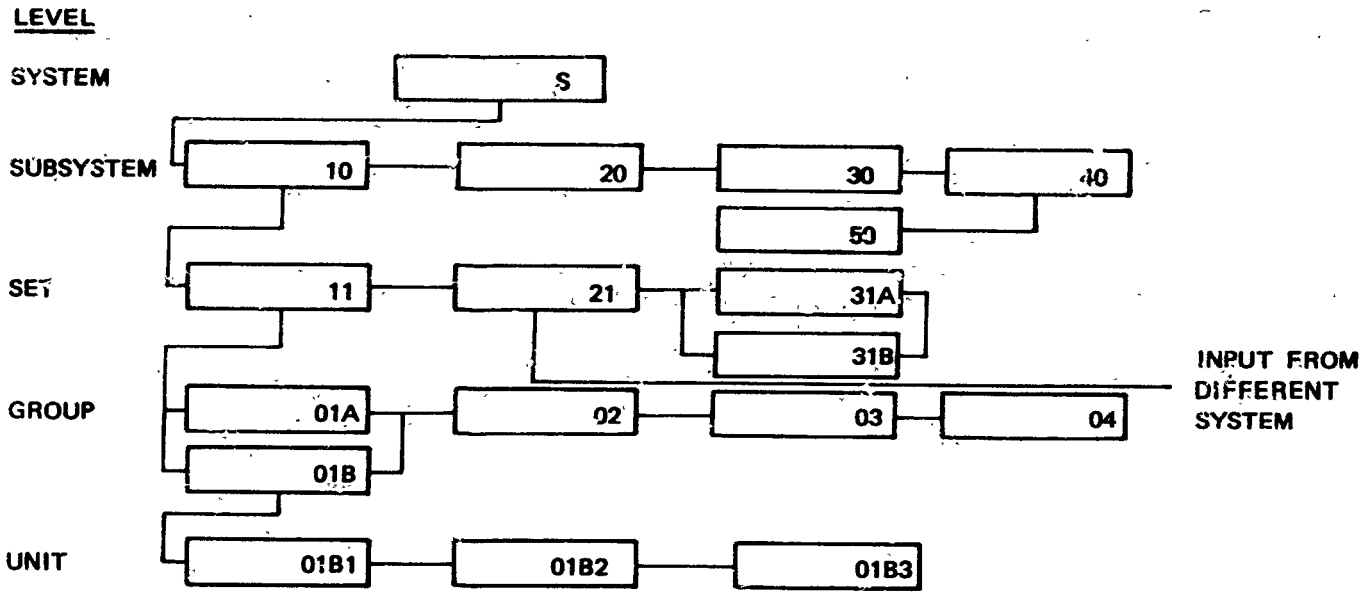
(1) The symbolic logic block diagram, failure effects analysis, coding, and critical items list are reviewed and brought up-to-date.

(2) Criticality is assigned, based on the item applicable failure mode, the system loss probability, the failure mode frequency ratio, and the item unreliability. The analysis of criticality is essentially quantitative, based on a qualitative failure effects analysis.

Criticality CR_i is defined by the equation:

$$(CR)_{ij} = \alpha_{ij}\beta_{ij}\lambda_i \qquad (8\text{-}1)$$

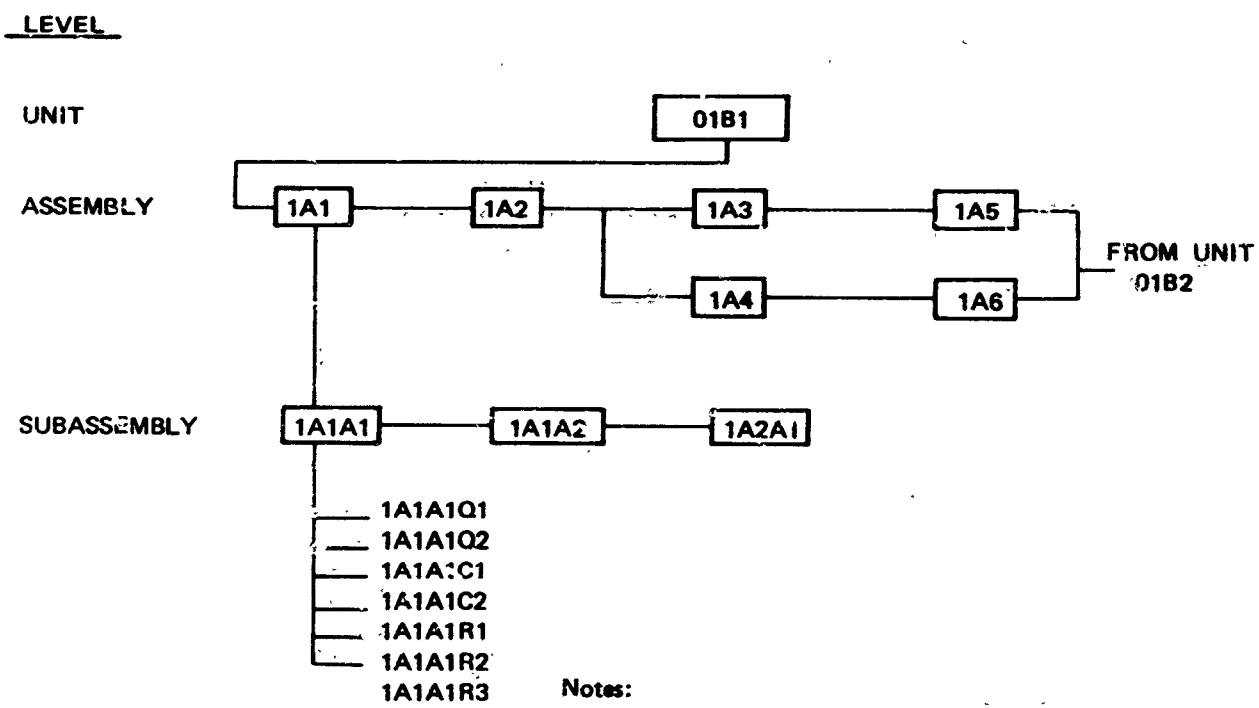
where



Notes;

1. The system depends on subsystems 10, 20, 30, and 40.
2. Subsystem 10 depends on sets 11, 21, 31A, and 31B.
3. Set 11 depends on groups 01A, 01B, 02, 03, and 04.
4. Group 01B depends on units 01B1, 01B2, and 01B3.
5. Sets 31A and 31B are redundant.
6. Groups 01A and 01B are redundant.
7. Subsystem 40 depends on subsystem 50.
8. Set 21 depends upon an input from another system.

FIGURE 8-1. Typical System Symbolic Logic Block Diagram[1]



Notes:

1. Unit 01B1 depends on assemblies 1A1, 1A2 AND either '1A3 AND 1A5' OR '1A4 AND 1A6.'
2. Assembly 1A1 depends on subassemblies 1A1A1 AND 1A1A2.
3. Assembly 1A2 depends on subassembly 1A2A1.
4. Subassembly 1A1A1 depends on all parts contained therein.

FIGURE 8-2. Typical Unit Symbolic Logic Block Diagram[1]

TABLE 8-1. PART FAILURE MODES[1]

PART	IMPORTANT FAILURE MODES AND APPROXIMATE PERCENTAGES OF OCCURRENCE	
Bearings	Loss or deterioration of lubrication	45
	Contamination	30
	Misalignment	5
	Brinelling	5
	Corrosion	5
Blowers	Winding failures	35
	Bearing failures	50
	Sliprings, brushes, and commutators	5
Capacitors-Fixed Ceramic Dielectric	Short circuits	50
	Change of value	40
	Open circuits	5
Capacitors-Fixed Electrolytic Aluminum	Open circuits	40
	Short circuits	30
	Excessive leakage current	15
	Decrease in capacitance	5
Capacitors-Fixed, Mica or Glass Dielectric	Short circuits	70
	Open circuits	15
	Change of value	10
Capacitors-Fixed Metallized Paper or Film	Open circuits	65
	Short circuits	30
Capacitors-Fixed Paper Dielectric	Short circuits	90
	Open circuits	5
Capacitors-Fixed, Electrolytic, Tantalum	Open circuits	35
	Short circuits	35
	Excessive leakage current	10
	Decrease in capacitance	5
Choppers	Contact failures	95
	Coil failure	5
Circuit Breakers	Mechanical failure of tripping device	70
Clutches-Magnetic	Bearing wear	45
	Loss of torque due to internal mechanical degradation	30
	Loss of torque due to coil failure	15
Coils	Insulation deterioration	75
	Open winding	25
Connectors, Interstage	Shorts (poor sealing)	30
	Mechanical failure of solder joints	25
	Degradation of insulation resistance	20
	Poor contact resistance	10
	Miscellaneous mechanical failures	15
Connectors, Standard	Contact failure	30
	Material deterioration	30
	Mechanical failure of solder joints	25
	Miscellaneous mechanical failures	15
Crystal Units, Quartz	Open	80
	No oscillations	10
Diodes, Silicon and Germanium	Short circuits	76
	Intermittent circuits	18
	Open circuits	6
Electron Tubes (Subminiature)	Degradation (gm, Ihk, Ip, etc.)	90
	Catastrophic (shorts, opens, cracked envelopes, etc.)	10

TABLE 8-1. PART FAILURE MODES[1] (cont'd)

PART	IMPORTANT FAILURE MODES AND APPROXIMATE PERCENTAGES OF OCCURRENCE	
Hose Assemblies (Rubber)	Material deterioration	85
	End fitting mechanical failure	10
Indicator Lights	Catastrophic (opens)	75
	Degradation (corrosion, solderability)	25
Insulators	Mechanical breakage	50
	Deterioration of plastic material	50
Lamps, Incandescent	Catastrophic (filament breakage, glass breakage)	10
	Degradation (loss of filament emission)	90
Magnetrons	Window puncturing	20
	Cathode degradation (resulting from arcing and sparking)	40
	Gassing	30
Meters, Ruggedized	Catastrophic (opens, glass breakage, open seals)	75
	Degradation (accuracy, friction, damping)	25
Motors, Drive and Generator	Winding failures	20
	Bearing failures	20
	Slipring brushes, and commutators	5
Motors, Servo and Tachometer	Bearing failures	45
	Winding failures	40
Oil Seals (rubber)	Material deterioration	85
O-Rings (rubber)	Material deterioration	90
Relays	Contact failures	75
	Open coils	5
Resistors-Fixed, Carbon and Metal Film	Open circuits	80
	Change of value	20
Resistors-Fixed, Composition	Change of value	95
Resistors-Variable, Composition	Erratic operation	95
	Insulation failure	5
Resistors-Variable, Wirewound	Erratic operation	55
	Open circuits	40
	Change of value	5
Resistors-Variable, Wirewound, Precision	Open circuits	70
	Excessive noise	25
Switches, Rotary	Intermittent contact	90
Switches, Toggle	Spring breakage (fatigue)	40
	Intermittent contact	50
Synchros	Winding failures	40
	Bearing failures	30
	Slipring and brush failures	20
Thermistors	Open circuits	95
Transformers	Shorted turns	90
	Open circuits	5
Transistors Germanium and Silicon	High Collector to base leakage current (Icfo)	59
	Low Collector to emitter breakdown voltage (Bvcec)	37
	Open terminals	4

TABLE 8-1. PART FAILURE MODES[1] (cont'd)

PART	IMPORTANT FAILURE MODES AND APPROXIMATE PERCENTAGES OF OCCURRENCE	
Valves-Check and Relief	Poppets sticking (open or closed)	40
	Valve seat deterioration	50
Varistors	Open circuits	95
Vibration Isolators (rubber type)	Material deterioration	85
Vibration Isolators (spring type)	Degradation of damping medium	80
	Spring fatigue	5
Vibrators	Contact failures	80
	Open winding	5
	Spring fatigue	15

(1) ITEM	(2) CODE	(3) FUNCTION	(4) FAILURE MODE	(5) FAILURE EFFECT	(6) LOSS PROBABILITY, P

FIGURE 8-3. Failure Effects Analysis Form[1]

TABLE 8-2. COLUMN DESCRIPTIONS FOR FIGURE 8-3

COLUMN	NOMENCLATURE	DESCRIPTION
1	Item	Item name
2	Code	Item identification or circuit designation code
3	Function	Concise statement of the item's function
4	Failure Mode	Concise statement of the mode(s) of item failure
5	Failure Effect	Explanation of the effect of each failure mode on the performance of the next higher level in the symbolic logic block diagram
6	Loss Probability, β	Numerical index indicating the probability of system loss if the item fails in the mode indicated

α_{ij} = failure mode frequency ratio of item i for the failure mode j (see Table 8-1 for an example); i.e., the ratio of failures of the type being considered to all failures of the item

β_{ij} = loss probability of item i for failure mode j (i.e., the probability of system failure if the item fails). A suggested scale is Certain Loss-1.00, Probable Loss-0.50, Possible Loss-0.10, No Effect-0.0

λ_i = failure rate of item i

$(CR)_{ij}$ = system failure rate due to item i's failing in its mode j.

The system criticality is given by Eq. 8-2.

$$(CR)_s = \sum_{i=1} \sum_{j=1} (CR)_{ij} \qquad (8\text{-}2)$$

$(CR)_s$ = system criticality (failure rate)

Σ_j = sum over all failure modes of item i

Σ_i = sum over all items.

A form useful for conducting the criticality analysis is given in Fig. 8-5. This form is a modification of Fig. 8-3 to include the failure mode frequency ratio and the failure rate.

Example Problem No. 12 illustrates the procedure.

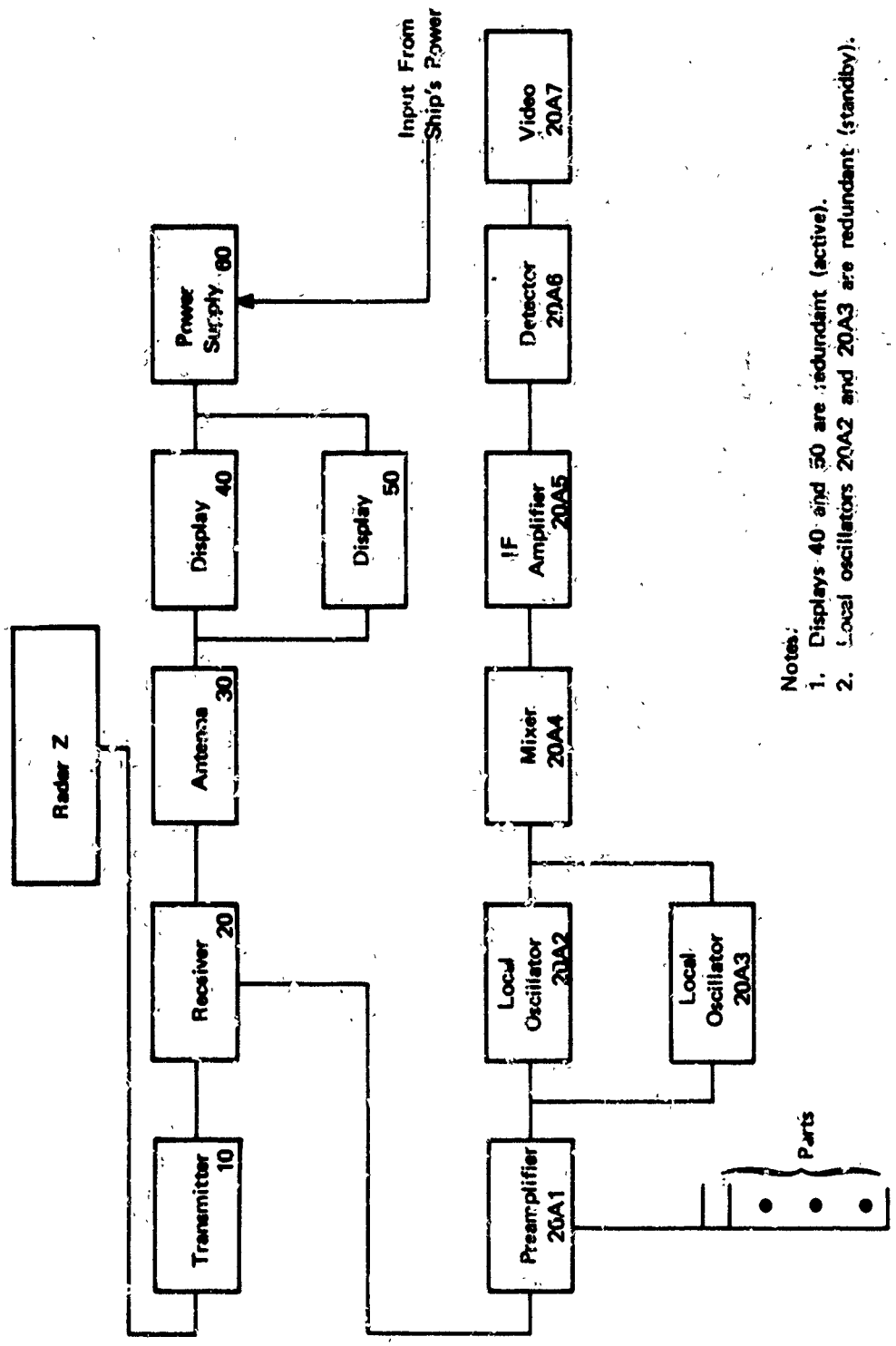
The CR value of the preamplifier unit is 4.6 per 10^6 hr (rounded off to 2 significant figures). This number can be interpreted as the predicted total number of system failures per hour due to preamplifier failures. Whether or not this number is excessive, and thus calls for corrective action, depends upon the requirements for the system and the criticalities for other units in the system. If the number is excessive, it can be reduced by any of the following actions:

(1) Lowering the failure rates of parts in the system by derating
(2) Decreasing the failure mode frequency ratio through selection of other parts
(3) Decreasing the loss probability by changing the system or preamplifier design
(4) Redesign using various techniques such as redundancy, additional cooling, or switching.

Example Problem No. 12

The detail design of a radar system requires the use of FMEA to determine the effect of item failure on the system. The FMEA analysis must be performed at this time prior to freezing the design. Perform an FMEA analysis as follows:

Procedure	Example
(1) Develop a symbolic logic block diagram of the radar system. The units making up the receiver subsystem are shown in detail. In an actual analysis, symbolic diagrams must be constructed for all other subsystems.	See Fig. 8-4.
(2) Fill in the work sheets for all units in the receiver subsystem. Repeat this procedure for all subsystems.	See Fig. 8-5.
(3) Qualitatively estimate the values of loss probability β for each part.	An analysis indicates that for this system the following values of β are applicable: 1.0, 0.1, and 0.
(4) Determine the failure mode frequency ratio α for each failure mode of every part.	The resistor 20A1R1 is fixed, film (Fig. 8-5); from Table 8-1, it has two failure modes: open and drift. α(open) = 0.8 and α (drift) = 0.2.
(5) Tabulate failure rates for each component.	λ(20A1R1) = 1.5 per 10^6 hr for example.
(6) Compute the CR value for each failure mode of each part by Eq. 8-1.	CR(20A1R1 − open) = 0.80 × 1.00 × 1.5 × 10^6 hr = 1.2 per 10^3 hr CR(20A1R1 − drift) = 0.20 × 0.10 × 1.5 per 10^6 hr = 0.030 per 10^6 hr (8-3)
(7) Compute the total CR for the unit $(CR)_t$ by Eq. 8-2.	The total CR for the preamplifier unit is 4.635 per 10^6 hr (See Fig. 8-5).



Notes:
1. Displays 40 and 50 are redundant (active).
2. Local oscillators 20A2 and 20A3 are redundant (standby).

FIGURE 3-4. Symbolic Logic Block Diagram of Radar Example[1]

CRITICALITY WORK SHEET

SYSTEM Radar (Z)
SUBSYSTEM Receiver 20

UNIT Preamplifier 20A1
Parts

PAGE 1 OF 2

(1) Item	(2) Code	(3) Function	(4) Failure Mode	(5) Failure Effect	(6) Loss Probability (β)	(7) Failure Mode Frequency Ratio (α)	(8) Failure Rate (Per Million Hours) (λ)	(9) Criticality (CR)	(10) Comments
Resistor	20A1R1	Voltage Divider	Open	No Output	1.00	0.80	1.5	1.200	Film Resistor
Resistor	20A1R1	Voltage Divider	Change of Value	Wrong Output	0.10	0.20	1.5	0.030	Film Resistor
Resistor	20A1R2	Voltage Divider	Open	No Output	1.00	0.80	1.5	1.200	Film Resistor
Resistor	20A1R2	Voltage Divider	Change of Value	Wrong Output	0.10	0.20	1.5	0.030	Film Resistor
Capacitor	20A1C3	Decoupling	Open	No Effect	0.00	0.35	0.22	0.000	Tubular Tantalum
Capacitor	20A1C3	Decoupling	Short Circuit	No Output	1.00	0.35	0.22	0.077	Tubular Tantalum
Capacitor	20A1C3	Decoupling	High Leakage Current	No Effect	0.00	0.20	0.22	0.000	Tubular Tantalum
Capacitor	20A1C3	Decoupling	Decrease in Capacitance	No Effect	0.00	0.10	0.22	0.000	Tubular Tantalum
Diode	20A1CR3	Voltage Divider	Short Circuit	No Output	1.00	0.75	1.0	0.750	
Diode	20A1CR3	Voltage Divider	Intermittent Ckt.	No Output	1.00	0.20	1.0	0.200	
Diode	20A1CR3	Voltage Divider	Open Circuit	No Output	1.00	0.05	1.0	0.050	
Transistor	20A1Q4	Amplifier	High Collector to Base Leakage Current	No Output	1.00	0.60	3.0	1.800	
Transistor	20A1Q4	Amplifier	Low Beta	No Output	1.00	0.35	3.0	1.050	
Transistor	20A1Q4	Amplifier	Open Terminals	No Output	1.00	0.05	3.0	0.150	
Transformer	20A1T5	Coupling	Shorted Turns	Wrong Output	0.10	0.80	0.30	0.024	

CRITICALITY TOTAL FOR UNIT 4.635

TOTAL 4.561

FIGURE 8-5. Determination of Preamplifier Criticality[1]

CRITICALITY WORK SHEET

SYSTEM Radar (2)
SUBSYSTEM Receiver 20

UNIT Preamplifier 20A1
Parts

PAGE 2 OF 2

(1) Item	(2) Code	(3) Function	(4) Failure Mode	(5) Failure Effect	(6) Loss Probability (β)	(7) Failure Mode Frequency Ratio (α)	(8) Failure Rate (Per Million Hours) (λ)	(9) Criticality (CR)	(10) Comments
Transformer	20A1T5	Coupling	Open Ckt.	No Output	1.00	0.20	0.30	0.060	Composition
Resistor	20A1R8	Bias	Open Ckt.	No Output	1.00	0.05	0.006	0.000	Composition
Resistor	20A1R6	Bias	Change of Value	No Effect	0.00	0.95	0.006	0.000	Composition
Capacitor	20A1C7	Bypass	Open Ckt.	No Effect	0.00	0.40	0.48	0.000	Aluminum
Capacitor	20A1C7	Bypass	Short Ckt.	Wrong Output	0.10	0.30	0.48	0.014	Electrolytic
Capacitor	20A1C7	Bypass	High Leakage Current	No Effect	0.00	0.20	0.48	0.000	
Capacitor	20A1C7	Bypass	Decrease in Capacitance	No Effect	0.00	0.10	0.48	0.000	

CRITICALITY TOTAL FOR UNIT 4.63

TOTAL 0.074

FIGURE 8-5. Determination of Preamplifier Criticality (cont'd).

8-4 COMPUTER ANALYSIS

A computer can be quite useful in performing an FMEA, since a large number of computations and a large amount of record keeping are often required for systems of reasonable size.

In the failure effects portion of the analysis the computer is used primarily for function evaluation, using performance models. On the assumption that the computer program contains the design equations relating system outputs to various design parameters, each item is allowed to fail in each one of its modes, and the effect on the system is computed.

Several computer programs are available for evaluating circuits. The NET-1 (Ref. 3) network analysis program can be used for a failure effects analysis of a circuit containing transistors and passive circuit elements. The value of all of the circuit performance parameters would be printed out for each abnormal condition. NET-1 does not automatically consider failure modes of circuit parts such as shorts and opens; investigation of these require manually setting up a new run for each set of values of the parts. A shorted resistor would have zero resistance and an open resistor would have infinite resistance.

Circuit analysis programs such as ECAP (Electronic Circuit Analysis Program) (Ref. 4), which accept a topological input description of the circuit and synthesize the circuit equations, can be used to evaluate failure effects, but computer running time can become excessive since the circuit equations may have to be generated over again for each run. For extreme failure modes such as an open or a short of a part, the circuit configuration is changed and a completely new solution is required.

The AMAP (Automated Failure Mode Analysis Program) (Ref. 5) is a circuit analysis program that automates the failure effect analysis for DC circuits. It repeatedly solves the circuit equations, computing and printing circuit node voltages, for failure modes such as open and short of parts and shorts between all node pairs. However, AMAP includes only resistors, diodes, transistors, power supplies, and nodes. This automated approach to failure effects analysis can be used effectively in other types of systems such as structures and propulsion systems, but no programs are known which provide these capabilities.

Two other programs that can be used for FMEA are:

(1) IM 045-NAA: Analyzes failure mode effects at system, subsystem, or part level. (Ref. 6)
(2) IM 066-NAA: Revision of IM 045-NAA. (Ref. 8)
(3) IM 063-NAA: Analyzes failure mode effects at system, subsystem, or part level. (Ref. 7).

REFERENCES

1. *Bureau of Ships Reliability Design Handbook*, NAVSHIPS 94501, *Change* 2, Fleet Electronics Effectiveness Branch, Bureau of Ships, 28 February 1965.
2. MIL-STD-16, *Electrical and Electronic Reference Designations*.
3. A. F. Malmberg, "NET-1 Network Analysis Program". *Proceedings of the Eleventh National Symposium on Reliability and Quality Control*, 510-517, 1965.
4. H. N. Tyson, Jr., et al., "The IBM Electronic Circuit Analysis Program (ECAP)". *Proceedings of the 1966 Annual Symposium on Reliability*, 45-65 (1966).
5. D. A. Hausrath and R. Ranalli, "Computer Studies of Abnormally Operating Circuits", *Proceedings of the 1966 Annual Symposium on Reliability*, 66-86 (1966).
6. K. R. Brown, *Failure Mode Analysis Program (IM-045)*, Report No. 63-C5G-043-20-36, North American Aviation, Inc., Downey, California, September 1963.

7. K. L. Bond and D. S. Kordell, *Ground Support Equipment Mode Analysis Program (IM-063)*, Report No. 64-CT-043-14-41, North American Aviation, Inc., Downey, California, March 1964.

8. D. S. Kordell, *Airborne Failure Mode Analysis Program (IM-066)*, Report No. 64-CT-043-14-14, North American Aviation, Inc., Downey, California, January 1964, AD-459 212.

CHAPTER 9 MODELS FOR FAILURE

9-0 LIST OF SYMBOLS

A = parameter in Eq. 9-50
a,b = width and length of a plate
Cdf = Cumulative distribution function
C_l, C_l' = coefficients in linear expansion, defined by Eqs. 9-31C, D
D = diameter
d = design load factor
E = Young's modulus, modulus of elasticity (units of stress)
e = strain (dimensionless)
F = strength
f = stress
G_ϕ = $Cdf\ \{\phi\}$
$\bar{G}_\phi$ = $Sf\ \{\phi\}$
g_ϕ = $pdf\ \{\phi\}$
$gauf$ = Cdf for a standard s-normal (Gaussian) variable
$gaufc$ = Sf for a standard s-normal (Gaussian) variable
G,H = parameters in Eq. 9-50
h = thickness of a plate
l = length
MS = margin of safety
n = limit load factor
n = number of x_i's
N_T, N_S = parameters in Eq. 9-50
p = power, Eq. 9-50
pdf = probability density function
p_o = parameter in Eq. 9-50
P, P_L, P_d = load, limit load, design load
PSM = probabilistic safety margin
Q = probability of failure
Sf = Survivor function, $Sf \equiv 1 - Cdf$
T = temperature, Eq. 9-50
t,u = subscripts → tensile, ultimate
u = stress or strength, random variable
x_i = random variable i
y = a function
α = scale parameter (same units as u)
β = shape parameter (dimensionless)
γ = location parameter (same units as u)
γ_ϕ = coefficient of variation, defined by Eq. 9-31B
δ = elongation
η = defined by Eq. 9-36
λ_R, λ_E = failure rates, see Eqs. 9-49, 9-50
μ_ϕ = mean value of ϕ
π_R, π_E = application factors for resistor failure rates
Σ_E = failure rate term, see Eq. 9-49
σ_ϕ = standard deviation ϕ
Θ = parameter s of a distribution
Θ_k = parameter k of a distribution
ϕ = general name for a random variable, it can be f, F, or $F \cdot f$

9-1 INTRODUCTION

Two main classifications of material behavior are introduced for "things that cause failure", i.e.,

(1) Stress-strength. Any stress below the failure-stress (strength) produces only a reversible effect (such as elongation or increased electric-current flow). When the stress is removed, there is no damage—no evidence that the stress was ever there. A good example is tensile stress in a steel bar.

(2) Damage-endurance. The application of a damager (such as a corrosive fluid) produces damage that cumulates (usually irreversibly). When the damager is removed, the damage remains; if the damager is applied again, the damage increases again. The item fails when the damage exceeds the endurance of the material. A good example is fatigue damage in aluminum alloys due to fluctuating bending stresses.

Both can be treated either deterministically or probabilistically. Data on probabilistic behavior are very difficult (expensive and time consuming) to obtain.

The simple explanations of stress-strength and damage-endurance belie the complicated nature of failure in materials. Structural materials have many modes of failure; e.g., tensile, bending, shear, corrosion, impact, ductile, brittle, fatigue, corrosion-fatigue, stress-cor-

rosion, embrittlement, fretting corrosion, and mechanical abrasion. A description of a steel alloy as "high strength" can be very misleading. Usually, in that case, only uniaxial tension failure is implied, and all other failure modes are neglected. The impact strength, or ductile-brittle transition temperature might be very poor.

Generally speaking, when specialty materials are being used, a specialist on each material ought to be consulted. Metallurgists and material engineers are the most likely consultants in this area. MIL-HDBK-5 (Ref. 3) is a good source of material, but does not cover all failure modes. Handbooks such as Refs. 10, 11 are helpful. Ref. 12 is a good book which describes some failure modes of metals and gives case histories. Every designer should read some case histories of structural failures. It can be a sobering, humble experience.

This chapter introduces several types of mathematical analysis; it does not discuss the detailed knowledge of materials that is so necessary to good structural design. The designer ought also to be aware that it is one thing to specify a material with certain guaranteed properties; it is another thing to get the properties, month after month, on every bit of material delivered under that specification.

The stress/strength notation used in this chapter is taken from MIL-HDBK-5 (Ref. 3, July 72 update). It uses F for strength and f for stress.

9-2 DETERMINISTIC STRESS-STRENGTH

A general stress-strength model can be stated.

> "There exist a scalar S and a value of that scalar S^* such that the part fails if and only if $S > S^*$ (S^* is the strength), values of $S < S^*$ do no damage to the part; in fact, damage less than failure has no meaning. S can only depend reversibly on the environment (mechanical, electric, fluid, temperature, etc.) of the part."

The breakdown voltages of semiconductor devices and tensile failures of structural materials are presumed to be adequately described by this model.

Even in mechanics where this model is applicable, determining the parameter S is not always easy. Ref. 13 lists six stress-strength models for failure with multiaxial stresses: maximum principal stress (Rankine), maximum shear stress (Coulomb), maximum strain energy (Beltrami), maximum distortion energy (Huber, von Mises, Hencky), maximum strain (Saint-Venant), and internal energy (Mohr). For ductile materials the distortion energy model is best when the tension/compression properties are the same, and the internal energy model is best when they are not the same (Ref. 13). Safety codes tend to use the maximum shear model for ductile materials and maximum principal stress model for brittle ones. In each case, the strength is derived by comparison with the parameter of the model when evaluated for uniaxial stress. This detailed example illustrates the complexity of the subject even in a situation that "everyone knows and understands" and where generalization is easy. In this example, even though more than one dimension of stress are combined, they are of the same nature, viz., mechanical stress. The complexity that can arise when this is not true is not often appreciated.

The criteria for failure have been implicitly presumed to exist. Failure must be explicitly defined, and S^* depends on that definition. For example, there are both yield and ultimate strengths of metals which are defined differently, and, for semiconductor devices, the breakdown voltages usually are defined in terms of a specific current or a change in current.

It is conceptually easy to extend the simple stress-strength theory to the case where several different failure modes exist. If they are independent, the resultant strength is fairly simple. If not, the synergistic effects can be taken into account in principle. In practice, the problem is difficult if not impossible and is not pursued very far. Instead, simplifying assumptions are made and life marches on.

9-2.1 TENSILE STRENGTH

This paragraph deals with tensile/compressive stress. The same principles are appli-

cable to other mechanical stress and to more generalized "stresses" such as electric field. MIL-HDBK-5 (Ref. 3) ought to be consulted for a more comprehensive discussion. No mechanical designer ought ever to be without the latest version of MIL-HDBK-5.

A structural nonviscoelastic material undergoes strain when a uniaxial stress is applied. Most such materials have a linear region, i.e., Hooke's law holds as long as the stress is not too high.

$$f_t = eE \tag{9-1}$$

where

f_t = tensile stress, force/area

e = strain (elongation/original length), dimensionless. Strain is often given "units" of inches/inch.

E = modulus of elasticity, force/area.

Even though the modulus of elasticity is independent of stress and strain in the linear region (by definition of linear region), it does depend on temperature and on material composition and structure. Although for ferrous alloys, it is remarkably independent of composition and structure.

Beyond the limits of Hooke's law, strain increases as the stress increases, but the linearity ceases. Plotting stress against strain for any material gives the tensile-test diagram, Fig. 9-1. Fig. 9-1(A) is typical of a ferrous material such as carbon or alloy steel, and Fig. 9-1(B) is typical of some nonferrous materials such as brass and aluminum and of some stainless steels. The important distinction between the two curves is that Fig. 9-1(A) shows a definite inflection point and change of curvature, whereas Fig. 9-1(B) does not.

Certain points on these curves have been defined and are important material properties. Consider first the stress-strain curve in Fig. 9-1(A). The region from zero to A is a reasonably straight line, showing that the material is obeying Hooke's law (say, within 0.1% or so). This leads to the definition of point A as the *proportional limit*. It readily can be seen that the equation of this line is the familiar $f_t = eE$, where E is the slope.

