COPY 13

REPORT NO. FAA-RD-76-84

RELIABILITY METHODOLOGY AND PROCEDURES

GEORGE MILLER

ALEX FURSKA

NAFEC
LIBRARY
NOV 26 '76

APRIL 1976

FINAL REPORT

Document is available to the public through the
National Technical Information Service,
Springfield, Virginia 22161.

Prepared for

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
Systems Research & Development Service
Washington, D.C. 20590

NOTICE

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FAA-RD-76-84		

4. Title and Subtitle	5. Report Date
Reliability Methodology and Procedures	April 1976
	6. Performing Organization Code: SRDS/RADC
7. Author(s): George Miller, Alex Furska	8. Performing Organization Report No.
9. Performing Organization Name and Address: Hughes Aircraft Corporation, Fullerton, California 92634	10. Work Unit No. (TRAIS)
	11. Contract or Grant No.: DOT-FA72WA-2725
12. Sponsoring Agency Name and Address: Department of Transportation, Federal Aviation Administration, Systems Research and Development Service, Washington, D.C. 20590	13. Type of Report and Period Covered: Final Report, January 1972 - March 1974
	14. Sponsoring Agency Code: ARD-352

15. Supplementary Notes

16. Abstract

This report is a reliability handbook geared to instructing the user how to implement a reliability program based upon the type of procurement. It lists program content versus type of procurement. Additionally, some fundamental reliability relations are definitized along with some minimal consideration given to redundancy and modeling.

Included is a companion document, "Reliability Program Plans and Procedure Requirements for Electronic and Associated Support Equipment." This document is basically a specification and contains in specification format the reliability programs identified in the Reliability Handbook.

17. Key Words	18. Distribution Statement
Reliability Handbook and Reliability Specification	Document is available to the public through the National Technical Information Service, Springfield, Virginia 22151

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
UNCLASSIFIED	UNCLASSIFIED	215	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

METRIC CONVERSION FACTORS

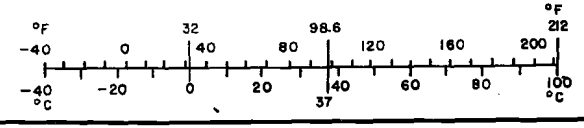
Approximate Conversions to Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
		LENGTH		
in	inches	*2.5	centimeters	cm
ft	feet	30	centimeters	cm
yd	yards	0.9	meters	m
mi	miles	1.6	kilometers	km
		AREA		
in^2	square inches	6.5	square centimeters	cm^2
ft^2	square feet	0.09	square meters	m^2
yd^2	square yards	0.8	square meters	m^2
mi^2	square miles	2.6	square kilometers	km^2
	acres	0.4	hectares	ha
		MASS (weight)		
oz	ounces	28	grams	g
lb	pounds	0.45	kilograms	kg
	short tons (2000 lb)	0.9	tonnes	t
		VOLUME		
tsp	teaspoons	5	milliliters	ml
Tbsp	tablespoons	15	milliliters	ml
fl oz	fluid ounces	30	milliliters	ml
c	cups	0.24	liters	l
pt	pints	0.47	liters	l
qt	quarts	0.95	liters	l
gal	gallons	3.8	liters	l
ft^3	cubic feet	0.03	cubic meters	m^3
yd^3	cubic yards	0.76	cubic meters	m^3
		TEMPERATURE (exact)		
°F	Fahrenheit temperature	5/9 (after subtracting 32)	Celsius temperature	°C

*1 in = 2.54 (exactly). For other exact conversions and more detailed tables, see NBS Misc. Publ. 286, Units of Weights and Measures, Price $2.25, SD Catalog No. C13.10:286.

Approximate Conversions from Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
		LENGTH		
mm	millimeters	0.04	inches	in
cm	centimeters	0.4	inches	in
m	meters	3.3	feet	ft
m	meters	1.1	yards	yd
km	kilometers	0.6	miles	mi
		AREA		
cm^2	square centimeters	0.16	square inches	in^2
m^2	square meters	1.2	square yards	yd^2
km^2	square kilometers	0.4	square miles	mi^2
ha	hectares (10,000 m^2)	2.5	acres	
		MASS (weight)		
g	grams	0.035	ounces	oz
kg	kilograms	2.2	pounds	lb
t	tonnes (1000 kg)	1.1	short tons	
		VOLUME		
ml	milliliters	0.03	fluid ounces	fl oz
l	liters	2.1	pints	pt
l	liters	1.06	quarts	qt
l	liters	0.26	gallons	gal
m^3	cubic meters	35	cubic feet	ft^3
m^3	cubic meters	1.3	cubic yards	yd^3
		TEMPERATURE (exact)		
°C	Celsius temperature	9/5 (then add 32)	Fahrenheit temperature	°F



FOREWORD

1. PURPOSE. This handbook has been prepared to provide agency personnel guidance and direction in the specifying of reliability requirements and programs in procurement documents. It is intended to supplement and amplify the requirements of FAA Specification, "Reliability Program Plans and Procedural Requirements for Electronic and Associated Support Equipment." The Handbook presents general background information relative to reliability concepts and a reliability program. It provides guidance to FAA personnel in establishing reliability requirements in specifications and procurement documents. Lastly, it provides the contractor with guidance in accomplishing the elements of the required reliability program.

2. CANCELLATION. None applicable.

3. CHANGES. Changes will be made to this document whenever there are a sufficient quantity of modifications or changes manifested in reliability and/or quality assurance technologies or in procurement procedures or types.

4. BACKGROUND. This Handbook is intended to support FAA Specification, "Reliability Program Plans and Procedural Requirements for Electronic and Associated Support Equipment." Specifically, Handbook Chapter 3 relates each paragraph of the FAA Specification to the Handbook paragraph providing instructions and guidance for accomplishing that reliability program element. Additionally, in the Handbook instructional text, each Handbook paragraph indicates the Specification paragraphs the former is intended to support.

TABLE OF CONTENTS

	Page No.
CHAPTER 1. GENERAL.	1
SECTION 1. INTRODUCTION.	1
1. Purpose and Scope of Handbook.	1
2. Establishment of the Required Reliability Program.	2
3. Handbook Application to Reliability Program Implementation.	4
SECTION 2. BASIC CONCEPTS.	19
4. Reliability.	19
5. Maintainability.	21
6. Availability.	22
7. Redundancy.	22
8. Impact of Part Screening on Equipment Reliability.	26
CHAPTER 2. FAA RELIABILITY TASKS IN PROCUREMENTS.	29
SECTION 1. RELIABILITY GOALS AND REQUIREMENTS.	29
9. Goals vs. Requirements.	29
10. Establishing Goals for the NAS Functions.	29
11. Establishing Reliability Requirements for the New Equipment.	34
SECTION 2. FAA SPECIFICATION ACTIVITY.	39
12. Reliability Requirements in Procurements.	39
13. Specification of the Reliability Performance Requirement.	39
14. Specification of the Reliability Program.	40
15. Selection and Specification of the Reliability Demonstration Test.	41
16. Establishing the Required Deliverable Documentation.	45
SECTION 3. FAA POST CONTRACT AWARD ACTIVITY.	48
17. FAA Contract Activity Objectives.	48
18. Monitoring the Contractor Reliability Program.	48
19. Monitoring the Reliability Demonstration Test.	53

CHAPTER 3. INSTRUCTIONS FOR CONTRACTOR IMPLEMENTATION OF REQUIRED PROGRAM. 55

SECTION 1. INTRODUCTION TO INSTRUCTIONS. 55
20. The Required Program. 55
21. Scope of Instructions. 55

SECTION 2. PROGRAM MANAGEMENT. 57
22. The Program Plan. 57
23. Supplier and Subcontractor Control. 58
24. Reliability Program Reviews. 61

SECTION 3. RELIABILITY ANALYSIS. 63
25. The Reliability Mathematical Model. 63
26. The Functional and Reliability Block Diagrams for the Mathematical Model. 63
27. Maintenance Policies Pertinent to the Mathematical Model. 66
28. Establishing the Mathematical Model. 68
29. Apportionment (Allocation) of Reliability Requirements. 71
30. Reliability Prediction Techniques and Applicability. 73
31. Reliability Prediction Requirements (Performance/Submittal). 77
32. Detail-Stress Reliability Prediction Procedure. 77
33. Part-Count/Average-Stress Reliability Prediction Procedure. 79
34. Reliability Prediction by Similar Functional Equipments and/or Modules. 80
35. Part Failure Rate Data Sources. 81
36. Environment and Electrical Stress Levels for Reliability Predictions. 83
37. Predictions for Reliability Impact Studies. 84
38. Degradation Analysis of Circuits. 85

SECTION 4. PARTS,ASSEMBLIES,MATERIALS, AND PROCESSES. 88
39. The Parts,Materials,and Processes Program. 88
40. The Reliability Design Guide. 89
41. Parts, Materials, and Process Application Review and Verification. 91

TABLE OF CONTENTS (continued)

SECTION 5. FAILURE MODE AND EFFECT ANALYSIS,AND CRITICAL ITEMS. 93
42. Effective Failure Mode and Effect Analysis in the Reliability Program. 93
43. Levels of FMEA. 95
44. General Procedures for Performing FMEA. 97
45. Critical Items Identification, Control, and Handling. 100

SECTION 6. DESIGN REVIEWS. 103
46. The Design Review Program. 103
47. The Design Review Board and Review Participation. 106
48. General Reliability Review Considerations. 108
49. The Formal Study Reviews. 109
50. Reliability in the Preliminary Design Review. 110
51. Reliability in the Critical Design Review. 111
52. Reliability in the First Article Configuration Inspection. 112
53. Detailed Design Review Activity. 113

SECTION 7. EFFECTS OF STORAGE,SHELF-LIFE, PACKAGING,TRANSPORTATION, HANDLING,AND MAINTENANCE. 116
54. Effects of Storage,Shelf-Life, Packaging,Transporation,Handling, and Maintenance. 116

SECTION 8. DESIGN SPECIFICATION,DRAWING RELEASE,AND DESIGN CHANGES. 117
55. Design Specification Inputs. 117
56. Design Approval. 117
57. Engineering Design Changes. 118

SECTION 9. RELIABILITY TESTING. 119
58. The Reliability Development Testing Program. 119
59. Types of Reliability Development Tests. 121
60. The Reliability Demonstration Test. 123
61. Reliability Acceptance Tests in Production. 125
62. Reliability Testing Plans, Procedures, and Reports. 125

TABLE OF CONTENTS (continued)

SECTION 10. FAILURE DATA COLLECTION, ANALYSIS, AND CORRECTIVE ACTION. 128
63. Design of a Failure Reporting and Data Collection System. 128
64. The Failure Review Board and Corrective Action. 130
65. Failure Analysis. 132

SECTION 11. DOCUMENTATION AND DATA REQUIREMENTS. 134
66. Deliverable and Non-Deliverable Data or Documentation. 134
67. Standard Deliverable Data Items. 135

TABLE OF CONTENTS (continued)

	Page No.
APPENDIX 1. GLOSSARY. (5 Pages)	1
1. Abbreviations and Symbols.	1
2. Definitions of Terms.	2
APPENDIX 2. COMPUTER PROGRAMS. (8 Pages)	
1. Existing Circuit Analysis Programs.	1
2. System Modeling Programs.	2
3. Life Testing Programs.	2
4. Test Data Analysis Programs.	3
5. MIL Standards Programs.	4
6. Limit Estimation Programs.	4
7. Probability Calculation Programs.	5
8. Data Comparison Programs.	5
9. Distribution Testing Programs.	6
APPENDIX 3. DELIVERABLE DATA ITEM DESCRIPTIONS. (13 Data Items)	1
R-1. Reliability Program Plan.	
R-2. Reliability Allocations, Assessments, and Analysis Report.	
R-3. Defective or Inadequate Parts and/or Specifications Notification.	
R-4. Failure Data Reporting and Feedback, Failure Summary Reports.	
R-5. Reliability Test and Demonstration Plan.	
R-6. Acceptance Test Procedure.	
R-7. Reliability Program Status Reports.	
R-8. Reliability Test and Demonstration Reports.	
R-9. Suspect Material Deficiency Notice Response.	
R-10. Critical Items Report.	
R-11. Failure Mode and Effects Analysis Report.	
R-12. Design Review Report.	
R-13. Parts, Materials, and Processes Application Review Report.	
APPENDIX 4. REFERENCE DOCUMENTS AND SERVICES (10 Pages)	1
1. Reference Documents.	1
2. Reference Services.	9
APPENDIX 5. SAMPLE SPECIFICATION (41 Pages)	1

CHAPTER 1. GENERAL

SECTION 1. INTRODUCTION

1. PURPOSE AND SCOPE OF HANDBOOK. The Handbook contains the guidance to fulfill the reliability-pertinent requirements imposed in a procurement. More specifically, the Handbook tells the contractor how to go about accomplishing the elements of a reliability program, as specified from the FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT. The FAA is given guidance and direction in establishing reliability performance requirements, the required reliability program, required documentation and testing requirements. The Handbook will also be used as a guide for FAA program monitors at the contractor's facility.

   a. Organization of Text. The body of the Handbook is divided into three distinct chapters. A brief description of their contents is given in the following sub-paragraphs.

      (1) Chapter 1. General. This first chapter presents general background concepts. Reference material and information is given in Appendix 4.