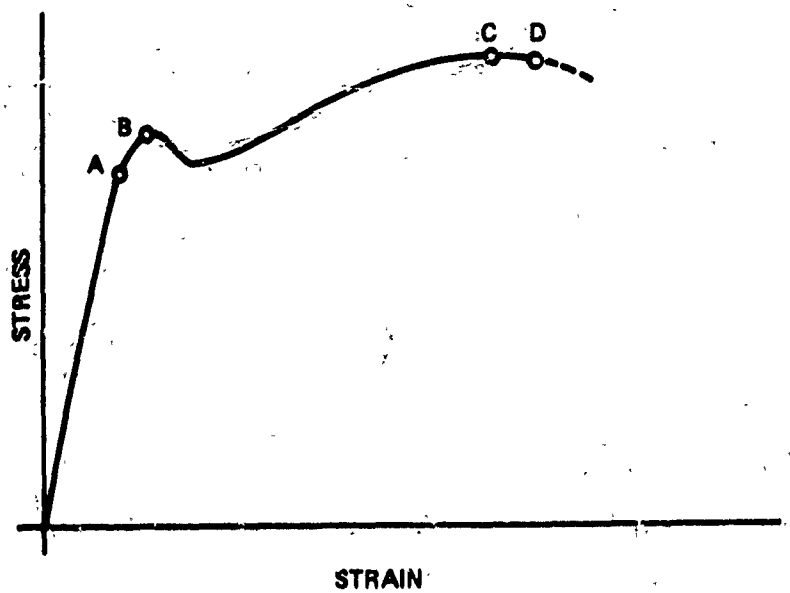
Beyond point A linearity ceases, and at point B a sudden increase in elongation takes place with little or no increase in load. This phenomenon is called *yielding*, and point B is called the *yield point* of the material. The stress associated with this point is the *yield stress*. Once this point is reached in the material, all load can be removed from the specimen and the stress returned to zero, but a residual strain, *permanent set*, will remain. Any permanent set is usually considered detrimental to a structural member.

Beyond point B, stress and elongation continue to change until the maximum stress, the *ultimate stress*, is reached at point C. Rupture of the material occurs at point D, which is reached without any increase in stress or load. In fact, decreasing the load beyond point C will not necessarily avert fracture. The curve of Fig. 9-1(A) exhibits this definite, observed yield point; one which easily can be recognized as it occurs during a tensile test. The region near M is very machine dependent. The fall-off in stress is caused by the slow-rate of pulling the specimen by the tensile machine.

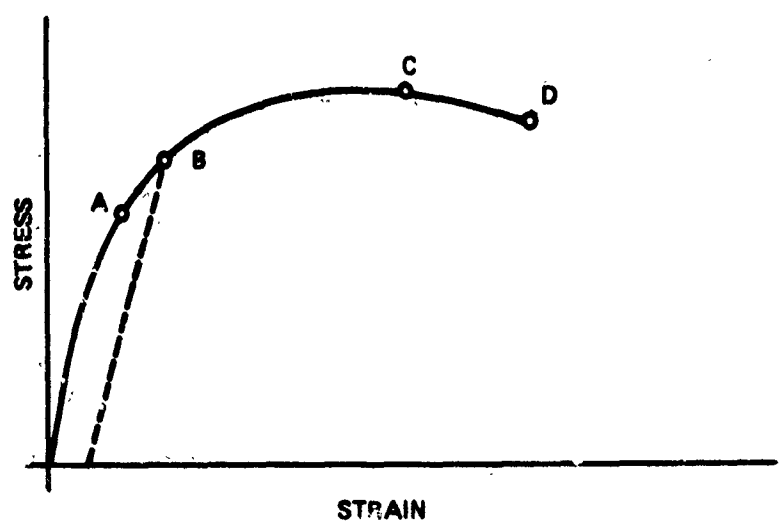
The materials represented by Fig. 9-1(B), however, do not exhibit as definite a yield point, although the other points on the curve are defined in the same manner as their counterparts in Fig. 9-1(A). In materials such as those represented by Fig. 9-1(B), it generally is accepted that the yield point is the stress at the 0.2 percent "offset point", viz., the point at which the actual strain exceeds the linearly extrapolated strain by 0.002. To find this point, draw a line through the point (e = 0.002, S = 0) with a slope of E; where this line intersects the curve is the 0.2 percent yield point of the material.

Similar diagrams will result for tests in compression and in shear, although the modulus might be different. These structural properties are listed in tables in various handbooks, such as MIL-HDBK-5 (Ref. 3) which has joint military service approval.

The properties presented in most handbooks are room-temperature properties. If a problem involves elevated temperatures, the allowable properties must be those for the elevated temperature; these are usually lower than the room temperature properties. Although the tables in MIL-HDBK-5 generally are room-temperature values, some curves do give the effects of temperature. If these curves



(A) Ferrous Metals Such as Carbon or Alloy Steel



(B) Brass, Aluminum, and Some Stainless Steel

FIGURE 9-1. Typical Tensile-test Diagrams[3]

are inadequate, the Military Specifications governing the specific materials ought to present the elevated-temperature data required if they exist. It is easy for the designer to be lulled by a false sense of security by data in handbooks and supplier's literature. Not much really is guaranteed unless:

(1) The data to be guaranteed appear in the purchase order
(2) The receiving inspection actually checks it
(3) No waivers are given for discrepant material.

9-2.2 SAFETY FACTORS, LOAD FACTORS, AND MARGIN OF SAFETY

Load analysis is used to determine the loads which exist on the structure under consideration. Stress analysis is the means by which the designer determines whether his structure is adequate to withstand these loads without failure. Since no universal criteria for failure exist, they must be defined to suit each problem. Mechanical failure can be divided into four general categories:

(1) *Rupture.* A physical parting of the fibers or grains of the material when the ultimate (tensile or shear) stress is exceeded.
(2) *Yielding.* The stress in the material exceeds its yield stress in tension, compression, or shear and permanent set takes place.
(3) *Buckling.* The stress exceeds an allowable stress that is determined by the geometry of the loaded member. For example, columns buckle at a stress which depends upon the length to radius-of-gyration ratio; thin flat panels buckle under a shear stress that depends upon the ratio of panel width to metal thickness.
(4) *Deflection.* Since all structural members deflect under load, this deflection becomes a failure criterion in certain problems, particularly those associated with vibration environments.

Some confusion exists among designers in the definition and use of safety factors, load factors, and margins of safety.

Therefore, to clarify their use in the following discussion, they are defined here.

Safety Factors. Safety factors are numbers representing a degree of uncertainty in the expected load, the material properties, or other pertinent data of the problem. These are applied to reduce the nominal properties of the material to a lower value that shall then not be exceeded in the design calculations. For example, tensile ultimate stress for 2024T4 aluminum alloy extruded bar stock is published in MIL-HDBK-5 (July 72 update) as 57,000 psi (for < 0.50 in. diameter; L,A basis). A safety factor of 3 applied to a member designed in the alloy would reduce this ultimate stress to an allowable stress of 19,000 psi. Fatigue from repeated or cyclic loads sometimes is treated by applying a safety factor to the ultimate stress of the material but it is better to use fatigue curves if they are available.

Abrupt changes in cross section, notches, grooves, or other discontinuities ought to be avoided in the design of structural parts, since these function as stress raisers. When these cannot be avoided, the designer must apply specific design factors in these local areas. Many handbooks publish tables and examples or guides to the magnitude of design factors which can be used and which are considered adequate. However, the engineer must be cautioned to use care in his selection of a design factor from a handbook since the degree of uncertainty of the data usually is not presented.

Load Factors. Load factors are numbers representing multiplying factors applied to the *load* on the structure. Loads can be caused by any number of environmental conditions such as an aircraft in arrested landing or in catapult take-off, a truck proceeding across country on rough or bumpy roads, or a ship subjected to an underwater blast or the firing of its own guns. Load factors usually are expressed in terms of *g*, or gravity units. Since the load analysis has been performed under a 1-*g* condition, the load factors easily can be taken into account by multiplying calculated loads and reactions by the proper load factor. By this simple means, it is easy to take into account different loading conditions in different directions or at different points in

the structure without directly affecting the original load analysis.

Limit Load. Limit load is the load that the structure is expected to experience—it is the limit of the load on the structure.

Design Load. Design load is larger than the limit load and is used to compare the stress in the structural members. Usual practice for airborne equipment is to define:

$$\text{Design Load} = 1.5 \times (\text{limit load}) \quad (9\text{-}2)$$

Although the 1.5 design load factor can be modified by the individual designer, it is recommended that the range of selection remain between 1.5 and 2.0. Larger factors tend to be too conservative and result in an overweight and more costly structure.

Margin of Safety. Margin of safety *MS* is the fraction increase of the computed stress required to equal the allowable stress. It is calculated by the relationship:

$$MS = \frac{\left(\begin{matrix}\text{allowable}\\ \text{stress}\end{matrix}\right) - \left(\begin{matrix}\text{computed}\\ \text{stress}\end{matrix}\right)}{\text{computed stress}} \quad (9\text{-}3)$$

If the computed stress equals the allowable stress, there is obviously a zero margin of safety, and failure is imminent. Therefore, a positive margin is desired in all design, and experience has shown that a 15-percent margin is adequate for most purposes. Exceptions should be made to this rule in some instances where a single bolt carries the load in tension (50-percent margin recommended), or where a particularly severe design condition has a negligible possibility of occurrence (zero margin may be acceptable).

Allowable Stress. An allowable stress is defined as the stress that a member may be allowed to reach (zero margin) and beyond which failure as previously defined is imminent. When yielding is the failure criterion, the allowable stress is the yield stress as modified by any imposed safety factors. For all other cases (e.g., when rupture is the failure criterion), the allowable stress is the ultimate stress of the material (whether taken from a handbook or calculated from a formula such as Euler's column formula) as modified by any imposed safety factors. In some special problems where it is specified that the yield stress shall be used as the failure criterion, the limit load can be multiplied by some lower, minimum design load factor, e.g., 1.15, instead of the 1.5 previously noted (to conserve weight and cost). All problems and examples in this discussion, however, consider the design load factors, and the margins of safety are computed on the ultimate stress.

Some sample problems will illustrate the preceding discussion; Example Problem No. 13 follows.

9-3 PROBABILISTIC STRESS-STRENGTH

Probabilistic stress/strength analysis is a reliability analysis technique used to analyze structures and mechanical and electrical components. Pioneering work in this field was accomplished by Robert Lusser at Redstone Arsenal. A summary of Lusser's work is presented in Ref. 1. For mechanical systems, the technique consists of computing the probability that the applied stress exceeds the material strength, assuming that the strength varies from item to item and the applied stress is variable. The strength of a particular class of component or item varies because of irregularities in the manufacturing process. By this technique a system can be designed in such a way that the probability of failure is below some prescribed value. Once the allowable failure probability is specified, the system design parameters can be computed.

Probabilistic stress/strength analysis is concerned with the problem of determining the probability of failure of a part which is subjected to a stress f and which has a strength F (Ref. 4). Both f and F are assumed to be random variables with known distributions; the *pdf*'s of f and F are illustrated in Fig. 9-3. Failure occurs whenever stress exceeds strength. Therefore, the probability of failure is equivalent to the probability that stress exceeds strength.

The definitions of terms used in Fig. 9-3 and used later in the chapter follow:

pdf = probability density function
Cdf = cumulative distribution function
Sf = survivor function
Θ = parameters of the distribution, $\Theta \equiv \{\theta_1, \theta_2, \ldots\}$

Example Problem No. 13

A 2024T4 aluminum-alloy rod, 10 in. long ℓ, is loaded with 2000 lb P as shown in Fig. 9-2. Find the diameter D of rod required to support this load when subjected to a limit load factor n of 3.2, a design load factor d of 1.5, and a minimum margin of safety MS of 15 percent: (a) to avoid rupture, and (b) to have a maximum elongation δ of 0.04 in. under 1-g conditions.

Procedure	Example	
(1) State the basic conditions.	$\ell = 10$ in. $p = 2{,}000$ lb $n = 3.2$ $d = 1.5$ $MS = 15\%$	(9-4)
(2) Determine the ultimate stress F_{tu} for the 2024T4 aluminum rod from MIL-HDBK-5 (pp. 3-50, July 72 update).	$F_{tu} = 57 \times 10^3$ psi(L,A basis)	(9-5)
(3) Since rupture is the defined failure criterion and no safety factor is involved, the allowable stress F is taken as the ultimate stress F_{tu}. From the equation for margin of safety MS (Eq. 9-3), the computed stress f_t is: $f_t = F/(1+MS)$ (9-6)	$f_t = 57 \times 10^3/(1 + 0.15)$ $= 49.6 \times 10$	(9-7)
(4) Compute the required limit load P_L by: $P_L = nP$ (9-8)	$P_L = 3.2 \times 2{,}000$ $= 6{,}400$ lb	(9-9)
(5) Compute the design load P_d by: $P_d = dP_L$ (9-10)	$P_d = 1.5 \times 6{,}400$ $= 9{,}600$ lb	(9-11)
(6) Compute the required cross-sectional area A_{req} of the rod by: $A_{req} = \pi D^2/4 = P_d/f_t$ (9-12)	$A_{req} = 9{,}600/49{,}600$ $= 0.194$ in.^{2}	(9-13)
(7) Compute the required diameter D_{req} of the rod by: $D_{req} = (4A/\pi)^{1/2}$ (9-14)	$D_{req} = (4 \times 0.194/\pi)^{1/2}$	(9-15)
(8) Compute the elongation δ of the rod by: $\delta = P\ell/(AE)$ (9-16) where E is the modulus of elasticity = 10.8×10^6 psi (from MIL—HDBK-5, pp. 3-50, July 72 update).	$\delta = 2{,}000 \times 10/(0.194 \times 10.8 \times 10^6)$ $= 0.0095$ in.	(9-17)

The elongation (0.0095 in.) is well within the elongation limit (0.04 in.). Therefore, the required diameter is 0.496 in., and if the standard machine-shop tolerance is ± 0.010 in., the nominal diameter to be specified is 0.506 in. Standard 0.500 in. diameter extruded bar stock available from a warehouse is probably the practical choice in this problem, because the tolerance on the stock is less than ± 0.010 in., which eliminates the need for machining.

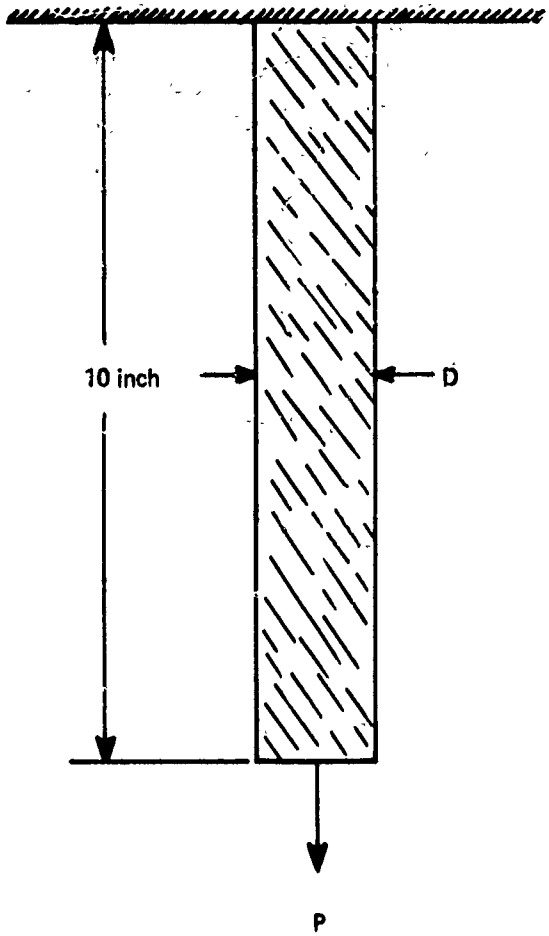


FIGURE 9-2. Aluminum Simple Uniaxial Tension[2]

f = stress (also used as subscript)
F = strength (also used as subscript)
F-f = exceedance of strength over stress (also used as subscript)

$g_\phi(\cdot;\Theta_\phi)$ = *pdf* of ϕ; the parameters of the distribution are Θ_ϕ
$G_\phi(\cdot;\Theta_\phi)$ = *Cdf* of ϕ; the parameters of the distribution are Θ_ϕ
$\bar{G}_\phi(\cdot;\Theta_\phi)$ = *Sf* of ϕ; the parameters of the distribution are Θ_ϕ
ϕ = general name for any random variable; it can be f,F, or $F-f$

The Θ need not always be written, because a distribution always has parameters; but often it helps to show the parameters explicitly. The distributions of stress and strength are usually assumed to be one of the tractable smooth distributions such as s-normal (Gaussian), Weibull, or lognormal; but nature itself is rarely restricted by mathematical tractability.

The concept of safety factor can be incorporated into probabilistic stress/strength analysis (Ref. 5). In par. 9-3.2, a method is described for quantitatively defining a safety factor in terms of the possible variations of component design variables and for computing the probability of safety for a given load.

9-3.1 COMPUTING PROBABILITY OF FAILURE

To compute the probability of failure, one must compute the probability that one random variable, called stress, exceeds another random variable, called strength (Ref. 4). In practical applications, these random variables are s-independent of each other.

There are 3 forms in which the probability of failure can conveniently be written.

$$Q\{\Theta_f, \Theta_F\} = \int_0^\infty g_f(u;\Theta_F)G_F(u;\Theta_f)du \quad (9\text{-}18)$$

$$Q\{\Theta_f, \Theta_F\} = \int_0^\infty g_F(u;\Theta_F)\bar{G}_f(u;\Theta_f)du \quad (9\text{-}19)$$

$$Q\{\Theta_{F-f}\} = G_{F-f}(0;\Theta_{F-f}) \quad (9\text{-}20)$$

where $Q\{\cdot\}$ is the notation for probability of failure. Eqs. 9-18 and 9-19 can be readily transformed into each other by integrating by parts.

Eq. 9-18 is obtained from Fig. 9-3 as follows. Pick a value of u as illustrated by the vertical dashed line. The element of probability-of-failure is the probability $g_f(u;\Theta_f)du$ that the stress is in the neighborhood of u times the probability $G_F(u;\Theta_F)$ that the strength is below u. This element of probability is integrated over all possible values of u to give the probability of failure.

Eq. 9-19 is similarly obtained except that the element of probability-of-failure is the

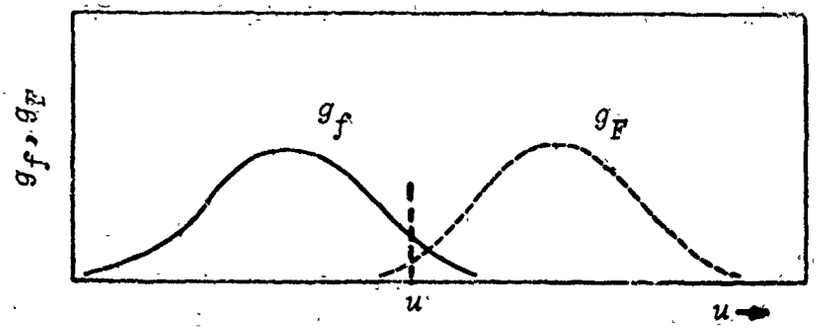


FIGURE 9-3. Typical Probability Density Function g of Stress f and Strength F.

probability $g_F(u;\Theta_F)du$ that the strength is in the neighborhood of u times the probability $G_f(u;\Theta_f)$ that the stress is above u.

Eq. 9-20 is derived by considering the distribution of F-f. $G_{F-f}(u;\Theta_{F-f})$ is the *Cdf* of F-f at the point u. The failure probability is the probability that F-$f < 0$; this probability is $G_{F-f}(0;\Theta_{F-f})$ by definition of the *Cdf*.

Even though it is possible to use any of the three equations 9-18, 9-19, 9-20 in a calculation, usually one will be much more tractable than the others.

The solution of practical problems requires the evaluation of an integral. For some stress and strength factors, these integrals can be expressed in terms of known functions. In other cases, the integrals must be numerically evaluated. Several practical cases are considered:

(1) *s-Normally Distributed Strength and s-normally Distributed Stress*

Given:

(1) Stress f has s-normal (Gaussian) distribution with mean μ_f and standard deviation σ_f.
(2) Strength F has s-normal (Gaussian) distribution with mean μ_F and standard deviation σ_F.
(3) Stress and strength are s-independent, given that the parameters of their distributions are known.

Find: Probability of failure.

Solution: Eq. 9-20 is easiest to use because the distribution of F-f is easily calculated. If 2 random variables are s-independently and s-normally distributed, their difference has a s-normal distribution whose mean is the difference of the 2 means and whose variance is the sum of the 2 variances. (This statement is true regardless of the distributions, but the results are very tractable for the s-normal distribution.) Therefore F-f has a s-normal distribution with mean μ_{F-f}

$$\mu_{F-f} = \mu_F - \mu_f \tag{9-21}$$

and standard deviation σ_{F-f}

$$\sigma_{F-f} = (\sigma_F^2 + \sigma_f^2)^{1/2}. \tag{9-22}$$

The probability of failure Q is, from Eq. 9-20

$$Q = gauf\left(\frac{-\mu_{F-f}}{\sigma_{F-f}}\right) \tag{9-23}$$

where *gauf* is the *Cdf* of the standard s-normal (Gaussian) distribution. (Named analogously to the error function.)

Example Problem No. 14 illustrates the procedure.

(2) *Weibull Distributed Strength and Weibull Distributed Stress*

The Weibull distribution is more difficult to work with than the s-normal distribution. The probability of failure cannot be obtained in closed form. The procedure used to compute the probability of failure for cases in which both stress and strength have Weibull distributions is to develop the integral expression for probability of failure and to evaluate this integral numerically. A detailed table of values of the integral for Weibull parameter values pertinent to mechanical problems is given in Ref. 6.

Example Problem No. 14:

A mechanical component has a s-normal strength distribution with $\mu_F = 22 \times 10^3$ psi and $\sigma_F = 1.5 \times 10^3$ psi. The applied stress is s-normally distributed with $\mu_f = 19 \times 10^3$ psi and $\sigma_f = 2.0 \times 10^3$ psi. What is the probability of failure?

Procedure	Example	
(1) State the parameters of the strength distribution.	$\left.\begin{array}{l}\mu_F = 22 \times 10^3 \text{ psi} \\ \sigma_F = 1.5 \times 10^3 \text{ psi}\end{array}\right\}$	(9-24)
(2) State the parameters of the applied stress.	$\left.\begin{array}{l}\mu_f = 19 \times 10^3 \text{ psi} \\ \sigma_f = 2.0 \times 10^3 \text{ psi}\end{array}\right\}$	(9-25)
(3) Compute μ_{F-f} and σ_{F-f} by Eqs. 9-21 and 9-22.	$\mu_{F-f} = 22 \times 10^3 - 19 \times 10^3 = 3 \times 10^3 \text{ psi}$	(9-26)
	$\sigma_{F-f} = \left[(1.5 \times 10^3)^2 + (2.0 \times 10^3)^2\right]^{1/2} = 2.5 \times 10^3 \text{ psi}$	(9-27)
(4) Determine the probability of failure Q by Eq. 9-23. This probability can be evaluated using tables of *gauf*, viz., s-normal (Gaussian) *Cdf*.	$Q = gauf\left(\frac{-3 \times 10^3}{2.5 \times 10^3}\right) = gauf(-1.2) = 0.115$	(9-28)

The most useful form of the Weibull *Cdf* for stress/strength reliability prediction is:

$$Cdf\{u\} = \exp\left[-\left(\frac{u-\gamma}{\alpha}\right)^{\beta}\right] \qquad (9\text{-}29)$$

where

γ = location parameter (same dimension as u)
α = scale parameter (same dimension as u)
β = shape parameter (dimensionless)
u = stress or strength

See *Part Six, Glossary and Mathematical Appendix* for more discussion of the Weibull distribution. Eq. 9-18 or 9-19 is used for the calculation of Q.

(3) *Weibull Distributed Strength and s-normally Distributed Stress*

This, too, is intractable. Eq. 9-18 or 9-19 must be numerically evaluated for every case. Ref. 6 has some tables for this case.

The reasons that stress and strength are often assumed to be s-normally distributed are:

(1) It is not a terribly bad approximation.

(2) Probabilities of failure are calculated readily, once the data are known.

(3) It is difficult enough to get good data for your problem, even with this simple assumption. Most structural metals are ordered by a specification that is not well related to a sophisticated probabilistic analysis. Most receiving inspections are even less well able to assure that the material being received has the properties that were assumed in the calculations.

9-3.2 PROBABILISTIC SAFETY MARGIN

The probabilistic safety margin relates the mean difference between stress and strength to the uncertainty in that difference. This concept generally is attributed to Lusser (Ref. 1). The definition of probabilistic safety margin is:

$$PSM \equiv \frac{\mu_{F-f}}{\sigma_{F-f}} = \frac{\mu_F - \mu_f}{(\sigma_F^2 + \sigma_f^2)^{1/2}} \qquad (9\text{-}30)$$

where

PSM = probabilistic safety margin
F = strength
f = stress
μ_{F-f} = mean of F-f
σ_{F-f} = standard deviation of F-f

F and f are presumed to be s-independent; so Eqs. 9-21 and 9-22 hold.

The PSM is sometimes called a safety limit.

The statistical properties of F are presumed to be known directly; while those of f must be calculated from other information. Suppose that f is a function of several random variables whose coefficients of variation are small enough that the function can reasonably be linearized. The following notation is used:

$f = y(x_1, x_2, \ldots, x_n)$
i = index, $i=1, \ldots, n$
x_i = random variable which affects f (9-31A)
n = number of variables
μ_i = mean of x_i
σ_i = standard deviation of x_i

$$\gamma_i = \sigma_i/\mu_i \qquad (9\text{-}31B)$$
= coefficient of variation of x_i, $\gamma_i < 1$

$$c_i = \frac{\partial y}{\partial x_i}$$

$$c_i = \left.\frac{\partial y}{\partial x_i}\right|_{\mu_1, \ldots, \mu_n} \qquad (9\text{-}31C)$$

$$c_i' = \frac{x_i}{y}\left.\frac{\partial y}{\partial x_i}\right|_{\mu_1, \ldots, \mu_n} = \left.\frac{\partial \ln y}{\partial \ln x_i}\right|_{\mu_1, \ldots, \mu_n} \qquad (9\text{-}31D)$$

Then y is presumed to be expanded in a Taylors series, so the following relationships will hold:

$$y - \mu_f = c_1(x_1 - \mu_1) + \ldots + c_n(x_n - \mu_n) \qquad (9\text{-}32)$$

$$\mu_f = y(\mu_1, \mu_2, \ldots, \mu_n) \qquad (9\text{-}33)$$

$$\sigma_f^2 = c_1^2\sigma_1^2 + \ldots + c_n^2\sigma_n^2 \qquad (9\text{-}34)$$

$$\gamma_f^2 = (c_1'\,\gamma_1)^2 + \ldots + (c_n'\,\gamma_n)^2 \qquad (9\text{-}35)$$

The variations are given usually in terms of the σ_i or γ_i; e.g., the 2-in. thick bar has a thickness variation of $\sigma = 0.01$ in., or, it has a thickness variation of $\gamma = 0.5\%$.

The random variable η defined by:

$$\eta = \frac{F - f}{\sigma_{F-f}} \qquad (9\text{-}36)$$

has a distribution which generally is not known. Its mean and standard deviation are easily shown to be:

$$\left.\begin{aligned} \mu_\eta &= PSM \\ \sigma_\eta &= 1 \end{aligned}\right\} \qquad (9\text{-}37)$$

since η is just the F-f, normalized by its standard deviation. Eq. 9-20 can be used to find the probability of failure, for a given *PSM*, if the distribution is known. In the absence of knowing the distribution, Chebyshev's (also spelled Tchebycheff) limit often is used. This limit gives the greatest fraction of any distribution that can be in the tail region (μ and σ must be known exactly). The greatest 2-sided fraction is achieved for the unlikely probability mass function which consists of a large "spike" of mass $1-\epsilon^*$ at the mean μ, and two smaller spikes just beyond $\mu \pm \eta\sigma$, each of mass $\epsilon^*/2$, where

$$\epsilon^* = 1/\eta^2 \qquad (9\text{-}38)$$

Eq. 9-38 is Chebyshev's 2-sided limit, i.e., the maximum fraction of a distribution which can be outside the range $\mu \pm \eta_\sigma$. A similar analysis shows that the 1-sided limit, the fraction that can be beyond $\mu + \eta_\sigma$, is $1/(\eta^2 + 1)$. Table 9-1 compares the Chebyshev inequality with the s-normal (Gaussian) distribution.

For example, if a *PSM* were 3.0, the maximum (Chebyshev) probability of failure (1-sided) is 10%, while the s-normal (Gaussian) distribution shows 0.14%. While nature is rarely as bad as it could be, it is often much worse than we would like. So be wary of using the s-normal distribution to calculate very low probabilities.

The procedure for using the *PSM* is to find the standard deviation of f from Eqs. 9-34 or 9-35 and then to calculate the *PSM*. Usually the failure probability is calculated from the Chebyshev and the s-normal formulas, and the engineer uses whatever means of reconciling the two he wishes; the Reasonable-Engineering-Guess for this purpose is explained and tabulated in Table 9-1.

Example Problem No. 15 shows how the method works in practice.

9-4 SIMPLE CUMULATIVE DAMAGE

Fatigue and corrosion are very common examples of failure caused by a cumulation of damage. MIL-HDBK-5 contains fatigue curves for many metals. It takes many complicated curves to show the fatigue behavior of one metal. Even then, probabilistic effects are ignored. Such curves are usually median curves—about 50 percent of the specimens will fail above the curve, and 50 percent below the curve.

When the severity level of the damager ("stress") changes, it is difficult to calculate the cumulative effect. The most common assumption is a linear one, that the rate of cumulating damage at any one severity level is constant over the life of the item and is independent of any damage the item has already cumulated. It is not really a very good assumption, but in everyday design work, it's about as good as can be done.

Some of the treatments in pars. 9-2 and 9-3 can be applied to cumulative damage since their main message is how to handle uncertainties and how to pay attention to detail.

MIL-HDBK-5 is also a valuable source of information on cumulative damage failure-modes other than fatigue, but it doesn't take the place of a material specialist

9-5 SEVERITY LEVELS FOR ELECTRONIC EQUIPMENT

Detailed procedures have been developed which permit the computation of electronic component catastrophic failure rates as a function of applied "stress" caused by operating and environmental conditions (Ref. 8). A detailed description of the technique is given for a specific category of component, the fixed, composition resistor, Style RC22,

TABLE 9-1

Comparison of the Chebyshev-limit, the *s*-normal distribution and the Reasonable-Engineering-Guess (REG)* (Both the mean and standard deviation are presumed known exactly.)

1-sided tail

(Table gives the fraction beyond k standard deviations, in %)

k	Chebyshev limit (CL) $1/(k^2+1)$	*REG gaufc(0.8k)	*s*-Normal (N) gaufc(k)	$\sqrt{N \times (CL)}$/REG **
1.0	50	21	16	1.3
1.5	31	12	6.7	1.2
2.0	20	5.5	2.3	1.2
2.5	14	2.3	.62	1.3
3.0	10	.82	.14	1.4
3.5	7.5	.26	.023	1.6
4.0	5.9	.069	.0032	2.0
4.5	4.7	.016	.00034	2.5
5.0	3.8	.0032	.000029	3.3

2-sided tails

(Table gives the fraction outside ±k standard deviations, in %)

k	Chebyshev limit (CL) $1/k^2$	*REG 2 gaufc(0.8k)	*s*-Normal (N) 2 gaufc(k)	$\sqrt{N \times (CL)}$/REG **
1.0	100	42	32	1.3
1.5	44	23	13	1.0
2.0	25	11	4.6	.97
2.5	16	4.6	1.2	.95
3.0	11	1.6	.27	1.1
3.5	8.2	.51	.047	1.2
4.0	6.3	.14	.0063	1.4
4.5	4.9	.032	.00068	1.8
5.0	4.0	.0063	.000057	2.4

* The Reasonable-Engineering-Guess (REG) for the fraction lying in a tail region is a quick-and-dirty way of being less pessimistic than the Chebyshev limit and the *s*-normal distribution tail area. In order to make it easy to work with, the REG is calculated from the *s*-normal tables, as follows. The number of standard deviations, k, is calculated; then the *s*-normal tables are entered with 0.8k instead of k in a straightforward way in either a 1-sided or 2-sided calculation as shown in the tables above.

There is nothing "theoretically true" about either the geometric mean or the Reasonable-Engineering-Guess; they are just seat-of-the-pants. But the REG can be very useful and easy to use. It helps an engineer be more realistic about the tail areas of distributions than either the *s*-normal or Chebyshev calculation is likely to be.

** This column gives the ratio of the "geometric mean of the Chebyshev limit and the *s*-normal tail area" to the Reasonable-Engineering-Guess.

Example Problem No. 15

Given:

(1) Rectangular steel plate, type AISI 4340, heat-treated to a nominal (mean) yield strength of $F = 90 \times 10^3$ psi, $\gamma_F = 20\%$
(2) Plate size (see Fig. 9-4): width $a = 30$ in. nominal (mean), $\gamma_a = 5\%$, length $b = 10$ ft nominal (mean), $\gamma_b = 2\%$, thickness h to be calculated, $\gamma_h = 0.4\%$
(3) Loading, uniform applied load $P = (80 \pm 20)$ lb/ft² (0.556 psi).
(4) Plate is supported simply (no bending), along each end, but not the sides.
(5) The plate ought not to yield in service near room temperature.
(6) Characteristics in (1)-(4) are s-independent.

Find:

(1) Plate thickness (nominal) for a $PSM = 4$
(2) Plate thickness by conventional calculations
(3) The failure probability corresponding to $PSM = 4$.

Procedure	Example	
(1) State the geometrical characteristics of the plate.	$\left.\begin{array}{l}\mu_a = 30 \text{ in.}, \gamma_a = 5\% \\ \mu_b = 10 \text{ ft} = 120 \text{ in.}, \gamma_b = 2\%\end{array}\right\}$ $\mu_h = ?, \gamma_h = 0.4\%$	(9-39)
(2) State the strength. State the load (assume worst-case for σ).	$\mu_F = 90 \times 10^3$ psi, $\gamma_F = 20\%$ $\mu_P = 80$ lb/ft² $= 0.556$ psi, $\gamma_P = \frac{20}{80} = 25\%$	
(3) Check Ref. 2 pp. 372, 404 for the formulas for maximum stress. Adapt to this problem. f does not depend on a.	$f = \frac{3Pb^2}{4h^2}$ $\ln f = \ln(3/4) + \ln P + 2\ln b - 2\ln h$	(9-40)
(4) Calculate partial derivatives of $\ln f$ with respect to $\ln P$, $\ln b$, $\ln h$ in Eq. 9-40. Evaluate at the mean values.	$c_p' = 1, c_b' = 2, c_h' = -2$	(9-41)
(5) Calculate γ_f by Eq. 9-35. It is obvious, here, that the variation in load is the only important variation.	$\gamma_f^2 = (1 \times 25\%)^2 + (2 \times 2\%)^2 + (-2 \times 0.4\%)$ $\gamma_f = 0.253$	(9-42)
(6) Use Eq. 9-30, with $\sigma_f = \mu_f \times \gamma_f$.	$4 = \frac{90 \times 10^3 \text{psi} - \mu_f}{[(20\% \times 90 \times 10^3 \text{psi})^2 + (0.253\mu_f)^2]^{1/2}}$	(9-43)
(7) Solve by trial and error for μ_F (the mean of F) (or other convenient method).	$\mu_f = 16.2 \times 10^3$ psi	(9-44)

(8) Find μ_h (the mean of h) from Eq. 9-40, by substituting mean values. Nominal plate thickness is 0.61 in.

$$16.2 \times 10^3 \text{ psi} = \frac{3 \times 0.556 \text{ psi} \times (120 \text{ in.})^2}{4h^2} \tag{9-45}$$

$$\mu_h = 0.61 \text{ in.}$$

(9) Just for fun, go back to Eq. 9-43 and evaluate σ_F and σ_f. Thus the major contributor to σ_{F-f} is σ_F.

$$\begin{aligned} \sigma_F &= 20\% \times 90 \times 10^3 \text{ psi} \\ &= 18 \times 10^3 \text{ psi} \\ \sigma_f &= 0.253 \times 16.2 \times 10^3 \text{ psi} \\ &= 4.1 \times 10^3 \text{ psi} \end{aligned} \tag{9-46}$$

(10) Make the conventional calculation. Use a safety factor of 1.5 on the yield stress and the maximum load. Use nominal plate size. Use Eq. 9-40.

$$\frac{90 \times 10^3 \text{ psi}}{1.5} = \frac{3 \times \left(\frac{100}{144} \text{ psi}\right) \times (120 \text{ in.})^2}{4h^2} \tag{9-47}$$

(11) Find the failure probability corresponding to $PSM = 4$. Use Table 9-1 with $k = 4.0$; find the 1-sided probabilities.