      (2) Chapter 2. FAA Reliability Tasks in Procurements. The first part of this chapter presents an approach for the FAA to use in establishing Reliability Goals and Requirements. Next is a discussion of the FAA Tasks involved in establishing the equipment specification and/or procurement documentation. Finally, the chapter discusses the FAA monitoring, participation, and support of the active Contract Reliability Program.

      (3) Chapter 3. Instructions for Contractor Implementation of Required Program. This chapter gives the instructions required for the implementation and/or accomplishment of the elements of the required reliability program. Specifically, guidance is given for: (a) Reliability Program Management; (b) Reliability Engineering and Analysis Tasks; (c) Design Reviews and Design Control; (d) Reliability Testing; (e) Failure Data Collection, Analysis, and Corrective Action; and (f) Fulfillment of the Documentation Requirements.

b. Appendices. Four Appendices are provided with the Reliability Handbook. The first is a GLOSSARY giving a list of pertinent abbreviations, definitions, and symbols. The second appendix is on COMPUTER PROGRAMS; and, it gives a listing, with description, of time-share computer programs available for application to reliability analysis tasks. The third appendix, DELIVERABLE DATA ITEM DESCRIPTIONS, gives the full Data Item Descriptions for thirteen standard Data Items specific to the documentation and/or data for a Reliability Program. The fourth and last appendix contains reference documents and services listings.

2. ESTABLISHMENT OF THE REQUIRED RELIABILITY PROGRAM. The required reliability program will be specified by imposing specific paragraphs of the FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED EQUIPMENT. Five standard reliability programs are so tabulated in Table 1, wherein an asterisk indicates that the specification paragraph is imposed. A "standard" program is then imposed by simply specifying the identifying number of the Reliability Program as listed in paragraph 3.3.2.3 of the aforementioned Specification, and tabulated in Table 1.

a. Selection of a Standard Reliability Program. As listed in Table 1 and the FAA Specification, the standard reliability programs are suitable for application to Study Contracts, Developmental Equipments, Prototype (preproduction) models, and Production Model Contracts. The following paragraphs define the basic reliability effort required for each of these contract types and the applicable standard program(s).

(1) Study Contracts. These contracts They are concerned with the study of concepts, probable design details and/or existing equipment configurations. Standard Reliability Program (1) is applicable to the design study effort. No hardware end item is anticipated.

(2) Development Model Contract. In the development model effort, the basic reliability effort is directed to the evaluation of design concepts or approaches. The two basic end goals for the reliability program are an analytical evaluation of the achieved reliability; and an assessment of the reliability potential for the production model. Standard Reliability Program (2), of

Table 1, is the applicable program for this effort.

(3) The Prototype (Preproduction) Model. In the prototype or preproduction effort, designs develop into essentially final form; and final parts are selected. The basic reliability effort is now directed to part selection and application; detail design support; reliability allocations and detail assessment; and, normally, a program of reliability testing and demonstration. Standard Reliability Program (3) is designed to provide a adequate reliability program for the average prototype effort. Where the effort involves either a high risk of accomplishment or low risk of accomplishment of the reliability requirements causes a modification of standard program as indicated above.

(4) The Production Model Contract. In the production model contract, the primary goal of the reliability effort is to assure that the "designed-in" reliability is not degraded by the production process. The reliability program is therefore concerned with process, parts, materials, and design change monitoring and control. However, there are significant differences in required effort between the pure reprocurement and the initial production.

(a) A reprocurement with modifications (allowed and/or required) requires that reliability monitoring and control be increased to ensure that the modifications do not degrade reliability. Standard Reliability Program (4) is suitable for the reprocurement with moderate modifications. (Extensive modifications would require treatment as an initial production contract.)

(b) The initial production contract requires a full monitoring and control of process and all changes. Normally, a demonstration test of some level is also imposed. Standard Reliability Program (5) fulfills the requirements for a reliability program on the initial production of equipment with a reliability performance requirement.

(5) Summary of Standard Reliability Programs Applicability. The following tabulation summarizes the contract applicability of the Standard Reliability Programs given in Table 1.

(a) Standard Reliability Program (1). Design Study.

(b) Standard Reliability Program (2). Development Model Equipment Contract.

(c) Standard Reliability Program (3). Prototype (preproduction) Equipment Contract, with moderate risk of accomplishing the required reliability performance.

(d) Standard Reliability Program (4). Reprocurement Production Contract, with moderate modifications allowed and/or required.

(e) Standard Reliability Program (5). Initial Production Contract.

b. Non-Standard Reliability Program. The previous indications, and tabulation, of Standard Reliability Program applicability are not "required" use - they indicate only "normal" use of the Standard Reliability Programs. Furthermore, in special situations, none of the Standard Reliability Programs may be suitable or desirable. In these cases, the Standard Program should be modified as required by adding or deleting specific paragraphs of the FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED EQUIPMENT.

3. HANDBOOK APPLICATION TO RELIABILITY PROGRAM IMPLEMENTATION. As has been previously indicated, the required reliability program will be specified by imposing paragraphs of the FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT. Chapter 3 of this Handbook provides the basic instructions and/or guidance needed by the contractor to implement the required reliability program and accomplish the required tasks. Each of the instructional paragraphs of Chapter 3 is cross-referenced to the pertinent paragraphs of the above FAA Specification. Table 2 presents a summary cross-reference relating the FAA Specification

paragraphs requiring instruction or guidance to the pertinent Handbook paragraph.

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
1.1	Scope					
2.0 through 2.3, 3.1 through 3.3.2	Applicable Documents (General)	*	*	*	*	*
3.3.2.1	Study Contracts	*				
3.3.2.2	Equipment Contracts		*	*	*	*
3.3.2.2.1	Development Model		*			
3.3.2.2.2	Prototype/Preproduction Model			*		
3.3.2.2.3	Production Model				*	*
3.3.2.3, 3.4 through 3.4.1	Specified Programs, Management	*	*	*	*	*
3.4.1.1, 3.4.1.2	Program Plan, Rel. Interface Compatibility		*	*	*	*
3.4.1.3	Reliability Program Control	*	*	*	*	*
3.4.1.4	Supplier/Subcontractor Control		*	*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.4.1.4.1, 3.4.2	Supplier/Subcontractor Design Reviews, Program Reviews		*	*		
3.5 through 3.5.1.1.2	Engineering, Design and Analysis through Model Results Application	*	*	*	*	*
3.5.1.2	Reliability Apportionment	*	*	*		
3.5.1.3 through 3.5.1.3.1	Reliability Predictions through Prediction Techniques	*	*	*	*	*
3.5.1.3.1.1	Similar Functional Equipment Rel. Prediction					
3.5.1.3.1.2	Similar Card/Module/Assembly Equivalent Reliability Prediction	*				
3.5.1.3.1.3	Average Stress Reliability Prediction		*			
3.5.1.3.1.4	Detailed Stress Reliability Prediction				*	*
3.5.1.3.2	Failure Rate Sources/Justification		*	*	*	*
3.5.1.3.3	Use Environment for Predictions	*		*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT

Paragraph Number	Paragraph Heading	Reliability Program A (1)	(2)	(3)	(4)	(5)
3.5.1.3.4 through 3.5.1.3.4.3	Reliability Studies through Ambient Temperature Variations	*	*			
3.5.1.3.4.4	Part Reliability/Quality Classes	*	*			
3.5.1.3.4.5	Part Quality Control Programs	*	*			
3.5.1.3.4.6	Reliability Cost	*	*	*		
3.5.1.3.5	Reliability Prediction Frequency	*	*	*	*	*
3.5.1.4	Degradation Analysis	*	*	*		
3.5.1.4.1	Parameter Variation Analysis Method		*			
3.5.1.4.2	Worst-Case Analysis Method	*		*		
3.5.1.4.3	Variance Analysis Method			*		
3.5.1.4.4	Monte Carlo Simulation Method					

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.5.1.5	Design Specification Inputs	*	*	*	*	*
3.5.2 through 3.5.2.1.1	Parts/Materials/Process Control through Derating Policy and Design Tolerance Values				*	*
3.5.2.2	Verification of Part Application Stresses			*	*	*
3.5.2.2.1	Thermal Analysis				*	*
3.5.2.3 through 3.5.2.5	Parts/Materials/Process Application Review through Suspect Item Deficiencies			*	*	*
3.5.3	Parts/Assemblies/Material Handling				*	*
3.5.4	Failure Mode, Effect Analysis (FMEA)	*	*	*	*	*
3.5.4.1	Functional Level FMEA	*	*			
3.5.4.2	Circuit Level FMEA			*	*	*
3.5.5	Critical Items		*	*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.5.6	Design Reviews	*	*			*
3.5.6.1	Study Design Reviews	*				
3.5.6.2	Equipment Design Reviews		*	*		*
3.5.6.3	Design Tradeoffs				*	
3.5.7	Design Approval		*	*	*	*
3.5.8	Effects of Storage, Shelf-Life, Packaging, Transportation, Handling, and Maintenance			*	*	*
3.6	Production Reliability				*	*
3.6.1	Production Failure Reporting				*	*
3.7 through 3.7.1	Reliability Testing through Test Types		*	*	*	*
3.7.1.1	Development Testing					

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.7.1.2	Reliability Demonstration Testing			*	*	*
3.7.1.3 through 3.7.1.3.4	Conditioning Tests through Equipment Vibration Level - Option 2				*	*
3.7.1.4	Production Reliability Tests					*
3.7.2	Reliability Test Program Plans		*	*		*
3.7.3	Reliability Demonstration Plan			*		*
3.7.4 through 3.7.4.5	Reliability Test Procedure through Test Demonstration Environment			*	*	*
3.7.5	Design/Reliability Requirements Compatibility			*	*	*
3.7.6 through 3.7.7.5	Maximum Preacceptance Operation Test Report			*		*
3.8 through 3.8.1	Failure Data Collect., Analysis, Corr. Action through Initiation of Failure Reporting		*	*	*	*
3.8.1.1	Program Initiation During Design		*			

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.8.1.2	Program Initiation at Acceptance				*	*
3.8.2 through 3.8.5.1	Failure Review Board through Failure Summary Reports		*	*	*	*
3.8.5.2	Weekly Failure Reports			*		*
3.8.5.3	Hot-Line Reports			*		*
3.9	Engineering Design Changes		*	*	*	*
3.10, 3.10.1	Data Requirements, Status Reports	*	*	*	*	*
3.10.2	Computerized Reliability Predictions	*	*	*	*	*
4.1	Intended Use	*	*	*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 2. HANDBOOK GUIDANCE FOR IMPLEMENTING RELIABILITY PROGRAM TASKS (page 1 of 6)

Program Tasks from FAA Specification, "Reliability Program Requirements For Electronic and Associated Support Equipment"		Applicable Guidance in Reliability Handbook	
Paragraph Number	Paragraph Heading	Paragraph Number	Paragraph Heading
3.4.1.1	Program Plan	24	The Program Plan
3.4.1.4	Supplier/Subcontractor Control	25	Supplier and Subcontractor Control
3.4.2	Program Reviews	26	Program Reviews
3.5.1.1	Reliability Modeling	27	The Reliability Mathematical Model.
		28	The Functional And Reliability Block Diagrams for the Mathematical Model.
		29	Maintenance Policies Pertinent to the Mathematical Model.
		30	Establishing the Mathematical Model.
3.5.1.1.1	Model Requirements		
3.5.1.1.2	Model Results Application	27	The Reliability Mathematical Model.
3.5.1.2	Reliability Apportionment	31	Apportionment (Allocation) of Reliability Requirements.
3.5.1.3	Reliability Predictions	32	Reliability Prediction Techniques and Applicability.
3.5.1.3.1	Prediction Techniques		

TABLE 2. HANDBOOK GUIDANCE FOR IMPLEMENTING RELIABILITY PROGRAM TASKS (page 2 of 6)

Program Tasks from FAA Specification, "Reliability Program Requirements For Electronic and Associated Support Equipment"		Applicable Guidance in Reliability Handbook	
Paragraph Number	Paragraph Heading	Paragraph Number	Paragraph Heading
3.5.1.3.1.1	Similar Functional Equipment Reliability Prediction	32	Reliability Prediction Techniques and Applicability.
3.5.1.3.1.2	Similar Card/Module/Assembly Equivalent Reliability Prediction	36	Reliability Prediction by Similar Functional Equipments and/or Modules.
3.5.1.3.1.3	Average Stress Reliability Prediction	32	Reliability Prediction Techniques and Applicability.
		35	Part-Count/Average-Stress Reliability Prediction Procedure.
3.5.1.3.1.4	Detailed Stress Reliability Prediction	32	Reliability Prediction Techniques and Applicability.
		34	Detailed-Stress Reliability Prediction Procedure.
3.5.1.3.2	Failure Rate Sources/Justification	37	Part Failure Rate Data Sources.