Chebyshev	5.9%
Normal	0.0032%
Reasonable-Engineering-guess	0.069%

(9-48)

Look back at the results. The $PSM = 4$ approach produced a ridiculously low value of yield stress to use. It turns out to be a safety factor of about 5. Not many designs can afford that luxury. Some test programs on receiving inspection and some better heat-treat control in manufacture are in order, to reduce the variation in yield strength. The benefit of this calculation is not the 0.61 in. thickness calculated for the plate, but the increased understanding of the failure causes and where they ought to be reduced.

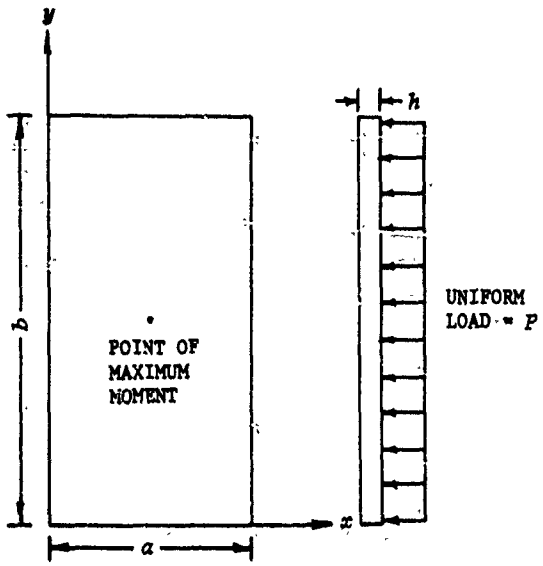


FIGURE 9-4. Simply Supported Rectangular Plate Subject to Uniform Load P

MIL-R-11/4E (Ref. 9). Although the specific equations and constants may be different for other components, the general approach is applicable. The discussion is adapted from the RADC *Reliability Notebook*, Volume II (Ref. 8). (Ref. 8 has been replaced by Ref. 13, but the procedure is similar.)

The fixed, composition resistor, RC22, consists of a mixture of finely divided carbon and binder, either in the form of a slug or a heavy coating on a glass tube. Specially formed wire leads are embedded in the resistance element. An insulating case, usually phenolic, is molded around the resistor forming a one-piece enclosure to support the leads and provide moisture sealing.

The prediction methods permit the catastrophic failure rate and the percent resistance degradation over time to be computed. The basic resistor equation is:

$$\lambda_R = (\lambda_B)(\Pi_R)(\Pi_E) + \Sigma_E \qquad (9\text{-}49)$$

where

λ_R = catastrophic failure rate
λ_B = basic failure rate and is a function of the physical characteristics of the component and the applied stress
Π_R = resistance factor; it is a constant that depends on the value of the resistor (Table 9-2)
Π_E and Σ_E = environmental factors (Table 9-3)

TABLE 9-2. RESISTANCE FACTOR Π_R FOR RC-22 RESISTORS[8]

Resistance Range (ohms)	Π_R
< 100	1.1
100 to 100 k	1.0
> 0.1 M to 1.0 M	1.1
> 1.0 M to 10 M	1.6
> 10 M	2.5

The basic failure rate λ_B is given by the equation:

$$\lambda_B = A \exp\left[\left(\frac{T}{N_T}\right)^G\right] \exp\left[\left(\frac{P/P_o}{N_s}\right)^H\right] \qquad (9\text{-}50)$$

where

N_T = temperature constant, °K
N_s = stress constant, dimensionless
G = acceleration (of degradation) constant, dimensionless
H = acceleration constant, dimensionless
P = operating power, W
P_o = power rating, W
A = adjustment factor for resistor type and style, %/1000 hr
T = operating temperature, °K.

The constants in Eq. 9-50 have been derived experimentally. They are listed in Table 9-4. An extensive set of curves has been plotted for use in computing λ_B as a function of operating conditions. These curves were computed using the constants in Table 9-4. The numbers in the second column ("λ_B Curve Figure") of Table 9-4 refer to the specific set of curves (in Ref. 8) to be used for a particular resistor style. The values of N_T do not refer to actual temperatures; they are

TABLE 9-3. ENVIRONMENT FACTORS, Π_E, Σ_E, AND LONGEVITY, L, FOR MIL-R-11 RESISTORS[8]

Π_E is dimensionless
Σ_E is in % per 1000 hours

Environment (E)	Grade of Reliability	Π_E All Styles	Σ_E RC-22, 07,12	Σ_E RC-05,20, 32,42	Σ_E RC-08	*Longevity, L (hr)
Laboratory	Upper	1.0	0.0001	0.0002	0.0005	50,000
	Lower	1.5	0.001	0.002	0.001	5,000
Satellite, Orbit	Upper	1.04	0.0001	0.0002	0.0005	50,000
	Lower	1.5	0.001	0.002	0.001	5,000
Ground, Fixed	Upper	2.0	0.0004	0.0005	0.001	5,000
	Lower	4.0	0.002	0.003	0.003	1,500
Ground, Portable	Upper	5.0	0.0008	0.001	0.002	1,500
	Lower	10.0	0.004	0.005	0.006	500
Airborne, Inhabited	Upper	4.0	0.0006	0.001	0.001	1,000
	Lower	8.0	0.003	0.005	0.003	500
Ground, Mobile	Upper	7.0	0.001	0.002	0.002	500
	Lower	14.0	0.005	0.008	0.006	100
Airborne, Uninhabited	Upper	8.0	0.001	0.002	0.002	500
	Lower	20.0	0.005	0.008	0.006	100
Satellite, Launch	Upper	15.0	0.005	0.002	0.002	50
	Lower	40.0	0.010	0.008	0.006	10
Missile	Upper	20.0	0.005	0.003	0.003	5
	Lower	80.0	0.010	0.010	0.010	1

* Longevity is that time period for which the failure rate can be considered to be constant at some given severity level.

TABLE 9-4. CONSTANTS FOR USE IN COMPUTING λ_B[8]

Style	λ_B Curve Figure*	Model Constant Value				
		N_T	N_S	G	H	A
RC-22	**2 and 3	25°K	0.28	1	11	1.95×10^{-11}
RC-07 RC-12	4 and 5	25°K	0.31	1	1	3.99×10^{-11}
RC-05 RC-20 RC-32 RC-42	6 and 7	25°K	0.42	1	1	1.2×10^{-10}
RC-08	8 and 9	25°K	0.625	1	1	3.6×10^{-10}

* These numbers are the numbers of figures in Ref. 8.
** Curve Figure No. 2 in Ref. 8 is shown as Fig. 9-5 in this chapter.

merely constants which appear in the equations.

The assumption that "the catastrophic failure rate for part types is constant with time" has been replaced by the knowledge that any specific failure rate can be treated as constant only for a certain longevity period following reliability screening. The length of the first longevity period during which the catastrophic failure rate can be considered constant varies not only with the part type, but with the stress of the environment in which the part is applied. The concept of one nominal failure rate for each part type has been replaced by the more realistic concept that there is a range of quality grades available for each part type. The fact that the quality grade interacts with application and stress parameters prohibits the use of a common adjustment constant between upper and lower grade. The relationships among the environmental factors, grade of reliability, and longevity are given in Table 9-3.

Example Problem No. 16 illustrates the procedure.

9-6 OTHER MODELS

The models for failure presented in this chapter are the conceptually simple ones. Failures of real structural materials are caused by many competing and interacting failure mechanisms. The older general purpose alloys have good resistance to many failure modes—that is why they were general purpose alloys. The newer "high-strength" alloys are often more susceptible to some of the less usual failure mechanisms. Their behavior in the presence of many competing failure mechanisms is not well understood in many cases. Refs. 11 and 12 are good treatments for the design engineer on the failure modes of metals.

Example Problem No. 16

Given a 1.0-megohm resistor (±5 percent), style RC22, operated at 75°C and 0.4 rated load P/P_o find the catastrophic failure rate λ_R in a ground fixed environment and determine the degradation of resistance Δ_R and failure rate after 2 years of service (15,000 hr).

Procedure	Example	
(1) Use the curves based on Eq. 9-50 and Fig. 9-5 to determine λ_B for 75°C and 0.4 rated load (stress ratio $S = P/P_o$).	λ_B = 0.00009 percent/1000 hr	(9-51)
(2) Determine Π_R from Table 9-2.	Π_R = 1.1 for a 1.0-megohm resistor	(9-52)
(3) Determine Π_E and ΣE for ground, fixed, service from Table 9-3.	Π_E (upper grade) = 2.0 Π_E (lower grade) = 4.0	(9-53)
	Σ_E (upper grade) = 0.0004 percent/1000 hr Σ_E (lower grade) = 0.002 percent/1000 hr	(9-54)
(4) Compute λ_R by Eq. 9-49.	λ_R (upper grade) = 0.00009 × 1.1 × 2.0 + 0.0004 = 0.0006 percent/1000 hr λ_R (lower grade) = 0.00009 × 1.1 × 4.0 + 0.002 = 0.0024 percent/1000 hr	(9-55)
(5) Use Table 9-3 to determine longevity periods L corresponding to upper and lower grade reliabilities for ground, fixed, service.	L (upper grade) = 5,000 hr L (lower grade) = 1,500 hr	
(6) Compute the ratio of service time to longevity period for upper grade r_1 and lower grade r_2 reliabilities:		
$r_1 = \frac{\text{service time}}{\text{upper grade longevity}}$ $r_2 = \frac{\text{service time}}{\text{lower grade longevity}}$	$r_1 = \frac{15{,}000}{5{,}000} = 3$ $r_2 = \frac{15{,}000}{1{,}500} = 10$	(9-56) (9-57)
(7) From Fig. 9-6 determine longevity factor Π_L.	Π_L = 1.5 for r_1 = 3 Π_L = 3.6 for r_2 = 10	(9-58)

(8) Compute the catastrophic failure rate λ_{RL} at the end of 15,000-hr service by:

$$\lambda_{RL} = \lambda_R \Pi_L \tag{9-59}$$

$$\lambda_{RL}\ \text{(upper grade)} = (0.0006\ \text{percent per 1000 hr}) \times (1.5) = 0.0009\ \text{percent per 1000 hr}$$

$$\lambda_{RL}\ \text{(lower grade)} = (0.0024\ \text{percent per 1000 hr}) \times (3.6) = 0.00864\ \text{percent per 1000 hr} \tag{9-60}$$

(9) Compute the approximate resistor body operating temperature T_B by:

$$T_B = T + \left(\frac{0.5°\text{C}}{\text{percent-rated-load}}\right) \times (\text{percent-rated-load}) \tag{9-61}$$

where

T = operating temperature, °C

$0.5°\text{C}/(\text{percent-rated-load})$ = heat dissipation factor

$$T = 75 + \left(\frac{0.5°\text{C}}{\text{percent-rated-load}}\right) \times (40\ \text{percent-rated-load}) = 75 + 20 = 95°\text{C} \tag{9-62}$$

(10) Determine the percent decrease in resistance ΔR at 15,000 hr, for T_B = 95°C, from Fig. 9-7.

$$\Delta R = 2.5\ \text{percent decrease} \tag{9-63}$$

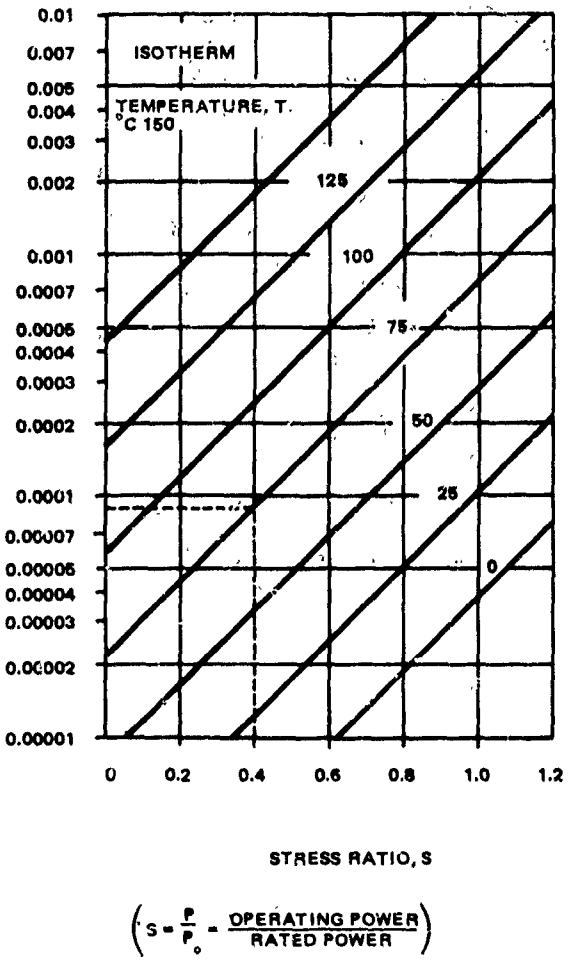


FIGURE 9-5. Determination of Failure Rate λ_B as Related to Stress Ratio S for MIL-R-11/4E Resistors, RC-22[8]

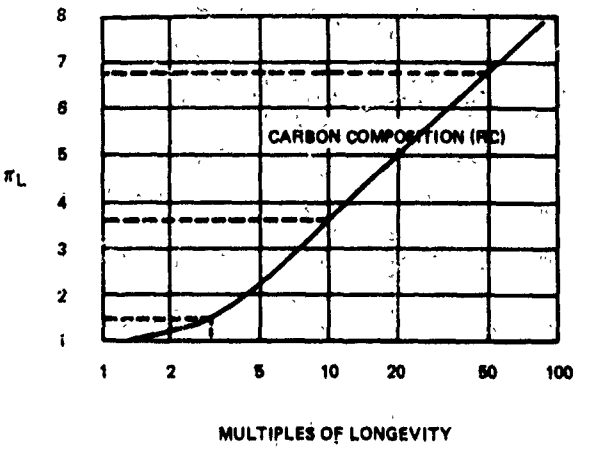


FIGURE 9-6. Determination of Longevity Factor π_L for MIL-R-11 Resistors, All Styles[8]

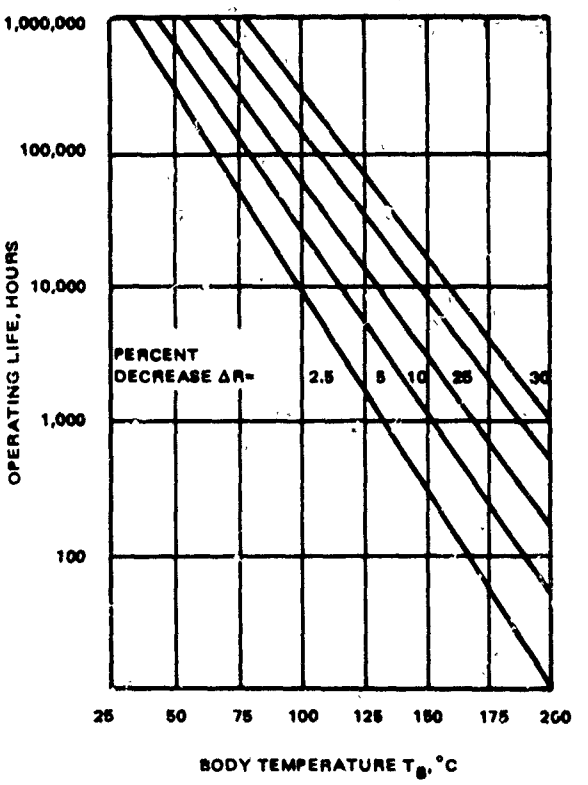


FIGURE 9-7. Determination of Resistor Longevity as Related to Body Temperature, for MIL-R-11 Resistors, All Styles[8]

REFERENCES

1. R. Lusser, *Reliability Through Safety Margins*, Redstone Arsenal, Ala., October 1958.
2. Marks and Baumeister, Eds., *Mechanical Engineer's Handbook*, McGraw-Hill, New York, 1958.
3. MIL-HDBK-5, *Metallic Materials and Elements for Aerospace Vehicle Structures.*
4. R. L. Disney, "The Determination of the Probability of Failure by Stress/Strength Interference Theory", *Proceedings of the 1968 Annual Symposium on Reliability*, 417-22 (1968).
5. Hsuan-Loh Su, "Design by Quantitative Factor of Safety", *Journal of Engineering for Industry* (November 1960).
6. C. Lipson, S. Narendra, and R. Disney, *Reliability Prediction Mechanical Stress/Strength Interference Models*, RADC-TR-66-710, Rome Air Development Center, Griffiss AFB, N.Y., March 1967.
7. Barer and Peters, *Why Metals Fail*, Gordon and Breach, New York, 1970.
8. C. Ryerson, S. Webster, and F. Albright, *RADC Reliability Notebook, Volume II*, RADC-TR-67-108, Volume II, Rome Air Development Center, Griffiss AFB, N.Y., September 1967.
9. MIL-R-11/4E, *Resistor, Fixed, Composition (insulated), Style RC22*, February 1970.
10. Oberg and Jones, Eds., *Machinery's Handbook*, Industrial Press, Inc., New York, 1971.
11. T. Lyman, Ed., Metals Handbook, Vol. 1, *Properties and Selection of Metals*, 1961, and Metals Handbook, Vol. 10, *Failure Analysis and Prevention*, 8th Edition, 1975, American Society for Metals, Metals Park, Ohio 44073.
12. D. J. Wulpi, *How Components Fail*, Metal Progress Reprint Series, ASM, Metals Park, Ohio 44073.
13. MIL-HDBK-217B, *Reliability Prediction of Electronic Equipment.*

CHAPTER 10 PARAMETER VARIATION ANALYSIS

10-0 LIST OF SYMBOLS

C = capacitance
Cdf = Cumulative distribution function
Cov = Covariance of
f = frequency
f_i = fraction, in cell i
k = number of standard deviations
L = inductance
N = number of cells, par. 10-3
n = number of units or characteristics
o = subscript, implies nominal value, see Eq. 10-11
P = random variable, characteristic of a part
$\bar{P}$ = mean of P; sometimes used with subscripts
pdf = probability density function
p_j = characteristic j
P_{MIN}, P_{MAX} = tolerance limits for P
PSM = probabilistic safety margin
R = Resistance, par. 10-3
$\bar{R}$ = mean Resistance, par. 10-3
R_{ci} = Resistance at center of cell i, par. 10-3
REG = Reasonable-Engineering-Guess
S_{ij}, S_{ij} = sensitivity coefficients, see Eqs. 10-12, 10-13
T_f = tolerance limit
Var = Variance of
V_i = performance characteristic i
y = a function
γ_i' = coefficient of variation of Vi, see Eq. 10-25
γ_j = coefficient of variation of P_j, see Eq. 10-25
Δf = frequency change
Δf_{max} = maximum Δ_f
σ = standard deviation (often used with a subscript)
σ_i' = standard deviation of V_i

10-1 INTRODUCTION

Parameter variation analysis, sometimes referred to as variability analysis, consists of a useful set of tools for designing reliable systems. Through the use of these tools, the effects of variations of individual design parameters on system performance and reliability can be determined. The techniques need not be statistical. Ref. 18 is a good discussion of parameter variation analysis; it is written for practical use by engineers.

The worst-case method of variability analysis is a nonstatistical approach (Ref. 18) that can be used to determine whether it is possible, with given parameter tolerance limits, for the system performance characteristics to fall outside specifications. The answer is obtained by using system models in which parameters are set at either their upper or lower tolerance limits. Parameter values are chosen to cause each performance characteristic to assume first its maximum and then its minimum expected value. If these performance-characteristic values fall within specifications, the designer can be sure that the system has high drift reliability. If specifications are exceeded, drift-type failures are possible, but the probability of their occurrence remains unknown.

Statistics is combined with system analysis techniques in the moment method to estimate the probability that performance will remain within specified limits (Ref. 18). The method applies the propagation-of-variance formula to the first two moments of component-part frequency distributions to obtain the moments of performance-characteristic frequency distributions. On the basis of this information, the probability that specific system parameters drift out of their acceptable range or drift reliability can be computed.

In the Monte Carlo method a large number of alternate replicas of a system are simulated by mathematical models (Ref. 18). Component values are selected randomly, and the performance of each replica is determined for its particular set of components. The performance of the replicas are compared with specification limits to yield an accurate estimate of system reliability.

Each of these methods and the basic mathematical theory of parameter variation analysis are discussed in the paragraphs that follow.

The fundamental approach in each method involves the systematic manipulation of a suitably arranged system model to give the desired information. All depend on the speed and accuracy afforded by the modern digital computer to manipulate the model and to process the data resulting from this manipulation.

The nonstatistical, worst-case approach is designed to give basic information concerning the sensitivity of a configuration to variability in the parameters of its component parts. This information is useful to the designer in selecting economical but adequately stable components for the circuit and in modifying the configuration to reduce the critical effects of certain parameters. On the other hand, the moment and Monte Carlo methods, which are statistical, use actual parameter-variability data to simulate real-life situations and predict the probability that performance is inside tolerance specifications. The moment method prediction of performance variability is usually less accurate than the Monte Carlo method, but still adequate for most purposes. The moment method provides information that is extremely useful to the designer in pinpointing sensitive areas and reducing this sensitivity to parameter variability.

In addition to providing data on drift-type failures, the techniques are all capable of giving "stress level" information of the type needed for estimating catastrophic-failure rates. They are useful, powerful tools for predicting overall reliability.

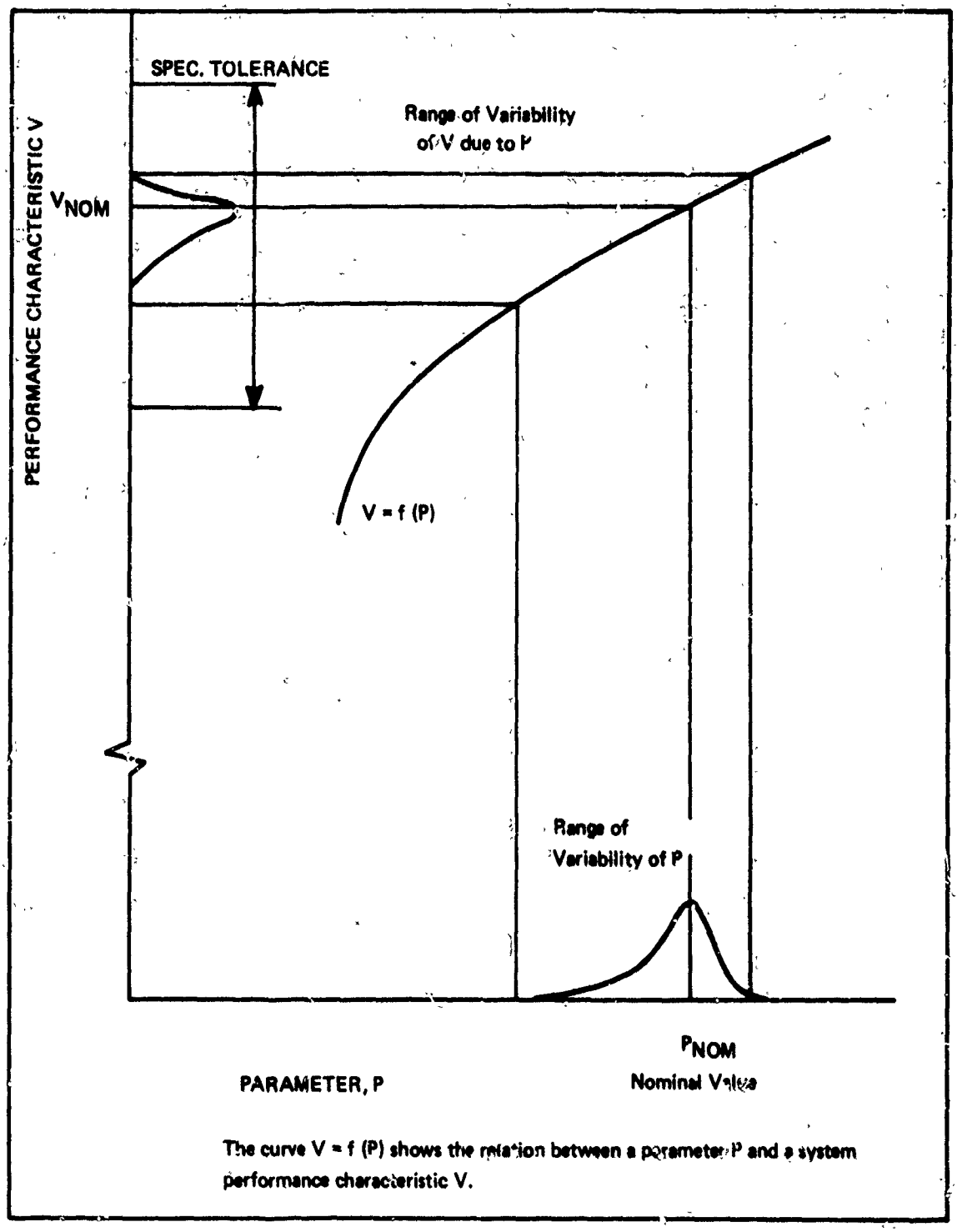
10-2 DESCRIPTIONS OF VARIABILITY

The performance of a system depends on the parameters of its component parts and on the particular set of values assigned to those parameters. Since these parameter values vary because of imperfect parts and environmental effects, system performance variability is inevitable. This concept is illustrated in Fig. 10-1, where a performance characteristic V of a system is plotted as a function of parameter P. V might represent the voltage or pressure at some point in the system, and P might represent the resistance of a resistor or the diameter of a nozzle.

Data for a plot of this type can be obtained by holding all parameters and environmental conditions, except P, constant at nominal values while P is varied over a range above and below its nominal value. The nominal value of P falls at the point on the curve $V = f(P)$ at which $V = V_{nom}$ the design center. This curve describes the relationship between V and P. When actual component parts are obtained for the system, the values of P are found to lie, not exactly at P, but in the range indicated in the lower frequency distribution. The effect on V of this variability in P can be determined by projecting the P distribution up to the curve $V = f(P)$ and over to the V axis. If the curve is essentially linear, the distribution of V will have basically the same shape as the distribution of P. Similarly, if the curve is highly nonlinear in the range of interest, the distribution of V will be a distorted version of that of P.

This concept of performance variability is understood readily on a parameter-by-parameter basis, and it can be handled easily, in this manner, by the designer. What really is needed, however, is a means of handling real-life situations such as that shown in Fig. 10-2, where performance variability is influenced by several parameters simultaneously. Comparison of the functional relationships shows a positive correspondence between V, P_1, and P_3, and a negative correspondence between V and P_2. V depends highly on P_1 and P_2, but only slightly on P_3. The net variability of the performance characteristic V is influenced by all three parameters, and the contribution of each is a function of its importance in determining the value of V, as well as its own variability.

All of the probability density functions (referred to as frequency distributions in Fig. 10-2) have an area of unity, regardless of shape. This means, of course, that those with a narrow base (low variability) have relatively greater height (high relative frequency). The 3-variable *pdf* of performance characteristic V has a broader base than any of the 1-variable



The curve V = f (P) shows the relation between a parameter P and a system performance characteristic V.

FIGURE 10-1. Performance Variability[1]

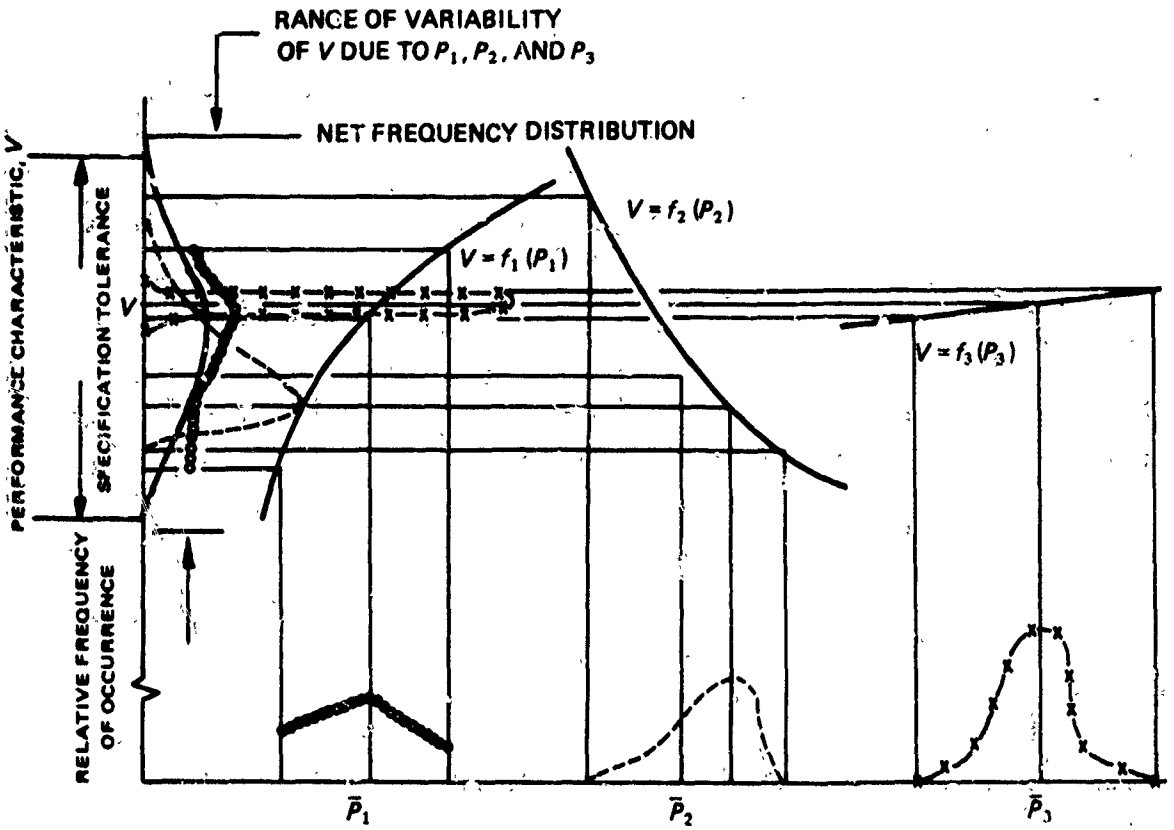


FIGURE 10-2. Performance Variability of a System as a Function of the Variability of Three Parameters[1]

distributions of V, as might be expected. None of these individual *pdf*'s indicates a serious degree of shift in V, but their combined net effect is a *pdf* having tails slightly outside the upper and lower specification limits. The portion of this distribution that falls outside of the specification limits represents drift failure.

The term "tail" is used quite often for a probability distribution; it refers to the noncentral portions of the *pdf*—they are usually long and narrow like a tail. Most *pdf*'s are drawn with smooth tails, but there is no law of nature that says they must be smooth. Rarely, if ever, are enough data available to describe the tails of a distribution, say in the 1% region or less. It is worthwhile estimating the fraction of the distribution which lies outside the region where the distribution is described by the tractable formula. This external region ought to be described only by the fraction estimated to be in it; one may wish to have two external regions—one above and one below the internal (main) region and to estimate separately the fraction in each. The external region is not used to estimate the parameters of the distribution for the internal region.

If an analysis requires a further assumption about the shape of the distribution in the external region, then a pessimistic assumption ought to be made, e.g., the entire fraction lies 2 standard deviations beyond the boundary of the internal region. If you can't afford the pessimistic assumption in your analysis, then you need more data about the external region. A real pessimist would assume that the fraction estimated to be in the external region is completely defective.

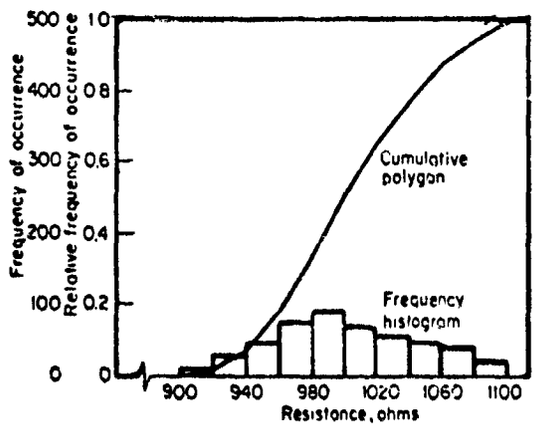


FIGURE 10-3. Frequency Histogram and Cumulative Polygon for a Typical Frequency Distribution[1]

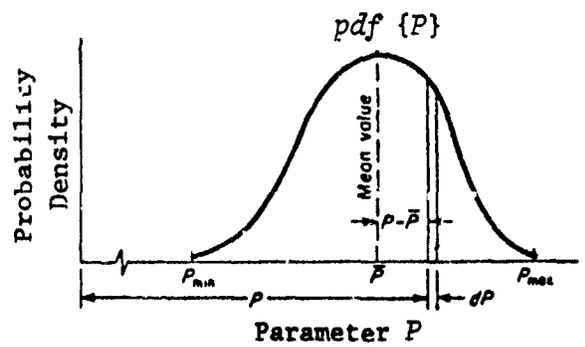


FIGURE 10-4. Moments of a Distribution[1]

10-3 SOURCES OF VARIABILITY

In any sample group of similar components that have passed successfully through the production and inspection process (for example, 500, ± 10%, 1000 Ω resistors), many units will have nearly nominal resistance, some will have resistance values near the tolerance limits, and a few might have values outside of the tolerance limits. The distribution of resistance values is important because it can affect circuit performance variability.

The frequency histogram and the cumulative polygon provide a method of visualizing the distribution of resistance values. The histogram is formed by dividing the tolerance range (e.g., 900 to 1100 ohms) into a number of cells. In Fig. 10-3, 20-ohm cells are used. The column height for each cell is determined by the number of resistors whose values fall within the cell; it is an approximation to the *pdf*. The cumulative polygon is formed by cumulatively adding the number of resistors in each cell; it is an approximation to the *Cdf*. Relative frequency of occurrence is the frequency of occurrence divided by the total number of observations (500 in this case).

A smooth frequency distribution (Fig. 10-4) can be obtained by fitting a curve to the histogram. The discussion that follows presumes that the sample was "infinitely" large; so that the smooth curve really does accurately represent the whole population. The first moment of the distribution is its mean value $\bar{P}$, and is taken from the origin:

$$\bar{P} = \int_{P_{min}}^{P_{max}} P \times pdf\{P\}dP \qquad (10\text{-}1)$$

The first moment corresponds to the center of gravity of a plane area. The sum of first moments about the mean is zero, since positive and negative moments balance:

$$0 = \int_{P_{min}}^{P_{max}} (P - \bar{P}) \times pdf\ \{\bar{P}\}\ dP \qquad (10\text{-}2)$$

The second central moment, i.e., (taken about the mean) is called the variance σ_P^2:

$$\sigma_P^2 = \int_{P_{min}}^{P_{max}} (P - \bar{P})^2 \times pdf\ \{P\}\ dP \qquad (10\text{-}3)$$

The variance corresponds directly to the moment of inertia of a plane area. The variance and its square root, the standard deviation σ_P, are both used as measures of variability. Higher moments of a distribution are sometimes useful in defining skewness, peakedness, etc. If the distribution is s-normal (or any other that has no more than 2 parameters), only the first two moments are needed to determine its parameters.

First and second moments of the sample can be calculated directly from the histogram if it is assumed that within each cell all component values occur at the midpoint of the cell or if the usual correction for grouping is used.

Example Problem No. 17 illustrates the procedure.

When a single component has several important parameters, there may be relationships among the parameter distributions. For example, for a semiconductor diode with a given offset voltage V_D and dynamic resistance R_D, some internal physical relationship may define a value or range of values for R_D with respect to V_D. Another example can be given for a solid fuel rocket motor. The static pressure in the chamber is a function of fuel grain density, burning index, nozzle area, and burn surface area of the grain. Varying these parameters causes variations in chamber pressure, which can lead to unacceptable performance. Thus variations in the design parameters of a particular system can depend upon each other. The extent of direction of the linear component of the dependence, called the linear correlation, can be computed for the sample from:

$$\rho = \frac{\frac{1}{n}\sum_{j=1}^{n} (P_{aj} - \bar{P}_a)(P_{bj} - \bar{P}_b)}{\sigma_a \sigma_b} \qquad (10\text{-}9)$$

where

ρ = linear-correlation coefficient
n = number of individual units tested
P_{aj}, P_{bj} = measurements of parameters P_a and P_b on unit j
σ_a, σ_b = standard deviations for parameters P_a and P_b

The linear-correlation coefficient ρ lies between +1 and −1. If the linear-correlation coefficient is negative, increases in one parameter correspond to decreases in the other. If the linear-correlation coefficient is positive, increases in one parameter correspond to increases in the other. The statistical literature usually uses the term correlation rather than linear-correlation for this concept. But since an engineer tends to think of correlation and dependence as synonyms, the more complete description linear-correlation is used in this handbook.

10-4 EFFECTS OF VARIABILITY

Variability models can be made up of physical components (Ref. 18), but mathematical models are used whenever possible because they are easier to manipulate. The greatest obstacle to the use of mathematical models in the past was difficulty in calculating numerical values for performance characteristics. Modern digital and analog computers have solved this calculative problem, but have not eliminated the need for simplifying assumptions. For example, linear equivalents are usually used to represent nonlinear devices, such as transistors and diodes. In some systems, however, the inaccuracies introduced by the assumption of linearity may be intolerable.

In general, the model must be accurate enough to simulate the behavior of the system over its entire range of operation. Furthermore, it must express the relationships between each performance characteristic and all parameters. The range of accurate simulation can be much smaller than for safety analyses where unusual, undesired operation can cause unsafe conditions.

If the operating region of the system components changes, it may be necessary to modify the mathematical model during the analysis. A new operating region for a component such as a transistor usually requires a new equivalent circuit, and each of these equivalent circuits must be tested for accurate simulation. The required tests and necessary changes can be performed in a routine manner by the computer program.

The variability analysis methods are adaptable to many diverse types of systems: electrical circuits, mechanical systems, and, indeed, any system for which design equations can be developed.

Either the loop-current approach or the node potential approach can be used to form the equation for an electrical or mechanical equivalent circuit, but experience has shown that the node potential approach is often preferable for a variability analysis. This direct

Example Problem No. 17

Determine the mean and standard deviation of the resistance values for the sample described in Fig. 10-3.

Procedure	Example
(1) Determine the midpoint resistance R_{ci} of each cell in the frequency histogram.	The cell midpoints are at 910, 930, 950, 970, 990, 1010, 1030, 1050, 1070, 1090, ohms.
(2) Determine the relative frequency of occurrence f_i of resistance values within each cell.	The relative frequency of occurrence known to be are 0.02, 0.06, 0.10, 0.16, 0.18, 0.14, 0.12, 0.10, 0.08, 0.04.
(3) Compute the mean resistance $\bar{R}$ of the sample by: $\bar{R} = \sum_{i=1}^{N} f_i R_{ci}$ (10-4) where N = number of cells.	$\bar{R} = 0.02 \times 910 + 0.06 \times 930 + 0.1 \times 950 + 0.16 \times 970 + 0.18 \times 990 + 0.14 \times 1010 + 0.12 \times 1030 + 0.1 \times 1050 + 0.08 \times 1070 + 0.04 \times 1090 = 1002$ ohms (10-5)
(4) Compute the standard deviation σ_R of the sample resistance by: $\sigma_R^2 = \sum_{i=1}^{N} f_i (R_{ci} - \bar{R})^2$ (10-6)	$\sigma_R^2 = 0.02(910 - 1002)^2 + 0.06(930 - 1002)^2 + 0.1(950 - 1002)^2 + 0.16(970 - 1002)^2 + 0.18(990 - 1002)^2 + 0.14(1010 - 1002)^2 + 0.12(1030 - 1002)^2 + 0.1(1050 - 1002)^2 + 0.08(1070 - 1002)^2 + 0.04(1090 - 1002)^2 = 1954$ (10-7)
	$\sigma_R = 44.2$ ohms (10-8)

procedure yields a complete, nonredundant set of circuit equations. The node potentials calculated by solving the circuit equations can be used directly to determine "stress" levels and performance characteristics, such as terminal-to-terminal voltages, current flows, power dissipations, gains, velocities, pressures, forces, and torques.

The first step in analyzing a node potential model is to identify all independent nodes (junctions) where three or more circuit branches meet. Usually, the ground or stationary node is selected as a reference; then the current in each branch is expressed in terms of the node potentials and the branch impedance. Kirchhoff's law (sum of currents into a node is zero) is then applied at each node. The resulting simultaneous equations are set up in matrix form and solved by a computer using a matrix inversion program.

The sound practice of verifying the mathematical model ought to be followed by comparing the computed results with measurements taken from a breadboard model of the circuit, or from a working model of the mechanical system. It is essential that all parameter values be the same in both the mathematical and physical models. The performance of the physical model ought closely to approach the original design performance goals. If these goals are not met, the basic design must be modified.

If the construction of a mathematical model of the system is not feasible, a physical model sometimes can be used for the variability analysis. The physical model is similar to a conventional model, except that it must provide means for conveniently varying parameters.

When a suitable model has been developed, variability data for all component parts are needed so that they can be applied to the model to observe and interpret its response. Three variability analysis techniques are discussed in the paragraphs that follow.

10-5 WORST-CASE METHOD

The worst-case method of variability analysis is a nonstatistical approach (Refs. 1,18) that can be used to determine whether it is possible, with given parameter tolerance limits, for the system performance characteristics to fall outside specifications (Fig. 10-5). The answer is obtained by using system models in which parameters are set at either their upper or lower tolerance limits. Parameter values are chosen to cause each performance characteristic to assume first its maximum and then its minimum expected value. If the performance characteristic values fall within specifications, the designer can be confident that the system has high drift-reliability. If specifications are exceeded, drift type failures are possible, but the probability of their occurrence remains unknown.

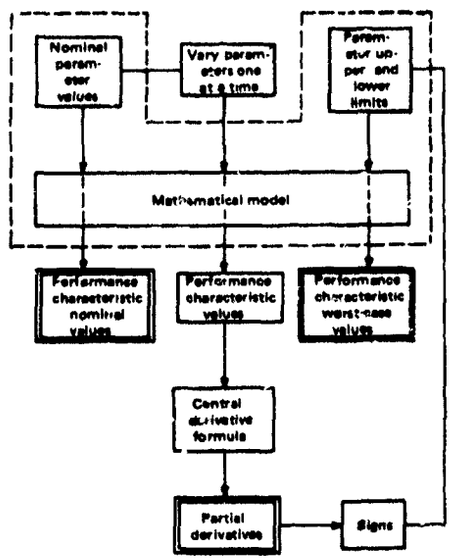


FIGURE 10-5. Worst-case Method[1]

Worst-case analysis is based on expressing the model performance parameters V_i as functions of design parameters $P_1, P_2, ..., P_n$ and expanding these functions in Taylor series about the nominal values. The design parameters include all pertinent part characteristics inputs, loads, and environmental factors. Let the model for a performance parameter V_i be:

$$V_i = y(P_1, P_2, P_3, \ldots, P_n) \quad (10\text{-}10)$$

The linear expression which relates changes in V_i to changes in the design parameters $P_1, P_2, ..., P_n$ is:

$$\Delta V_i = \sum_{j=1}^{n} \left(\left. \frac{\partial V_i}{\partial P_j} \right|_0 \Delta P_j \right) \qquad (10\text{-}11)$$

where

$\partial V_i/\partial P_j$ = partial derivatives of the performance parameter V_i with respect to the design parameter P_j

0 = evaluated at the nominal conditions, usually the mean values

ΔP_j = the variation of design parameter $P_j = P_{j0} - P_{jmin}$ or $P_{jmax} - P_{j0}$

A set of these equations must be derived to relate all performance factors to all design variables. The partial derivatives of the V_i with respect to each dependent variable P_j must be computed. Several techniques for calculating these derivatives are given in Refs. 2, 3, 4, and 5.

One of the most important steps in a worst-case analysis is to decide whether to use a high or low parameter-tolerance limit for each component part when analyzing a specific performance characteristic. If the slope of the function that relates a parameter to a performance characteristic is known, the selection of parameter limit is easy: when the slope of the parameter function is positive, the upper tolerance limit is chosen if the maximum value of the performance characteristic is desired. For parameter functions with negative slopes, the lower tolerance limit corresponds to the maximum performance-characteristic value.

An important part of worst-case analysis is to determine the sensitivity of system performance to variations in input parameters. Although several definitions of sensitivity are found in the literature (Refs. 4 and 6, for example), the sensitivity of a system essentially is measured as the effect of parameter variations on the system performance. In equation form, sensitivity can be expressed by:

$$S_{ij} = \left. \frac{\partial V_i}{\partial P_j} \right|_0 \qquad (10\text{-}12)$$

where

S_{ij} = the sensitivity of the performance measure V_i to the variation in the system design parameter P_j

An alternate form is the normalized sensitivity:

$$s_{ij} = \left(\frac{P_{j0}}{V_{i0}} \right) \frac{\partial V_i}{\partial P_j} = \left. \frac{\partial \ln V_i}{\partial \ln P_j} \right|_0 \approx \frac{\Delta V_i / V_i}{\Delta P_j / P_j} \qquad (10\text{-}13)$$

which is more frequently used.

The forms of the variation equation which correspond to the two sensitivities are:

$$\Delta V_i = \sum_{j=1}^{n} S_{ij} \, \Delta P_j \qquad (10\text{-}14)$$

$$\frac{\Delta V_i}{V_{i0}} = \sum_{j=1}^{n} s_{ij} \frac{\Delta P_j}{P_{j0}} \qquad (10\text{-}15)$$

Eq. 10-15 is more convenient when the performance equation is a product of terms and the tolerances are expressed in percent.

If a design fails the worst-case analysis, look at the absolute values of the individual terms in Eq. 10-14 or 10-15. The ones which contribute the most ought to be reduced—they are the bottlenecks. It does little good to reduce the small terms because they have so little effect on the total variation. It is not unusual to have well over half the variation due to one or two parameters. If several performance parameters have too much variation, the major contributors ought to be listed for each. If a few parameters are causing most of the difficulty, attention can be devoted to them. If not, an extensive redesign might be necessary.

Example Problem No. 18 illustrates the procedure.

10-6 MOMENT METHOD

Statistics are combined with circuit-analysis techniques in the moment method to

Example Problem No. 18

A proposed design of a simple, series-tuned electronic circuit consists of a 50 microhenry (μH) ± 10% inductor and 30 picofarad (pF) ± 5% capacitor. Perform a worst-case and sensitivity analysis on the circuit. Does the initial design meet specifications if the maximum allowable frequency shift is ± 200 kHz? Which component is the most likely candidate for tightening tolerances in order to meet the frequency specification? (Note: micro is 10^{-6}, pico is 10^{-12}.) We presume s-independence between variations in inductance L and capacitance C.

Procedure	Example	
(1) State the nominal values and tolerances of the components. We assume that the specified tolerances include purchase tolerance, reversible effects due to temperature and voltage, and drift during manufacture and use.	$\left.\begin{aligned} L_0 &= 50\ \mu\text{H} \\ \lvert \Delta L/L_0 \rvert &= 10\% \\ C_0 &= 30\ \text{pF} \\ \lvert \Delta C/C_0 \rvert &= 5\% \end{aligned}\right\}$	(10-16)
(2) State the performance equation. (There is only one; so we will drop the i subscript.)	$f = \dfrac{1}{2\pi(LC)^{1/2}}$	(10-17)
(3) Since Eq. 10-17 contains only products of the parameters, convert it to the ln form.	$\ln f = -\ln 2\pi - \dfrac{\ln L}{2} - \dfrac{\ln C}{2}$	(10-18)
(4) Determine the normalized sensitivities s_j.	$\left.\begin{aligned} s_L &= \left.\dfrac{\partial \ln f}{\partial \ln L}\right\rvert_0 = -\tfrac{1}{2} \\ s_C &= \left.\dfrac{\partial \ln f}{\partial \ln C}\right\rvert_0 = -\tfrac{1}{2} \end{aligned}\right\}$	(10-19)
(5) Write the variation equation corresponding to Eq. 10-15.	$(\Delta f/f_0) = -\tfrac{1}{2}(\Delta L/L_0) - \tfrac{1}{2}(\Delta C/C_0)$	(10-20)
(6) State allowed value of frequency shift. Calculate the nominal frequency from Eq. 10-17.	$\left.\begin{aligned} \Delta f_{max} &= 200\ \text{kHz} \\ f_0 &= \dfrac{1}{2\pi(50 \times 10^{-6}\,\text{H} \times 30 \times 10^{-12}\,\text{F})} \\ &= 4.11\ \text{MHz} \end{aligned}\right\}$	(10-21)
Calculate the allowed fractional frequency shift.	$(\Delta f_{max}/f_0) = \dfrac{200 \times 10^3\,\text{Hz}}{4.11 \times 10^6\,\text{Hz}} = 4.9\%$	

(7) Calculate actual maximum fractional frequency shift from Eq. 10-20.

$$|\Delta f/f_o| = (\tfrac{1}{2} \times 10\%) + (\tfrac{1}{2} \times 5\%) = 5\% + 2.5\% = 7.5\% \qquad (10\text{-}22)$$

(8) Compare with allowed value in Step (6).

$$7.5\% > 4.9\%$$

(9) What to do? Obviously the inductor tolerance must be reduced since it alone causes greater than allowed deviations. However, it is probably cheaper to get a narrower tolerance on the capacitor. A reasonable compromise is to alot 2/3 of the variation to the inductor and 1/3 to the capacitor. Calculate the new maximum frequency shift.

$$(\Delta L/L_o)_{new} = 4.9\% \times \frac{2/3}{1/2} = 6.5\%$$

$$(\Delta C/C_o)_{new} = 4.9\% \times \frac{1/3}{1/2} = 3.2\% \qquad (10\text{-}23)$$

$$(\Delta f/f_o)_{new} = (\tfrac{1}{2} \times 6.5\%) + (\tfrac{1}{2} \times 3.2\%) = 4.9\%$$

As mentioned in Step (1), these tolerances on the component parameters include sources other than purchase tolerance. The purchase tolerance ought to be a standard one and probably no more than half the allowed tolerance.

estimate the probability that performance will remain within specified limits (Refs. 1, 7, and 18). The basic procedure is much like that in par. 10-5 for the worst-case method. First, the performance equation is linearized, usually by taking logarithms of both sides or by a Taylor's series expansion (Ref. 18). Assume that the equation has been linearized and is in the form of Eq. 10-14 or 10-15.

Two theorems from statistical/probability theory are used. For the sum of random variables (from any distributions),

(1) The mean of the sum is the sum of the means.
(2) The variance of the mean is the sum of the variances and covariances.

So, in Eqs. 10-14 and 10-15, the nominal condition (indicated by the zero subscript) will be taken as the mean value. Then the first theorem is automatically satisfied. The second theorem states that (for Eq. 10-14)

$$\begin{aligned}\mathrm{Var}\{\Delta V_i\} &= \sum_{j=1}^{n} \mathrm{Var}\{S_{ij}\Delta P_j\} \\ &\quad + 2\sum_{j=1}^{n}\sum_{m=j+1}^{n} \mathrm{Cov}\{S_{im}\Delta P_m S_{ij}\Delta P_j\} \\ &= \sum_{j=1}^{n} S_{ij}^2\ \mathrm{Var}\{\Delta P_j\} \\ &\quad + 2\sum_{j=1}^{n}\sum_{m=j+1}^{n} S_{im}S_{ij}\,\mathrm{Cov}\{\Delta P_m \Delta P_j\} \\ &= (\sigma_i^*)^2 = \sum_{j=1}^{n} S_{ij}^2\ \sigma_j^2 \\ &\quad + 2\sum_{j=1}^{n}\sum_{m=j+1}^{n} S_{im}S_{ij}\rho_{mj}\sigma_m\sigma_j \end{aligned} \tag{10-24}$$

where

σ_j = standard deviation of parameter P_j
σ_j^* = standard deviation of V_i
ρ_{mj} = linear-correlation coefficient of parameters P_m and P_j ($\rho_{mj} = \rho_{jm}$)

A similar development for Eq. 10-15 results in

$$(\gamma_i^*)^2 = \sum_{j=1}^{n} s_{ij}^2\gamma_j^2 + \sum_{j=1}^{n}\sum_{m=j+1}^{n} s_{ij}s_{im}\rho_{jm}\gamma_j\gamma_m \tag{10-25}$$

where

$\gamma_j = \gamma_j/P_{jo}$ = coefficient of variation of P_j
$\gamma_i^* = \gamma_i/V_{io}$ = coefficient of variation of V_i

Eqs. 10-24 and 10-25 are similar in form (exact in content) to Eqs. 9-34 and 9-35 where $\rho_{jm} = 0$ (s-independence was assumed, it implies no linear-correlation) which were developed for the probabilistic safety margin (*PSM*). The standard deviation σ and coefficient of variation γ are measures of variability or of uncertainty. The sensitivities s_{ij} or S_{ij} are found by differentiation; the σ_j or γ_j are usually given; and the σ_i^* or γ_i^* is to be calculated. It is often worthwhile calculating each term in Eq. 10-24 or 10-25 to find the total effect of a parameter variation on the performance variation. That way the important parameters can be identified and, if need be, analyzed for ways of reducing their impact. The impact is reduced by reducing the sensitivity or the standard deviation. The sensitivity depends on system design; the standard deviation depends on part behavior.

Fig. 10-6 shows a flow chart for the moment method—so named because the mean is the first moment and the variance (square of standard deviation) is the second central (about the mean) moment. A computer routine ought to print out not only the σ_{ij} (or γ_{ij}), S_{ij} (or s_{ij}), but also the product $\sigma_{ij}S_{ij}$ (or $\gamma_{ij}s_{ij}$).

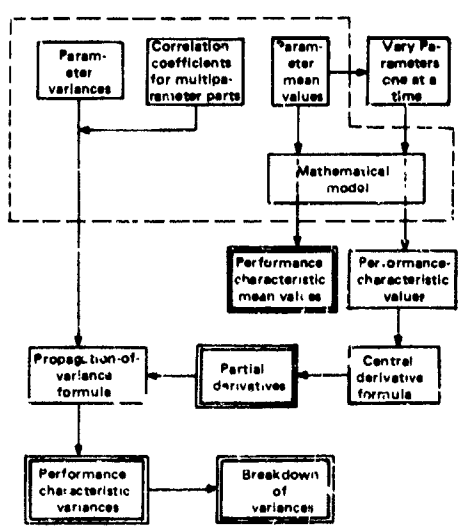


Figure 10-6. Moment Method

This method for analytically estimating the drift reliability of a system necessitates that five requirements be satisfied:

(1) Specification limits must be supplied for the performance characteristic of all subsystems under consideration. Performance outside these limits constitutes a subsystem failure.

(2) A way must be found to relate performance of a subsystem to the parameters of its components. This need is met by deriving a suitable mathematical model.

(3) The variability of each parameter from one component to another and in the same component with time and environment must be known or be accurately predictable.

(4) A technique (the propagation of variance formula) must be established to combine this information to produce an estimate of overall variability incorporating the simultaneous effect of all sources of variability.

(5) Variability of performance characteristics must be translated into an estimated probability of failure as an aid in predicting reliability.

It is not easy to convert the standard deviation of V_i or the allowed limits on V_i to a probability of failure. As explained in par. 9-3.2, especially Eq. 9-38 and Table 9-1, the s-normal distribution may give a too low probability of failure, while the Chebyshev limit may give too high a probability of failure.

A not unreasonable guess for the probability of failure is the geometric mean of the s-normal and Chebyshev probabilities. Since that is a complicated parameter to calculate, the Reasonable-Engineering-guess has been defined as shown in Table 9-1; it is easy to calculate and is reasonably near the geometric-mean.

In the process of applying the moment method, very serious consideration must be given to fulfilling requirements 2, 3, and 5 previously mentioned. Requirement 1 usually is satisfied by establishing performance characteristic limits as the point where the component ceases to produce the desired characteristic, so that the performance of the associated system becomes inadequate. Requirement 4 is met by means of the propagation of variance formula.

Development of a mathematical model of a component necessarily goes hand in hand with the desired performance characteristics on which certain limits are placed, and with the determination of parameter degradation with time. It is necessary that the mathematical model relate the internal parameters to the performance characteristics. Essentially, the mathematical model is the set of governing equations that describes both quantitatively and qualitatively the physical significance of all parameters in determining the performance characteristics. Development of the mathematical model requires that the component or design be completely analyzed, from which an analysis of each mode of failure can be determined and related to the influencing parameters. Then, the governing equations can be written. The resulting set of equations usually is programmed on an electronic computer, since this greatly simplifies manipulations of the model. These manipulations include the calculation of the sensitivities (viz., partial derivatives of each performance characteristic with respect to each contributing parameter) and the magnitude of the terms in Eq. 10-24 or 10-25. They help to indicate the relative importance of a particular parameter in determining the variation of the performance characteristic.

Once the performance limits have been established, modes of failures determined, and partial derivatives calculated, the causes and mechanisms of time-dependent parameter degradation under environmental operating conditions must be quantitatively evaluated. This evaluation can be accomplished by:

(1) Obtaining reliability and failure data from the manufacturer and the user

(2) Analyzing data from real-time simulated environmental operating tests

(3) Extrapolating data from tests run for a short time period

(4) Simulated tests of individual or multiple parameter configurations

(5) Theoretical analysis

(6) Combinations of these methods. It is essential, of course, that theoretical analyses and simulated testing be related to actual operating experience whenever possible.

Data utilized in evaluating the propagation of variance formula include:

(1) Partial derivatives of each component performance characteristic with respect to each contributing parameter

(2) Parameter mean values

(3) Parameter variances

(4) Linear-correlation coefficients for interdependent parameters.

Partial Derivatives The partial derivatives, viz., sensitivities, are quite useful since they show the sensitivity of each performance characteristic to variations in each parameter affecting it. It is usually a good idea to calculate both S_{ij} and s_{ij} (plain and normalized sensitivities). It is also worthwhile printing the product $S_{ij}\sigma_j = s_{ij}\sigma_j$ to show the total variation in V_i due to P_j.

Mean Values The mean values of the performance characteristics obtained from the model are used to evaluate the ability of the model to simulate the behavior of the actual device. The accuracy of simulation can be determined by comparing the mean performance values derived from the mathematical model with design centers and with corresponding values obtained from empirical tests of the component being analyzed.

Conventional wisdom in the USA has it that the tolerance limits are equivalent to $\pm 3\sigma$ limits. If all tolerances are divided by a number k to find the standard deviation and (tolerance/k) is substituted for σ in Eq. 10-24 and (relative tolerance/k) is substituted for γ in Eq. 10-25, then the factor of k^2 could be cancelled from both sides of revised Eqs. 10-24 and 10-25 and those equations will be true when the σ's and γ's are interpreted as tolerances (absolute and relative). When only tolerance limits (not standard deviations) are known, this latter procedure is recommended. When it finally comes time to estimate probabilities from performance variability, a decision on k will have to be made. But at least, then, we will not have forgotten how we chose k, nor what we meant by it.

Performance Characteristic Variances The performance characteristic variances are indices of the variability of the behavior of the component, and form the basis for evaluating the component design from the point of view of reliability. Standard deviations can be used in predicting reliability by expressing performance characteristic tolerance limits in terms of multiples of standard deviations and by estimating the portion of the total performance characteristic distribution that lies inside these limits (see Table 9-1).

Breakdown of Variance In the event that an excessively high value of variance for a performance characteristic indicates a lower-than-desired reliability, it is essential to locate the source(s) of excessive variability. The breakdown of variance facilitates this step, because it tells what portion of the total variance is contributed by each parameter and, thus, immediately spotlights the major contributor(s). Since the contribution of each parameter to the whole depends on both its partial derivatives and its variance, the designer quickly can determine whether reliability can be improved by tightening the parameter tolerance limits (i.e., attempting to reduce parameter variance). He can also modify the design to reduce sensitivity (partial derivative) of the performance characteristic to that particular parameter.

Accuracy of the results of the moment method analysis is subject to four obvious limitations:

(1) The mean value and variance are incapable of reflecting by themselves such characteristics of a distribution as skewness and peakedness. Since these characteristics are not a part of the input to the moment-method, they cannot be expected to appear in its output.

(2) The variations in parameter value and variance with time and environmental conditions must be known accurately to produce an accurate reliability estimate.

(3) The function that relates a performance characteristic to some parameter of the device is presented in the moment method by its slope (partial derivative), evaluated at the mean point on the curve. If the curve exhibits a high degree of curvature in the region of interest, the inability of the tangent to adequately represent the curve can be a source of error.

(4) The moment method, like any drift-reliability analysis, yields most useful information when it is applied during a time inter-

val in which drift failures are more prevalent than catastrophic failures.

All the admonitions listed immediately above in this paragraph are very important; however, rarely if ever can an engineer satisfy them all. Nevertheless, the engineer will go ahead with the analyses. The purpose of the admonitions then is to make the engineer very wary of taking the analytic results as gospel.

Example Problem No. 19 illustrates the procedure.

10-7 MONTE CARLO METHOD

In the Monte Carlo method, a large number of replicas of a circuit are simulated by mathematical modeling (Ref. 18). Component values are randomly selected in accordance with their probability of occurrence, and the performance of each replica is determined for its particular set of randomly generated components. The performance of each replica is compared with specification limits. The ratio of the number of replicas falling within the specification limits to the total number of replica trials is a measure of the circuit drift reliability. This method can yield a more accurate estimate of circuit reliability than any of the other methods discussed in this chapter; furthermore, it can approximate the actual distribution. Fig. 10-7 is a block diagram of the Monte Carlo method.

The Monte Carlo method gives very little help in identifying and correcting failures. Even though a complete list of performance characteristics and parameter values is printed out for each failed replica, the offending parameters are not spotlighted and the reason for failure must be deduced from the available information. If the analysis is not truncated because of an excessive failure count, a specified number of replicas are analyzed and the results are recorded.

Single-parameter components with oddly shaped frequency distributions can be modeled by using a histogram or a cumulative polygon. The cumulative plot is better suited for random selection. For each random number between 0 and 1 (corresponding to a relative frequency of occurrence), a component value is determined by the cumulative

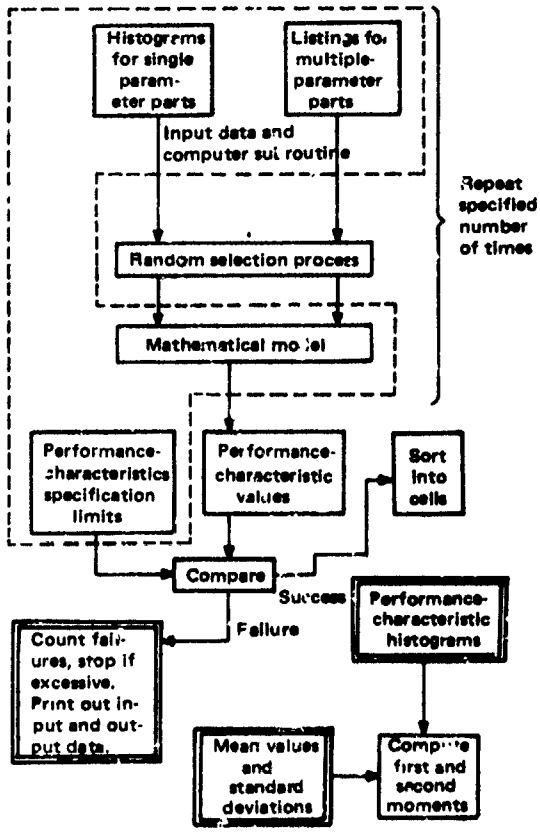


FIGURE 10-7. The Monte Carlo Method[1]

polygon. For more efficient computation a smooth, continuous mathematical function can be fitted to the polygon.

When correlations exist among the various parameters of a multiparameter system, a list of measured sets of values is prepared. Each set represents the behavior of an individual part and is assigned a serial number. The serial numbers are then randomly selected from the list. After a complete set of parameter values has been inserted into the mathematical model (selected from the list), the performance characteristics for that particular replica are determined. If the characteristics exceed performance limits for a predetermined number of replicas, the circuit design is considered unreliable and must be modified.

Drift reliability is computed as the proportion of successful replicas. The reliability confidence level is the likelihood that the computed reliability represents all possible replicas. Mean values and standard deviations

Example Problem No. 19

Compute the drift reliability of the tuned circuit for which the worst-case analysis was performed (par. 10-5).

Procedure	Example
(1) State the tolerances in L and C. As mentioned in the text, interpret the γ's in Eq. 10-25 as relative tolerances. Do not yet choose k, the ratio of tolerance to standard deviation.	$\left.\begin{array}{l}\Delta L/L_o = 10\%, \gamma_L = 10\%/k \\ \Delta C/C_o = 5\%, \gamma_C = 5\%/k\end{array}\right\}$ (10-26)
(2) State the sensitivities, s_L and s_C, computed previously (Eq. 10-19).	$s_L = -\frac{1}{2}, s_C = -\frac{1}{2}$ (10-27)
(3) Compute γ_f^2 (and thus γ_f) from $\gamma_f^2 = (s_L\gamma_L)^2 + (s_C\gamma_C)^2$ (10-28)	$\gamma_f^2 = (-\frac{1}{2} \times 10\%/k)^2 + (-\frac{1}{2} \times 5\%/k)^2 = (0.05/k)^2 + (0.025/k)^2 = 0.0031/k^2 = (0.056/k)^2$ (10-29)
$\rho_{LC} = 0$ because of the s-independence assumption.	$\gamma_f = 5.6\%/k$
(4) State the tolerance limit T_f on relative frequency, from Eq. 10-21.	$T_f = \pm 4.9\%$ (10-30)
(5) Calculate T_f/γ_f which is an indicator of how well the specification is being met. Obviously, if we mean the same thing by "tolerance" for f as we did for L and C, then we are exceeding the allowed tolerance.	$T_f/\gamma_f = 4.9\%/(5.6\%/k) = 0.88\,k$ (10-31) The fraction of the population which corresponds to $0.88k$ will fall outside the tolerance limits of $\pm T_f$.
(6) Estimate the failure probability of the circuit. We must choose k. Try several reasonable values; for each, use the Reasonable-Engineering-guess (REG)—see Table 9-1—and the s-normal distribution for failure probabilities.	The 2-sided probabilities are appropriate since deviations either way are bad.

k	$0.88k$	Estimated Failure Probability REG	*Normal*
2.5	2.2	7.8%	2.8%
3.0	2.6	3.8%	*0.92%
3.5	3.1	1.3%	0.19%

(10-32)

The *value is conventional wisdom as mentioned in the text. Since the choice of both k and the distribution is left to engineering judgment (in the absence of extensive tests), there is quite a range from which to choose a failure probability.

are computed for each performance characteristic and are quite similar to those obtained by the moment method. A frequency distribution can be computed for each performance characteristic. These distributions can be plotted for further interpretation of the data. Fitting a smooth mathematical function to the distributions often can be helpful in evaluating the tails which tend to be poorly defined unless a large number of replicas have been computed. In no instance, of course, ought the tails of a performance-characteristic distribution extend beyond the worst-case limits.

10-8 METHOD SELECTION

In the early stages of circuit design when realistic tolerances must be selected for the component parts (tolerances that will be economical and yet restrict performance within prescribed limits), the worst-case method is extremely useful. This method makes no attempt to simulate the real system closely, but is intended to give basic design information. If the circuit passes the worst-case test, the variability analysis can be considered complete, since drift failures will not occur if parameter tolerances are not exceeded.

Since it is often not feasible to modify a circuit so it can pass the worst-case test, the probability of successful operation must be estimated. Both the moment and the Monte Carlo methods can be used to make this estimate. The moment method is usually less accurate because of the omission of higher-order terms in the propagation-of-variance formula, but the numerical values of the partial derivatives and breakdown of variance are extremely useful in guiding the modification of the design. The Monte Carlo method is capable of estimating the probability of success with high accuracy and should be considered when final approval of a design is needed. The moment and worst-case methods are more suitable during the earlier design stages, since the Monte Carlo method provides little feedback or redesign information. The component-variability data collected with the moment or worst-case method can be expanded later to implement a Monte Carlo analysis.

10-9 COMPUTER PROGRAMS

A number of computer programs for parameter variation analysis are available for use by the engineer. Some of these programs are listed in Table 10-1.

10-9.1 A GENERAL PROGRAM

A FORTRAN listing of a general program that implements nearly all of the techniques discussed is given in Ref. 8. It is described here briefly. A flow diagram of the program is shown in Fig. 10-8. As can be seen from the figure, the program is keyed to the subroutine which evaluates the performance model. To make the program applicable to any kind of system, no built-in performance model subroutine is included. This subroutine must be supplied by the user of the program (Ref. 4).

The input to the program is a mathematical description of the system model (and the time behavior of the model, if required), the number of random and fixed variables involved, and the means or nominal values of the input variables. Other components of the input are the standard deviations or step sizes in the input variables, the input variable distributions, if available, and the correlations of the input variables. An additional input that is required for some analyses is a selection of values of the element parameters at which the performance model is to be evaluated. Additional programs are described in Refs. 9 through 12.

10-9.2 ECAP AND NASAP

The Electronic Circuit Analysis Program (ECAP) (Ref. 9) is used widely and is available for use on the IBM 1620, 7000 series and 360 series computers (Ref. 14). It has been suitably modified for use on a variety of other computers and has some valuable additional features for parameter variation analysis.