TABLE 2. HANDBOOK GUIDANCE FOR IMPLEMENTING RELIABILITY PROGRAM TASKS (page 3 of 6)

Program Tasks from FAA Specification, "Reliability Program Requirements For Electronic and Associated Support Equipment"		Applicable Guidance in Reliability Handbook	
Paragraph Number	Paragraph Heading	Paragraph Number	Paragraph Heading
3.5.1.3.4	Reliability Studies		
3.5.1.3.4.1	Design Variations		
3.5.1.2.4.2	Stress Variations		
3.5.1.3.4.3	Ambient Temperature Variations	39	Predictions for Reliability Impact Studies
3.5.1.3.4.4	Part Reliability/Quality Classes		
3.5.1.3.4.5	Part Quality Control Programs		
3.5.1.3.4.6	Reliability Cost		
3.5.1.3.5	Reliability Prediction Frequency	33	Reliability Prediction Requirements.
3.5.1.4	Degradation Analysis		
3.5.1.4.1	Parameter Variation Analysis Method		
3.5.1.4.2	Worst-Case Analysis Method	40	Degradation Analysis of Circuits.
3.5.1.4.3	Variance Analysis Method		
3.5.1.4.4	Monte Carlo Simulation Method		
3.5.1.5	Design Specification Inputs	57	Design Specification Inputs.
3.5.2	Parts/Materials/Process Control	41	The Parts, Materials, and Processes Program.
3.5.2.1	Design Guide	42	The Reliability Design Guide.
3.5.2.1.1	Derating Policy and Design Tolerance Values		
3.5.2.2	Verification of Part Application/ Stresses		
3.5.2.2.1	Thermal Analysis	43	Parts, Materials and Process Application Review and Verification.
3.5.2.3	Parts/Materials/Process Application Review		

TABLE 2. HANDBOOK GUIDANCE FOR IMPLEMENTING RELIABILITY PROGRAM TASKS (page 4 of 6)

Program Tasks from FAA Specification, "Reliability Program Requirements For Electronic and Associated Support Equipment"		Applicable Guidance in Reliability Handbook	
Paragraph Number	Paragraph Heading	Paragraph Number	Paragraph Heading
3.5.2.4	Defective or Inadequate Items		
3.5.2.5	Suspect Item Deficiencies	41	The Parts, Materials, and Processes Program.
3.5.3	Parts/Assemblies/Material Handling		
3.5.4	Failure Mode, Effect Analysis (FMEA)	44	Effective Failure Mode and Effect Analysis (FMEA) in the Reliability Program.
		46	General Procedures for Performing FMEA.
3.5.4.1	Functional Level FMEA	45	Levels of FMEA.
3.5.4.2	Circuit Level FMEA	46	General Procedures for Performing FMEA.
3.5.5	Critical Items	47	Critical Items Identification, Control and Handling.
3.5.6	Design Reviews	48	The Design Review Program.
		49	The Design Review Board and Review Participation.
		50	General Reliability Review Considerations.
		52	Reliability in Preliminary Design Reviews.
		53	Reliability in Critical Design Review.
		54	Reliability in First Article Configuration Inspection.

TABLE 2. HANDBOOK GUIDANCE FOR IMPLEMENTING RELIABILITY PROGRAM TASKS (page 5 of 6)

Program Tasks from FAA Specification, "Reliability Program Requirements For Electronic and Associated Support Equipment"		Applicable Guidance in Reliability Handbook	
Paragraph Number	Paragraph Heading	Paragraph Number	Paragraph Heading
3.5.6.1	Study Design Reviews	49	The Design Review Board and Review Participation.
		51	The Formal Study Design Reviews.
3.5.6.2	Equipment Design Reviews	49	The Design Review Board and Review Participation.
		52	Reliability in Preliminary Design Review.
		53	Reliability in Critical Design Review.
		54	Reliability in First Article Configuration Inspection.
3.5.6.3	Design Tradeoffs	50	General Reliability Review Considerations.
3.5.7	Design Approval	58	Design Approval.
3.5.8	Effects of Storage, Shelf-Life, Packaging, Transportation, Handling and Maintenance	56	Effects of Storage, Shelf-Life, Packaging, Transportation, Handling and Maintenance.
3.7.1.1	Development Testing	60	The Reliability Development Testing Program.
		61	Types of Reliability Development Tests.
3.7.1.2	Reliability Demonstration Testing	62	The Reliability Demonstration Test.

TABLE 2. HANDBOOK GUIDANCE FOR IMPLEMENTING RELIABILITY PROGRAM TASKS (page 6 of 6)

Program Tasks from FAA Specification, "Reliability Program Requirements For Electronic and Associated Support Equipment"		Applicable Guidance in Reliability Handbook	
Paragraph Number	Paragraph Heading	Paragraph Number	Paragraph Heading
3.7.1.4	Production Reliability Tests	63	Reliability Acceptance Tests in Production.
3.7.2 3.7.3 3.7.4 3.7.7.5	Reliability Test Program Plans Reliability Demonstration Plan Reliability Test Procedure Test Report	64	Reliability Testing Plans, Procedures, and Reports.
3.8	Failure Data Collection, Analysis and Corrective Action Program	65	Design of a Failure Reporting and Data Collection System.
3.8.2	Failure Review Board	66	The Failure Review Board and Corrective Action.
3.8.3	Failure Analysis	67	Failure Analysis.
3.8.4	Corrective Action	66	The Failure Review Board and Corrective Action.
3.9	Engineering Design Changes	59	Engineering Design Changes.
----------	"general requirements for documentation"	68	Deliverable vs Non-deliverable Data and/or Documentation.
----------	"requirements for deliverable documentation"	69	Standard Deliverable Data Items.

SECTION 2. BASIC CONCEPTS

4. RELIABILITY. The reliability of an equipment is defined as the PROBABILITY that the equipment will perform satisfactorily for a specified period of time, when used under specified conditions. This probability expressed as a function of the time is called a Reliability Function, R(t).

   a. Failure Rate and Mean-Time-Between Failure. Failure Rate and Mean-Time-Between-Failures (MTBF) are also useful indicators of equipment reliability. Failure Rate is defined as the number of failures occurring per unit of time. The instantaneous failure rate, or hazard rate, λ , is related to the Reliability Function by the following equation.

$$\lambda_1(t) = \frac{-d \ln R(t)}{dt} \qquad \text{(equation 1)}$$

   And, MTBF is related to the Reliability Function as in the following equation.

$$MTBF = \int_0^{\infty} R(t)\,dt \qquad \text{(equation 2)}$$

   b. The Exponential Function. Failure distributions for most electronic and electrical parts, which have been screened and "burned-in", have been found to follow the negative-exponential curve (as a function of time). The same distribution then applies to "debugged" conventional (i.e., without significant redundancy) electronic equipment. The Reliability Function under these conditions is given by the following equation.

$$R(t) = e^{-\lambda t} \qquad \text{(equation 3)}$$

   Applying equations (1) and (2), the failure rate is found to be the constant, λ ; and the MTBF is found to be the inverse of this failure rate.

      (1) Life-Cycle Failure Rate for Electronic Equipment. It is important to note that electronic equipment follows the exponential, constant-failure-rate, curve for only a part of its total lifetime. This part generally represents the useful life; and electronic equipment is characterized by a relatively long "useful life". Prior to this phase, the failure rate is higher and decreasing in what is commonly called the debugging, or infant mortality, phase, After the constant-failure-rate portion of its life,

the equipment enters a "wear-out" phase, where the failure rate increases at an increasing rate. These three periods of the equipment life form what is commonly called a "bathtub" curve for the failure rate as a function of time.

c. The Weibull Function. The failure distributions for mechanical elements and certain electronic parts (such as vacuum tubes) do not follow the above exponential, constant-failure-rate, curve. For these, the Weibull distribution is more applicable; and has been found to be extremely useful. Under a Weibull distribution, the Reliability Function may be written as in the following equation.

$$R(t) = e^{-\lambda t^{\alpha}} \qquad \text{(equation 4)}$$

The instantaneous failure rate, or hazard rate, under a Weibull distribution is then defined by the following equation.

$$\lambda := \alpha \lambda t^{\alpha - 1} \qquad \text{(equation 5)}$$

The failure rate for the general Weibull is therefore not constant. Note that when α is 1, the Weibull becomes the exponential, with constant failure rate. When this parameter is less than 1, a decreasing failure rate is obtained; and when the parameter is greater than 1, an increasing failure rate is obtained.

(1) Life-Cycle Failure Rate for Mechanical Equipments. This type of equipment and/or part generally does not have a constant-failure-rate phase in its lifetime. Initially, the failure rate is decreasing. After reaching some minimum value, the failure rate immediately begins increasing.

d. Combining Reliabilities. Since the Reliability Function is a probability function, the laws of probability apply when determining the reliability of a group of elements, with the individual reliabilities being known. Application to "redundant" configurations is discussed in a following paragraph of this section. For the present, consider an equipment consisting of "n" elements, all of which are required for the equipment to operate properly. If R is the reliability of these elements, the reliability of the equipment is simply the product of these individual reliabilities. If all elements follow the exponential failure distribution, the

equipment Reliability Function is therefore given by the following equation.

$$R(t) = e^{-(\lambda_1+\lambda_2+\dots+\lambda_n)t} \quad \text{(equation 6)}$$

In this equation, the λ's are the individual element failure rates. It is clear that the failure rate of this equipment is constant, and is the sum of the individual element failure rates. (It will later be shown that the failure rate is not constant when redundant elements are involved.)

e. MTBF vs. MTBM. In defining and determining MTBF, only those element failures are counted which prevent the prime function from operating satisfactorily. Where redundancy is involved, there will be element failures which do not cause failure of the prime function. These latter do, however, still require a maintenance action to be performed. As a measure of required maintenance, then, a Mean-Time-Between-Maintenance (MTBM) action is defined and/or determined. MTBM counts all element failures, whether or not the prime function is operating satisfactorily.

5. MAINTAINABILITY. The maintainability of an equipment is generally defined and measured in terms of the time required to perform maintenance actions.

a. Inherent vs. Operational Maintainability. The "inherent" maintainability is "designed-into" the equipment; and its determination assumes that all required instruments, tools, and spares are immediately available. Thus, inherent maintainability does not consider the effect of administrative and/or logistics delays in accomplishing a maintenance action. The inherent maintainability is generally defined in terms of a Mean-Time-To-Repair (MTTR) the equipment; and includes the time required to fault locate and/or isolate, remove and replace the faulty element, and verify effectiveness of the repair. "Operational" maintainability, on the other hand, additionally takes into account the administrative and logistics delays involved in the maintenance action. This operational maintainability is generally defined as a Mean-Down-Time (MDT). Note that, except as indicated in the following, the "down-time" in MDT refers to the failed element being down (inoperative). For equipments without redundancy, this would also mean the prime function is inoperative.

b. System MTTR and MDT. In determining the Availability of an equipment, it will be necessary to determine MTTR and MDT for only those maintenance actions performed with the equipment itself inoperative. The inoperativeness may be caused by the maintenance action itself and/or by the failure of the faulty element requiring the action. When such determination is intended, the required terms should be clearly so designated; as, for example, MTTR(system) and MDT(system).

6. AVAILABILITY. The availability of an equipment is the probability that it will be operationally ready when needed at any point during a specified mission, or duty, time. Availability therefore takes into account both equipment "up" time; and equipment "down" time for maintenance. In equation form, then, "inherent" availability (i.e., "designed-in" availability) is defined by the following.

$$A_1 = \frac{MTBF}{MTBF + MTTR(system)} \quad \text{(equation 7)}$$

Operational Availability is definable by the following equation.

$$A_0 = \frac{MTBF}{MTBF + MDT(system)} \quad \text{(equation 8)}$$

7. REDUNDANCY. A "success" path for an equipment function is any set of operating elements REQUIRED to accomplish that function successfully. If more than one such success path is provided, the paths are said to be redundant. Clearly, the reliability potential for the function increases with the number of alternate success paths provided.

a. Basic configurations. In the simplest configuration of redundant equipment elements, "n" unique sets of elements are provided and only one set is REQUIRED for successful operation. In constructing a reliability block diagram, this is usually indicated by simple parallel sets of elements. In the general redundancy case, "n" sets are provided and "m" (with m less than n) are required for success. The reliability block diagram now requires an indication of the number of sets required for "success". The degree of redundancy is usually indicated by taking the ratio of the number of element sets provided to the number required; i.e., "n/m". Most cases of

alternate, redundant success "paths" can be reconfigured into combinations of reliability-wise parallel (in the present sense) and serial elements. (In the reliability sense, serially-indicated elements are all required for success.)

b. Implementation of Redundancy. There are two basic approaches to implementing these reliability-parallel elements. One is to have "active" redundancy; and the other is "standby" redundancy.

(1) Active redundancy is implemented with all elements actively operating in the equipment function. Conceptually, this is the simplest approach, since no switch-over mechanisms are required. Quite often, however, this approach presents insurmountable circuit design problems.

(2) Stand-by redundancy is implemented by providing for switching in a stand-by element when the actively operating element fails. In its stand-by status, the redundant element is not active in the equipment function. Furthermore, the stand-by status may be "cold" (totally non-operating), "hot" (fully operating), or "warm" (partially operating). From the reliability standpoint, the "coolest" stand-by is preferable, since the failure rate in stand-by is then lower. However, to permit immediate switch-over without adjustment, circuit and/or part limitations may require a "warmer" stand-by operational condition.

(3) Maintenance of the redundant set is an important consideration in designing the equipment to obtain optimum reliability potential from the redundancy. In the simplest design approach, repair action is not instituted until failure of the function provided by the redundant set. On the other hand, if failed elements of the redundant set can be repaired while the equipment continues operating, tremendous reliability advantage is generally gained if repair action is instituted immediately as the elements fail. The first case is normally referred to as non-repairable redundancy; while the second case is normally termed repairable redundancy.

c. Reliability Evaluation. The following sub-paragraphs review the reliability impact of the redundancy factors considered in the preceding.