The basic versions of ECAP have the following computational capabilities (Ref. 15):

(1) For DC analysis, ECAP computes partial derivatives of voltage at a particular circuit node with respect to a circuit parameter in a particular branch; sensitivity of a

TABLE 10-1. PROGRAMS FOR PVA[8]

PROGRAM CODE	PROGRAM DESCRIPTION	REFERENCE
PV-RTI	Performance Variation analyses; general program for worst-case, moments, simulation, etc.	4
MCS-IBM	Monte Carlo Simulation for performance variation analysis with programmed functional model.	9
MCS-GDC	Monte Carlo Simulation for performance variation analysis with programmed functional model.	10
PV-LS	Performance Variation analysis program for systems.	11
PV-SE	Performance Variation analysis program using Monte Carlo simulation with programmed mathematical model.	12
MANDEX-NAA	Modified AND EXpanded worst-case method for analysis of circuit performance variations with circuit equations.	3
MM-NAA	Moment Method for circuit performance variation analysis with circuit equations; computer mean and variance; correlation included.	3
MCS-NAA	Moment Method for circuit performance variation analysis with circuit equations; correlation included.	3
VINIL-NAA	VINIL method for circuit performance variation analysis with circuit equations.	3
PVM-NAA	Parameter Variation Method for circuit performance variation analysis with circuit equations; one-at-a-time and two-at-a-time analyses.	3

Monte Carlo Simulation for circuit performance variation analysis with circuit equations; correlation included.

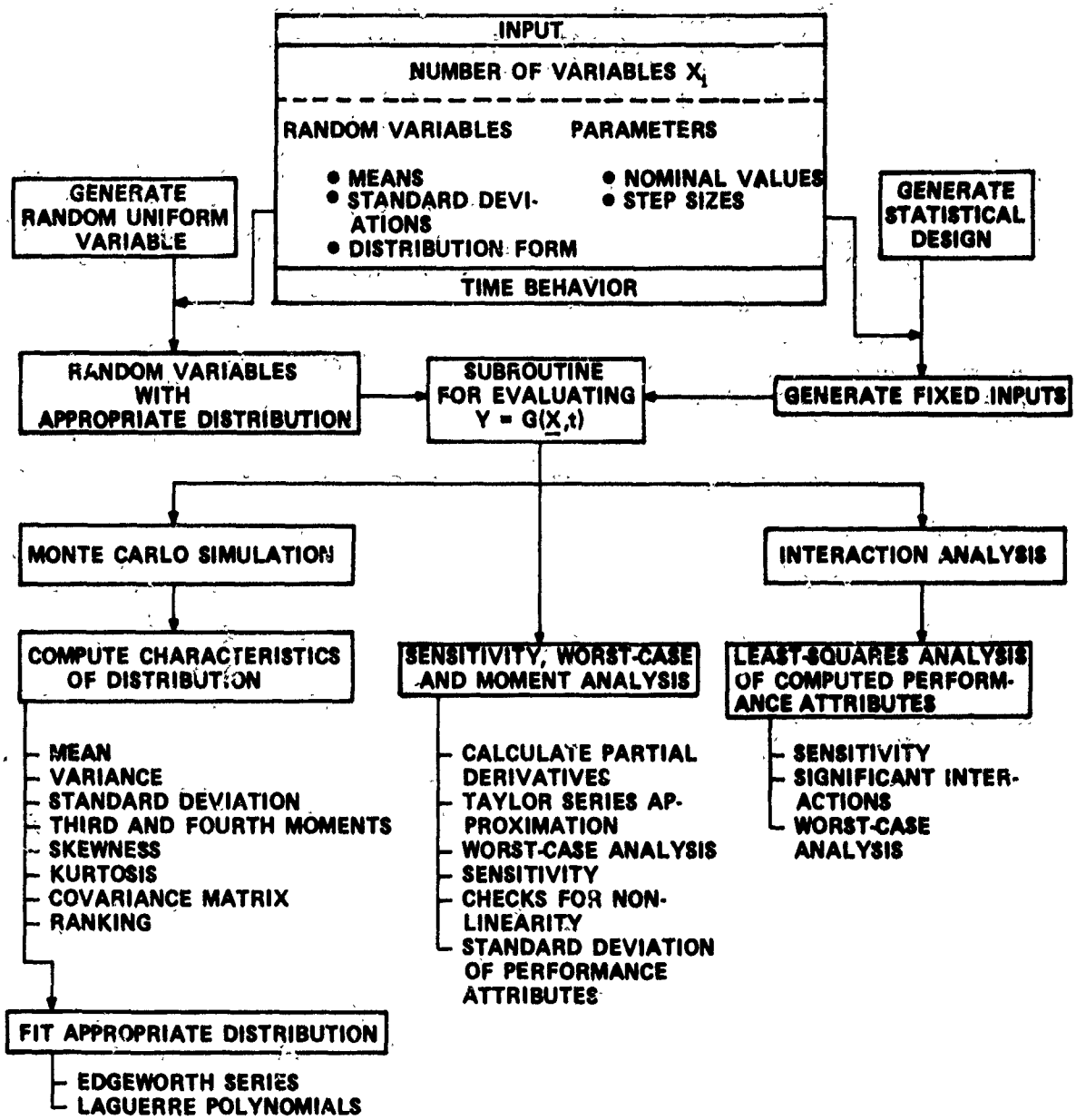


FIGURE 10-8. Flow Diagram for General PVA Program.

node voltage with respect to a branch parameter; worst-case solutions; standard deviation of circuit output variation; and automatic parameter variation, which allows a parameter to be incremented over a range of values with a circuit solution computed for each value.

(2) For AC analysis, a version of ECAP includes a capability for automatic parameter variation analysis. Additional capabilities that also have been incorporated in ECAP include AC sensitivity analysis and solution of the propagation-of-variance equation (Ref. 14).

The Network Analysis for System Application Program (NASAP) has been developed by the NASA Electronics Research Center in a cooperative effort involving about 20 users of the program (Ref. 16). NASAP is unique among circuit analysis programs in that it uses flowgraph techniques to analyze networks,

instead of matrix-oriented techniques. It also manipulates circuit symbolic parameters instead of actual parameters until the final step of the analysis. This symbol-manipulation feature has some interesting ramifications, one of which is the ability to calculate partial derivatives and sensitivities symbolically (Ref. 17).

In addition to the capabilities noted, NASAP incorporates an optimization procedure which eliminates from a circuit input those parameters having less than a preassigned amount of influence on circuit performance parameters. The procedure is, in effect, a tolerance analysis (Ref. 17).

NASAP originally was written in FORTRAN IV for use on the CDC 3600 computer. It also is now in use on several other computers.

REFERENCES

1. D. G. Mark and L. H. Stember, Jr., "Variability Analysis", *Electro-Technology*, (July 1965).
2. W. E. Milne, *Numerical Calculus*, Princeton University Press, Princeton, N.J., 1949.
3. *Reliability Analysis of Electronic Circuits*, Autonetics Division, North American Aviation, 1964. AD-461 303.
4. A. C. Nelson et al., *Development of Reliability Methodology for Systems Engineering, Vols. I and II*, Research Triangle Institute, Research Triangle Park, North Carolina 27709, April 1966.
5. Abramowitz and Stegun, Eds., *Handbook of Mathematical Functions* AMS 55, National Bureau of Standards, U S Government Printing Office (1972).
6. C. Drof, "Computer-Analyze Your Circuit", *Electronic Design*, (July 21, 1967).
7. R. E. Mesloh et al., *Research and Study of Analytical Techniques For Predicting Reliability of Flight-Control Systems*, Report FDL-TDL-64-50, Battelle Memorial Institute, Columbus, Ohio, August 1964.
8. NASA CR-1127 *Practical Reliability, Volume II - Computation*, N68-32760, Research Triangle Institute, Research Triangle Park, North Carolina 27709, August 1968.
9. F. P. Kiefer et al., *Final Report on Prediction of Circuit Drift Malfunction of Satellite Systems*, Report ARPA 168-61, IBM, FSD Space Guidance Center, Owego, New York, for Rome Air Development Center, Griffiss Air Force Base, 1961.
10. R. A. Hayward and J. I. Ingber, *Monte Carlo Flight Performance Reserve Program*, Report GD/C-BTD-65-176, General Dynamics, Convair Division, 1966.
11. H. M. Markowitz et al., *Launch Vehicle Optimization - Phase II Final Report, Vol. II - Techniques Development*, Lear Siegler, Inc., 1965.
12. I. Bosinoff et al., *Transfer Functions in Mathematical Simulation for Reliability Prediction, Final Report*, Report RADC-TDR-63-87, Sylvania Electronic Systems Command, 1963.
13. *1620 Electronic Circuit Analysis Program*, IBM Publication H20-0170-1, IBM Technical Publications Department, White Plains, New York, 1965.
14. H. M. Wall, "ECAP-1966", *NEREM Record*, 84-5 (1966).
15. H. N. Tyson, G. R. Hogsett, and D. A. Nisewanger, "The IBM Electronic Circuit Analysis Program (ECAP)", *Proceedings of the 1966 Annual Symposium on Reliability* 45-65 (1966).
16. R. M. Carpenter, "NASA-Network Analysis for System Application Program - Presents Capabilities of a Maintained Program", *Computer-Aided Circuit Design Seminar Proceedings*, Kresge Auditorium, MIT, 83-94 (1967).
17. R. M. Carpenter and W. Happ, "Computer-Aided Design - Part 3, Analyzing Circuits with Symbols", *Electronics* 92-8 (December 12, 1966).
18. NASA CR-1126, *Practical Reliability, Vol. I - Parameter Variations Analysis*, Research Triangle Institute, Research Triangle Park, North Carolina 27709, July 1968. (N68-31478).

CHAPTER 11 DESIGN AND PRODUCTION REVIEWS

11-1 INTRODUCTION

Reviews ought to be conducted throughout the life cycle of an item, from concept to field use. The reviews during design and production are perhaps the most important. The preproduction review is essential because drawings and other specifications are never complete, and the design, as it emerges from the design group, rarely is directly suited for mass production. Regardless of the arguments between engineering and production about who is right, the production department's implementation of the drawings and specifications must be reviewed by both the design and reliability groups.

This chapter dwells on the design review to illustrate the kinds of attention to detail that are required. Similar considerations will hold for reviews at the other stages in the life cycle.

The formal review of equipment design concepts and design documentation for both hardware and software is an essential activity in any development program. Standard procedures ought to be established to conduct a review of all drawings, specifications, and other design information by the contractor's technical groups such as equipment engineering, reliability engineering, and manufacturing engineering. This review should be accomplished prior to the release of design information for manufacturing operations. Such a review is an integral part of the design-checking reviews. Responsible members of each reviewing department meet to consider all design documents, resolve any problem areas uncovered, and signify their acceptance of the design documentation by approving the documents for their departments.

Reliability engineering, in conjunction with the equipment engineering groups, ought to conduct an intensive review of the system during initial design. The design review includes the following major tasks:

(1) Analysis of environment and specifications
(2) Formal design review of engineering information
(3) Reliability participation in all checking reviews.

Prior to the formal design review, the requirements defined in applicable military and equipment specifications are reviewed. The expected environmental extremes of the system are studied to determine suspected detrimental effects on equipment performance. Checklists, based on these studies, are prepared to assure that the objectives of formal design reviews are fulfilled.

The formal design review, which is instituted prior to the release of drawings, is intended to do the following:

(1) Detect any conditions that could degrade equipment reliability.
(2) Provide assurance of equipment conformance to applicable specifications.
(3) Assure the use of preferred or standard parts as far as practical.
(4) Assure the use of preferred circuitry as far as possible.
(5) Evaluate the electrical, mechanical, and thermal aspects of the design.
(6) Provide stress analysis to assure adequate part derating.
(7) Assure accessibility of all parts that are subject to adjustment.
(8) Assure interchangeability of similar subsystems, circuits, modules, and subassemblies.
(9) Assure that adequate attention is given to all human factors aspects of the design.
(10) Assure that the quality control effort will be effective.

This formal design review is conducted with schematic diagrams, initial parts lists, layout drawings, design and development reports, technical memoranda, and breadboard test results. To insure that the recommendations of the design review group are carried out and are incorporated in all released drawings, reliability engineering personnel should attend all of the final checking reviews.

A detailed schedule for design review must be included in program plans developed for a system design effort. This schedule shows the names of personnel responsible for

the review. The final program plans must also include copies of typical checklists to be used in the design review program.

All major changes to the system must be subjected to design review. This review will be similar to that performed during initial design. All subcontracted portions of the system are also subjected to a design review. Recommendations are to be made to subcontractors for corrective action as required, and to the quality control group for incoming inspections.

11-2 ORGANIZING FOR THE REVIEWS

Design review teams ought to include:

(1) Technically oriented personnel from all groups associated with the product

(2) Design specialists from groups that have no direct association with it.

Customer participants also may be present, usually at the critical final review. Normally, however, participation ought not to exceed 20 people in order to maintain effective control and prevent undue loss of time. Frequently, the experience of the members of the design review team provides the knowledge for a "design break-through" which might not otherwise occur.

The prime task of the design review team is to conduct a detailed design review of the system, including subcontracted items, during the development phase and to review all design changes during the preproduction phase. The design review team also will review the data developed during system tests. The development phase design review is divided into two levels: (1) conceptual review and (2) development review. The conceptual review is conducted after the preliminary design is complete and is oriented to unit and subassembly specifications. The developmental review is conducted prior to release of the design to production and is oriented to cabinet and subassembly design (to validate the actual hardware design for compliance with cabinet and subassembly specifications). In addition, special design reviews are held when significant reliability or performance difficulties are identified during manufacturing or testing. Data submissions, except for engineering drawings, ought to be as follows:

(1) Drawings, schematics, sketches, flow diagrams, or specifications submitted for review as part of a data package are not required to be in their final form but must contain the final information in a clear complete format,

(2) All linework, symbols, numbers, and letters must be clearly discernible at normal desk top working distance,

(3) Sketch or drawing numbers and revision numbers will be included,

(4) Reports will include title, issue or revision data, and originating individual or activity.

The functions of design review team members are briefly summarized in Table 11-1.

11-2.1 REVIEW BOARD CHAIRMAN

Personality, position, and technical competence are important factors in the selection of a review board chairman. The task requires a high degree of tact, a sound knowledge and understanding of the design requirements, and an unbiased point of view concerning the proposed design. He ought not to be a member of the design staff or of the reliability or other support groups. The configuration management manager is frequently chosen for this position.

The chairman's duties are as follows:

(1) To establish criteria for selecting specific items for review and the type of review to be conducted.

(2) To schedule reviews at the earliest date consistent with the design and development of each item reviewed.

(3) To coordinate and assist the design organization in the preparation of the design data required for the review.

(4) To insure that preliminary copies of agenda, drawings, and related data are sent to the appropriate organizations. This must be done sufficiently in advance of each review to facilitate their prior evaluation and submission of preliminary comments in preparation for each review.

(5) To chair the design review meeting, supervise publication of the minutes, evaluate comments resulting from reviews, and initiate followup action as appropriate.

TABLE 11-1.

DESIGN REVIEW GROUP, RESPONSIBILITIES AND MEMBERSHIP SCHEDULE

GROUP MEMBER	RESPONSIBILITIES
Chairman	Calls, conducts meetings of group, and issues interim and final reports.
Design Engineer (s) (of product)	Prepares and presents design and substantiates decisions with data from tests or calculations.
*Reliability Manager or Engineer	Evaluates design for optimum reliability, consistent with goals.
Quality Control Manager or Engineer	Ensures that the functions of inspection, control, and test can be efficiently carried out.
Manufacturing Engineer	Ensures that the design is producible at minimum cost and schedule.
Field Engineer	Ensures that installation, maintenance, and operator considerations were included in the design.
Procurement Representative	Assures that acceptable parts and materials are available to meet cost and delivery schedules.
Materials Engineer	Ensures that materials selected will perform as required.
Tooling Engineer	Evaluates design in terms of the tooling costs required to satisfy tolerance and functional requirements.
Packaging and Shipping Engineer	Assures that the product is capable of being handled without damage, etc.
Design Engineers (Not associated with unit under review)	Constructively review adequacy of design to meet all requirements of customer.
Customer Representative (optional)	Generally voices opinion as to acceptability of design and may request further investigation on specific items.

*Similar support functions performed by maintainability, human factors, value engineering, etc.

(6) To revise the system definition documentation when the proceedings of a review warrant it.

11-2.2 DESIGN GROUP

The design group prepares and transmits preliminary copies of agenda, drawings, and related data to appropriate organizations sufficiently in advance of each review to facilitate their prior evaluation, and provides documentation, drawings, and data required for each review. This may include, as appropriate: block diagrams, layouts, sketches, schematics, interface data and drawings, detail drawings, weigh analyses and graphs, appropriate system or item specifications, failure mode and effect analyses, Cause-Consequence charts (fault trees), predictive reliability estimates, reliability block diagrams, critical item lists, and detail study results (e.g., those from stress-strength and parameter variation analyses).

With support from special groups such as reliability, maintainability, human factors, and logistics, the design group plans, conducts, and makes the design review presentation. All design reviews must describe system or end item requirements, configuration, how the requirements have been met by the proposed design, installation considerations, system or item interfaces with other systems, ground support equipment, etc.

Included in the design review are items such as anticipated development schedules; reliability, maintainability, system safety, human factors, and value engineering factors; producibility considerations including costs, special tools, and facilities requirements; trade studies; test requirements and plans; performance characteristics, including inputs, outputs, and tolerances; and electromagnetic interference.

The design group participates in the preparation of minutes and the evaluation and classification of comments resulting from reviews. They initiate configuration changes if warranted, followup on all comments that require further study, and provide a list of accountability for all design review comments in order to define responsibility for all design improvements.

11-2.3 OTHER REVIEW TEAM MEMBERS

The formal inputs from specialized review team members are defined by the individuals responsible for the design group presentation. The essential responsibility of the specialists is to critique the design from the standpoint of the design requirements of their specialty and to offer recommendations for improvements. Thus, reliability and other support personnel contribute to a design review by presenting data on compliance with reliability, maintainability, safety, and human factors engineering requirements and standardization. They may propose study projects to develop improvements in their areas of technical responsibility and competence.

The production engineering staff can add measurably to possible design improvements by supplying manufacturing research data and by applying review recommendations to the refinement of production and procurement planning.

Quality assurance personnel can review technical data and documentation; provide quality assurance data, reports, and analyses; determine constraints, qualification acceptance, and test requirements as they apply to the quality assurance program; and use review recommendations to refine quality and inspection planning techniques.

11-2.4 FOLLOWUP SYSTEM

To achieve maximum results from a design review, a followup system must be established to insure that all corrective actions are performed. All individuals concerned with a design review must recognize their responsiblility for followup.

Design changes that have been recommended and approved must be incorporated into the system design as early as practical. A proven technique is to provide all design change information to a closed loop corrective action system established for the project. Good recordkeeping will avert repeated coverage of the same problems and prevent significant loss of insight. Good continuity and followup enable each successive review to be

directed to new areas as the system design proceeds toward production and use.

11-3 REVIEW CYCLES

The design review cycle, as subsequently described, must be performed for both system hardware and software. Both the Army and its contractors participate in the design review effort. Typical phases are listed in this paragraph.

11-3.1 TECHNICAL EXCHANGE PHASE

The design review cycle is initiated upon receipt of the preliminary design data package by the contractor's design review team from the engineering group. Preliminary data packages contain all the information necessary for the performance of a design review. A minimum list of the information necessary for the performance of a design review is given in pars. 11-4 and 11-5. The independent consultants representing the various disciplines ought to contact the counterpart design engineer to initiate technical exchange. Subsequent to this, each consultant documents his comments and recommendations. The multidiscipline comments and recommendations will be integrated by the design team and forwarded to the engineering group. A documented response from engineering completes the technical exchange phase.

11-3.2 INTERNAL DESIGN REVIEW MEETING/AGREEMENT PHASE

Formal, contractor, design review meetings ought to be held a minimum of once a month. All items in the documented response from engineering must be included in the minutes of these formal, internal, design review meetings. If the engineering response for any item does not agree with the design review team's recommendation, this item is to be discussed at the meeting. The purpose of these meetings is to seek agreement on all such items. Where agreement is not achieved, available information must be documented and presented to management for resolution. Minutes of internal design review meetings record all items covered at the meetings, specific designs reviewed, and decisions made.

11-3.3 ARMY INVOLVEMENT IN INTERNAL DESIGN REVIEW

At the time of submission to the contractor's design review team, the Army is furnished several copies of the same preliminary data package(s) that are submitted to the contractor's design review team. The Army uses the preliminary data packages for information only. All items covered at the design review meetings are included in the meeting minutes. Army personnel can attend the contractor internal design review meeting as observers but do not participate in the discussions.

11-3.4 DESIGN DATA PACKAGE PHASE

The contractor's engineering group revises the preliminary data package according to the results of the design review activity and agreements of the internal design review meeting. The updated preliminary data package is submitted to the design review team for review and approval. This package, when approved by the design review team, is called the design data package. Design data packages are submitted to the Army for review and are placed under internal contractor documentation control.

11-3.5 CHANGE DATA PACKAGE

All changes to design data packages must be documented. A change data package is prepared and submitted for internal contractor design change review. An engineering change review is performed to retain configuration control during preproduction and production. Subsequent to contractor formal approval by its design review team, the change data package is forwarded to the Army.

11-3.6 PERFORMANCE SPECIFICATION CHANGES

All performance specification change proposals must be submitted to the Army for approval. Changes to the performance specification must be accomplished by contract modifications.

11-3.7 GOVERNMENT RESPONSE

Within some reasonable period of time after receipt of each contractor submission (except for preliminary data packages), the Army furnishes the contractor with a detailed critique.

11-3.8 UNSATISFACTORY DESIGN DATA

If any design data submitted by the contractor are considered unsatisfactory, and so documented by the Army critique, the contractor must state his planned action.

11-3.9 ARMY/CONTRACTOR REVIEW MEETING

If requested by the contractor, comments resulting from the Army reviews will be discussed in informal meetings between the Army and the contractor. All items covered at the meeting are included in the meeting minutes.

11-3.10 STANDARD REVIEW

System data items that include technical design standards ought to be reviewed by the contractor's design review team for completeness and adequacy as a design standard. Subsequent to this review, the detailed system data are submitted to the Army for review and comment.

11-3.11 SUBCONTRACTOR DESIGN REVIEW

A design review of subcontracted items must be performed. The contractor design review unit treats subcontracted items like contractor-prepared items.

11-4 MINIMUM REQUIREMENTS IN CONCEPTUAL-PHASE REVIEW

The applicable documents listed in system specification and data packages are the basis for the review. Each conceptual review considers the results of the engineering activity documented in the data package. A data package is prepared after engineering has completed the following activities:

(1) *Hardware:*

(a) Prepared functional block diagrams, including interfaces.

(b) Partitioned the diagram into units (cabinets), new and modified.

(c) Allocated system reliability requirements to the unit level.

(d) Prepared a development specification for each unit to include reliability, maintainability, and mechanical packaging requirements.

(e) Prepared cabinet block diagrams.

(f) Partitioned the cabinet into subassemblies.

(g) Allocated cabinet requirements to the subassembly level.

(h) Prepared design specifications for each subsystem and circuit subassembly (including outside vendor items). Include reliability, maintainability, and mechanical packaging requirements.

(2) *Software:*

(a) Identified functions to be implemented within the system computer, identified subroutines required for each function, and estimated memory and computation time required for each subroutine.

(b) Prepared a development specification for each computer subroutine.

(c) Defined major functions of the computer program.

(d) Defined detailed functional requirements.

(e) Defined data requirements with respect to system environment, parameters, and capacities.

The conceptual-phase data-package ought to include at least the following:

(1) *Hardware:*

(a) System description that clearly relates to the system performance specification while unmistakably giving an overview of system operation

(b) Equipment development specification for each unit (cabinet) with detailed references to the system performance specification

(c) Functional block diagram that

includes signal flow and characteristics as well as clearly delineating those portions of the system/cabinet involved in each operational mode

(d) System interface tabulation (include input/output wire and cable data as well as signal information and characteristics)

(e) Reliability/maintainability concepts and predictions, including a detailed analysis of the reliability model

(f) Government Furnished Equipment (GFE) tabulation

(g) Contractor Furnished Equipment (CFE) tabulation

(h) Preliminary installation planning data

(i) Digital logic characteristics completely specified (e.g., frequency response, noise margin, fan in/fan out, impedance, reliability, environmental characteristics, and mechanical configuration)

(j) Concept for computer-aided analysis of linear and digital circuits and mechanical assemblies and structures

(k) System human factors concepts

(l) Clear description (electrical, mechanical) of unit characteristics and function as part of the total system (including a complete and concise listing of interface data such as signal levels, impedances, and waveforms)

(m) Design specifications for each circuit subassembly in the unit

(n) Unit functional block diagram(s), including signal flow and characteristics within the unit and interface data (signal and impedance levels, waveforms, etc.) pertinent to all inputs and outputs to the unit

(o) Unit interfaces (inputs and outputs), including signal flow and signal characteristics (e.g., voltage and current levels, frequencies, impedances, and unusual conditions)

(p) Unit power consumption estimate

(q) Unit weight estimate

(r) Unit maintenance and fault location design

(2) *Software:*

(a) Computer program development specification

(b) Computer interface definition

(c) Timing and sequencing definition

(d) Description of major functions of each program

(e) Input and output data definition

(f) Processing descriptions

(g) Environmental data

(h) System parameters and program capacity requirements.

11-5 MINIMUM REQUIREMENTS FOR DEVELOPMENTAL-PHASE REVIEW

The applicable documents listed in the system specification and data packages previously reviewed provide a basis for developmental review. Each such review considers the results of the conceptual design reviews documented in the data package. Such packages are prepared for each unit, circuit subassembly (including outside vendor items), and for the computer programs after engineering has completed the following design activities:

(1) *Hardware:*

(a) Designed a unit (cabinet) to perform the desired functions.

(b) Performed trade-off and design analyses.

(c) Prepared engineering sketches to document the cabinet design (including schematics, block diagrams, parts list information, and assembly layouts).

(d) Documented a description of unit operation and recommended method of test.

(e) Designed subsystem and circuits to perform the desired function.

(f) Analyzed and tested the design, utilizing engineering breadboards and computer-aided analysis techniques where applicable.

(g) Prepared engineering schematic and parts list information to document the design.

(h) Documented a description of system operation and a recommended method of test.

(2) *Software:* Data packages must be prepared for each subroutine after engineering has completed the following design activities:

(a) Prepared computer program product specifications.

(b) Specified functional allocations.

(c) Prepared storage allocations.

(d) Prepared functional flow diagrams.

(e) Prepared narrative descriptions.

(f) Defined modularity.

(g) Selected subroutines.

The developmental data package ought to include at least the following.

(1) *Hardware:*

(a) Engineering schematics, block diagrams, interunit wiring, and parts list information

(b) Nonstandard electrical and mechanical part specification sheets

(c) Description of unit operation supporting compliance with unit specification

(d) Recommended method of calibration, alignment, and test

(e) Reliability prediction for the unit (include electrical and mechanical stress data). The prediction ought to include a detailed explanation of the reliability model, including substantiated failure rates and hardware content of each block of the reliability model.

(f) Front panel drawings of cabinets having display and control functions (include human factors data)

(g) Mechanical design layouts and assembly diagrams (include structural and thermal analyses)

(h) Engineering schematic and parts list information

(i) Description of circuit operation supporting compliance with circuit specifications

(j) Reliability prediction for the subassemblies (include electrical and mechanical stress data). The model used as the basis for these predictions will be included.

(k) Information such as signal flow paths, signal levels, impedances, gains, waveforms, bias levels, Boolean expressions, or truth tables ought to be shown on schematics or otherwise provided.

(l) Maintainability analysis data

(m) A variability analysis ought to be performed. The analysis will consider the effects of component tolerances, random part selection, aging, and environmental and electrical stresses. The method will be selected from the following: worst-case, moment, or Monte Carlo.

(n) Description of EMI/EMC suppression techniques

(o) Analysis of personnel hazard problems

(p) Test point selection, identification, and tabulations.

(2) *Software:*

(a) Computer program product specification

(b) Computer program and subroutine descriptions

(c) Subroutine listings.

11-6 CHECKLISTS

Checklists are useful as reminders. A list of items is prepared for the design review team. Each factor is evaluated separately during the design review, and is documented to substantiate the decisions reached. A typical design review checklist is presented in Table 11-2. Appendix A contains a detailed set of checklists that can be used by Army engineers for evaluating a variety of systems.

TABLE 11-2. RELIABILITY ACTIONS CHECKLIST

Design Title		Number				
		Responsibility				
No. Item	Completed	Design		Reliability		Notes and Comments
1. System Constraints						
a. Success Criteria		D		X		
b. Environmental Stresses		D		X		
c. Compatibility Factors		D		X		
d. User Skill Levels		D		X		
2. Feasibility Study		D		X		
3. Reliability Apportionment				R		
4. Preliminary Reliability Review		D		R		
5. Trade-off Studies		D		X		
6. Functional Schematics		D		X		
7. Block Diagram		D		X		
8. Cause and Effect Analysis		D		X		
9. Worst Case Analysis		D		X		
10. *Subsystem and Equipment Reliability Prediction:*						
a. Part Failure Rate Method		D		X		
b. Safety Margin Method		D		X		
c. Drift Rate and Tolerance Method		D		X		
11. Intermediate Design Review		D		R		
12. Time/Cycle Recording Requirements		D		X		
13. Failure Reporting Requirements		D		X		
14. Serialization Requirements		D		X		
15. Procurement Specification Review				R		
16. Vendor Proposal Review				R		
17. Source Selection Review				R		
18. Parts Selection and Application Review		D		X		
19. Reliability Signoff - Top Assy. & Inst. Dwgs.				R		
20. Vendor Design Review				R		

CODE

D - Prime Action by Designer—check off, sign and date as completed.
R - Prime Action by Reliability Engineer—check off, sign and date as completed.
X - Check by Reliability Engineer—initial and date.

TABLE 11-2. RELIABILITY ACTIONS CHECKLIST (con.)

Design Title		Number				
No. Item	Completed	Responsibility				Notes and Comments
		Design		Reliability		
21. Critical Design Review		D		R		
22. Process Controls		D		X		
23. Manufacturing Procedure Controls		D		X		
24. Qualification Test Review		D		X		
25. Acceptance Test Review		D		X		
26. Integration Test Review		D		X		
27. Reliability Demonstration Test Review		D		X		
28. System Test:						
a. Test Requirements Review		D		X		
b. Test Plans Review		D		X		
c. Reliability Tests				R		
29. Reliability Summary Sheet				R		

D - Prime Action by Designer—check off, sign and date as completed.
R - Prime Action by Reliability Engineer—check off, sign and date as completed.
X - Check by Reliability Engineer—initial and date.

APPENDIX A DESIGN DETAIL CHECKLISTS

A-1 INTRODUCTION

In Chapter 11 the concept of checklists is discussed. This appendix provides several checklists addressed to specific design features that influence reliability. These checklists ought to be used in the formal design review and will also be helpful in the day-to-day development of a design. Checklists always should be reviewed before applying them. Inapplicable items are deleted, and the list is supplemented with additional requirements that are appropriate for the specific design being evaluated. Unique developments or problems may require special checklists.

A-2 PROPULSION SYSTEMS

(1) Specified pressure levels for leak checks will not damage sensitive components (diaphragms, burst discs, etc.).

(2) Electrical systems within engine areas will operate when exposed to high temperature and propellants.

(3) Propulsion system installation includes heat protection for primary structure.

(4) Shutdown or "zero thrust" capability is included if a test-range launch is proposed.

(5) All materials are proved compatible with fuel or propellant.

(6) All lines and components are properly identified.

(7) Critical functions on propulsion systems are monitored.

(8) Turbines have minimum possibility of tank damage in case of overspeed failure.

(9) Cartridge starters and other engine ordnance are protected from inadvertent ignition.

(10) Heat isolation is specified whenever structure, electrical components, or other heat-sensitive systems can be damaged by high temperature.

(11) Fuel tanks are not located in, or above, engine compartments.

(12) Subsystems located near engine hot sections are protected from heat.

(13) Nuts, bolts, and fittings that can cause leakage are mechanically locked or wired.

(14) Reservoir caps have an indicator showing closed and locked positions.

(15) Filler cap access covers cannot be installed without first locking reservoir cap.

(16) Flammable fluid tanks include shutoff valves.

(17) Interlocks are provided between fuel valves and/or tank valves to prevent oil tank shutoff while engine is operating.

(18) Oil coolers are heat isolated and not located in the engine hot section.

(19) Auxiliary power unit compartments are ventilated.

(20) Pressure relief is specified if the oil cooler is designed for less than 200 psi.

(21) Air induction systems have no items which can be ingested into the engine.

(22) Particle separation is specified for helicopter induction systems.

(23) Engine inlet screens are retractable.

(24) Ice removal and detection are provided for engine inlet screens.

(25) Overspeed protection is provided for engine starters.

(26) Continuous oil level indication and warning are provided.

(27) Filters are provided with a bypass feature immune to clogging and icing.

(28) Chip detectors are provided in engine sumps.

(29) Fuel, oil, and alcohol system drain outlets are located so that no drainage can enter induction systems.

A-3 FUEL/PROPELLANT SYSTEM

(1) Incompatible systems are separated sufficiently to prevent inadvertent mixing.

(2) Adjacent incompatible systems are designed so that it is impossible to interconnect.

(3) Components are qualified for use with the system fuel or propellant.

(4) Systems are identified by system function, commodity, pressure, and direction of flow.

(5) Insulation is nonabsorbent and can-

not react chemically with the system commodity.

(6) Cleaning agents cannot be retained in the system.

(7) Tank pressure will be relieved prior to exceeding structural limitations.

(8) Components and systems are located to minimize danger of ignition in hazard areas.

(9) Electrical equipment is approved for operation with the fuel or propellant.

(10) All possible connectors have been omitted from inhabited areas.

(11) Lines are routed to minimize the effects of leakage.

(12) Structural support is provided for heavy components.

(13) Heat resistant lines are provided in potential fire areas.

(14) Reference-pressure lines are protected from freezing at high altitude.

(15) Electrical controls are protected from short circuits.

(16) Flow of propellant stops if line ruptures.

(17) Proper cleaning levels are specified.

(18) System component interchange requirements are specified.

(19) Thermal overheat protection is provided where applicable.

(20) Effects of fuel or propellant leakage have been minimized.

(21) Static electricity protection is provided.

(22) Fuel tank locations minimize effects of lightning strikes.

(23) Fuel and propellant tanks are located for maximum crash protection.

(24) Ventilation and drainage are provided where leakage into confined areas is possible.

(25) Fuel tanks are not located in engine compartments.

(26) Tanks are located to minimize effects of leakage near engine compartments

(27) Fuel tanks are not located in the plane of the engine turbine.

(28) Effects of vapors are minimized in engine compartments, crew compartments, incompatible electrical equipment, and hot air bleed ducts by using vapor and liquid seals.

(29) Single failure of a tank pressurization system will not exceed tank structural limitations.

(30) Vent systems safely dispose of hazardous vapors.

(31) Lines avoid inhabited areas.

(32) Closed loop venting is provided for toxic hazards.

(33) Jettisoned fuel will not impinge on the vehicle.

(34) Materials are qualified for use with the system commodity.

(35) Pressure relief and bleed allow for cryogenic expansion.

(36) Reactions of high energy cryogenics are understood and allowed for in the system design.

A-4 HYDRAULIC SYSTEMS

(1) A component is designed so that it cannot be installed backwards. Directional arrows and color codes are in addition to positive mechanical constraints, not in lieu of them.

(2) Specific design instructions are provided for system proof check.

(3) All materials have been checked for fluid compatibility and, where compatibility is doubtful or unknown, tests have been made.

(4) Emergency systems are completely independent of primary systems.

(5) A pressure regulator accompanies each power pump.

(6) Ground test connectors are provided.

(7) No possibility exists for interconnecting pressure and return systems.

(8) Internal surfaces have rounded corners and do not invite fatigue failure.

(9) System-routing bypasses inhabited areas.

(10) Control system filters are of the no-bypass type.

(11) Back-up rings are provided where pressures can cause O-ring stress.

(12) Sharp corners are eliminated to reduce installation damage.

(13) Nonflammable hydraulic fluid is specified.

(14) Primary control systems are separate and have no other function.

(15) Pressure range does not exceed 15,000 psig, and peak system pressure does not exceed 135 percent of design operating pressure.

(16) Fluid temperatures do not exceed those specified in MIL-H-5440.

(17) Reservoirs are located for maximum protection and never located in the engine compartment.

(18) Fluid does not leak through reservoir vents.

(19) No gas from gas pressurized reservoirs is introduced into the fluid.

(20) Filters are consistent with contamination level required.

(21) Specified preoperational testing is strictly controlled to prevent excessive system wear.

(22) Where ground test connections are provided, pressure line is removed prior to removing the return line.

A-5 PRESSURIZATION AND PNEUMATIC SYSTEMS

(1) Storage pressure can be bled off to allow replacement of components. Pressure readout is provided to insure that pressure is below hazard levels.

(2) System is protected so that a regulator malfunction will not cause downstream system failure.

(3) Relief valves will initially (transient conditions) limit system pressure to no higher than 110 percent of working pressure.

(4) Reservoirs and storage vessels have shutoff valves for maintenance.

(5) Adjacent or incompatible system pressure connectors are keyed or sized so that it is physically impossible to connect the wrong unit or pressure level.

(6) All lines are identified by contents, pressure, and direction of flow.

(7) Separate pressurization sources are specified downstream of primary regulation when pressurizing noncompatible commodities.

(8) Pressure relief is specified where source pressure can exceed the design levels of the system.

(9) Trapped gas can be bled from between components.

(10) Relief valves exceed the maximum flow capacity of the pressure source.

(11) Inert gases cannot be introduced into inhabited areas.

(12) Proper proof checks are performed as specified.

(13) If system relief is not provided, safety factors are sufficient to contain safely the source pressure.

(14) Relief valve outlets are ported directly to the atmosphere.

(15) Lubricants and other materials are acceptable for use with the system gas.

(16) Pressure reservoir type and temperature rating are correct for the system working range.

(17) Components and systems are qualified and acceptable for use in the intended environment.

(18) Selection of compressions has considered explosion hazards.

(19) Check valves are placed to prevent critical air loss.

(20) Lines or components are protected from damage due to baggage and equipment stowage or personnel access.

(21) Routing of inert or toxic gas systems avoids inhabited areas.

(22) Hot air ducts are routed or insulated to protect structure from overheat.

(23) All direct pressure readout Bourdon tube gages are equipped with shatterproof glass and blow-out plugs.

(24) Components cannot be installed backwards.

A-6 ELECTRICAL/ELECTRONIC SYSTEMS

(1) Materials have been selected with due consideration for operational environment such as explosive or corrosive atmospheres.

(2) It is not possible to ignite or contribute to the ignition of adjacent materials regardless of the operational atmosphere.

(3) Materials will not emit toxic or explosive gases when operated at elevated temperatures.

(4) Use of dissimilar metals in contact is avoided.

(5) Design philosophy considers the most extreme possible environment.

(6) System operation is not degraded by temperature extremes.

(7) System design provides compensation such as hermetic sealing and pressurization for all pressure-sensitive elements.

(8) Components used in areas with flammable fluids are incapable of causing ignition.

(9) Wiring and component identification are proper.

(10) Routing of wires and location of components will not impose undue mechanical strain on termination points under any combination of anticipated service conditions.

(11) Routing of wires and location of components do not create interference with adjacent systems.

(12) Connections and terminations are at an absolute practical minimum.

(13) Sensitive circuits are isolated where degradation can be induced by adjacent circuits.

(14) Positive protection is provided for terminal blocks to prevent shorts resulting from contact with miscellaneous debris or from elements of the environment.

(15) Connectors are limited only to those applications requiring frequent disconnection.

(16) Sufficient space is allowed around connectors for engaging and disengaging, particularly where wrenches are required.

(17) Termination of power and signal leads on adjacent pins of connectors is avoided.

(18) Elements of a redundant system do not pass through the same single connector as elements of the primary system.

(19) Special tools, materials, and processes clearly are specified in the design.

(20) All reasonable effort has been expended to eliminate the possibility of the system contributing to flame propagation or toxic outgassing.

(21) Polyvinyl chloride or other low temperature polymers are not used as wire insulation (high temperatures are always a hazard).

(22) External power receptacles are located as far as possible from points of potential flammable vapor or fluid concentration.

(23) Lead-acid batteries are vented to areas where ignition is not possible.

(24) Battery vent outlets are designed to eliminate vent system backflow and so that battery acid cannot be ejected from the vent outlet.

(25) Equipment is protected from lightning strikes.

(26) The basic structure has been analyzed to insure compliance with electrical bonding requirements, particularly in areas of discontinuity.

(27) Electrical shielding is specified wherever it is necessary to suppress radio-frequency interference and other sources of spurious electrical energy.

(28) Circuits and equipments are protected from overload.

(29) It is not possible to induce a dangerous vehicle circuit overload from a malfunction of the ground system in the power circuits.

(30) It is not possible to induce a dangerous ground system circuit overload from a malfunction of the vehicle power circuits.

(31) Primary and redundant system circuits are not supplied from the same power bus or circuit breaker.

(32) Fuses and circuit breakers are easily accessible and are provided with a visual means to indicate their condition (open or closed).

(33) All elements requiring periodic service are accessible.

(34) Protection is provided from the hazards of loose articles, tools, and debris.

(35) Access covers, components, or equipment requiring specific installation orientation have asymmetric mounting features.

(36) Access is designed for easy handling of heavy components.

(37) Interlocks, shielding, safety guards, barriers, and warning markings have been specified where a personnel hazard can exist.

(38) Handholds, mechanical guides, rails or slides are specified wherever handling of slippery, bulky, heavy, or otherwise hard-to-handle equipment is involved.

(39) Electrical wire bundles avoid routes adjacent to fuel lines, hot air ducts, or mechanical linkages.

(40) High temperature wire and cable insulation is specified for designated fire zones and near high temperature sources.

(41) Routing provides for slack and a

service loop with enough excess wire for three connector replacements.

(42) Wires attached to normally moving parts are routed to twist with rather than bend across adjacent moving parts.

(43) Supports are provided to prevent abrasion or chafing of wires and cables.

(44) System-verification test-circuits do not indicate the command; rather, they indicate the actual response of the system.

(45) Power application will not actuate critical circuits as a result of function switches that may be cycled without indicating the on-off position during a power-off phase (i.e., push-on/push-off switches).

(46) Complex system operational test requirements are minimized during actual use.

(47) Continuous monitoring is provided for tests requiring judgments rather than standards.

(48) Test points are provided for rapid malfunction isolation.

(49) Connectors and other delicate protrusions cannot be used as footholds or for mechanical leverage.

(50) Maintainability specifications identify any hazards involved in removing, replacing, and testing of elements in the system.

(51) All power can be isolated from specific equipment to allow maintenance or removal.

A-7 VEHICLE CONTROL SYSTEMS

(1) Design is as simple as possible for the task it will perform.

(2) Electrical and mechanical components are compatible mutually and with the anticipated service environment.

(3) Limiting devices, emergency disconnects, alternate systems, or other safety measures are incorporated to safeguard critical parameters if a malfunction occurs.

(4) Circuit protection devices do not exist in signal circuit or in other circuits where unsafe control motions of the vehicle would occur if the device opened.

(5) Possibility of electrical cross-connections or phase reversals is minimized.

(6) No component or element of the system will interfere with crew rescue or escape.

(7) Adequate visual indication of the system operational status is presented to concerned crew members.

(8) Interlocks or limiting devices protect the structure from maneuvers in excess of the structural limit load factor.

(9) Redundant emergency power systems are provided.

(10) Installation requirements minimize the system vulnerability to defined mission hazards such as enemy action and environmental extremes.

(11) Installation requirements provide the maximum serviceability and maintenance features with a minimum of specialized tools or procedures.

(12) Installation requirements insure that position-sensitive components can be installed only in their proper orientation.

(13) Manual overpower capability is provided with the control system fully engaged and operating (piloted aircraft).

(14) Elements of the system are routed, covered, or otherwise protected from jamming from dropped or loose items, maintenance operations, cargo shift, etc.

(15) Elements of the system are protected from moisture or fluid accumulation, by draining potential fluid traps. In addition to normal corrosion hazards, trapped fluids can freeze at high altitudes and jam critical control elements.

(16) Elements of stability, accuracy, and reliability have been evaluated and verified for each component of the guidance and control system.

(17) There is a means of verifying satisfactory operation of each redundant path at any time it is determined that the system or subsystem requires testing.

(18) Redundant paths of the system are located such that an event that damages one path is not likely to damage the other.

(19) Failure in any portion of the system will not cause or create additional or cumulative hazards.

(20) Guards are provided over bolted ends of torque tubes.

(21) Unsymmetrical components cannot be installed incorrectly.

(22) Consideration has been given to pulley diameter versus cable wrap angle and applied force.

(23) Control-column openings are covered by flexible boots.

(24) Control cables are isolated effectively or protected from electrical equipment.

(25) Control mechanisms are located to afford maximum protection to preclude possibility of jamming or damage.

(26) Routing of cables, push-pull rods, and torque tubes considers structural deflection and its effect on function.

(27) Bolt length or reverse bolt installation will not cause system interference.

(28) Sleeves, rub-strips, or guards are provided where contact with stationary objects is possible.

(29) Provisions are made for frequent inspection of fatigue-prone areas.

(30) Inspection plates or access covers will not interfere with movement if installed incorrectly.

(31) Structural deflection will not cause cables to slack sufficiently to cause fouling.

(32) Guards are installed on all vertical pulleys to prevent jamming by foreign objects.

(33) Inspection doors are hinged from the top to prevent falling into any mechanism.

(34) Bracket attachment structure is reinforced properly to accept applied loads and repeated stresses.

(35) Actuating arms and levers are provided with pins, bolts, or serrations to prevent slippage.

(36) Unfavorable working conditions will not cause maintenance errors.

(37) Turnbuckles and push-pull rods are not subjected to bending forces.

(38) Universal joints are provided where torque tube misalignment can be excessive.

(39) Rod ends have rounded threads.

(40) Corrosion-resistant materials are specified where leaking acid or other corrosive liquids can contact mechanisms.

(41) Insert-bushings are used in attachment fittings in place of removable washers.

(42) Bolts are specified to attach rod ends to hollow tubes.

(43) It is impossible to cross-connect inadvertently any control cable or rod to the wrong fitting.

(44) Pulleys are positively attached to the bearing hub.

(45) Incorrect bolt length will not cause system interference.

(46) System and its components are compatible in all cases from the standpoint of durability, deflections, wear, and the danger of one component or system creating a hazard by proximity to other components or systems.

(47) Fabrication techniques have not subjected materials to temperatures or stresses which can affect design strength.

A-8 GUIDANCE AND NAVIGATION SYSTEMS

(1) Design will be as simple as possible for the task it will perform.

(2) Electrical and mechanical components are compatible one with the other, and with the anticipated service environment.

(3) Limiting devices, alternate systems, or other safety measures are incorporated when feasible to safeguard critical parameters if a malfunction occurs.

(4) No circuit protection devices exist in signal circuits, or in other circuits that control vehicle motion and where opening of such a device would produce unsafe motions.

(5) Possibility of electrical cross connections or phase reversals is minimized.

(6) Elements of stability and accuracy have been evaluated and verified for each component of the guidance and navigation system.

(7) System self-check features are provided to allow the operator to detect the presence of systematic random or cumulative error.

(8) A fail-safe or redundant system design philosophy is applied in a manner consistent with mission objectives.

(9) Redundant or double-redundant

design techniques are considered when critical parameters are displayed and are essential during approach and landing.

(10) There is a means of verifying satisfactory operation of each redundant path at any time the system or subsystem is determined to require testing.

(11) Redundant paths of the system are located so that an event that damages one path is not likely to damage the other.

(12) No element of the guidance or navigation system will interfere with crew escape.

(13) Installation requirements minimize the system vulnerability to defined mission hazards such as enemy action or environmental extremes.

(14) Installation requirements provide the maximum serviceability and maintenance features with a minimum of specialized tools or procedures.

(15) Installation requirements insure that position-sensitive components can be installed only in their proper orientation.

(16) Adequate visual indication of the system operational status is presented to concerned crew members.

(17) Minimum direct forward visibility is not severely limited by the installation of any navigational system.

A-9 COMMUNICATION SYSTEMS

(1) Redundancy is incorporated where required.

(2) Single component failure will not damage or diminish the use of redundant or related systems.

(3) Redundant systems can be operated from separate and independent power sources.

(4) Adequate design precaution is taken to eliminate or control electromagnetic interference (EMI) effects upon circuit components.

(5) Shielding design complies with MIL-E-6051.

(6) Interference control of the integrated system complies with MIL-STD-826.

(7) System is compatible and in compliance with "worst case" system requirements.

(8) System separation of the transmitter and receiver is such that direct excitation of the receiving antenna cannot exceed 10μV.

(9) Status displays are incorporated in all system functions that monitor hazardous operations.

(10) Compatibility with all relay links is possible within the allocated frequency of the proposed communication system design.

(11) Maximum continuous RF exposure of operational personnel or vehicle crew members does not exceed 10 mW cm^{-2}.

A-10 PROTECTION SYSTEMS

(1) Explosive vapor detectors are specified where explosive vapors can collect.

(2) Explosive vapor detection system will trigger an alarm at 20 percent of the lower explosive level.

(3) Toxic vapor detectors are specified wherever toxic gases or vapors can enter inhabited areas.

(4) Fire detection systems are specified for all potential fire zones.

(5) Smoke detectors are specified in nonventilated baggage or cargo areas.

(6) All possible design action has been taken to prevent false indication.

(7) Hazard warning systems can be reset to indicate a hazard recurrence.

(8) Explosive vapor detectors can operate in an explosive atmosphere without initiating an explosion.

(9) Deviation from normal performance will cause an explosive vapor detection system malfunction indication.

(10) All detection systems are completely compatible with the environment in which they must operate.

(11) All hazard detection systems receive power from the essential-equipment bus.

(12) Detector reaction time is at its absolute minimum.

(13) Provisions are made to allow periodic system calibration and checking.

(14) Malfunction detection systems sense critical system deviations.

(15) Critical instruments have positive failure warning.

(16) Instrument malfunction flags are not used to designate emergency conditions.

(17) All emergency conditions or malfunctions initiate a warning.

(18) Emergency conditions requiring immediate action initiate an audible warning in addition to visual warning.

(19) Audible warning is not specified in the communication system when constant monitoring is not required.

(20) Sound levels will not interfere with essential communications.

(21) Verbal audible warnings are clear, concise, intelligible, and reflect calmness and urgency.

(22) Audible warning override is provided where prolonged warning will interfere with effective corrective action.

(23) Volume controls do not reduce warnings to an inaudible level.

(24) Component interlocks are specified whenever out-of-sequence operation can create a system hazard.

A-11 FIRE EXTINGUISHING AND SUPPRESSION SYSTEM

(1) Potential fire zones are identified.

(2) Potential fire zones are isolated by fire barriers or firewalls.

(3) Titanium is not used structurally where it may contact molten metal.

(4) Firewalls are as liquid- and vapor-proof as possible.

(5) Access doors have not been installed in firewalls.

(6) Firewalls are not stressed by mounted equipment.

(7) Materials used on the protected side of firewalls will not burn as a result of high temperature in the fire zone.

(8) Air ducts passing through fire zones are fabricated to insure fire containment.

(9) Air ducts originating in fire zones can be closed to stop airflow.

(10) Flammable fluid lines with flow into or through a fire zone are provided with shutoff valves.

(11) Fire will have no effect on the operation of shutoff valves or control circuits.

(12) Flammable fluid lines in fire zones are made of stainless steel or equivalent.

(13) Flammable fluid flexible hose will withstand 2000°F when routed in or near fire zones.

(14) Fire detection is specified for all potential fire zones.

(15) Fire extinguishing systems are specified for all potential fire zones. (Ref. MIL-E-5352.)

(16) The most effective extinguishing agent is specified consistent with both safety and design goals.

(17) Toxicity is considered where it is possible for fumes to enter inhabited areas.

(18) Extinguishing agent containers are designed for maximum possible protection from crashloads or gunfire.

(19) Extinguishing agent containers have safety relief.

(20) Visual indication is provided that safety relief has occurred.

(21) Pressure gages are readily accessible for inspection and maintenance.

(22) Squib actuated discharge valves are designed so that electrical connection cannot be made unless the squib is installed.

(23) Interfaces between control systems and other systems cannot cause extinguishing system failure.

(24) Redundancy is specified where relays are used in the control system.

(25) Separate initiation circuits and dual squibs are provided for each container.

(26) Routing of control wiring does not pass through potential fire zones unless it can withstand at least 2000°F without system degradation.

(27) Automatic explosion-suppressing devices are considered wherever an explosion can occur too swiftly for crew reaction.

(28) Suppressing-system status is provided to indicate system has actuated.

(29) Flame-proof containers or compartments are specified for storage of items with low ignition temperature or high flame-propagation rates.

(30) Toxic products of combustion are considered when cabin interior materials are selected.

(31) Tests have been specified to determine if combustion products are toxic when unknown or doubtful.

(32) Electrical equipment will not provide an ignition source when operating in any hazardous atmosphere.

(33) Flammable fluid line routing avoids inhabited areas or is restricted.

(34) Complete fire hazard analysis has been made.

(35) Fuel lines and tank structures are designed to contain fuel as much as possible within the system under crash-induced loadings.

(36) Fuel lines and tanks are protected from penetration during a crash by mounting behind heavy structure and avoiding areas where penetration is likely.

(37) Provisions are made to deactivate systems that can provide an ignition source on crash impact.

(38) Spark-producing metals are not exposed to crash friction.

(39) Flammable fluid components are located where ground contact cannot occur and where crash damage is unlikely.

(40) All possible consideration is given to use of gelled or other ignition-inhibited fuels.

(41) Interior finishes and materials are selected for inability to support combustion and minimum toxic products of combustion.

(42) Flammable materials specified for use in an interior are at a minimum and flame retardants are specified for any flammable material used.

(43) Passenger compartments are provided with fire resistant storage compartments for combustible materials.

(44) Hand fire-extinguishers are provided.

(45) Cargo areas have fire detecting and extinguishing systems.

(46) Ventilation and cargo areas can be closed off during the extinguishing cycle.

(47) Lighting in cargo areas is protected from damage and contact with flammables.

(48) System actuation cannot be misdirected to the wrong fire zone.

(49) A single control handle will shut off flow of flammables and ignition sources.

(50) Audible alarm is provided where fire warning lights may go unnoticed.

(51) Audible alarm override is provided.

(52) System actuating switches are protected from inadvertent operation.

A-12 CREW STATION SYSTEMS

(1) Dimensional allowances for safe crew accommodations and work places comply with the 5th through 95th percentile.

(2) Surface colors properly depict the appropriate physical hazards by coding.

(3) Shape and location of emergency controls are such that crew members are able to operate them without visual reference.

(4) Operating controls are designed and located to minimize inadvertent activation.

(5) Emergency controls are readily visible and accessible.

(6) Materials and finishes selected for the crew stations are compatible with the environment.

(7) Types and characteristics of auditory and warning devices are suitable for providing the discrimination necessary under all operating conditions. Caution and advisory lights are located outside the flight instrument group. The brightness of the translucent areas of light indicators is at least 150 ft-lamberts in the bright mode.

(8) Displays are designed to minimize reading errors.

(9) Master caution and all warning lights can be dimmed to approximately 15 ft-lamberts when instrument lights are on and all other lights dimmed to approximately 1.5 ft-lamberts.

(10) Labels or placards are plainly legible under both day and night conditions. Warning and caution indicator lights are readily visible to crew members while at their stations.

(11) Proper equipment is provided to maintain safe cabin temperature and airflow requirements.

(12) Fuel and oil are prevented from contaminating the air in the crew compartments.

(13) Suitable decontamination and filtration devices are provided.

(14) There is proper access for the removal and replacement of filters or filter media.

(15) High-pressure, high-temperature bleed air ducts are located to prevent overheating of walls and compartments and the bypass areas containing combustible fluids.

(16) Check valves, shutoff valves, and other devices are provided for sealing off or regulating pressurized compartments.

(17) Insulation of the ducts is located properly and made of materials to prevent heat loss and contact with, or absorption of, combustible fluids.

(18) Range of temperatures in the crew compartment complies with the thermal comfort zone and specified exposure times for heat and cold.

(19) There are emergency provisions for assisted or unassisted escape from the crew compartment.

(20) Crew personnel are provided with an unimpeded path out of, and away from, the vehicle.

(21) Emergency lighting is incorporated in the crew compartment.

(22) Safety belts, harnesses, and straps are provided.

(23) Crew and their personal equipment are protected from thermal radiation caused by the explosion of nuclear weapons, including eye protection against flashblindness.

(24) Alarms and warning signs are designed, installed, and located so that they can be heard or read directly by crew members.

(25) Fire and overheat systems are designed and located to alert crew members of such conditions.

(26) Portable fire extinguishers are designed and mounted in locations where they are readily usable by crew members.

(27) Circuit overload protection devices are adequate.

(28) Interconnecting wires and cables are secured and protected to avoid inadvertent contact or wire chafing.

(29) Equipment cooling ducts and the equipment are located to provide adequate cooling of hot spots.

(30) Equipment is sufficiently accessible for manual fire extinguisher utilization.

(31) If a bipropellant is used, the oxidizer and fuel components are separated as far as possible.

(32) There are propellant shutoff and fuel jettison valves.

(33) Electrical wires, cables, and heat-producing equipment are isolated from the propellant components.

(34) All electrically operated motors, valves, solenoids, relays, etc., are of approved explosion-proof type.

(35) All materials used within the pressurized compartments are fire resistant. Interior materials do not generate toxic and noxious gases when exposed to heat and flame.

(36) Electrical and heat-producing items are separated from oxygen systems.

(37) A complete fire detection and extinguishing system is built into the vehicle.

(38) Fire extinguishing agents are compatible with the vehicle structure and environmental control systems.

(39) Environmental control system is equipped with filters for noxious gas and noxious gas neutralizing systems.

(40) If a toxic propellant is used, the lines and connections associated with it are routed outside the crew compartment.

(41) Pressurized compartment is sealed off from components that could generate toxic gas.

(42) Pressurized compartments are capable of being vented and purged to remove toxic gas.

(43) A complete toxic gas warning system is installed in the vehicle.

(44) Interior is free from sharp objects that could cause crew injury.

(45) All protrusions are removed, padded, labeled, or otherwise shielded.

(46) All electrical systems are labeled, interlocked, isolated, or otherwise designed to minimize electrical shock.

(47) Adequate provisions for the storage, protection, and accessibility of equipment and supplies are provided.

(48) Electrical power supply is redundant.

(49) An alternate power source is available for environmental control system operations. If not, insure that a stand-by or emergency environmental control system is available.

(50) Emergency power is supplied from a separate source and from an independent power bus.

(51) Vehicle pressure wall is designed so that proper quality control and testing procedures will ascertain pressure reliability.

(52) Crack propagation is limited.

(53) Faulty seals can be detected.

(54) Where wear or damage can occur, double seals are used.

(55) Seals or sealing devices are designed so that replacement or emergency repairs can be made.

(56) Shielding is provided adjacent to equipment that could structurally fail and puncture the cabin wall.

(57) Delicate components are located where they will not be damaged while the unit is being worked on.

(58) Internal controls, such as switches and adjustment screws, are not located close to dangerous voltages.

(59) Components that retain heat or electrical potential after the equipment is turned off are not located where maintenance personnel may touch them inadvertently upon opening the equipment.

(60) Irregular protrusions such as cables, wave guides, and hoses are easily removable to prevent damage during maintenance.

(61) Rests or stands are provided on which units can be set to prevent damage to delicate parts. Rests or stands are designed as a part of the basic chassis.

(62) Fold-out construction is provided for units wherever feasible, and parts and wiring are arranged so that they are not damaged when the assembly is opened or closed.

(63) Covers and cases are sufficiently larger than the units they enclose to preclude damage to wires and other components when the cases are removed or replaced.

(64) Corners and edges of covers and cases are rounded for safety while handling.

(65) Ventilation holes in covers are small enough to preclude inadvertent insertion of any object that might touch high-voltage sources or moving parts.

(66) Handles are shaped so that they do not cut into the hand of the holder.

(67) Guards or other protection are provided for easily damaged conductors such as high-frequency cables or insulated high-voltage cables.

(68) Plugs with a self-locking safety catch are used in preference to plugs that must be safety-wired.

(69) Internal fillets that might injure the hands or arms of maintenance personnel are provided with rubber, fiber, or plastic shielding on the edges.

(70) On accesses that lead to equipment with high voltages, safety interlocks are provided that deenergize the circuit when the access panel is opened. If maintenance is required on equipment with circuits energized, insure that a "cheater" switch is provided that bypasses the interlock and that automatically resets when the access panel is closed.

(71) Warning labels are provided on all access panels leading to high voltage or moving parts.

A-13 ORDNANCE AND EXPLOSIVE SYSTEMS

(1) Sensitivity, shattering effect, and power of the explosive are evaluated fully for each application.

(2) Degree of sensitivity of the initiator is evaluated fully for each application.

(3) Materials are without dangerous defects, and will resist changes due to aging.

(4) Degree of confinement of the device is evaluated fully for each application. Explosive energy release is more hazardous in areas of closer confinement.

(5) Items with critical manufacturing tolerances are avoided where possible since such items are more susceptible to accidental ignition.

(6) Termination interruptions in the firing circuit are held to the absolute minimum.

(7) Maximum protection from inadvertent operation is provided by proper circuit design and use of safe/arm devices.

(8) The most electrically or mechanically insensitive device commensurate with the application is used.

(9) Specifications for storage comply with existing regulations and requirements.

(10) Specifications for storage do not permit the use of static electricity generators—such as plastic sheets, wraps, and covers—in any part of the packing and storage process.

(11) Test and evaluation are carried out properly through detailed test specifications

showing test objectives, methods, equipment, personnel, and special precautions necessary as determined by the design.

(12) The insulation for ordnance firing circuits possesses the optimum dielectric characteristics for the design environment.

(13) Shielding to protect the squib and firing circuits from stray voltage is evaluated properly and optimized for each design.

(14) Ordnance circuits are routed with minimum exposure to physical damage and potential electrical ignition sources.

(15) Ordnance control circuit design is compatible with the vehicle shock and vibration environment.

(16) Ordnance devices and the firing circuits have been reviewed separately and as an integrated system, giving strong emphasis to subsystem interfaces.

(17) Applicable range safety manuals have been reviewed for ordnance system performance requirements prior to design selection.

(18) A hazard analysis is conducted on all ordnance systems to evaluate their hazard potential. A hazard analysis is conducted on all liquid-propellant and solid-propellant systems to an acceptable hazard level of operation.

(19) Hazard analysis has identified all potential modes of vehicle failure and has indicated design approaches, corrections, or recommendations to minimize the level of the indicated hazard.

(20) Design has been corrected in accordance with the findings of the hazard analysis consistent with program objectives.

(21) All hazards have been evaluated either by experiment or empirical knowledge.

(22) Effectiveness and necessity of an explosion suppression and inerting system have been evaluated.

(23) All ignition sources are identified and corrective measures are taken to reduce the probability of their contribution as an explosion source.

(24) Design requirements subject a minimum of personnel to the acceptable hazard level determined by the system hazard analysis.

(25) Fuze/safing-arming mechanism has at least two independent safing features, any one of which can prevent an unintended detonation. Each is activated by a different environmental input. At least one feature includes an arming delay adequate to spare the user from injury in case of premature functioning of the system. The item is fail-safe when all safing features are subverted.

(26) Detonation of any primer or detonator in a fuze/safing-arming mechanism that is in the safe condition will be physically barred from causing further functioning of the explosive train.

APPENDIX B
RELIABILITY DATA SOURCES

B-1 INTRODUCTION

In recent years, a large number of reliability information centers and data banks have been established. These data banks provide information in a variety of formats useful to reliability engineers. Advances in the field of computer storage and retrieval, microfilming, microfiche techniques, and other processes have made it possible to store and retrieve large quantities of information. Information retrieval techniques have been developed which permit the engineer to retrieve stored data and perform statistical evaluations.

The accumulation of numerical reliability data has been aided technically and economically by the use of computers. Most of the early data banks were established to provide the designer with the information he needed for a specific system development. The more recent programs are broader in scope and have made some efforts to alleviate some of the shortcomings of their predecessors. Some early programs have been combined with others or eliminated.

Ref. 4 is a comprehensive listing of Reliability and Maintainability sources associated with the Air Force. Three major data banks are described in pars. B-2, B-3, and B-4. Some of the special circumstances that the designer must consider in using data bank information are discussed in par. B-5. A partial listing of data banks is presented in par. B-3.

B-2 GIDEP, GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM

B-2.1 INTRODUCTION

The Government-Industry Data Exchange Program (GIDEP) was originated in 1959 by the Army, Navy, and Air Force Ballistic Missile Agencies. Known at that time as IDEP—Interservice Data Exchange Program—its intent was to eliminate duplicate testing of parts and components by disseminating pertinent test data among Department of Defense contractors and various Government agencies. The Navy FARADA program also has been integrated into GIDEP.

In 1966, both the National Aeronautics and Space Administration and the Canadian Military Electronics Standards Agency (CAMESA) recognized the value of the data provided by the program and became participants. Today, GIDEP provides the interchange of reliability data to all the military services, participating Government contractors, and numerous Government agencies such as the Energy Research and Development Administration, Federal Aviation Administration, Defense Supply Agency, and the Small Business Administration.

GIDEP operates under a charter agreed upon by the Army and Navy Materiel Commands, the Air Force Systems and Logistics Commands, and NASA. The Program Manager, organizationally located within the Department of the Navy, is responsible for policies and procedures, both national and international. The GIDEP Administration Office located at FMSAEG, Corona, California, is the operational arm of the program. Working directly under, and responsible to, the Program Manager, the Administration Office maintains the GIDEP data banks and is responsible for all operational phases of the program. The GIDEP management team includes Government and Industry advisory groups.

Availability of a microfilm reader-printer is the only equipment requirement for the frequent GIDEP data user. Participants are not subject to fees or assessments of any kind, nor is there any payment for contributions of data. Participation at contractor facilities usually is considered part of the normal reliability or quality assurance program. However, with the recent issuance of Regulations by the Military Services and NASA, participation is now becoming a mandatory requirement.

The objectives of the GIDEP program are to:

1. Reduce or eliminate duplicate expenditures for development parts and components
2. Increase the confidence level in the reliability of systems using these parts and components
3. Expedite research and development projects by avoiding repetition of tests previously accomplished
4. Assist in the preparation of more realistic proposals
5. Standardize procedures for reporting test information
6. Encourage direct intercontractor communications among technical personnel working on related projects
7. Generate information for an alternate source of parts through more dependable data
8. Create a general source for test data
9. Provide for the exchange of test equipment calibration procedures and related metrology data.

This description has been adapted from Ref. 3.

B-2.2 FUNCTIONS

GIDEP data are contained in four separate information banks: the Engineering Data Bank, the Failure Experience Data Bank, the Failure Rate Data Bank, and the Metrology Data Bank. No classified or company proprietary information is included.

B-2.2.1 Engineering Data Bank

The Engineering Data Bank contains primarily laboratory data relating to parts, components, and materials. These data cover Qualification and Environmental Testing, Research and Development, Evaluation Reports, and other meaningful engineering data such as nonstandard part justification, test planning, and manufacturing processes.

B-2.2.2 Failure Experience Data Bank

The Failure Experience Data Bank contains failure experience data; failure analysis reports from the field, laboratory, and production; and information from a pilot effort for a Defective Parts and Components Control Program (DPCCP), which includes failure analysis data by component types derived from an operation and maintenance level. The function of the DPCCP is to identify and eliminate or control defective parts. Methodology includes both the avoidance of specifying suspect parts in new designs and the purging of these suspect parts from current Government inventory if required.

Part of the Failure Experience Data Bank is an important function known as the ALERT system. The ALERT is a highly effective means of rapidly providing all participants with information concerning an actual or potential problem involving a part, material, test equipment, process, or safety hazard. Any participant who finds a situation that he feels to be of general concern to other participants, fills out an ALERT form. The ALERT form is submitted to the Administration Office where it is reviewed and distributed to all participants as an ALERT. Generally, this process is completed within 24 hr. The ALERT system may be used for any type of pertinent information relating to any of the data banks. It is issued to identify such items as faulty design, faulty test equipment or calibration procedures, or other production and processing problems.

B-2.2.3 Failure Rate Data Bank (FARADA)

The Failure Rate Data Bank contains field performance data relating to parts and components. Detailed information concerning failure rates, stress levels, mean time to repair, level of test specification, failure mode, test environment, and other pertinent information is contained in the Failure Rate Data Bank. The FARADA program—which collected field experience and reliability demonstration test data for use in Reliability Prediction, Spares Provisioning and Logistics Support studies—has been integrated into GIDEP as of July 1973. This has enlarged the GIDEP data bank and provides a broader range of participating organizations. It also provides parts and components performance data obtained under

actual field operational conditions, so that correlation studies can be made to compare laboratory tests with field experience.

B-2.2.4 Metrology Data Bank

The Metrology Data Bank contains calibration procedures and general information on test equipment. Calibration procedures prepared by both the military and industry, covering most electrical and mechanical test equipment, are available to participants. Under a program called SETE (Secretariat for Electronic Test Equipment), which is aligned with GIDEP, other types of information such as test equipment evaluation reports are available. These reports greatly influence reliability improvement in test equipments and instrumentation. Groups concerned with the measurement of physical and electrical attributes, or development of measurement standards and instrumentation, are primary users of this data bank.

The International Reliability Data Exchange with the EXACT program is headquartered in Sweden. Functioning at an international level, EXACT provides for the exchange of reliability test data with a dozen foreign countries. GIDEP provides test reports to EXACT which document successful qualification and evaluation laboratory tests on parts and materials. The increasing use of foreign-made parts in our military systems makes availability of information on those materials of obvious value. EXACT provides for data exchange among all member countries.

B-2.3 OPERATIONS

The GIDEP program operates as a self-regenerating, closed-loop system. Engineering, Failure Experience, Failure Rate, and Metrology data are submitted by Government or industry participants to the Administration Office for inclusion into the GIDEP Data Banks. When a GIDEP Representative submits data to the Administration Office, he assigns it a 9-digit generic index code. The first 3 digits of the code define the major part classification, such as: transformer or antenna. The last 3 pairs of digits provide relative levels of detail information covering such areas as function, application, construction, and even detailed data such as pressure range, working voltage, power rating, and frequency range. The codes for indexing GIDEP data are contained in the *GIDEP Policies and Procedures Manual* (Ref. 1).

Once data have been screened and indexed, the index is placed in the GIDEP computer, and the full report is placed in microfilm cartridges that are distributed along with a hard copy index biweekly to all participants. The Administration Office distributes a complete updated index to all participants annually. Participants may request a computer index search and copies of reports directly from the Administration Office, or they, through a terminal, address any of the four GIDEP data banks individually or collectively. The user can enter a year date to restrict his data search to relatively current information, or he can run an entire historical search of all data in a particular area.