(1) Active Redundancy, Non-Repaired. The reliability function for this type of redundancy is a simple combination of independent, NON-CONDITIONAL, probabilities. For example consider the set of two elements (with Reliabilities R and R) with only one element needed. The Reliability Function for the set is readily obtained, and is given by the following equation.

$$R = R_1 + R_2 - R_1 R_2 \qquad \text{(equation 9)}$$

If the redundant set consists of electronic elements, with failure rates , and , the Reliability is then given by the following.

$$R = e^{-\lambda \cdot t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t} \qquad \text{(equation 10)}$$

And if the elements all have equal failure rates, as is the common case in applications of active redundancy, the Reliability Function simplifies to the following.

$$R = 2e^{-\lambda t} - e^{-2\lambda t} \qquad \text{(equation 11)}$$

Similar equations are readily developed for the general case of active, non-repaired, redundancy with n elements and m required.

(a) Failure Rate of the redundant set is no longer constant, even though the individual elements have constant failure rates. This may be proven by applying equation (1) to the above equation (11). Thus, the failure rate of the redundant set is not additive to element failure rates in obtaining equipment failure rate.

(b) MTBF of the redundant set may be determined by application of equation (2) to the Reliability Function. For the simple case illustrated by Equation (11), the MTBF is found to be 1.5θ, where θ is the MTBF of the element. Note that the MTBF is no longer the inverse of the hazard rate defined by equation (1). This is generally true when the constant failure-rate characteristic is no longer valid.

(c) The Reliability of a properly applied redundant set is better than that of an individual element. Note equations (9) through (11). This reliability improvement

increases as the degree of redundancy increases.

(2) Stand-by Redundancy, Non-Repaired. The case of "hot" stand-by is essentially that of the active redundancy case; except that the set reliability is degraded by the need for a switching mechanism. Hence, in this case, care must be taken that the "unreliability" of the switching mechanism does not override any advantage given by the redundancy. As the stand-by state becomes "cooler", the reliability improves over the active and hot stand-by implementations. For stand-by states below "hot", the development of Reliability Functions is not the simple matter it was with active redundancy. The failure rate of the stand-by unit is now a function of the condition of the operating unit. Several books (see Section 2, paragraph 4d) are available to give specific equations for specific conditions of stand-by redundancy (see reference d.(1) of paragraph 4.) Consider the simple case of one electronic unit operating, with a second, similar unit in "cold" stand-by. If the reliability of the switching mechanism is ignored, the Reliability Function of the set is given by the following equation.

$$R = e^{-\lambda t} \quad (1+\lambda t) \qquad \text{(equation 12)}$$

(a) The Failure Rate is, again, not constant; in spite of the fact that the elements do have constant failure rate characteristics.

(b) The MTBF can be determined if the Reliability Function can be defined. For the simple case of Equation (12), the MTBF of the set is found to be twice the MTBF of the element, as should be expected for cold stand-by.

(c) The Reliability of the stand-by implementation is theoretically better than that achievable with active redundancy, provided the stand-by status is less than "hot". However, when considering this form of redundancy for its reliability advantage (and not because of circuit and/or part requirements), extreme care should be taken that the required switching mechanism does not absorb all the advantage possible.

(3) Impact of Repaired Redundancy. All of the preceding discussion in sub-paragraph c. is based on the premise that repair action is not initiated until the function fails (i.e. the number of elements falls below the minimum required). If repair action is initiated immediately as the element fails, and if the equipment design allows the equipment to continue operating while the repair is performed, the reliability gain can be tremendous. The required equations and computations can be complex for any significant redundancy. For most cases of redundancy with the present types of parts and components, a "repair-while-hot" capability on the redundant set results in a Reliability that is essentially unity; that is, the result is an effectively nonfailing function.

8. IMPACT OF PART SCREENING ON EQUIPMENT RELIABILITY. The use of high quality parts does not guarantee that a reliable equipment will result. However, the use of poor quality parts does effectively prevent the possibility of a high resulting reliability. Part screening is an effective approach to obtaining reliable parts; and, hence, a POTENTIALLY reliable equipment.

a. Significant Part Screens. The most significant "standard" part screens, applicable to control of electronic part quality, are listed below.

(1) Visual Inspection. This is the simplest form of part screen. It is designed to eliminate the obvious fabrication faults, which would either cause immediate failure or lead to very early failures. In microcircuits, semiconductors, and other capped or encapsulated parts, the visual inspection is done in two phases - "pre-cap" and "post-cap".

(2) Seal Hermeticity Tests. This test verifies the validity of the hermetic seal of capped units. Microcircuits and semi-conductors are special candidates for this screen. The primary aim is to reduce humidity-induced failures in the field.

(3) Temperature Cycling Screen. The aim of this screen is to reduce field failures resulting from high or low AMBIENT temperatures. It is equally applicable to all electronic parts.

(4) Thermal Shock Screen. This is similar to the preceding, except that the investigation is directed toward the effect of SUDDEN CHANGES in temperature. Thermal shock can produce mechanical stresses which can either induce immediate failure or make the part failure-prone. The screen is especially applicable to structurally "delicate" parts, such as hybrid microcircuits.

(5) Mechanical Shock Screen. The intent here is to reduce field failures resulting from vibration (and of course, shock). This type of test is most useful on a structured-equipment basis. On a part level, this screen does have some use on parts of a "structural" nature; which would include all hybrid microcircuits, some integrated circuits and semiconductors, RF coils, and mechanically adjustable parts.

(6) Burn-In Screen. The preceding screens were either of a "quality control" nature; or they were directed toward reducing the effect of a severe use environment. In the burn-in screen, the parts are operated at high temperatures with full electrical stress. The burn-in process is intended to accelerate the obtaining of a low, constant-failure-rate characteristic for the part class. Burn-in is the most significant of the screens in establishing the BASE failure rate to be obtained of the part class.

b. Reliability Impact. A great variety of equipments have been built using parts of specified control "levels". Reliabilities (field, test, and/or analytic) have been established for these equipments. These serve as a base for indicating the equipment-reliability impact of part screening. The following subparagraphs compare the reliabilities achieved with specific part-screening control to that achieved using essentially unscreened parts.

(1) Commerical-Grade Equipment. Most commercial grade equipment uses essentially unscreened parts. At the most, visual inspections and hermeticity tests may be carried out; but only on a sampling basis. The MTBF obtained for such equipments shall be used as a base of comparison for the following specified control levels.

(2) Level C Parts. Parts controlled to "Level C" will go through visual inspection, temperature cycling, and seal hermeticity (as applicable) screens. Equipments built with parts controlled to this level have been found to have an MTBF approximately TWO times that of similar commercial-grade equipment.

(3) Level B Parts. Parts controlled to "Level B" will add thermal shock and burn-in screens to those required for Level C. And, the burn-in is of approximately 170 hour duration. Equipments built with Level B parts have resulted in MTBF's on the order of SIX times that obtained in similar commercial-grade equipment.

(4) Level A Parts. "Level A" part control uses ALL of the screens listed in the preceding sub-paragraph. This adds the mechanical shock screen to those defined for Level B control. And, the burn-in is now extended to 240 hours. (Note that, here and in the preceding levels, individual screen types are applied only to pertinent part classes.) The use of Level A parts has been estimated to yield equipment MTBF approximately FIFTEEN times better than that of similar commercial equipment.

CHAPTER 2. FAA RELIABILITY TASKS IN PROCUREMENTS

SECTION 1. RELIABILITY GOALS AND REQUIREMENTS

9. GOALS vs. REQUIREMENTS. For purposes of the following, an effectiveness goal is the effectiveness (measured in terms of availability and/or reliability) needed to fulfill functional requirements in the overall system context. Here, "system" refers to the total National Airspace System (NAS). A reliability requirement, on the other hand, is the contractual reliability required of implementing hardware or functions within the NAS. The reliability requirement does consider factors outside of the system itself.

   a. A contractual reliability requirement should always be based on a previously determined effectiveness goal. Conversely, the goals related to a specific unit or equipment may be influenced by the reliability achieved for other units of the NAS system. Thus, the degree to which a particular unit's requirements are actually fulfilled will affect the goals related to other system units. Goals must therefore be considered as a dynamic set of figures. In the early stages of system evolution, goals can be very volatile - changing as reliability requirements are exceeded or not met; and as system mission and/or needs change, or are redefined. Requirements, on the other hand, are fixed over the course of a contracted effort.

   b. A generalized procedure for establishing reliability requirements for procurement packages is given in the following two paragraphs. The first stage is to establish the effectiveness goals as needed for the NAS functions. At this point, factors outside of the NAS itself are not considered. The second stage is to establish the reliability requirements for the specific implementing hardware or function.

10. ESTABLISHING GOALS FOR THE NAS FUNCTIONS. The following procedure is directed toward establishing effectiveness goals for the NAS functions. Effectiveness is measured in terms of Availability and/or Reliability. Ideally, the procedural steps should be applied to the NAS system as a whole. However, the procedure can be applied to consider only the NAS functions and interfaces specific to a particular intended development and/or procurement. The former procedure application is particularly applicable to the development and/or procurement which involves the definition of new NAS functions. The latter, limited procedure application would be

applicable to the procurement which involves the upgrading of an existing function.

a. Step 1 - Develop a Functional Block Diagram of the NAS. The intent of the diagram is to define the "total" system into which the new developments/procurements are to be integrated. First, define the elemental NAS functions required for the NAS to fulfill its assigned missions. The function description shall define the type of data, information, or control being handled; and shall encompass data acquisition, transmission, processing, and handling. Then, define the major subsystem elements involved in the performance of these functions. With these elements and functions defined, construct a block diagram which depicts the functional relationships of the major NAS elements. To limit the complexity of the diagram, use typical elements or classes of elements wherever possible. Be careful, however, to always define the "class" or the criteria for being considered "typical". For example, use Airport Terminal Classes instead of terminals at specific locations.

b. Step 2 - Establish the NAS System "Use Environment". Define the traffic conditions within which the NAS system must function. The air traffic density at the various points of the system (Terminals, ARTCC's, Flight Service Stations, etc.) must be established. Then define the significantly different aircraft types to be encountered. These are "different" in the sense of requiring significantly distinct services and/or imposing significantly distinct system restrictions. Some of the characteristics for defining significantly different aircraft are: speed differences, VSTOL vs. Normal Take-Off/Landing, and Commercial vs. Private vs. Military. This "use environment" may be structured into a matrix giving the density of a particular aircraft type to be expected at a particular system point.

c. Step 3 - Define the "Operations Profile" for the NAS Elements. Define the operational events occurring at the NAS elements. Structure these into an "operations profile" which delineates the sequence and duration of the events. Relate the operations events to the aircraft movement events which either initiated the operation or resulted from it. In as much as possible, also define the relationship between operations profiles of different NAS elements. When done manually, the operations

profiles are developed by following the movement and control of one aircraft at a time. In a computer simulation of the NAS system, the operations profiles would be based on "real-world" air traffic movement problems.

d. Step 4 - Define Function Performance Levels. Define the performance characteristics of each of the subsystem functions. These shall be of the level necessary to define functional failures and/or degraded performance levels. The more characteristics used, the more realistic will be the definition of function performance. On the other hand, the number of characteristics must be limited to keep the problem at a manageable level. For example, if establishment of the goals is to be accomplished manually, it may be adequate to use only range as the performance characteristic for radar surveillance data acquisition; and capacity as the performance characteristic to describe the control radar function. In a computer simulation of the NAS system, more characteristics can be used. For example, the performance characteristics for the control radar function could be expanded to include range, accuracy, and capacity. Assign units of measure to each of the performance characteristics used. Where a computer simulation is not available, the units may simply be in terms of percent of "full-up" performance. On the other hand, in a computer simulation of the NAS system, specific parameters should be used. In addition to defining "full-up" performance, degraded levels should be defined and associated with degree of acceptability. It is not necessary that the degree of acceptability be defined in an absolute sense. It is only necessary that the degree of acceptability defined for one function be relatively the same as defined for other functions.

e. Step 5 - Determine Manned-or-Unmanned Status of Functions. Categorize the functions as to Manned, Unmanned, or Manned/Unmanned. A manned function is always performed at, or by, a manned facility; and/or maintenance is available on an essentially "as required" basis. An unmanned function is always performed at, or by, an unmanned facility; maintenance is not available "as required"; and maintenance is available on only a "time-scheduled" basis. A manned/unmanned function is performed at, or by, both facilities of the "manned" category and facilities of the "unmanned" category.

f. Step 6 - Determine the Effectiveness of Functions Already Implemented. Determine the "a priori" effectiveness of functions implemented only as a contract for hardware; as well as functions implemented in actual field operation.

(1) For functions of the unmanned category, use Reliability as the effectiveness measure. Reliability is the probability of successful operation, over a given period of time. Specifically, the "time" is the period between maintenance visits.

(2) For functions of the manned category, use Operational Availability as the measure of effectiveness. Operational Availability is a function of MTBF and MDT; where the "down time" considered includes logistic and administrative delays in addition to the active repair time.

(3) For functions of the manned/unmanned category, use both measures of effectiveness. A later step will evaluate which measure presents the more severe reliability requirement.

g. Step 7 - Determine Preliminary Effectiveness Goals for the NAS Functions.

(1) Based on the criticality of the functions, and acceptable probabilities of failure (or required probabilities of success), assign preliminary effectiveness goals to all NAS functions. This initial assignment of goals does not consider whether or not the function is already implemented; nor, does it yet take into account the effectiveness achievements defined in the preceding step.

(2) Costs will ultimately also have to be considered in the assignment of effectiveness goals (leading to reliability requirements). Generally, increased effectiveness goals mean increased costs for development, procurement, and support related to the function implementation. From the cost-effective viewpoint, then, this is probably the most significant point in the evolution of a new development and/or procurement. It is therefore extremely important that the assigned effectiveness goal be no greater than DICTATED by function criticality.

h. Step 8 - Adjust Preliminary goals to Account for Achieved Effectiveness. Compare the preliminary Effectiveness goals (determined in Step 7) against the Effectiveness of the implemented functions (Step 6) to determine whether or not goal adjustment is necessary or desirable. The determination is broken down into four basic cases to consider.

(1) Case 1 - Effectiveness of Implemented Function GREATER than Preliminary Assigned Goal; and Function NOT PERFORMED by Procurement or Development being Considered. Review the preliminary goals to determine if the goals of other functions (particularly the ones of immediate concern) can be reduced because of the greater effectiveness of the implemented function. If they can, adjust all goals accordingly. If the other goals cannot be lowered, do not change ANY goals - including the one with a proven higher effectiveness.

(2) Case 2 - Effectiveness of Implemented Function GREATER than Preliminary Assigned Goal; and Function IS PERFORMED by Procurement or Development being Considered. Review the preliminary goals to determine if the goals of the other functions can be reduced as a result. If they can, replace the preliminary goal of the function of immediate concern with the proven, higher value; and adjust the other goals to correspond. If the other goals cannot be lowered, make NO goal changes.

(3) Case 3 - Effectiveness of Implemented Function LOWER than Preliminary Assigned Goal; and Function NOT PERFORMED by Procurement or Development being Considered. Review the preliminary goals to determine if the lower Effectiveness can be compensated for by increased goals for the other functions (particularly the ones of immediate concern). If they can compensate, adjust all goals accordingly (this increases the goal for the function of immediate concern). If compensation cannot be achieved, retain the preliminary assigned goals; and flag (for special attention) the function whose implementation yields an Effectiveness lower than the goal.

(4) Case 4 - Effectiveness of Implemented Function LOWER than Preliminary Assigned Goal; and Function IS PERFORMED by Procurement or Development being Considered. In this case, make no changes in any of the preliminary assigned Effectiveness goals.

11. ESTABLISHING RELIABILITY REQUIREMENTS FOR THE NEW EQUIPMENT. The following procedure is directed toward establishing the reliability requirements for new hardware developments and/or procurements. The previously established NAS function definitions and effectiveness goals are used as a starting point. The intent of the following steps is to then translate this starting point into reliability requirements for procurement packages - with the reliability requirement stated in terms of Mean-Time-Between-Failure or Failure Rate.

a. Step 1 - Develop Functional Block Diagram for the New Equipments. Construct a block diagram which depicts the functional relationships of the major elements of the equipment set under consideration. The diagram must clearly define the elements involved in the NAS functions being implemented. Major interfaces with the NAS System must be defined. The level of the diagram will depend on the amount of information available and/or the stage of equipment evolution. Thus, for new developments, the diagram can only indicate a conceptual design. To the extent possible, the conceptual design should be so structured that the elements can be related to similar equipments. Also to the maximum extent possible, the diagram should be so structured that the major functions are performed by independent sets of blocks. Where applicable, the procurement and/or contract packages must be indicated on the diagram. Finally, identify the Effectiveness goals previously defined for the NAS functions implemented by the equipment.

b. Step 2 - Define the Operation Profile and Operating Modes. Based on the previously established "Operations Profile" for NAS Elements (a. of paragraph 12.), define the operation profile for the equipments under consideration. Define the significant operating modes for the total equipment set and relate these to the NAS functions implemented. Also define these operating modes per procurement or contract package. The number of operating modes will depend on the functional (as opposed to hardware) complexity of the system formed

by the equipment set. For example, a basic transceiver will have transmit, receive, and stand-by modes. The last mode, however, is not significant. A basic receiver will only have one operating mode.

c. Step 3 - Define Operating Mode Performance Levels. Define the performance characteristics of each of the operating modes. Assign units of measure to each of the characteristics. To the extent that information is available, use specific parameters as the units of measure. Where such information is not yet available, the measure may simply be percent of "full-up" operating mode. In terms of these performance characteristics and units of measure, define the "fully operational" operating modes; and, where applicable, the definable degraded levels of operation. These are then used to define a failed equipment or system and/or acceptable levels of degradation.

d. Step 4 - Construct a Reliability Block Diagram. Construct a reliability block diagram which relates each of the operating modes to the reliability-effect of the equipment elements. The diagram must define all existing or planned redundancies. And, where applicable, acceptable degraded performance levels must be relatable to the reliability block diagram. Structure the diagram so that the procurement or contract packages are readily separable in terms of reliability. To enable ultimate estimation of the feasibility of reliability requirements, structure the diagram with blocks for which similar equipments can be defined.

e. Step 5 - Establish the Use and Maintenance Environment. Define the use and maintenance environment for the packages of the new equipment. To assist in defining operational down time resulting from corrective maintenance, the environment description should define spares policies and locations, administrative failure procedures, test equipment availability, skill/training levels, and any other factors contributing to logistics/administrative delays. Also, the environment description must define the maintenance policies which contribute directly to effective reliability. For example, the reliability of a unit in the unmanned category is a direct function of the period between maintenance visits. Where an equipment or system involves redundant elements, it is significant to effective reliability

that repair action starts as soon as an element fails; or repair action starts only when the function of the combination fails. Where the equipment definition involves acceptable degraded performance levels, it is important to establish maintenance policies relative to performance levels: 1) Shall repair wait for scheduled maintenance as long as some acceptable performance level remains; 2) Is immediate repair initiated while operating in a degraded mode; or, 3) Does repair action start only when some unacceptable performance level is reached, at which point the system is shut down.

f. Step 6 - Derive the Mathematical Models. For each of the procurement or contract packages, derive the mathematical equations (models) which relate the over-all reliability in each mode to the reliability of the equipment elements. Where acceptable degraded levels are involved, the equations must define the reliability at these levels. Where applicable, the effect of the maintenance policies defined in the previous step must be included in the mathematical models.

g. Step 7 - Establish "Similar Equipment" Reliability for the New Equipment Packages. Select and define similar equipments for each of the Reliability Block Diagram elements. These are selected on the basis of similarity in function, operating modes, use or application, and type of design and/or construction. Assuming an arbitrary, but defined, level of reliability program, determine or estimate the failure rates of the similar equipments. Adjust this value for estimated complexity differences. Where the similar equipment is of a lower "state-of-the-art" than planned for the new equipments, the failure rate of the similar equipment is adjusted by an estimated "state-of-the-art" improvement factor. Using these adjusted, "similar" failure rates in the Mathematical Models (Step 6), establish the similar-equipment failure rates for the new equipment packages.

h. Step 8 - Establish Reliability Requirements for New Equipment Packages.

(1) Where the system function of the new equipment set is of the unmanned category (per e. of paragraph 12.), the effectiveness goal was established in terms of reliability over the period between "maintenance visits". Define the required or expected interval between mainten-

ance visits (where there is some question, use the greater interval). Translate this into a failure rate goal. Maintaining the same relative failure rates established in the previous step, allocate the failure rate goal to the new equipment packages. Pending possible readjustment by the next step, these are the reliability requirements.

(2) For equipment sets in the manned category, the function goals were established in terms of Operational Availability. Based on environment, maintenance policies (Step 5), and "use environment" experience, estimate an average Down Time due to logistic/ administrative delays (but not including the active repair times). Taking this value, together with a required MTTR or a similar equipment estimate of MTTR, translate the Operational Availability goal into a failure rate goal. As before, allocate this into failure rate requirements for the new equipment packages.

(3) For equipment sets of the manned/unmanned category, determine failure rate requirements through both of the above approaches. Select the lower value as the actual failure rate requirement.

i. Step 9 - Review the Reliability Requirements for Feasibility. Compare the failure rate requirements established in the previous step with the similar-equipment failure rates determined in Step 7. For each package, calculate an improvement factor by taking the ratio of the Similar-Equipment-Failure-Rate to the Failure-Rate-Requirement. Based on the histories of previous equipment developments and expected "state-of-the-art" improvements, evaluate the feasibility of achieving the improvement factor. The evaluation may be organized into the following four levels of feasibility.

(1) Level 1 - Practical. This level of feasibility would require only a nominal reliability program applied to conventional design approaches.

(2) Level 2 - Practical/Conditional. This would apply to an improvement factor somewhat above that for a "Practical" level. This level of feasibility would require a rigorous reliability program applied to conventional design approaches.

requirement, care should be taken to unambiguously state the requirements as the "specified MTBF" (which becomes the parameter θ demonstration test specification); and NOT AS THE MINIMUM ACCEPTABLE (which becomes the test parameter θ). In the procurement of complex equipment, and/or where it is necessary to control the reliability of individual functions of the equipment, it may be necessary to impose distinctly specified MTBF's for the different portions of the equipment being procured.

a. Definition of Failure. The "failure" to which the specified MTBF applies should be clearly stated. This is important to avoid any confusion when redundancy is involved in the equipment design.

b. Statement of Conditions. It is important that the performance specification contain a clear statement of the operating environment under which the specified MTBF must be achieved. This would include a statement of temperatures, humidities, other significant climatic conditions, and the type of installation (such as fixed ground, mobile ground, or airborne). This statement of conditions (for the specified MTBF) should also include specification of the required and/or allowed preventive maintenance and/or periodic replacement or refurbishment (of wear-out items).

c. Special Considerations for Redundancy. For reliability control, the specified MTBF is applied as a measure of equipment reliability with the reliability effect of any redundancy taken into consideration. For the purpose of controlling maintenance frequency, especially where extensive redundancy is planned or expected, it will also be necessary to state a specified Mean-Time-Between-Maintenance actions (MTBM). The MTBM counts ALL component failures, whether or not an equipment performance failure is caused. Where specific redundancy is specified for the equipment, it should also be stated whether or not the redundancy is considered "repairable" for purposes of defining the "specified" MTBF.

14. SPECIFICATION OF THE RELIABILITY PROGRAM. It is essential that equipment programs provide adequate reliability control and monitoring prior to the operational phase. At that point, it is usually too late to make modifications for reliability improvement. To exercise some control of the reliability effort to be performed in a contract, a required reliability program

should be specified in the procurement documentation. The FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT, contains a "shopping list" of program elements. Any needed program can be formulated and imposed by specifying the specific paragraphs of this Specification as program requirements. The RELIABILITY PROGRAM Specification (and Table 1 of this Handbook) contains a set of five "standard" reliability programs applicable to study, development, prototype, and production contracts. A standard reliability program is imposed by simply specifying the identifying number of the program as listed in paragraph 3.3.2.3 of the FAA RELIABILITY PROGRAM Specification (and in Table 1 of this Handbook). Paragraph 2 of this Handbook discusses the contract applicability of these "standard" reliability programs; and the selection of "non-standard" reliability programs.

15. SELECTION AND SPECIFICATION OF THE RELIABILITY DEMONSTRATION TEST. Reliability Demonstration testing of an equipment involves an evaluation of its reliability under specified conditions. Two types of risks are necessarily always involved in any demonstration or acceptance test plan. (The test "plan" defines the accept-reject criteria.) One of these is the risk of rejecting an acceptable equipment - the "producer's" risk. The other is the risk of accepting an actually unacceptable equipment - the "consumer's" risk. The following subparagraphs will present the basic procedure for selecting a test; and, a discussion of the requirements for the specification of a demonstration test. The selection of the demonstration test shall be made by the responsible FAA engineer. It shall be included in the procurement specification as one of the test requirements in the quality assurance section of the document.

a. The Sequential Test Plan. In the sequential reliability test, a decision to accept or reject (or continue) is made at the detection of each failure. In a fixed-time test, on the other hand, the equipment must operate for a pre-determined time before any decision can be made. Under a sequential test plan, a good product is generally accepted quickly and a poor product is generally rejected quickly; while a questionable product may require longer test time than with other plans. On the average, however, the sequential demonstration (acceptance) test requires less time than under other types of test plan. The sequential test does, however, have the disadvantage that the exact length

of the test cannot be predetermined. An expected, or average, test time can be computed.

b. Selection of the Required Test. The required test plan, and the "level" at which it is to be performed, is normally selected from MIL-STD-781, RELIABILITY TESTS: EXPONENTIAL DISTRIBUTION. The following are the steps necessary in this selection.

(1) Define the "Acceptable" and "Unacceptable" MTBF's for the Test. The nominally acceptable MTBF is denoted by θ_0 . This is the specified MTBF, and is normally the same value stated as a performance requirement. The unacceptable range of MTBF's is defined by selecting a minimum acceptable MTBF (denoted by θ_1). These values determine the "discrimination ratio" (θ_0/θ_1) required of the test plan.

(2) Define the Allowable "Risks". A determination must be made of the allowable, or acceptable, risks - both the producer's risk and the consumer's risk.