The GIDEP computer is programmed so a participant can initiate a search using any of several approaches. The computer can be addressed to search by GIDEP generic code, manufacturer's part number, key work, industry standard part number, environmental code, or any other fields contained in the data banks. Once information is located, the computer provides the participant with a microfilm reel and access number in addition to a report number. All participants are provided with microfilm indexes. Thus, if a participant does not maintain microfilm records, he can request copies of specific reports or the loan of a microfilm reel from the Administration Office.

If an index and computer search fails to identify participant-required data in the GIDEP Data Banks, the user can initiate an Urgent Data Request (UDR). One of the most powerful tools of the GIDEP program, the Urgent Data Request is a means by which a participant submits an informal request to all other participants for information on a specific part, component, material, or test instrument. The GIDEP Administration Office, upon receipt of the UDR, reproduces the form and promptly distributes it

to all participants. When a participant finds information pertaining to the particular problem, he forwards the information directly to the requestor.

One of the key people in the GIDEP program is the GIDEP Representative. Assigned by each new participant from its in-house staff, his responsibility is to determine who in his organization (1) can use and (2) will generate GIDEP data. He, more than any other person in the program, directly influences his company's success or failure within the scope of the GIDEP program (Ref. 2).

B-2.4 COST SAVINGS

The GIDEP program provides participants with the vehicle to maintain and improve the reliability of their product and simultaneously minimize research time and eliminate duplicate testing of parts, components, and materials. The program, properly implemented and utilized, produces impressive cost effectiveness. In 1966 when the program was relatively new, the documented cost savings to participants, both Government and industry, was $5 million. In 1973 the GIDEP program has a cost savings over $10 million.

See par. B-6.1 for contect for further information.

B-3 RELIABILITY ANALYSIS CENTER—A DOD ELECTRONICS INFORMATION CENTER

The Reliability Analysis Center is a formal Department of Defense Information Analysis Center providing technical and information analysis services relating to semiconductor and passive electronic components. The overall objective of the Reliability Analysis Center is to aid Government and contractor engineers in improving the reliability of military and space electronic systems and equipments. The Reliability Analysis Center provides users with faster and more effective methods of achieving important product reliability improvement. This is accomplished through ready access to factual failure and reliability data on all component technologies, more effective device procurement and quality assurance practices, and elimination of redundant testing programs.

The Reliability Analysis Center analyzes and disseminates information that is generated during all phases of device fabrication, testing, equipment assembly, and operation. The Reliability Analysis Center maintains a comprehensive data base that continually is updated by the latest information generated by Government agencies, independent R&D laboratories, device and equipment manufacturers, system contractors, and field operations. Collection efforts concentrate on failure mode and mechanism analysis; material, device, and process technology; quality assurance and reliability practices; test results; and application experience.

A major feature of the center is its analysis capability. Information that is processed into its files is classified according to generic descriptors that encompass material, design, and process control characteristics. Correlation studies—which isolate dependencies and interrelationships among device properties, operating environments, and failure incidence—can be extended to new situations, new devices, and new applications.

The Reliability Analysis Center offers four basic services:

1. Publication of reliability data compilations, technical reports, handbooks, and related reference documents
2. Rapid information searches and referrals in response to direct user inquiry
3. Consulting services and in-depth studies
4. Maintenance and updating of the microcircuit portion of MIL-HDBK-217B.

The Reliability Analysis Center publishes and periodically updates several unique data compilations that report failure rates, environmental stress susceptibility, and part malfunction history. These publications assemble results of recent laboratory tests, factory checkout, and field operations into convenient form for direct application to the users' initial reliability control tasks. These data are compiled in two forms: (1) by part type

number and manufacturer and, (2) by physical (generic) part characteristics. Data analysis and related information concerning process control, quality assurance procedures, procurement practices, etc., are compiled in state-of-the-art reports and handbooks as the need arises.

Although fully prepared to perform literature search and referral services, the Reliability Analysis Center staff can contribute most directly to the solution of reliability problems through unbiased technical assessments and in-depth studies of its accumulated resources in response to user needs. The Reliability Analysis Center staff is augmented in the conduct of these studies by the RADC professional reliability staff who have reliability competence in both component and system areas and serve as the center of reliability expertise for the Air Force. Typical areas for consulting are: data analysis, failure problem investigation, reliability assessment and predictions, test and specification development, and in-depth data and technical surveys.

The Reliability Analysis Center services are available without restriction to Government agencies and contractors. As a DOD Information Analysis Center, the Reliability Analysis Center is required to charge all users an equitable amount for the service provided. See par. B-6.2 for the contact for further information.

B-4 ARMY SYSTEMS

B-4.1 THE ARMY EQUIPMENT RECORD SYSTEM (TAERS)

Information on TAERS is included—despite being replaced by TAMMS in 1969—because historical abstracts from the TAERS files generated between 1965 and 1969 are included in the TAMMS file.

TAERS was part of a program instituted by the Army to collect, analyze, and make use of information concerning Army materiel. The data handled were basically maintenance oriented, rather than reliability oriented—i.e., maintenance and management, part repairs and replacement frequency, maintenance resources, and manpower requirements. The system collected and processed data to provide the maintenance management information required by field commanders and managers in the following areas:

1. Equipment status and materiel readiness
2. Effectiveness of maintenance operations
3. Adequacy of resources
4. Support requirements.

The processed data were examined during the programming to indicate what equipment was failing, why it was failing, how often the failure was occurring, and the amount of time required for repairs. The results of the analysis provided statistical forecasts for planning purposes.

B-4.2 THE ARMY MAINTENANCE MANAGEMENT SYSTEM (TAMMS) INCLUDING SAMPLE DATA COLLECTION

The equipment record procedures known as TAMMS—which replaced TAERS in 1969—are used for control, operation, and maintenance of selected Army materiel.

The system is applicable to:

1. Equipment improvement recommendations
2. Recording and mandatory reporting of all modification work order requirements and accomplishments
3. Recording essential information to be used for evaluation of materiel readiness
4. Recording and reporting of failure data for design of new equipment, redesign of standard equipment, and product improvement
5. Collection of inventory, operational, and/or maintenance data on special one-time studies or projects. (In cases where the forms and procedures do not fully meet the requirements of such studies, approval for deviation must be obtained from Headquarters, Department of the Army.)
6. The periodic application by the Department of the Army of a sampling technique to obtain specific organizational maintenance action data from units located in a

specific geographic area. (This sampling will include only specific type/model/series of equipments for a limited time period.)

The exceptions to the application of the maintenance management system procedures are:

1. Installed equipment to provide utility services such as gas, steam, and water
2. Industrial production equipment
3. Locally purchased nonstock-numbered, nonstandard (nontype-classified) equipment, other than commercial vehicles
4. Equipment procured with nonappropriated funds.

Raw data generated at the user and support maintenance levels are entered onto prescribed forms. Commanders at the field level process data relating to expenditure of maintenance resources and materiel readiness indicators, and forward selected maintenance data to a national level data bank. Analyses, summaries, and reports subsequently are furnished to the national level materiel managers for their use in improving the materiel readiness condition of Army materiel in the hands of the user.

The basic data in the system represent day-to-day experience of using organizations in operating and maintaining materiel. Data are recorded on assemblies, end items, and systems. Reduced data provide quantitative information such as:

1. Materiel reliability, maintainability, and availability
2. Scheduled and unscheduled maintenance requirements
3. Repair part consumption
4. Utilization rates for personnel, materiel, and facilities.

Typical uses of the reduced data are to validate maintenance engineering analysis predictions, identify problems with regard to current support resources, forecast resource requirements, and to detect trends that indicate a need for materiel modification, or that materiel is nearing the end of its useful life. Additionally, the data are used to evaluate new materiel concepts and designs, and to estimate life cycle support costs for new materiel. TAMMS provides little data useful for engineering applications other than exception failure data through the Equipment Improvement Recommendations (EIR). The EIR's provide indicators of field problems that the user feels merit national attention or a response to his specific problem. Each EIR provides only a narrative description with little if any quantitative data.

B-5 PRECAUTIONS IN USE

Historical data on components, equipments, and systems can be applied to aid the design of new equipment or systems. Reliability requirements have become quite precise and are included in system contracts. Therefore, designers require data that are statistically valid, have been analyzed thoroughly, and are promptly available. The degrees to which these objectives have been achieved differ for various data banks.

The designer needs specific data—such as the failure rates in specific environments and/or stresses, preconditioning or screening procedures applied to the parts, and similar details. He also needs reliability data that have been collected, analyzed, stored, and disseminated in a form that is useful in the conceptual and design stage phases. Until such time as a reliability data bank that satisfies completely the needs of the designer is developed and made operational, he must proceed with caution in using the data now available to him.

There are several basic difficulties with any data bank and analysis center. Perhaps the most fundamental difficulty is that the data source is always suspect. Field failure reports are notorious for their inadequacies. The user/maintainer has many pressures to use the system/equipment correctly and to keep it functioning; the priority allotted to filling out failure reports is usually low. A difficulty with many contractor reports is that not all contractor personnel are highly competent; some reports are written by incompetent people. It is easier to blame failures on parts rather than on people.

The human factors aspects of data banks and analysis centers have not been resolved satisfactorily. Formal pronouncements by

headquarters staffs and company officials are not the same thing as implementation in the field.

Much time and good effort have gone into these data sources. If they are used cautiously and intelligently, they can be very helpful; if they are used blindly, the results often will be very unsatisfactory.

B-6 PARTIAL LISTING OF DATA BANKS IN OPERATION

B-6.1 GIDEP, GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM

This is a Government-sponsored cooperative program for exchange of reliability information to improve quality and reliability, and reduce cost of systems and equipments.

Technical Coverage. Engineering and Failure Experience Data on parts, components, and materials. Failure Rate Data from field operations, and Metrology Data including test equipment calibration procedures. Coverage of data is electronic, mechanical, hydraulic, and pneumatic.

Mission. Provides program for exchange of specialized data, and operates ALERT and UDR systems to provide communication network among participants.

Point of Contact.
Head, GIDEP Branch
Naval Fleet Missile Systems Analysis and Evaluation
Group Annex (Code 862)
Corona, CA 91720
Phone: (714) 736-4677
AV: 933-4677

B-6.2 RELIABILITY ANALYSIS CENTER

Technical Coverage. A designated DOD Information Analysis Center for the dissemination of reliability and experience information on electronic components with special emphasis on microcircuits.

Mission. Serves as the DOD focal point for the acquisition, reduction, analysis, and organization of reliability data in an authoritative, timely, and readily usable form to aid Government and contractor engineers in improving the reliability of electronic systems.

Services. Publishes failure rate, environmental susceptibility and malfunction data compendia, state-of-the-art surveys, handbooks, and reference bibliographies; conducts literature search and referral services; provides technical consulting services. Specialists in reliability are available to work directly with the user to define his problem, search out relevant data and information, evaluate and analyze results, and provide concrete recommendations, and guidance. The Reliability Analysis Center data files contain data and technical reports on reliability physics investigations, reliability improvement programs, part design, qualification and lot acceptance tests, equipment assembly, demonstration test and checkout results, and operational history.

Point of Contact.
Technical Director
Reliability Analysis Center
RADC/RBRAC
Griffiss AFB, NY 13441
Phone: (315) 330-4151
AV: 587-4151

B-6.3 EQUIPMENT RECORD AND MAINTENANCE MANAGEMENT SYSTEMS

A. THE ARMY EQUIPMENT RECORD SYSTEM (TAERS)

Technical Coverage. Historical only, 1965-1969. Maintenance-management data, part repair and replacement frequency, maintenance resources, and manpower requirements.

Mission. Management information necessary for evaluating: (1) equipment status and materiel readiness, (2) effectiveness of maintenance operations, (3) adequacy of resources, and (4) support requirements.

Point of Contact.
Appropriate NMP; example
Commander
USATACOM
ATTN: AMSTA-M(NMP)
Warren, MI 48090

B. THE ARMY MAINTENANCE MANAGEMENT SYSTEM (TAMMS)

Technical Coverage. Site location, usage, materiel readiness, and Equipment Improvement Recommendations.

Mission. Provides Fleet Management data and improvement recommendations to the national level. Provides maintenance management techniques (forms procedures to using unit level).

Point of Contact.

Commander
US Army Management Center
ATTN: AMXMD-MT
Lexington, KY 40507
Phone: (606)293-3020
AV: 745-3020

B-6.4 US ARMY ELECTRONICS COMMAND (ECOM)

Technical Coverage. Nuclear, plasma, and solid-state physics, geophysics, meteorology, radio communications, automatic data processing, aerospace electronics, combat radar, electronic warfare, detection systems, frequency controls, and electronic parts and components.

Mission. Coordinates in a single organization, the research, development, procurement, and production of Army communication and electronic materiel, by sponsoring and conducting of research and by publishing technical reports and a current newsletter.

Point of Contact.

Commander
US Army Electronics Command
Ft. Monmouth, NJ 07703

B-6.5 REDSTONE SCIENTIFIC INFORMATION CENTER

Technical Coverage. Aerospace logistics, operations, ballistics, fire control, fuzes, warheads, and related missile and rocket ordnance.

Mission. Serves as data bank for technical literature on missiles, rockets, rocket motors, and related items at Redstone Arsenal; issues data compilations, summaries, bibliographies, and reports; and maintains and disseminates accumulated data.

Point of Contact.

Commander
US Army Missile Command
ATTN: AMSMI-RB
Redstone Arsenal, AL 35809

B-6.6 BALLISTIC RESEARCH LABORATORIES (BRL)

Technical Coverage. Ballistic technology, vulnerability assessment and vulnerability reduction, weapon system evaluation, concept analysis, operations research, reliability, quality assurance, ballistic measurements, test-data analysis, probability, and mathematical analysis.

Mission. Conducts research in ballistics, vulnerability, and physical and mathematical sciences; evaluates and synthesizes data for contributions to weapon technology; provides technical assistance and consulting services; and issues technical reports.

Point of Contact.

Director
US Army Ballistic Research Laboratories
ATTN: STINFO Officer
Aberdeen Proving Ground, MD 21005

B-6.7 NONDESTRUCTIVE TESTING INFORMATION ANALYSIS CENTER (NTIAC)

Technical Coverage. Nondestructive-test data on materials, acquired through radiography, ultrasonics, electromagnetic, and other nondestructive test methods.

Mission. Collects, maintains, and disseminates, via rapid-retrieval system, data in the field of nondestructive testing; provides consulting and advisory services; and publishes bibliographic information.

Point of Contact.
Chief
Materials Testing Laboratory
US Army Materials and Mechanics Research Center
ATTN: AMXMR-TXT-Nondestructive Testing Information Analysis Center
Arsenal Street
Watertown, MA 02172

B-6.8 US ARMY BALLISTIC RESEARCH LABORATORIES (BRL) (Radiation Engineering Branch)

Technical Coverage. Nuclear radiation, residual radiation, shielding, radiological defense, and radiation effects.

Mission. Conducts research and field experiments, provides technical information and assistance, provides environmental monitoring and radiological safety support.

Point of Contact.
Chief
Radiation Branch, Vulnerability Laboratory
US Army Ballistic Research Laboratories
Aberdeen Proving Ground, MD 21005

B-6.9 US ARMY TANK-AUTOMOTIVE DEVELOPMENT CENTER

Technical Coverage. Automotive systems for combat vehicles, tactical wheeled vehicles, commercial wheeled vehicles, engineer and construction equipment (as of 1 July 1974), materials handling equipment (as of 1 July 1975), and trailers and semitrailers.

Mission. Design, development, testing, procurement, logistic support (Supply and Maintenance), and reconditioning of vehicle systems listed above.

Point of Contact.

1. For operational field data and maintainability data:

   Commander
   US Army Tank-Automotive Development Center
   ATTN: AMSTA-QR
   Warren, MI 48090

2. For test data and reliability data:

   Commander
   US Army Tank-Automotive Development Center
   ATTN: AMSTA-MS
   Warren, MI 48090

B-6.10 THERMOPHYSICAL AND ELECTRONIC PROPERTIES INFORMATION ANALYSIS CENTER
MACHINABILITY DATA CENTER
CONCRETE TECHNOLOGY INFORMATION ANALYSIS CENTER

Point of Contact.
Chief, Nondestructive Testing Industrial Applications Branch
US Army Materials and Mechanics Research Center
Arsenal Street
Watertown, MA 02172
Phone: (617) 926-1900
AV: 648-8250

B-6.11 PLASTICS TECHNICAL EVALUATION CENTER (PLASTEC)

Technical Coverage. Plastic materials, adhesives and composites, with emphasis on plastics in structural weapon systems, electrical and electronic applications, packaging, mechanical devices, and specifications.

Mission. Collects, exchanges, develops, and evaluates technical data for the DOD, related activities, contractors, and others on a fee basis as time permits. Serves as plastics information data source by consultation and publications.

Point of Contact.
Chief
Plastics Technical Evaluation Center
Picatinny Arsenal
ATTN: SARPA-FR-MD
Dover, NJ 07801

B-6.12 US ARMY TEST AND EVALUATION COMMAND (TECOM)

Technical Coverage. Development test data and test techniques on all materiel used by the Army in the field.

Mission. Conducts development test II (DT II) (except those DT II engineering phases pertaining to aircraft performance, stability, and control climatic hangar test) and development test III (DT III) of all AMC developed Army materiel intended for general use by the Army in the field. Plans, conducts, and reports on the developmental test objectives of combined development and operational tests, in conjunction with Operational Test and Evaluation Agency (OTEA), Department of the Army, and/or the AMC activity responsible for operational testing. Reports of all testing are available for Defense Documentation Center.

Point of Contact.
Reliability, Availability and Maintainability Directorate
HQ, US Army Test and Evaluation Command
Aberdeen Proving Ground, MD 21005

B-6.13 US ARMY COLD REGIONS RESEARCH AND ENGINEERING LABORATORY (CRREL)

Technical Coverage. Physical, mechanical, and structural properties and behavior of snow, ice, and frozen ground; geology, geophysics, geography, and meteorology; engineering and technology; environmental conditions and physics; military applications; and hydrology, waste water management, ice engineering.

Mission. Conducts research and engineering investigations for supporting and improving US military capabilities in cold regions.

Point of Contact.
CO/Director
US Army Cold Regions Research and Engineering Laboratory
ATTN: CRREL-TI
P.O. Box 282
Hanover, NH 03775

B-6.14 US ARMY HUMAN ENGINEERING LABORATORIES (HEL)

Technical Coverage. Scientific and technical information regarding human factors affecting military operations and materiel.

Mission. Assists the AMC in resolving human-factors engineering problems by performing research, giving courses, etc., to facilitate smooth man-machine operability.

Point of Contact.
Commander
US Army Human Engineering Laboratories
Aberdeen Proving Ground, MD 21005

B-6.15 PETROLEUM AND MATERIALS DEPARTMENT, US ARMY MOBILITY EQUIPMENT RESEARCH AND DEVELOPMENT COMMAND

Technical Coverage. Chemical cleaning and corrosion; paint, varnish, and lacquer; automotive chemicals; and fuels and lubricants.

Mission. Provides research, development, evaluation, and specification information in support of AMC; provides consultant services to other military agencies.

Point of Contact.
Chief, Petroleum and Materials Department
USAMERDC
Ft. Belvoir, VA 22060

B-6.16 US ARMY NATICK DEVELOPMENT COMMAND

Technical Coverage. Physics, biology, and engineering as applied to textile, clothing, body armor, footwear, organic materials,

insecticides and fungicides, subsistence, containers, food service equipment, field support equipment (as assigned), tentage and equipage, and air delivery equipment.

Mission. Conducts research, development, engineering, and standardization programs.

Point of Contact.
Commander
US Army Natick Development Command
ATTN: STSNLT-EQ
Natick, MA 01760

B-6.17 US ARMY ARMAMENT COMMAND (ARMCOM)

Technical Coverage. Engineering research data on munitions and weapon systems including cannon, mortars, howitzers, small arms, and antitank and antiaircraft weapons. Special topics include recoil mechanisms, fire control equipment, feed mechanisms, optical equipment, nondestructive-testing equipment, all munitions, all projectiles, rocket and missile warheads, mechanical fuze timers, mines and mine fuzing, pyrotechnics, propellant actuated devices, toxic chemical munitions, flame weapon systems, and incendiary devices. Services include numerical analysis, mathematical statistics, probability, and operations research methodology.

Mission. Supports and conducts research, development, and engineering to satisfy the need for new weapon systems and to improve existing systems; issues technical reports.

Point of Contact.
1. General inquiries:
   HQ, US Army Armament Command
   Research Development and Engineering Directorate
   Engineering Support Division
   ATTN: AMSAR-RDS
   Rock Island Arsenal
   Rock Island, IL 61201
2. Reliability/Availability/Maintainability data:
   HQ, US Army Armament Command
   Product Assurance Directorate
   ATTN: AMSAR-QA
   Rock Island Arsenal
   Rock Island, IL 61201

B-6.18 DEFENSE LOGISTICS STUDIES INFORMATION EXCHANGE, US ARMY LOGISTICS MANAGEMENT CENTER

Technical Coverage. Scientific and technical information regarding human factors affecting military operations and materiel.

Mission. Collects and stores documentation pertaining to logistic management. Disseminates information by the publication of an annual bibliography with quarterly supplements of studies relating to logistics, and the publication of an annual catalog of logistic models. Custom bibliographies may be developed upon request.

Point of Contact.
US Army Logistics Management Center
Defense Logistics Studies Information Exchange
Ft. Lee, VA 23801

B-6.19 US ARMY HARRY DIAMOND LABORATORIES (HDL)

Technical Coverage. System research in fuzing, ranging, guidance, and detection; instrumentation, measurement, and simulation; electronic and electrical components; nuclear weapon effects; and basic research in electromagnetic properties of plasma, nonlinear circuits, lasers, and fluidics.

Mission. Provides R&D engineering and consulting services in the physical and engineering sciences to meet Army requirements, and support other DOD elements.

Point of Contact.
Chief, Programs and Plans Office
US Army Harry Diamond Laboratories
Adelphi, MD 20783

B-6.20 PERFORMANCE DATA AND RETRIEVAL SYSTEM FOR NAVAL SURFACE-LAUNCHED MISSILES

Technical Coverage. Reliability, maintainability, and availability data for fire control radars and computers, search radars, guided missile launching systems, weapon direction systems, test equipment, and missiles.

Mission. Collects, processes, and analyzes reliability, maintainability, and performance data using information storage and retrieval systems.

Point of Contact.
Head, Surface-Launched Missile Department
US Naval FMSAEG
Corona, CA 91720

B-6.21 PERFORMANCE DATA AND RETRIEVAL SYSTEM FOR NAVAL AIR-LAUNCHED MISSILES

Technical Coverage. Reliability, maintainability, and availability data for fire control radars and computers, search radars, guided missile launching systems, weapon direction systems, test equipment, and missiles.

Mission. Collects, processes, and analyzes reliability, maintainability, and performance data using information storage and retrieval systems.

Point of Contact.
Head, Air-Launched Missile Department
US Naval FMSAEG
Corona, CA 91720

B-6.22 ADP SYSTEM FOR SUMMARIZATION OF QEEL SURVEILLANCE AND FLEET-FIRING OF VT FUZES

Technical Coverage. Component reliability of VT fuze performance.

Mission. Computer programs identify VT fuzes of specific manufacturers and provide printouts of test results.

Point of Contact.
Code 32300
Q.E.E. Laboratory
US Naval Weapons Station
Concord, CA 94520

B-6.23 ADP SYSTEM FOR SUMMARIZATION OF QEEL SURVEILLANCE OF NAVY GUN AMMUNITION

Technical Coverage. Performance reliability of Naval gun ammunition.

Mission. Data storage and retrieval system provides results of QEE and special tests performed on Navy gun ammunition and components, along with listings and summaries of specific ammunition types and components.

Point of Contact.
Code 32300
Q.E.E. Laboratory
US Naval Weapons Station
Concord, CA 94520

B-6.24 ADP SYSTEM FOR FLEET-FIRED NAVY GUN AMMUNITION

Technical Coverage. Reliability of stockpile ammunition.

Mission. Maintains an information system with an output of listings of ammunition lot performance from test data and statistical summaries.

Point of Contact.
Code 32300
Q.E.E. Laboratory
US Naval Weapons Station
Concord, CA 94520

B-6.25 ADP SYSTEM FOR AIR LAUNCHED MISSILE GUIDANCE AND CONTROL SECTIONS

Technical Coverage. Missile component reliability for SIDEWINDER and SPARROW III.

Mission. Provides an automated data and information storage and retrieval system for the results of G&C component testing of air-launched guided missiles. Assists in engineering and statistical analyses of test results.

Point of Contact.
Code 32300
Q.E.E. Laboratory
US Naval Weapons Station
Concord, CA 94520

B-6.26 ADP SYSTEM FOR NAVY CALIBRATION PROGRAM FOR MEC, POMONA

Technical Coverage. Reliability of test and measuring equipment.

Mission. This data processing system outputs data to optimize calibration intervals, provides reliability information, and thereby serves as a monitoring system toward improving equipment reliability.

Point of Contact.
Naval Weapons Representative
Metrology Engineering Center
Pomona, CA 91766

B-6.27 CHEMICAL PROPULSION INFORMATION AGENCY (CPIA)

Technical Coverage. Research, development, test, and evaluation information on chemical rockets, air breathing propulsion, and gun propulsion.

Mission. Acquires, correlates, analyzes, and disseminates RDT&E data via meetings, briefings, consultations, and publications to management and technical personnel.

Point of Contact.
AIR-330
Naval Air Systems Command
Washington, DC 20360

B-6.28 NAVSECNORDIV DATA BANK

Technical Coverage. Reliability, maintenance, and equipment performance data.

Mission. Receives data-element inputs from Naval activities not included in MDCS, keypunches the data, and forwards to the Naval Ship Research and Development Center for processing and storage in the data bank. Processed data then are analyzed by NAVSECNORDIV personnel in reliability and maintainability improvement programs.

Point of Contact.
Head, Statistical Engineering Branch
NAVSECNORDIV, Code 6643
Norfolk, VA 23511

B-6.29 OPERATIONAL TEST AND EVALUATION FORCE (OPTEVFOR)

Technical Coverage. Operational effectiveness and suitability evaluations of preproduction equipments and/or weapon systems.

Mission. Tests operationally and evaluates specific weapon systems, ships, aircraft, and equipments, including procedures and tactics, when directed by the Chief of Naval Operations.

Point of Contact.
Deputy Chief of Staff for Operations, Plans and Programs
Operational Test and Evaluation Force
US Naval Operating Base
Norfolk, VA 23511

B-6.30 UNDERWATER WEAPON SYSTEMS RELIABILITY DATA (UWSRD)

Technical Coverage. Reliability evaluations of underwater weapon systems.

Mission. Provides the technical data necessary for weapon system analyses, and reliability and effectiveness determinations by engineering and technical personnel.

Point of Contact.
Code RA32
US Naval Underwater Systems Center
Newport, RI 02840

B-6.31 AUTOMATED RELIABILITY AND MAINTAINABILITY MEASUREMENT (ARMMS)

Technical Coverage. Reliability and maintainability characteristics.

Mission. Designed to permit accurate measurement of aircraft characteristics; this data collection and analysis system will input Navy aircraft Maintenance Data Collection System data elements. Output will be used for weapon system evaluations.

Point of Contact.
Commander, Naval Air Test Center
Service Test Division (ST373)
US Naval Air Station
Patuxent River, MD 20760

B-6.32 OFFICE OF INFORMATION SERVICES

Technical Coverage. Nuclear science and related sciences.

Mission. Plans, directs, and operates a comprehensive nuclear technology information program for exchanging, processing, controlling, publishing, and exhibiting nuclear science and technology information to meet the needs of the Energy Research and Development Administration (ERDA), other Government agencies, industry, and the world technical community. Also establishes ERDA standards, policies, and procedures for information reporting and dissemination.

Point of Contact.
Office of Information Services
Energy Research and Development Administration
Washington, DC 20545

B-6.33 AFM 66-1 AIR FORCE MAINTENANCE DATA COLLECTION SYSTEM

Technical Coverage. Maintenance data; maintenance analysis and control; failed-part summaries; and maintenance manpower management in the areas of aircraft, missiles, electronic communications, ground equipment, and munitions.

Mission. Supports management of the maintenance resources at all levels of command, by providing information on required and current maintenance.

Point of Contact.
Director, Data Management Division
Reports Management Branch, MCCDQ
US Air Force Logistics Command
Wright-Patterson Air Force Base, OH 45433

B-6.34 AF/SAJ, OFFICE OF SPECIAL STUDIES

Technical Coverage. Reliability and accuracy; statistical and mathematical techniques. Space systems: testing, test analysis, and design. Weapon systems: evaluation, costs, logistics, and maintenance.

Mission. Issues scientific studies and current state-of-the-art information and provides consultant services for use in making technological, tactical, and strategic decisions.

Point of Contact.
Assistant for Special Studies
Operations Analysis Office
Headquarters, US Air Force
The Pentagon
Washington, DC 20330

B-6.35 METALS AND CERAMICS INFORMATION CENTER (MCIC)

Sponsor. Department of Defense, Office of the Director of Defense, Research and Engineering, under a Defense Supply Agency contract monitored by the Army Materials and Mechanics Research Center, Watertown, Massachusetts.

Technical Coverage:

1. Metals: Titanium, aluminum, and magnesium, beryllium, refractory metals, high-strength steels, superalloys (primarily nickel- and cobalt-base alloys), rhenium, and vanadium.

2. Ceramics: Borides, carbides, carbon/graphite, nitrides, oxides, sulfides, silicides, intermetallics, and selected glasses and glass-ceramics.

Composites of these materials; coatings; environmental effects; mechanical properties; materials applications; test methods; sources, suppliers, and specifications; other materials mutually agreed upon by the contractor and the Government.

Mission. Provides technical assistance and information on materials within the Center's scope, with emphasis on application to the defense community.

Publications. Monthly newsletter (disseminated free by the Center to anyone engaged in materials research, development, or utilization); a series of weekly reviews on developments in metals technology; a monthly review of ceramic technology; a variety of engineering reports and handbooks related to the use of advanced metals and ceramics. The reviews, reports, and handbooks are available at cost from the National Technical Information Service.

Services. Answers to technical inquiries, bibliographies, literature searches, and special studies are provided on a fee basis, depending on the time involved.

Point of Contact:

Metals and Ceramics Information Center
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201
Phone: (614) 299-3151

B-7 DISCONTINUED OR TRANSFERRED ACTIVITIES

1. NASA, PRINCE/APIC Information Center
   No longer exists as an active information center.
2. RATR, Reliability Abstracts and Technical Reviews
   Discontinued. Old copies are available from NTIS, Springfield, VA 22151.
3. IDEP, Interagency Data Exchange Program
   Integrated into GIDEP (See par. B-6.1.)
4. FARADA, Tri-Service and NASA Failure Rate Data Program
   Integrated into GIDEP (See par. B-6.1.)
5. AFREIC, Air Force Radiation Effects Information Center
6. AFEPIC, Air Force Electronic Properties Information Center
7. AFDMIC, Air Force Defense Metals Information Center
8. AFMPDC, Air Force Mechanical Properties Data Center (See par. B-6.10, Monitored by Nondestructive Testing Industrial Applications Branch, US Army Materials and Mechanics Research Center, Watertown, MA 02172.)
9. TAERS, The Army Equipment Record System
   Replaced by TAMMS. (See par. B-4.2.)

REFERENCES

1. *GIDEP Policies and Procedures Manual.* GIDEP Administration Office, Corona, California.
2. *GIDEP Representatives Handbook.* GIDEP Administration Office, Corona, California.
3. E. T. Richards, "Technology Transfer through GIDEP", *Proc. of 1974 Annual Reliability and Maintainability Symposium*, 266-273 (1974).
4. *Reliability and Maintainability Data Sources*, AFLC/AFSC Pamphlet 400-? (to be published in 1974). Check with HQ, Air Force Logistics Command, Wright-Patterson AFB, Ohio 45433 or HQ, Air Force Systems Command, Andrews AFB, Washington, DC 20331.
5. TM 38-750, *The Army Management Maintenance System (TAMMS)*, November 1972.

APPENDIX C
ANNOTATED BIBLIOGRAPHY ON HUMAN FACTORS
(from NTIS Government Reports Announcements)

AD-875 669
Army Test and Evaluation Command, Aberdeen Proving Ground, Md.
HUMAN FACTORS ENGINEERING.
Final rept. on materiel test procedure.

17 Jul 70, 26p MTP-8-3-509
Distribution Limitation now Removed.

Descriptors: (*Human engineering, Test methods), Chemical warfare, Biological warfare, Human engineering, Training, Operation, Maintenance, Military personnel.
Identifiers: Common service test procedures.

The Army Service Test Procedure describes test methods and techniques for evaluating the Human Factors Engineering aspects of chemical-biological equipment and its compatibility with the skills, aptitudes, and limitations of military personnel who will use the items. (Author)

N71-12334
National Aeronautics and Space Administration. Langley Research Center, Langley Station, Va.
FIXED-BASE VISUAL-SIMULATION STUDY OF MANUALLY CONTROLLED OPERATION OF A LUNAR FLYING VEHICLE.
G. K. Miller, Jr., and G. W. Sparrow. Dec 70, 42p
NASA-TN-D-5980, L-7320
Contract 127-71-34-03

Descriptors: *Control equipment, *Control simulation, *Lunar flying vehicles, *Manual control, Man-machine systems, Operations research, Pilot performance, Visual flight.

For abstract, see STAR 09 03.

PB-197 127
BISRA-The Corporate Labs. of the British Steel Corp., London (England). Operational Research Dept.
BISRA OPEN REPORT. SELECTION OF ABSTRACTS FROM ERGONOMICS ABSTRACTS, VOLUME 2 NO. 2.
1970, 14p BISRA-OR/HF/35/70
See also Volume 1, No. 3, PB-194 443.

Descriptors: (*Man-machine systems, Abstracts), (*Human factors engineering, *Abstracts), Psychology, Physiology, Anthropometry, Environmental engineering, Workplace layout, Clothing, Design, Great Britain.
Identifiers: *Ergonomics.

Contents: Man as a systems component—psychology, physiology, anthropometry, and biomechanics: The design of the man-machine interface—data presentation, input facilities, workplace and equipment design, environmental design, noise, vibration, atmosphere, thermal conditions, specialized and protective clothing; Systems design and organization—work organization, training, motivation, and attitudes; Methods, techniques and equipment in ergonomics—investigation of man as a systems component—physiology, anthropometry, and biomechanics; Methods, techniques, and equipment in ergonomics—investigation of the design of the man-machine interface—environmental design; Methods, techniques, and equipment in ergonomics—investigation of systems design and organization—work design and organization, implementation, and evaluation of industrial training procedures, and implementation of selection procedures.

AD-718 731
Army Test and Evaluation Command, Aberdeen Proving Ground, Md.
HUMAN FACTORS ENGINEERING
Materiel test procedure.

20 Dec 67, 5p Rept No. MTP-4-3-515

Descriptors: (*Test methods, *Human engineering), (*Ammunition, Human engineering), Compatibility, Handling, Safety, Assembling.
Identifiers: *Common service test procedures.