(a) The Producer's Risk (denoted by α) is the probability (normally stated in percent terms) of rejecting an equipment whose true MTBF is actually equal to the specified MTBF (θ_0). This is the risk taken by the contractor when he submits his product to the acceptance (demonstration) test.

(b) The Consumer's Risk (denoted by β) is the probability of accepting an equipment with a true MTBF equal to the minimum acceptable MTBF (θ_1). This is the risk taken by the customer, the FAA in this instance, when it determines product accep tability on the basis of an acceptance test.

(c) MIL-STD-781 risks are either 10%, 20%, or 30%; except for one short-run, high-risk test. Also, most of the test plans given are for equal risks to both producer and consumer.

(3) Select the Test Plan. The test "plan" is simply a statement of the accept and reject boundaries in terms of the cumulative test time and accumulated failures. Although this can be done graphically, a tabular presentation is preferable. The discrimination ratio determined

in (1) above and the risks determined in (2) define the test plan. These parameters are used to select the appropriate test plan from MIL-STD-781.

(4) Select the Required Test "Level". The test "level" is defined as the conditions of temperature, temperature cycling, vibration, vibration cycling, on-off cycling, and/or input-voltage cycling to be applied to the equipment during the demonstration test. MIL-STD-781 gives ten basic test levels. The least stringent of these, level A-1, operates with the equipment in an ambient temperature of 25°C and input-voltage cycling allowed. The most severe test level given by MIL-STD-781 is level J, which requires temperature cycling between -54°C and +125 C, vibration and vibration cycling with peak acceleration of 2.2G, on-off cycling, and input-voltage cycling. The test level should be selected to be as representative of expected operating conditions as possible. (It will usually be found necessary or desirable to modify the test levels of MIL-STD-781.)

c. Specification of the Required Test. In establishing the detailed specification of the required demonstration test, consideration must be given to the requirements for each of the following elements.

(1) Definition of the Basic Test Requirement. The required test plan, per the preceding is normally selected from MIL-STD-781; and the selection must be so stated. In special circumstances, only the consumer's risk (β) may be stated, with the required θ_0 and θ_1. The contractor would then be free to select his producer's risk (α); and to propose a test plan selected on that basis. The required test level, per the preceding, must also be specified as part of the basic requirement.

(2) Definition of the Test Subject. The allowed and/or required configuration of the test article must be defined. Where the procurement involves multiples of the contract item, the specific equipment(s) to be tested must be clearly identified.

(3) Pre-requisites for Entering the Demonstration Test Phase. All pre-requisites required by the FAA must be explicitly stated as such. For example, it should be stated that Demonstration Test Procedures must be submitted and APPROVED before performing the test. Normally, an acceptable prediction of meeting the specified MTBF is also specified as a pre-requisite to entering the Demonstration phase of the procurement. The contractor is normally allowed to operate, or "burn-in", the equipment before entering the demonstration test. If so, it must then be required that the same degree of "burn-in" be performed on all equipments delivered under the contract.

(4) Basic Test Performance Conditions. The specification of the demonstration test must be unambiguous with respect to the basic conditions under which the test is to be performed. At least the following should be considered.

(a) When a "duty cycle" is part of the equipment performance specification, the demonstration test specification must clearly state whether or not the duty cycle is allowed; and if the latter, at what specific levels for what times must the equipment operate. Similarly, where the equipment has multiple operating modes, the demonstration test specification must specify the mode or modes (with relative "on" times) to be used during the test.

(b) Any required deviations from the standard procedures of MIL-STD-781 must be clearly stated - for example, the specific method of temperature cycling. In the specification of the demonstration test as a selection from MIL-STD-781, care must be taken that undesired portions of the Standard are not inadvertently imposed.

(c) Monitoring requirements should be specified. These should take into account the periodicity of performance monitoring and a definition of the performance parameters to be monitored. The latter may take the form of "sufficient to assure that all performance specifications are met", allowing the contractor to propose the specific monitoring points.

(d) Maintenance allowed during the demonstration test must be defined. This should take into consideration both corrective and preventive maintenance, with special attention to the latter.

(5) Test Relevancy Definitions. It is especially critical that test-relevant failures be clearly and unambiguously defined. This should include a statement of the basic procedure for adjudication of questionable failures. The imposition of paragraph 3.7.4.1, Definition of Failure, of the FAA RELIABILITY PROGRAM REQUIREMENTS Specification, is generally adequate for defining relevant failures. However, if possible, it is preferable that the definitions of test-relevant failures be specific to the equipment under procurement. As part of the "relevancy" specification, relevant test time (i.e., equipment time counted in the cumulative test time) must also be defined. This definitization of failures shall be defined in the reliability demonstration plan, a document normally requiring FAA approval.

16. ESTABLISHING THE REQUIRED DELIVERABLE DOCUMENTATION. The delivery of SELECTED documentation is essential if the FAA is to effectively monitor, control, support, and coordinate the contract reliability effort.

a. Basic Guidelines for Specification of Data Requirements. The following are some basic guidelines for the specification of required documentation and/or data.

(1) Data requirements should only DOCUMENT reliability engineering and analysis tasks; and should NOT GENERATE, such tasks.

(2) Only essential, COST-EFFECTIVE documentation should be required.

(3) Avoid OVERLAPPING or DUPLICATE documentation of the same data.

(4) For follow-on contracts, specify only the ADDITIONAL data required.

(5) Consider the acceptability of data obtained and prepared according to the contractor's NORMAL INTERNAL practices and procedures, in lieu of a

formal data item. This would tend to keep data costs down.

(6) If the documentation delivery DATE cannot be firmly established, key the delivery requirement to a contract event MILESTONE.

(7) Use a standard DATA ITEM DESCRIPTION form from Appendix 3 to define the formal, deliverable data requirement.

b. The Data Item Description (DID). A standard Data Item Description (DID) form is used to define the specific, formally required, data items. This form is used for the data items defined in Appendix 3.

c. Standard Data Items. Certain items of data will be required on most contracts. Others will always be required in particular types of contracts. These should be considered as Standard Data Items. It is desirable that a Standard DID be developed for each of the Standard Data Items. The procurement documentation may then impose the entire DID (by title and number); or, the requirement may be restricted to only particular, specifically-designated, paragraphs of the PREPARATION INSTRUCTIONS section. Thirteen such Standard DIDs, pertinent to a required reliability program, are given in Appendix 3. These Standard DIDs are sufficient to define the deliverable data requirements for most reliability programs. The thirteen Standard DIDs are also listed in Table 3 by Title and Number.

(1) Contract Applicability. Table 3 indicates the type of contract to which each of the DIDs is applicable. "Applicable" does not mean "required". When a particular type of contract is encountered, the "applicable" DIDs should be considered for specific suitability to the particular contract. Where none of the Standard DIDs are adequate to obtain the desired data, a custom DID will have to be written. Custom, contract-unique, DIDs should be kept to a minimum; since their use tends to increase data management costs in the FAA.

(2) Data Delivery. Table 3 also lists a suggested delivery schedule for each of the standard DIDs. Specific, required schedules obviously could not be given. The required schedules actually imposed will vary with the length of the

contract, complexity of the equipment, feasibility of the reliability requirement, equipment delivery schedules, etc.

SECTION 3. FAA POST CONTRACT AWARD ACTIVITY

17. FAA CONTRACT ACTIVITY OBJECTIVES. The ultimate objective of all FAA activity during the course of a contract is to assure the receiving of a product which meets specifications - and within schedule and cost limits. And, the ultimate objective of FAA Reliability activity is the assurance that the product received will meet the reliability performance requirements. The FAA activity required in a contract reliability program may be defined in terms of five basic task objectives for that activity. These basic objectives are listed in the following.

    a. Verification that the required reliability program TASKS are PERFORMED.

    b. Verification of, and guidance for, appropriate and adequate DIRECTION and EMPHASIS of the reliability effort.

    c. Assurance (through monitoring and guidance) that the reliability requirement is treated as a DESIGN PARAMETER.

    d. Detection of ADVERSE failure and/or design TRENDS, or other problems, which may prevent achievement of the required reliability.

    e. Monitoring of the equipment RELIABILITY "GROWTH" from initial prediction through the reliability demonstration test.

18. MONITORING THE CONTRACTOR RELIABILITY PROGRAM. Formal communication, including the delivery of contractual documentation, between the FAA and the contractor is necessary; but, it alone certainly does not provide adequate monitoring of the contractor's reliability effort. An effective monitoring effort must provide for active design review participation; at-contractor-site review and inspection; and person-to-person interchanges between working-level contractor engineers and their FAA counterparts. The establishment of an active, working-level, interface should lead to best efforts on the part of the contractor; and to thorough understanding of the problems on the part of the FAA. The following subparagraphs discuss the requirements for effective implementation of the basic elements of a program monitoring effort.

a. Establish the FAA-Contractor Interface. The required reliability program, formal reviews, and documentation, together with the proposed program plan, constitute only the formal, legal interface between FAA and the contractor. As was pointed out in the previous paragraph, total reliance on just this interface is not advised. For the monitoring effort to be effective, a working, person-to-person, interface must be firmly established. The first step is to define the FAA Office(s) of Primary Responsibility (OPR) and identify the specific FAA Reliability Monitor(s). This should be accomplished before Contract Award. It would also be desirable that the FAA Monitor (to be) participate in the selection of the required reliability program. Then, shortly after contract award (and preferably within 30 days), the FAA Monitor should schedule and conduct a RELIABILITY INTERFACE meeting with the contractor - preferably at the contractor site. The only objective of the meeting should be to establish the needed working, person-to-person, interface between FAA and Contractor. The interface meeting should not be restricted to simply a formal discussion between the FAA Monitor and the Contractor's Reliability Manager. Working-level reliability personnel, from both sides, should also participate. This interface meeting should present, consider, and/or agree on at least the following items.

(1) FAA Personnel. Identify the pertinent FAA OPR's and the assigned FAA Monitor(s) - all monitors should be present. All FAA personnel directly supporting the Monitor should also be identified; and, as many of these as possible should be in attendance.

(2) Contract Requirements. Establish agreement on all contract requirements relating to reliability.

(3) Over-all Program. The over-all program milestones and/or schedules should be agreed upon; and the principal OPR's should be identified.

(4) Reliability Program Plan. Reaffirm, and clarify where needed, the proposed program plan. Define the contractor OPR's for each reliability task. Define the schedule, task, and personnel interface of the reliability program with the over-all program.

(5) Data Items. Define the specific data and/or information expected in each required data item. Agree on submittal requirements.

(6) Design Reviews. Agree on the reliability-pertinent intent of each required Formal Design Review. Define the pre-Review data package needed by the FAA.

(7) Communication Channels. Establish the communication channels which will be needed to supplement the documentation and design reviews. Establish a plan for holding future, informal meetings. Define telephone, TWX, mail, and personal points of contact on both sides.

b. Monitor the Deliverable, and Received, Documentation. The delivered documentation should, of course, be monitored for quality and adherence to contractual requirements. With some of the required documentation, this is all that is pertinent to the current program - either the information is pure documentation of "minutes", or the data is intended for the FAA data base for general application. Relative to the Reliability Program, the most the monitor can hope to get from the documentation is general program progress, reliability growth, and alerts to POSSIBLE potential problems. (Documentation relative to the Demonstration tests is discussed in the following paragraph.) The report most significant to monitor the overall reliability program progress is the RELIABILITY PROGRAM STATUS REPORT (DID R-7 of Appendix 3). Reliability design growth is monitored through, primarily, the RELIABILITY ALLOCATIONS, ASSESSMENTS, AND ANALYSIS REPORT (DID R-2 of Appendix 3). The detection of failure trends and/or POTENTIAL reliability problems is assisted by the monitoring of the FAILURE SUMMARY REPORTS (DID R-4). The PARTS, MATERIALS, AND PROCESSES APPLICATION REVIEW REPORT (DID R-13) may serve to alert the Monitor to POTENTIAL part application problems. The RELIABILITY ALLOCATIONS, ASSESSMENTS, AND ANALYSIS REPORT should also be reviewed for the following, specific potential faults in analysis.

(1) Mathematical Model. Since reliability growth evaluation is based on using the mathematical model, very early evaluation should be made of the model accuracy. It is not unknown for a series model to be used even when alternate modes and/or redundant equipments exist. It is

also common for exaggerated claims to be made for the reliability of repairable redundant combinations as well as for simple series models.

(2) Reliability Predictions. In the early stages of a development, it is necessary to make many assumptions relative to stress, environment, and operation in making a reliability prediction. However, as the design progresses and as failure data is collected and presumably processed, predictions should involve fewer of these assumptions. The predictions submitted should be monitored to see that the increasing failure and stress data is incorporated. (For example, see that the indications of the FAILURE SUMMARY REPORTS are considered in the predictions.)

c. Monitor, and Participate in, the Design Reviews. The FAA Reliability Monitor should actively participate in ALL Formal Design Reviews. (Participation in the detailed design reviews which are not contractually scheduled should be limited to only selected, critical areas; and/or as requested by the contractor.) It is essential that the Monitor do his "homework" before attending the Design Review; otherwise, he could do as well by simply reading the DESIGN REVIEW REPORT (DID R-12 of Appendix 3). The "homework" involves studying the pre-review data package and the agenda, and preparing a specific checklist for things to do and things to monitor. For reliability, the basic objectives of the Design Review are to assess the design reliability growth; the observed reliability problems, their effect, and proposed corrective actions; and the potential reliability problems. The FAA Monitor should, of course, monitor these objectives and participate in their fulfillment. The Monitor will be expected to provide reliability requirements guidelines and/or interpretation. The following are specific areas of Design Review conduct that deserve special attention by the Monitor.

(1) Action Items. Verify that OPR's are assigned to all action items resulting from the Review. Response to the action items can be monitored through the RELIABILITY PROGRAM STATUS REPORT (DID R-7), and by personal inspection.

(2) Review Preparation. Verify that participants are prepared for the Review; and, do in fact conduct a genuine engineering effort. (The danger to be avoided is that of having a Review which is, in effect, only a reading of a Program Status Report.)

d. Monitor the Program Effort Directly, at the Contractor Site. The general, broad objectives of the informal, on-site, monitoring are to validate the submitted documentation; evaluate actual implementation of the reliability program tasks; and provide direct, specific guidance. The intent is NOT to replace, or assist, contractor management. The Monitor should be careful to avoid interference with satisfactory program progress. The monitoring methods should include informal meetings (similar to the interface meeting of preceding sub-paragraph a.); direct interchange with working-level reliability and design engineers; and personal inspection of practices, procedures, and raw data. The following are the areas which should be given special attention in the on-site monitoring effort.

(1) Documentation Follow-Up. Resolve the ambiguities, errors, and/or otherwise questionable data turned up in monitoring documentation. Monitor action on indicated problems, and verify corrective actions.

(2) Design Review Follow-Up. Verify the resolution of action items resulting from the Design Reviews. This will probably have to be done on a selective basis, concentrating on only critical action items.

(3) Reliability-Design Interface. Verify that the communication between the Reliability Engineers and Design Engineers is adequate and responsive on both sides. This is necessary to assuring that reliability is treated as a design parameter; and that reliability assessments are up-to-date with respect to design and observed failures.

(4) Engineering Design Changes. Verify that all engineering design changes receive adequate reliability review; and that the changes are reflected in the reliability predictions.

(5) Failure Reporting, Analysis, and Corrective Action. To ensure the usefulness of the Failure Summary Reports, make an early evaluation of the Failure Reporting System and its actual use. Verify the adequacy of the Failure Analysis facilities and their use. Evaluate the effectiveness of the actual Corrective Action Procedures. Verify that the reliability predictions reflect the information gained from the failure reporting.

19. MONITORING THE RELIABILITY DEMONSTRATION TEST. The Demonstration Test monitoring effort has three distinct phases for the FAA Monitor: Plans and Procedures review, Test conduct, and Report evaluation.

a. Plan and Procedure. Review and approval of the submitted DEMONSTRATION PLAN (per DID R-5 of Appendix 3) and TEST PROCEDURE (per DID R-6) is the first step in the demonstration test monitoring effort. The PLAN is reviewed to verify that the specified demonstration requirements will be fulfilled. And the PROCEDURE is reviewed to verify that specific procedures do not invalidate the demonstration; and, that the detail is sufficient to allow total test repeatability from any point; and, that data collection is appropriate to the accept/reject criteria. In both PLAN and PROCEDURE, special attention should be paid to the acceptability of the relevant failure and relevant time definitions and adjudication procedures.

b. Test Conduct. During the conduct of the test, the basic function of the FAA Monitor is to ensure that both the approved Reliability Demonstration Plan and the Reliability Test Procedure are followed.

(1) Pre-Performance. Prior to actual test performance, the monitor should determine the pre-test operation or "burn-in" that was applied to the test specimen. (He must later verify that the same "burn-in" is applied to all delivered equipments.) Then, the monitor should verify that the test configuration and conditions are as defined in the accepted TEST PROCEDURE.

(2) Test Performance. During actual test performance, the implemented procedures are monitored to ensure that they do not deviate from the accepted PROCEDURE. Any such deviation requested must be reviewed and approved by the FAA Monitor. During test performance,

particular attention should be paid to failure detection and verification procedures, integrity of the elapsed-time metering and subsequent documentation, and accuracy of the test log in general. The Monitor must also review and approve all failure and test time relevancy decisions; corrective actions; and all test logs. He may also be called upon to decide whether or not to allow the test to continue on the basis of a PROPOSED corrective action; and then not counting failures which would (supposedly) be eliminated by the proposed action. From the FAA standpoint, the preferable decision should be that if the test continues, all relevant failures will count; but the contractor should be given the option to stop the test while corrective action is implemented. (The acceptance of the effectiveness of a PROPOSED corrective action is always questionable.) Finally, the FAA monitor must review and approve all test continuance decisions related to the ACCEPT/REJECT criteria (which at this point only indicate whether the test was passed or failed).

c. Test Report. The test report summarizes the test data and indicated results. The Monitor should first verify the accuracy of the contained data - comparing with the direct observations. The validity of any analysis and the conclusions must be assessed. Where more than one test is involved in the demonstration required for acceptance, the ACCEPTANCE decision must await the final report. Where a REJECT decision is reached, it may in some very rare cases be possible to ACCEPT on the basis of proposed corrective action, and verification of the efficacy of the correction. (Any corrective actions must be retrofitted into all equipments delivered under the contract, but prior to the demonstration.)

CHAPTER 3. INSTRUCTIONS FOR CONTRACTOR IMPLEMENTATION OF REQUIRED PROGRAM

SECTION 1. INTRODUCTION TO INSTRUCTIONS

20. THE REQUIRED PROGRAM. The FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT, contains a series of tasks from which a reliability program shall be developed. The selected reliability program specifies which of these tasks must be performed. Normally, this will be done by requiring performance of one of the "standard" reliability programs listed in the FAA Specification. The standard program listing then indicates which FAA RELIABILITY PROGRAM Specification paragraphs are required in the specified program. Table 1 (paragraph 2) of this Handbook also gives this listing of "Standard" Reliability Programs. The required reliability program may also be specified by requiring specific paragraphs of the FAA RELIABILITY PROGRAM Specification.

21. SCOPE OF INSTRUCTIONS. The following paragraphs of this Chapter provide the basic instructions and/or guidance for implementing the required reliability program and accomplishing the required tasks. Instruction and/or guidance is given for ONLY those program efforts which are NOT self-explanatory as defined in the FAA RELIABILITY PROGRAM REQUIREMENTS Specification. Table 2 (paragraph 3) of this Handbook lists the FAA Specification paragraphs covered by this Chapter; and, provides a crossreference to the specifically applicable Handbook paragraphs. Also, the heading for each of the following instruction paragraphs is directly keyed to the FAA RELIABILITY PROGRAM REQUIREMENTS Specification - by a parenthetical number prefixed by an "S" to indicate the Specification paragraph(s) to which the instruction and/or guidance applies. The following contractor instructions are grouped into ten sections, as follows.

a. Section 2. Program Management.

b. Section 3. Reliability Analysis.

c. Section 4. Parts, Assemblies, Materials, and Processes.

d. Section 5. Failure Mode and Effect Analysis, and Critical Items.

e. Section 6. Design Reviews.

f. Section 7. Effects of Storage, Shelf-Life, Packaging, Transportation, Handling, and Maintenance.

g. Section 8. Design Specification, Drawing Release, and Design Changes.

h. Section 9. Reliability Testing.

i. Section 10. Failure Data Collection, Analysis, and Corrective Action.

j. Section 11. Documentation and Data Requirements.

SECTION 2. PROGRAM MANAGEMENT

22. THE PROGRAM PLAN (S3.4.1.1). A detailed, complete program plan is essential to the effective management of a reliability program. Submittal to the FAA of the documented plan, per RELIABILITY PROGRAM PLAN (DID R-1 of Appendix 3), is intended to indicate understanding of the required program and intent to provide it.

a. Submittal Requirements. A preliminary reliability program plan is generally submitted to the FAA as part of the contractor's proposal. The proposed plan is reviewed with, or by, the assigned FAA monitor. A final reliability program plan shall then be submitted as soon as possible after contract award (at least, within 25 working days). A program plan, that has been approved and accepted by the FAA, has the effect of a contractual document. Any desired significant changes in the approved plan must be submitted to the FAA as distinct documents in a request for approval. Minor changes may be indicated in the periodically submitted PROGRAM STATUS REPORTS (DID R-7 of Appendix 3).

b. Basic Scope and Content of the Documented Plan. The MINIMUM scope of the program plan is defined by the required program specified by the FAA. The scope of the program in the documented program plan, however, must be sufficient to fulfill the basic Reliability requirement and demonstration. The detail in the plan must be sufficient to indicate an understanding of the problem(s) in design reliability. Specifically required program plan elements are adequately defined in paragraph 3.4.1.1 of the FAA RELIABILITY PROGRAM REQUIREMENTS Specification; and in the Data Item Description, RELIABILITY PROGRAM PLAN (DID R-1 of Appendix 3). In summary, the documented program plan must provide the following basic elements.

(1) Tasks or work elements to be accomplished; which must include the specified program elements and any other tasks that will be required to meet the Reliability performance requirements.

(2) Task description of the work to be accomplished under each task. This shall include purpose, methods, and expected results for each task.

(3) Time-phasing for each task. This shall be related to the time-phasing for the overall program.

(4) Man-loading assigned to the accomplishment of each task.

(5) Appropriate program milestone and design review points shall be defined, including the reasons for the selection.

(6) Assigned Office of Primary Responsibility (OPR) for implementation of the reliability program, and for individual tasks.

c. Supplemental information. Where they are not already included in the task descriptions, the following information items should also be part of the submitted reliability program plan (by Attachment is adequate).

(1) Supplier and/or Subcontractor Control methods to be employed. This should include considerations of reliability allocations, program plan requirements, and design and/or program reviews.

(2) Specific Reliability prediction techniques to be used. In addition to the analysis and modeling methods, this should also include a discussion of the forms used and the processing methods.

(3) Specific Reliability allocation techniques to be used for apportioning reliability requirements to lower elements of the contract item.

(4) Proposed Reliability Demonstration approach and methods. In addition to proposed test plans, this shall include methods of combining data where applicable.

(5) The Failure Data Collection, Analysis, and Corrective Action System (and program when such is required) should be fully described, including a description of the physical-chemical Failure Analysis capabilities.

23. SUPPLIER AND SUBCONTRACTOR CONTROL (S3.4.1.4). The achievement of a specified reliability performance level for the contract equipment requires that firm quantitative reliability performance levels be established for all supplier and/or subcontractor provided items. It is therefore necessary that the contractor impose, directly or indirectly, quantitative reliability requirements, program, and/or acceptance criteria on all levels of suppliers. An example of indirect imposition would be the selection of parts on the basis of their "a-priori"

established reliability levels. Specific supplier or subcontractor reliability control requirements cannot be established to apply to all cases. The following will discuss the general control requirements for "suppliers" as a class, and for "subcontractors" as a class.

a. Suppliers. A supplier may be defined as a source for parts, components, or items the procurement of which does not involve a development or design effort. A Reliability program is generally not explicitly imposed on this supplier. At one end of the procurement spectrum, the maximum failure rate of the item, without special controls, is known from experience; and is acceptable to the contractor. Specifications as such may not be involved in this sort of procurement. At the next stage, reliability control consists of SELECTION of items with reliability levels already established at the required level (such as the selection of ESTABLISHED RELIABILITY resistors of the required level). Depending on the contractor's experience with the particular supplier, the contractor may require acceptance test verification of the reliability. At the other extreme, the required reliability level may be such that no existing item fulfills the requirement. In this case, a specific quantitative reliability requirement and acceptance criteria must be imposed. In extreme cases, a failure data collection, analysis, and corrective action program (with summary reports) may also be imposed as a requirement on the supplier.

b. Subcontractor. A subcontractor is defined as a source for items the delivery of which DOES involve a development or design effort. In these cases, the contractor must impose specific quantitative reliability requirements, acceptance criteria, and a suitable reliability program on the subcontractor. A specific program applicable to all cases cannot be defined - the requirement will vary as a function of the subcontract item complexity, "state-of-art", and reliability required. And, of course, whatever the specific program, its progress and implementation should be monitored by the contractor.

(1) Subcontractor Reliability Program. The Reliability Program required shall be specified by selecting the required program elements from the FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT. The FAA shall be notified of the occurrence of any formally imposed sub-

contractor design reviews. The submittal of a reliability program plan shall generally be required of the subcontractor. The contractor's documented RELIABILITY PROGRAM PLAN shall contain a full disclosure of the subcontractor reliability programs and design review points.

(2) Quantitative Reliability Requirement. The reliability performance required shall be based on an apportionment of the reliability requirement imposed on the contractor. (The contractor is required to disclose the allocation and the methods used in his submitted RELIABILITY PROGRAM PLAN.) The subcontractor's reliability requirement must be specified in the procurement documentation for the desired item. The contractor should use paragraph 15. (Specification of the Reliability Performance Requirement) of this Handbook for guidance in establishing the reliability specification.

(3) Acceptance Criteria. The contractor shall impose reliability acceptance criteria by selecting an appropriate test from MIL-STD-781, RELIABILITY TESTS: EXPONENTIAL DISTRIBUTION. The selected test and required associated conditions must then be specified in the procurement documentation. Use paragraph 17. (Selection and Specification of the Reliability Demonstration Test) of this Handbook for guidance.