The objective of the Materiel Test Procedure is to evaluate, during testing involving ammunition, whether or not human factors considerations were engineered into the design of ammunition to assure maximum compatibility in the ammunition-weapon-crew relationship. (Author)

PRECEDING PAGE BLANK-NOT FILMED

AD-732 613
Illinois Univ. Savoy Aviation Research Lab.
EFFECTS OF THE MAN ON THE TASK IN COMPLEX MAN-MACHINE SYSTEMS,
Charles L. Hulin, and Kenneth M. Alvares.
Feb 71, 14p AFHRL-TR-71-7
Contract F41609-70-C-0027
See also related reports AD-731 191 and AD-732 612.

Descriptors: (*Man-machine systems, *Job analysis), Training, Factor analysis, Design, Effectiveness.
Identifiers: Pilot training.

This research tested the hypothesis that in a complex man-machine system, one of the many influences on the system is the man's constant reorganization of the tasks which constitute the system. The performances of 67 male college students receiving basic flight training were assessed by means of check rides at three different points of training. Factor analyses of each set of check ride data indicated systematic changes occurred in the structure of the task. A three-factor solution appeared in the 10-hour data, two factors were being assessed by the 25-hour point, and only one general factor appeared in the 35-hour data. This finding indicates that future man-machine systems research should no longer be designed under a fixed-task assumption. It is speculated that this assumption may be one cause of the generally found weak prediction of system performance effectiveness over meaningful intervals of time (Author)

AD-721 657
Dunlap and Associates Inc., Darien, Conn.
HUMFACTS SYSTEM THESAURUS.

Jan 71, 419p*
Contract DAHC04-69-C-0076

Descriptors: (*Dictionaries, *Human engineering), Information retrieval, Vocabulary, Subject indexing.

Identifiers: *Thesauri, HUMFACTS System Thesaurus.

The thesaurus contains words and phrases, concept-terms, which reflect the concepts to be indexed in support of the Human Factors, Engineering Information Retrieval (HUMFACTS) System. The concept-terms indicate structures which display the relationship between terms to at least two levels of detail in meaning. This developmental thesaurus is intended to serve as the authority list for subsequent indexing and retrieval processing but is not considered final. (Author)

AD-730 910
Bunker-Ramo Corp., Westlake Village, Calif.
DEVELOPMENT OF A HUMAN PERFORMANCE RELIABILITY DATA SYSTEM.
Technical rept.,
David Meister, and Robert G. Mills. Jun 71, 19p AMRL-TR-71-74

Contract F33615-70-C-1518
Presented at the Reliability and Maintainability Conference (10th), held on 28-30 Jun 71.

Descriptors: (*Performance (Human), *Reliability), (*Behavior, Classification), Man-machine systems, Data, Human engineering, Feasibility studies.
Identifiers: Taxonomy.

A study was performed to determine the requirements for and the elements of a human performance reliability (HPR) data system. The heart of the HPR system is a taxonomic structure for classifying behavioral studies. 140 studies from a variety of sources were coded using this taxonomy. To test the efficiency of this data bank to provide answers to system development questions, a number of tests were performed to determine the relevance of the data retrieved to the questions asked. The results of these tests indicated that it is possible to expand the HPR data base provided one is not restricted to a probabilistic metric. (Author)

AD-730 923
Michigan Univ., Ann Arbor Human Performance Center
SHORT-TERM MEMORY FOR QUANTITATIVE INFORMATION FROM THREE KINDS OF VISUAL DISPLAYS.
Technical rept.,
Vicki Vivienne Rhona Cohen. Jun 71, 89p
Rept Nos. 08772-82-T, TR-26 AFOSR-TR-71-2588
Contract AF 49(638)-1736, ARPA Order-461

Descriptors: (*Memory, Display systems), Human engineering, Recall, Motion.
Identifiers: Short term memory.

A series of four experiments was conducted to investigate whether the nature of a visual display affects short-term memory for numeric information extracted from it. Three different kinds of displays were chosen for study: a digital counter, a moving scale, and a moving pointer display. Experiment I examined reading performance using the moving scale and moving pointer displays. The results of this experiment, in which the moving scale yielded superior performance, provided baseline data with which to judge future performance and also enabled a judicious choice of exposure durations for the subsequent experiments. In Experiment II the Brown-Peterson paradigm with varied retention intervals was used to examine the short-term memory for quantitative information from the three kinds of displays. In general, the digital counter yielded the best recall performance, followed by the moving pointer and moving scale displays in that order. Experiments III and IV were between- and within-in subjects designs which tested this hypothesis using the Brown-Peterson paradigm with two different interpolated tasks, one of which interfered with the retention of verbal information and the other which interfered with the retention of both verbal and nonverbal information. The differences in error patterns obtained in Experiment II between the moving pointer and moving scale displays were again obtained when the interpolated activity was considered to be causing only verbal interference. However, this difference was abolished or considerably lessened when the interpolated activity was one that interfered with both verbal and nonverbal memory. (Author)

AD-729 855
Army Test and Evaluation Command, Aberdeen Proving Ground, Md.
HUMAN FACTORS ENGINEERING
Final rept. on materiel test procedure.
1 Sep 71, 22p Rept. No. MTP-10-2-505
Supersedes Rept. No. MTP-10-2-505 dated 19 Jul 67, AD-725 555.

Descriptors: (*Army equipment, Human engineering), (*Human engineering, Test methods), Measurement, Standards, Accuracy, Errors, Performance (Engineering), Performance (Human), Safety.
Identifiers: *Common engineering test procedures.

The document outlines procedures for evaluating the human factors associated with use of general equipment. (Author)

AD-729 964
Texas Tech Univ., Lubbock Center of Biotechnology and Human Performance.
PERFORMANCE, RECOVERY AND MAN-MACHINE EFFECTIVENESS.
Semi-annual progress Rept. 1 Mar—31 Aug 71, Richard A. Dudek. 15 Sep 71, 26p
Contract DAAD05-69-C-0102
See also Seminannual progress rept. dated 15 Mar 71, AD-723 430.

Descriptors: (*Man-machine systems, Effectiveness), (*Performance (Human), Environment), Stress (Psychology), Stress (Physiology), Behavior, Attention, Motivation, Nutrition, Vibration, Climatology, Exercise, Rhythm (Biology), Fatigue (Physiology), Group dynamics, Military personnel.

The goals of the research are the determination of optimal or near optimal work/rest schedules for individuals and crews to yield high performance with minimal decrement over time followed by recovery (after rest) to an acceptable high performance. The experimentation is further aimed at consideration of various task levels and differing conditions of environment. Experimentation in progress continues to focus attention on the assessment of human performance under continuous operations or relatively long term activity (2 hours or more of activity). Effects of circadian rhythms on performance will also be studied in connection with this project.

AD-725 555
Army Test and Evaluation Command, Aberdeen Proving Ground, Md.
HUMAN FACTORS EVALUATION
Materiel test procedure.

19 Jul 67, 8p Rept. No. MTP-10-2-505

Descriptors: *Army equipment, Human engineering), (*Human engineering, Test methods), Test facilities, Questionnaires, Technicians, Personnel management.
Identifiers: *Common engineering test procedures.

The objective of the materiel test procedure is to provide general testing procedures to be used in conducting the human factors portion of engineering tests of general supplies and equipment, and to evaluate the human factors requirements of the test items as set forth in QMR's, SDR's, technical characteristics, and as indicated by the particular design. These procedures are to be used along with other engineering test procedures to determine the technical and maintenance suitability of the test items for service tests. (Author)

AD-719 108
Army Test and Evaluation Command, Aberdeen Proving Ground, Md.
HUMAN FACTORS.
Final rept. on materiel test procedure.
11 Dec 70, 22p Rept no. MTP-7-3-510

Descriptors: (*Human engineering, Test methods), Test equipment, Noise, Visibility, Environment, Military facilities, Control systems, Display systems, Installation, Reliability, Maintenance, Safety, Data processing systems.
Identifiers: Evaluation, *Common engineering test procedures, *Avionics.

Human factor considerations applicable to aviation armament and avionics are described. (Author)

AD-727 658
Human Resources Research Organization, Alexandria, Va.
MAN IN CONTROL OF HIGHLY AUTOMATED SYSTEMS
Harry L. Ammerman, and William H. Melching.
May 71, 14p *Rept No. HUMRRO professional paper 7-71
Contract DAHC19-70-C-0012
Presented at the Annual Army Human Factors Research and Development Conference (16th). Fort Bliss, Texas Oct 70.

Descriptors: (*Performance (Human), Command + control systems), (*Automation, *Man-machine systems), Control panels, Decisionmaking, Reliability, Human engineering, Factor analysis.
Identifiers: *Highly automated systems.

The identification of what man should do as a decisionmaker and controller in the newly evolving man-machine systems is considered. Among the topics discussed are man's underlying basic functions in a complex system, task activities for individual jobs and their analyses, and training and the design of operational job positions. (Author)

AD-728 099
Human Resources Research Organization, Alexandria, Va.
SURVEY OF FACTORS INFLUENCING ARMY LOW LEVEL NAVIGATION.
Technical rept.,
Robert H. Wright, and Warren P. Pauley, Jun 71, 125p Rept No. H
Contract DAHC19-70-C-0012

Descriptors: (*Navigation, Low altitude), (*Human engineering, Navigation), Display systems, Navigation computers, Army training, Human engineering. Performance (Human), Mission profiles, Terrain, Climatology.
Identifiers: Low level navigation.

Factors that influence low level navigation and affect Army capability in conducting low level missions were surveyed. The nature of improvements in equipment, procedures, and training needed to provide the Army with effective operational capability in low level navigation were indicated. Major conclusions from the survey include limited capability in low level aerial navigation as affecting future Army combat effectiveness; the rapid reaction mission over unfamiliar terrain in low level navigation; potential improvements in training or procedures for present navigation system and equipment; a simple automatic dead reckoning navigation computer in routine attainment of operationally effective low level navigation performance; and reorienting navigation procedures and training to simplified line of position navigation techniques. (Author)

AD-717 257
Human Resources Research Organization, Alexandria, Va.
COLLECTED PAPERS PREPARED UNDER WORK UNIT REPAIR, TRAINING OF ELECTRONICS MAINTENANCE PERSONNEL.

Nov 70, 41p Rept No. HUMRRO professional paper-27-70
Contract DAHC19-70-C-0012

Descriptors: (*Maintenance personnel, *Army training), (*Radio receivers, Maintenance), Teaching methods, Radio communication systems, Sequences, Malfunctions, Circuits, Theory.
Identifiers: *Field radio repair courses, Troubleshooting, REPAIR work unit.

Papers in the collection report research in procedures in troubleshooting and repair of Army field radios that resulted in the construction of evaluations of the men and in experimental training courses. The papers are: The implementation of functional context training in a radio repairman course; A follow-up study of experimentally trained and conventionally trained field radio repairmen; REPAIR III: The development and evaluation of the experimental field radio repairman course; REPAIR IV: Comparison of experimental and standard course graduates after field experience. (Author)

AD-717 258
Human Resources Research Organization, Alexandria, Va.
AN APPROACH TO STANDARDIZING HUMAN PERFORMANCE ASSESSMENT.
John D. Engel. Oct 70, 14p *Rept No. HUMRRO-professional paper-26-70
Contract DAHC19-70-C-0012
Presented at the Planning Conference of 'Standardization of Tasks and Measures for Human Factors Research', held at Texas Technological Univ., Lubbock, Tex., Mar 70.

Descriptors: (*Performance (Human), Measurement), (*Test construction (Psychology), Standardization), (*Performance tests, Standardization), Test methods, Visual acuity, Auditory acuity, Decisionmaking, Symbols, Documentation.
Identifiers: Evaluation, Task analysis, Taxonomy, Manipulation.

The standardization and evaluation of methods of performance assessment represents an important area of concern. In this paper an approach that concentrates on two critical areas and the relationship between them is discussed. These are: (a) a task classification system, and (b) a performance measure classification system. An example is presented that illustrates some preliminary research related to the use of a performance measure classification system. The paper concludes by suggesting areas and directions for future research efforts. (Author)

AD-720 354
Applied Psychological Services Inc., Wayne, Pa. Science Center
DIGITAL SIMULATION OF THE PERFORMANCE OF INTERMEDIATE SIZE CREWS: APPLICATION AND VALIDATION OF A MODEL FOR CREW SIMULATION.
Technical rept.,
Arthur I. Siegel, J. Jay Wolf and Joseph Cosentino. Feb 71, 157 *Rept No. APS-7071-5
Contract N00014-68-C-0262

Descriptors: (*Naval personnel, Performance (Human)), (*Man-machine systems, Mathematical models), Organizations, Curve fitting, Mathematical prediction, Programming (Computers), Digital computers, Simulation, Military psychology, Mission profiles, Correlation techniques, Data processing systems, Vietnam.
Identifiers: Computerized simulation, Evaluation

Based on current psychological theory, military doctrine, and previously developed and tested functional relationships, selected psychosocial, personnel, and performance variables are woven into a stochastic mathematical model for digitally simulating closed man-machine systems operated by crews of from 4 to 20 members. This probabilistic model is presented in terms of a detailed logic and processing flow sequence. An operational mission (Vietnam river patrol) selected for the evaluation of the model is then described and

quantified as required for input to the model. The results of a series of evaluative simulation runs, in which the computer simulation model is applied to the mission, are reported. These results are compared with independent criterion data for the same mission. (Author)

AD-720 976
Army Test and Evaluation Command, Aberdeen Proving Ground, Md.
HUMAN FACTORS ENGINEERING.
Materiel test procedure.

27 Aug 69, 70p Rept No. MTP-6-2-502

Descriptors: (*Human engineering, Test methods), (*Man-machine systems, Human engineering), Display systems, Control panels, Warning systems, Auditory perception.
Identifiers: Common engineering test procedures, Auditory warning devices, Visual displays.

The objective of the Materiel Test Procedure is to provide methods of determining the appropriateness and effectiveness of human factors aspects at man-machine interfaces. (Author)

AD-726 306
Aerospace Medical Research Lab, Wright-Paterson AFB, Ohio
HUMAN FACTORS AND SYSTEMS EFFECTIVENESS.
Donald A. Topmiller. 1966, 11p Rept No. AMRL-TR-66-257
Presented at the Reliability and Maintainability Conference (5th) held on 18-20 Jul 66.
Availability: Pub. in Annals of Reliability and Maintainability, v5 p123-132, 1966.

Descriptors: (*Performance (Human), Effectiveness), (*Human engineering, Maintenance), Systems engineering, Reliability, Maintainability, Mathematical prediction, Statistical analysis, Errors, Time.

The paper treats human factors in systems effectiveness as a basic problem relating human performance to the major Systems effectiveness parameters of operability, reliability, and maintainability. The latter two parameters are topologically related to the primary dependent human performance variables used in laboratory research of errors and time respectively. The need is outlined to not only topologically relate these variables but to also develop a framework within which human engineering design can be quantitatively assessed. Two studies were reviewed in which human performance (time) was predicted from design evaluations and analysis of equipment. (Author)

AD-877 006
Naval Missile Center, Point Mugu, Calif.
DYNAMIC TARGET IDENTIFICATION ON TELEVISION AS A FUNCTION OF DISPLAY SIZE, VIEWING DISTANCE, AND TARGET MOTION RATE.
Technical publications,
R. A. Bruns, R. J. Wherry, Jr., and A. C. Bittner, Jr., 17 Nov 70, 64p NMC-TP-70-60
Distribution Limitation now Removed.

Descriptors: (*Closed circuit television, Design), (*Target acquisition, Closed circuit television), (*Naval aircraft, Closed circuit television), Human engineering, Accuracy, Television display systems, Ranges (Distance), Motion, Electrooptics, Air-to-surface, Simulation, Tactical warfare.
Identifiers: *Reconnaissance transparency projection systems, *Airborne television systems.

The report describes the results of a research study whose goal was the evaluation of the effects of (1) television display size, (2) display degradation, (3) observer viewing distance, and (4) target motion rate on target identification performance. Appendixes to the report describe (1) a reconnaissance transparency projection system used to simulate the televisual air-to-surface tactical target attacks used as test materiel in this study and (2) a rating procedure used to compare target briefing photographs in terms of qualities important for target identification. The target ratings are then used to predict target identification performance in the simulated target attacks. (Author)

JPRS-53244
Joint Publications Research Service, Washington, D.C.
INFORMATION CHARACTERISTICS OF DISPLAY SYSTEMS AND THEIR RELATIONSHIP TO PSYCHOPHYSIOLOGICAL

INDICATORS OF OPERATOR ACTIVITY
Yu. A. Ivashkin. 28 May 71, 13p
Trans. of Pribory i Sistemy Upravleniya (USSR)-4, p22-25, 1969.

Descriptors: (*Display devices, Information systems), Computer storage devices, Mathematical models, Information theory, Information capacity, Senses, Visual perception.

N71-23210
Advisory Group for Aerospace Research and Development, Paris (France).
FREQUENCY RESPONSE FUNCTIONS AND HUMAN PILOT MODELLING.
Mar 71, 65p AGARD-R-580-71
Lang—Mostly in English, Partly in French

Descriptors: *Aircraft structures, *Dynamic response, *Dynamic structural analysis, *Human factors engineering, *Mathematical models, *Pilot performance, *Transfer functions, Frequency response, Functional analysis, Gusts, Modal response.
Identifiers: NASA subject code 01.

For abstract, see STAR 0912.

AD-727 365
Aerospace Medical Research Lab, Wright-Paterson AFB, Ohio.
HUMAN FACTORS ENGINEERING CONSIDERATIONS IN SYSTEM DEVELOPMENT
Julien M. Christensen. 1969, 33p Rept No. AMRL-TR-69-82
Availability: Pub. in Proceedings of the DRG Seminar on Design of Equipment for Effective Utilization (5th), 21-23 Sep 69, p113-144.

Descriptors: (*Human engineering, *Systems engineering), Design.

The purpose of the paper is fourfold. First, the life cycle in the design and development of a typical system is described. Second, the nature of human factors engineering requirements is described. Third, these requirements are related to the systems development cycle and, finally, a brief evaluation will be made of the tools and information available to the human factors engineer. (Author)

N71-25943
Man Factors, Inc., San Diego, Calif.
DATABOOK FOR HUMAN FACTORS ENGINEERS. VOLUME 2 - COMMON FORMULAS, METRICS, DEFINITIONS.
C. Kubokawa, P. Selby, and W. Woodson, Nov 69, 371p NASA-CR-114272
Contract NAS2-5298

Descriptors: *Conversion tables, *Formulas (mathematics), *Human factors engineering, *Nomenclatures, Manuals, Nomographs, Symbols, Units of measurement.

For abstract, see STAR 09 14.

N71-25944
Man Factors, Inc., San Diego, Calif.
DATABOOK FOR HUMAN FACTORS ENGINEERS. VOLUME 1 - HUMAN ENGINEERING DATA.
C. Kubokawa, P. Selby, and W. Woodson, Nov 69, 260p NASA-CR-114271
Contract NAS2-5298

Descriptors: *Anthropometry, *Environmental index, *Human behavior, *Human factors engineering, *Physiological factors, Equipment specifications, Graphs (charts), Manuals, Tables (data).
For abstract, see STAR 09 14.

N71-26160
Bolt, Beranek, and Newman, Inc., Cambridge, Mass.
STUDIES OF MULTIVARIABLE MANUAL CONTROL SYSTEMS - A MODEL FOR TASK INTERFERENCE.
J. I. Elkind, W. H. Levison, and J. L. Ward. May 71, 229p NASA-CR-1746
Contract NAS2-3080
Coll- 229P Refs

Descriptors: *Manual control, *Mathematical models, *Pilot performance, *Task complexity, Display devices, Man-machine systems, Performance prediction, Tracking (position).
For abstract, see STAR 09 14.

AD-727 254
McDonnell Douglas Corp., Long Beach, Calif., Douglas Aircraft Div.

WHAT'S WRONG WITH HUMAN FACTORS IN SYSTEMS DEVELOPMENT AND HOW CAN THIS BE CORRECTED

Arthur S. Romero. 1 Sep 68, 3p Rept No. Douglas Paper 5208

Descriptors: (*Human engineering, Man-machine systems), Systems engineering, Problem solving, Philosophy, Documentation, Factor analysis, Effectiveness.

Problems of design, development and maintenance of sophisticated systems have brought forth a specialized approach to information about man known as human factors. Observation of design and development of systems and subsystems from the conceptual phase to mockup review reveals some of the underlying causes for the failure to incorporate human factors into the design. These causes and some recommendations for eliminating them from future design are discussed. (Author)

INDEX

A

Active element groups (AEG), 5-8
Allocation
  See: Reliability allocation
  See: Man/machine allocation
Availability, 1-5, 1-13

B

Block diagram
  See: Reliability diagram

C

Capability, 1-5
Cause-consequence charts, 6-3, 7-1
  construction, 7-6
Chebyshev limit, 9-12, 10-13
Checklists, A-1
  For following systems:
    communication, A-7
    crew station, A-9
    electrical/electronic A-3
    fire protection, A-8
    fuel/propellant, A-1
    guidance/navigation, A-6
    hydraulic, A-2
    ordnance/explosive, A-11
    pressure/pneumatic, A-3
    propulsion, A-1
    protection, A-7
    vehicle control, A-5
Correctability, 6-7
Corrective action, 8-1, 11-4
Correlation (linear), 10-6
Criticality, 8-1
Cumulative damage models, 9-12
Cumulative polygon, 10-5
Cut sets
  See: Minimal cut sets

D

Data bank
  See: Data source
Data
  package, 11-6
  sources, B-1
    Army systems, B-5
    discontinued, B-15
    GIDEP, B-1
    others, B-7
    RAC, B-4
Definitions
  availability, 1-5, 1-13
  capability, 1-5
  correctability, 6-7
  dependability, 1-5
  human performance reliability, 6-6
  maintainability, 1-9
  reliability, 1-1, 3-1
  system, 1-2
  system effectiveness, 1-4
  system engineering, 1-2
  THERP, 6-9
Dependability, 1-5
Design, 6-1
  checklists, *See*: Checklists
  review, 1-12, 11-1
  review team, 11-2
Drift failure, 10-4, 10-8, 10-13

E

ECAP, 10-17
Environmental, 2-1
  combinations, 2-3
  designing for, 2-8
  effects of, 2-3, 2-4
  prediction, 2-1
Ergonomics
  See: Human factors
Explosion, 2-18
Exponential distribution, 3-3, 3-4, 4-11

F

Failure
  distributions, 3-2
  mode, 9-1
  modes and effects analysis, 8-1
  rate, 3-3
  time, 3-5
  time between failures, 3-5
Fault trees
  See: Cause-consequence charts
FMEA, 8-1, 7-1
FMECA, 8-1

Fraction defective, 3-6
Frequency histogram, 10-5

G

Gaussian distribution
  See: s-Normal distribution
GIDEP, B-1, B-7

H

Hazard
  analysis, 1-14
  rate: *See*: Failure rate
Human
  engineering, 6-2
  factors, 6-1, 11-4, B-6, C-1
  performance, 6-3
  THERP, 6-9

I

Interference (stress-strength)
  See: Stress-strength models

K

Knowledge organization charts
  See: Cause-consequence charts
  See: FMEA

L

Linear cumulative damage, 9-12
Load factors, 9-5
Lognormal distribution, 3-3, 3-4

M

Maintainability, 1-1, 1-9
Maintenance
  See: Repair
Man/machine
  allocation, 6-5
  interactions, 6-3
  See also: Human factors
Margin of safety
  See: Safety margin
Mechanical failure, 9-5
Minimal cut sets, 7-3, 7-7
Models
  analytic
    analysis, 4-9
    building, 4-2
    simulation, 4-10
  failure, 9-1
    cumulative damage, 9-12
    stress-strength, 9-2, 9-6
Moisture, 2-17
Monte Carlo, 4-9, 7-15, 10-15

N

NASAP, 10-17
Node-potential model, 10-8
s-Normal distribution, 3-3, 3-4

O

One-shot device, 3-6
Optimization, 1-5, 1-6, 1-7, 5-13

P

Parameter variation analysis, 10-1
  computer programs, 10-17
  moments, 10-9
  Monte Carlo, 10-15
  worst-case, 10-8
Performance characteristic, 10-17
Primary event, 7-2
Product review
  See: Design review
Production, 6-1
  review, *See*: Design review
Pseudo-random numbers
  See: Random numbers

R

RAC (Reliability Analysis Center), B-4, B-7
RAM, 1-10, 1-11
  See also: Reliability, availability, maintainability

Random numbers, 4-10
Redundancy, 1-8, 4-3
REG (Reasonable Engineering Guess), 9-11, 10-13
Reliability
  allocation, 5-1
    systems with repair, 5-23
    systems without repair, 5-2
      nonredundant, 5-2, 5-3, 5-8, 5-9
      redundant, 5-13, 5-20
  block diagrams: *See*: Reliability diagram
  diagram, 4-2, 8-2
  measures, 3-1
Repair, 1-8, 1-9

S

Safety, 1-1, 1-13
  factors, 9-5
  margin, 9-5, 9-11
Sand and dust, 2-17
Sensitivities, 10-14
Shock and vibration, 2-15
Simulation, 7-15
Stimulus, 6-4
Stress-strength models, 9-2, 9-6
  deterministic, 9-2
  probabilistic, 9-6
System
  definition, 7-6
  effectiveness, 1-4, 6-2
  engineering, 1-2
  management, 1-2, 1-3, 6-2

T

Tails (of a distribution), 10-4
TAMMS, B-5, B-8
Task equipment analysis (TEA), 6-6, 6-8
Temperature, 2-14
Tensile strength, 9-2
THERP, 6-9
Top event, 7-2, 7-6
Trade-off, 1-1, 1-15, 1-16, 6-6, 6-8

V

Variability analysis
  See: Parameter variation analysis

W

Weibull distribution, 3-3, 3-4
Worst case analysis, 10-8

(AMCRD-TV)

AMCP 706-196

FOR THE COMMANDER:

ROBERT L. KIRWAN
Brigadier General, USA
Chief of Staff

OFFICIAL:

G. J. HAROLD
LTC, GS
Adjutant General

DISTRIBUTION:
Special

☆U.S. GOVERNMENT PRINTING OFFICE: 1976—603-770 / 308

ENGINEERING DESIGN HANDBOOKS

Available to DA activities from Letterkenny Army Depot, ATTN: AMXLE-ATD, Chambersburg, PA 17201. All other requestors--DOD, Navy, Air Force, Marine Corps, nonmilitary Government agencies, contractors, private industry, individuals, universities, and others--must purchase Handbooks from National Technical Information Service, Department of Commerce, Springfield, VA 22121. See Preface for further details and AMC policy regarding requisitioning of classified documents.

No. AMCP 706-	Title
100	Design Guidance for Producibility
104	Value Engineering
106	Elements of Armament Engineering, Part One, Sources of Energy
107	Elements of Armament Engineering, Part Two, Ballistics
108	Elements of Armament Engineering, Part Three, Weapon Systems and Components
109	Tables of the Cumulative Binomial Probabilities
110	Experimental Statistics, Section 1, Basic Concepts and Analysis of Measurement Data
111	Experimental Statistics, Section 2, Analysis of Enumerative and Classificatory Data
112	Experimental Statistics, Section 3, Planning and Analysis of Comparative Experiments
113	Experimental Statistics, Section 4, Special Topics
114	Experimental Statistics, Section 5, Tables
115	Environmental Series, Part One, Basic Environmental Concepts
116	Environmental Series, Part Two, Natural Environmental Factors
117	Environmental Series, Part Three, Induced Environmental Factors
118	Environmental Series, Part Four, Life Cycle Environments
119	Environmental Series, Part Five, Glossary of Environmental Terms
120	Criteria for Environmental Control of Mobile Systems
121	Packaging and Pack Engineering
123	Hydraulic Fluids
124	Reliable Military Electronics
125	Electrical Wire and Cable
127	Infrared Military Systems, Part One
128(S)	Infrared Military Systems, Part Two (U)
130	Design for Air Transport and Airdrop of Materiel
132	Maintenance Engineering Techniques (MET)
133	Maintainability Engineering Theory and Practice (METAP)
134	Maintainability Guide for Design
135	+Inventions, Patents, and Related Matters
136	**Servomechanisms, Section 1, Theory
137	**Servomechanisms, Section 2, Measurement and Signal Converters
138	**Servomechanisms, Section 3, Amplification
139	**Servomechanisms, Section 4, Power Elements and System Design
140	Trajectories, Differential Effects, and Data for Projectiles
150	Interior Ballistics of Guns
152	Fundamentals of Ballistic Impact Dynamics, Part One
159(S)	Fundamentals of Ballistic Impact Dynamics, Part Two (U)
160(C)	Elements of Terminal Ballistics, Part One, Kill Mechanisms and Vulnerability (U)
161(C)	Elements of Terminal Ballistics, Part Two, Collection and Analysis of Data Concerning Targets (U)
162(SRD)	Elements of Terminal Ballistics, Part Three, Application to Missile and Space Targets (U)
163(S)	*Basic Target Vulnerability (U)
165	Liquid-Filled Projectile Design
170(S)	Armor and Its Applications (U)
175	Solid Propellants, Part One
176	+Solid Propellants, Part Two
177	Properties of Explosives of Military Interest
178	+Properties of Explosives of Military Interest, Section 2 (Replaced by -177)
179	Explosive Trains
180	Principles of Explosive Behavior
181	Explosions in Air, Part One
182(SRD)	Explosions in Air, Part Two (U)
185	Military Pyrotechnics, Part One, Theory and Application
186	Military Pyrotechnics, Part Two, Safety, Procedures and Glossary
187	Military Pyrotechnics, Part Three, Properties of Materials Used in Pyrotechnic Compositions
188	Military Pyrotechnics, Part Four, Design of Ammunition for Pyrotechnic Effects
189	Military Pyrotechnics, Part Five, Bibliography
190	*Army Weapon System Analysis
191	System Analysis and Cost-Effectiveness
192	Computer Aided Design of Mechanical Systems, Part One
193	Computer Aided Design of Mechanical Systems, Part Two
195	*Development Guide for Reliability, Part One, Introduction, Background, and Planning for Army Materiel Requirements
196	Development Guide for Reliability, Part Two, Design for Reliability
197	Development Guide for Reliability, Part Three, Reliability Prediction
198	Development Guide for Reliability, Part Four, Reliability Measurement
199	*Development Guide for Reliability, Part Five, Contracting for Reliability
200	Development Guide for Reliability, Part Six, Mathematical Appendix and Glossary
201	Helicopter Engineering, Part One, Preliminary Design
202	*Helicopter Engineering, Part Two, Detail Design
203	Helicopter Engineering, Part Three, Qualification Assurance
204	Helicopter Performance Testing

No. AMCP 706-	Title
205	Timing Systems and Components
210	Fuzes
211(C)	Fuzes, Proximity, Electrical, Part One (U)
212(S)	Fuzes, Proximity, Electrical, Part Two (U)
213(S)	Fuzes, Proximity, Electrical, Part Three (U)
214(S)	Fuzes, Proximity, Electrical, Part Four (U)
215(C)	Fuzes, Proximity, Electrical, Part Five (U)
235	Hardening Weapon Systems Against RF Energy
237	*Mortar Weapon Systems
238	*Recoilless Rifle Weapon Systems
239	*Small Arms Weapon Systems
240(C)	Grenades (U)
242	Design for Control of Projectile Flight Characteristics (Replaces -246)
244	Ammunition, Section 1, Artillery Ammunition--General, with Table of Contents, Glossary, and Index for Series
245(C)	Ammunition, Section 2, Design for Terminal Effects (U)
246	+Ammunition, Section 3, Design for Control of Flight Characteristics (Replaced by -242)
247	Ammunition, Section 4, Design for Projection
248	+Ammunition, Section 5, Inspection Aspects of Artillery Ammunition Design
249	Ammunition, Section 6, Manufacture of Metallic Components of Artillery Ammunition
250	Guns--General
251	Muzzle Devices
252	**Gun Tubes
253	*Breech Mechanism Design
255	Spectral Characteristics of Muzzle Flash
260	Automatic Weapons
270	Propellant Actuated Devices
280	Design of Aerodynamically Stabilized Free Rockets
281(SRD)	Weapon System Effectiveness (U)
282	+Propulsion and Propellants (Replaced by -285)
284	Structures
290(C)	Warheads--General (U)
291	+Surface-to-Air Missiles, Part One, System Integration
292	+Surface-to-Air Missiles, Part Two, Weapon Control
293	+Surface-to-Air Missiles, Part Three, Computers
294(C)	+Surface-to-Air Missiles, Part Four, Missile Armament (U)
295(C)	+Surface-to-Air Missiles, Part Five, Countermeasures (U)
296	+Surface-to-Air Missiles, Part Six, Structures and Power Sources
297(C)	+Surface-to-Air Missiles, Part Seven, Sample Problem (U)
300	Fabric Design
312	Rotational Molding of Plastic Powders
313	Short Fiber Plastic Base Composites
327	Fire Control Systems--General
329	Fire Control Computing Systems
[illegible]	Compensating Elements
335(SRD)	*Design Engineers' Nuclear Effects Manual (DNEMM), Volume I, Munitions and Weapon Systems (U)
336(SRD)	*Design Engineers' Nuclear Effects Manual (DNEMM), Volume II, Electronic Systems and Logistics Systems (U)
337(SRD)	*Design Engineers' Nuclear Effects Manual (DNEMM), Volume III, Nuclear Environment (U)
338(SRD)	*Design Engineers' Nuclear Effects Manual (DNEMM), Volume IV, Nuclear Effects (U)
340	Carriages and Mounts--General
341	Cradles
342	Recoil Systems
343	Top Carriages
344	Bottom Carriages
345	Equilibrators
346	Elevating Mechanisms
347	Traversing Mechanisms
350	Wheeled Amphibians
355	The Automotive Assembly
356	Automotive Suspensions
357	Automotive Bodies and Walls
360	Military Vehicle Electrical Systems
361	Military Vehicle Power Plant Cooling
410	*Electromagnetic Compatibility (EMC)
411(S)	*Vulnerability of Communication-Electronic and Electro-Optical Systems (Except Guided Missiles) to Electronic Warfare, Part One, Introduction and General Approach to Electronic Warfare Vulnerability (U)
412(C)	*Vulnerability of Communication-Electronic and Electro-Optical Systems (Except Guided Missiles) to Electronic Warfare, Part Two, Electronic Warfare Vulnerability of Tactical Communications (U)
413(S)	*Vulnerability of Communication-Electronic and Electro-Optical Systems (Except Guided Missiles) to Electronic Warfare, Part Three, Electronic Warfare Vulnerability of Ground-Based and Airborne Surveillance and Target Acquisition Radars (U)
414(S)	*Vulnerability of Communication-Electronic and Electro-Optical Systems (Except Guided Missiles) to Electronic Warfare, Part Four, Electronic Warfare Vulnerability of Avionics (U)
415(S)	*Vulnerability of Communication-Electronic and Electro-Optical Systems (Except Guided Missiles) to Electronic Warfare, Part Five, Optical/Electronic Warfare Vulnerability of Electro-Optic Systems (U)
416(S)	*Vulnerability of Communication-Electronic and Electro-Optical Systems (Except Guided Missiles) to Electronic Warfare, Part Six, Electronic Warfare Vulnerability of Satellite Communications (U)
445	Sabot Technology Engineering
470	*Metric Conversion Guide for Military Applications

*UNDER REVISION--not available
**REVISION UNDER PREPARATION
+OBSOLETE--out of stock