(4) Documentation. When a reliability program is imposed on a subcontractor, appropriate documentation shall also be required. Use paragraph 18. (Establishing Required Deliverable Documentation) of this Handbook for guidance in defining the required Documentation. Review Appendix 3 of this Handbook for suitable Data Item Descriptions. The contractor should additionally impose the requirement that the subcontractor's submitted documentation format be compatible with that being used by the contractor.

(5) Monitoring and Control. When dealing with a subcontractor, the contractor must now act in the role of the "customer". It is essential that the reliability program be monitored and guided in direction and emphasis. The contractor should use paragraphs 19. (Activity Objectives), 20. (Monitoring Reliability Program, and 21.

(Monitoring Reliability Demonstration Test) for guidance.

24. RELIABILITY PROGRAM REVIEWS (S3.4.2). Reliability Program Reviews are NOT Design Reviews, although the two may be held concurrently. The Design Review is intended to monitor and assess the DESIGN reliability growth and problems. The Reliability Program Review is held to evaluate progress and adherence of the implemented reliability PROGRAM with respect to the program plan. The Reliability Program Review is essentially a MANAGEMENT audit of the reliability program in relation to the plan. The scope of the Reliability Program Review should be sufficiently broad to include audit of the control methods and program procedures internal to the program, not just the controls on the program plan itself. Suitable subjects for the Reliability Program Review are listed under the following sub-paragraph.

a. Subjects for Reliability Program Review. The agenda of the program review should be representative of the following subject items.

(1) Program Plan. The status of the planned program task elements should be reviewed with respect to accomplishment, schedule, and man-loading. If possible, a determination should be made of the potential effect on reliability achievement.

(2) Documentation and Data. The required Deliverable Documentation should, of course, be reviewed for quality and schedule. In addition, the distribution procedures internal to the contractor should also be reviewed for adequacy and timeliness. The review should also encompass the data items which are not deliverable; such as the internal workings of the Failure Reporting System and the Central Data File maintained for the program.

(3) Communications. The Reliability-Design interface should be reviewed in all its aspects for existence and responsiveness. The objective is to ensure that the reliability engineer gets all the design and configuration information he needs; and that reliability requirements are appropriately allocated to designers; and to ultimately ensure that the reliability performance requirement is in fact treated as a DESIGN PERFORMANCE requirement.

(4) Design Control. The review should ensure that procedures do provide that all designs and DESIGN CHANGES are reviewed for reliability and potential reliability problems.

(5) Design Reviews. Although the Program and Design Reviews may be held concurrently, the program review should ensure that all required information, data, and analysis will be prepared and available for consideration at the Design Reviews.

b. Review Conduct. Participants at the Program Reviews shall be of the management category; and shall, as a minimum, include the Reliability Program Manager, the Overall Program Manager, and the Managers of all other Discipline Programs which interface with the reliability program. An FAA representative will also attend. All participants required to be in attendance, including the FAA, shall be notified at least 10 working days in advance of the Review.

SECTION 3. RELIABILITY ANALYSIS

25. THE RELIABILITY MATHEMATICAL MODEL (S3.5.1.1 - S3.5.1.1.2). A mathematical reliability model is basically a mathematical representation of subsystem, or equipment, "success paths" which takes into account the reliability "statistics" of the system elements, redundancy between elements, and reliability-pertinent maintenance parameters. The model is then used to calculate the over-all system reliability, based on the reliability relationships of the subsystem elements.

    a. Applications. The following are the fundamental uses of the mathematical model in the reliability program.

        (1) Prediction and/or assessment of total equipment reliability.

        (2) Allocation of reliability requirements to equipment elements.

        (3) Establishing redundancy, and associated maintenance, requirements.

        (4) Monitoring total effect of reliability achievements for elements.

        (5) Critical items identification.

    b. Development of the Model. The development, or evolution, of the general mathematical model proceeds in four basic stages: 1) Definition of the FUNCTIONAL BLOCK diagram; 2) Construction of the RELIABILITY BLOCK diagram; 3) Establishment of the pertinent MAINTENANCE policies; and, 4) Establishment of the MATHEMATICAL MODEL. Simple equipments may not require that each stage be explicitly performed. However, all stages shall at least be considered in all cases. The basic requirements and/or procedures for these stages of model development are discussed in the following three paragraphs.

26. THE FUNCTIONAL AND RELIABILITY BLOCK DIAGRAMS FOR THE MATHEMATICAL MODEL (S3.5.1.1). The definition of a Functional block diagram and the definition of the Reliability block diagram are the first two steps toward the development of the mathematical model of the equipment. Their primary function is as visualization tools.

a. Definition of the Functional Block Diagram of the Equipment. The basic intent is to construct a block diagram which depicts the functional relationships between the elements of the equipment under consideration.

(1) Basic Requirements for the Definition. The diagram elements must first be selected - with the objectives being the enabling of a clear definition of the major equipment functions and operating modes. The level of these elements will clearly be a function of the data available, the complexity of the equipment or system, and/or the development stage at which the evaluation is being performed. The structure of the diagram must clearly identify all design-responsibility and procurement packages; and their functional interfaces. The diagram elements should be selected so that these "packages" use independent sets of elements. And, to the extent possible, the depicted equipment functions should also use independent sets of elements.

(2) Required Supplementary Data. In conjunction with the diagram itself, it is important that at least the following information items be determined and documented.

(a) Operations Profile and/or significant duty cycles definition.

(b) Success Criteria, including allowable or acceptable performance degradation definitions.

(c) Planned Functional Redundancies descriptions.

(d) Use environment description.

b. Definition of the Reliability Block Diagram. The reliability block diagram "pictorializes" the success paths for the operating modes of the equipment. In other words, the diagram pictures the elements REQUIRED in each operating mode.

(1) Basic Requirements for the Diagram Elements.

(a) Level and type sufficient to identify design- responsibility, procurement, and allocation "packages".

(b) Critical items should be entered with distinct, identifiable blocks.

(c) Planned redundancies, using elements defined by the above, should not be implicit in an individual block.

(d) Special Case 1. When the diagrams are to be used in predictions and/or allocations based on the reliability of similar equipments, divide the diagram into elements (within the first three basic requirements) for which similar equipments can be defined.

(e) Special Case 2. If an acceptable "a-priori" reliability prediction (or other form of assessment) exists for a group of elements, use a single block element to represent the group.

(2) Redundancy Consideration. Identify all groups of redundant elements (i.e., elements providing alternate success paths). Consideration and identification must also be given to sub-redundancies that can exist within elements of a redundant group. Define the basic redundancy "conditions" for each redundant group, or sub-group. These conditions include a definition of the number of elements AVAILABLE and the number of elements NEEDED for success. The operating state of standby elements must be defined.

(3) Structure and/or Configuration Notes.

(a) Element Description. Clearly identify each element, providing space for entry of failure rate or MTBF (and/or Reliability where applicable). For elements of a redundant group, provision should also be made for entry of the MDT (or MTTR).

(b) Organization. To the maximum extent possible, organize the block diagram in a functionally logical manner. Obviously, this will be limited by the basic requirement to demonstrate the success paths.

(c) Non-redundant Elements. Non-redundant elements are indicated by blocks connected in a "series" manner.

(d) Indicating Redundancy. The basic problem is to indicate the alternate success paths available; i.e., the alternate elements or element groups required for successful operation. This should be done graphically whenever an UNAMBIGUOUS representation is possible. When this is not possible, explanatory notation will have to be added to indicate the number of paths available and the number required; or to otherwise define the redundancy.

27. MAINTENANCE POLICIES PERTINENT TO THE MATHEMATICAL MODEL (S3.5.1.1). The next stage toward the evolution of the Mathematical Model is to define the maintenance parameters for each of the redundant groups. Maintenance policies are critical to determining the EFFECTIVE Reliability to be obtained from a group of redundant elements. The results of a mathematical model for redundant elements are only as valid as the definition of the pertinent maintenance factors. Figure 1 presents the more significant (to reliability) elements of a maintenance policy. The figure structures these elements into six possible basic policies, as described in the following.

a. Non-repairable Redundancy. Paths R-1 and R-2 contain the elements of a policy for restoring a failed system or equipment. In other words, maintenance is instituted only when the equipment FUNCTION fails.

b. Repairable Redundancy. Paths R-3 and R-4 define policies for initiating renewal of a redundant group BEFORE its function fails. Where this renewal is initiated at the first failure of an element, the essential parameter is the time (including logistics and/or administrative delays) required to repair the failed unit. In the diagram, this is indicated by MDT (Mean Down Time); which is not to be confused with MDT(system). The latter refers to time that the system FUNCTION is down; while the former refers only to down time of the UNIT while the function remains "up". In the case of renewal initiated only after the "Xth" failure, the pertinent parameter is the mean down time for the "X" failed units, MDT.

c. Scheduled Maintenance. The pertinent elements of scheduled maintenance start at point "S" in Figure 1. Generally, it is almost impossible to handle the effect of all of these details in an analytically stated mathematical model. If this is the intent, it will be adequate to simply determine the main-

tenance interval, and assume that all failed units or elements are then fully restored. On the other hand, a SIMULATION model would be able to handle all the details; and, thus provide more realistic results.

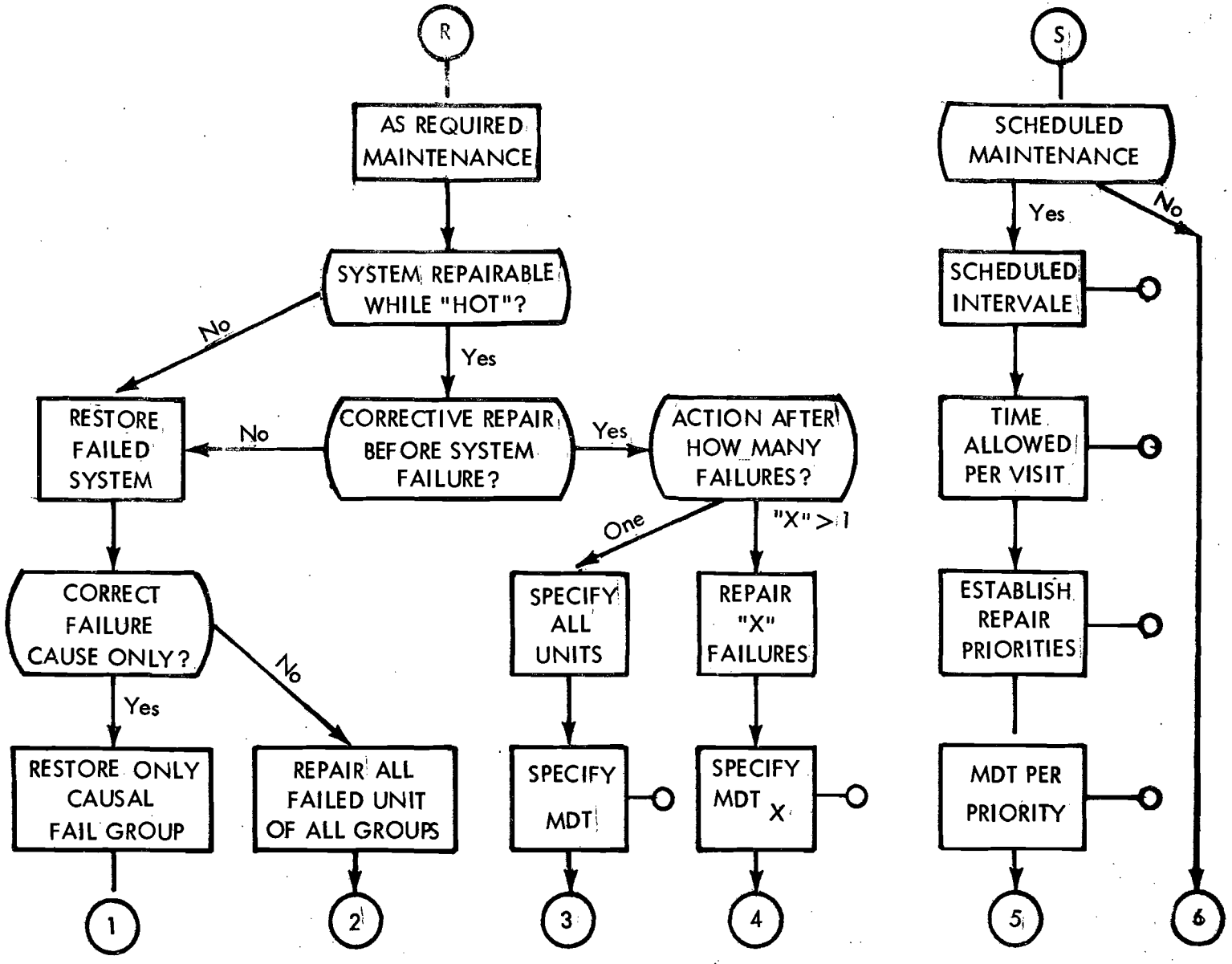


FIGURE 1. MAINTENANCE POLICY ELEMENTS

28. ESTABLISHING THE MATHEMATICAL MODEL (§3.5.1.1). The mathematical model incorporates the reliability block diagram representation and conditions, and the pertinent maintenance elements, into a mathematical statement defining the reliability of the total equipment. The model may be of an analytic nature or it may be a simulation model.

a. Development of an Analytic Mathematical Model. The development is described below in terms of four basic steps.

(1) Step 1 - Basic System Equation. From the Reliability Block diagram, identify the serial elements and the groups of redundant elements needed for "success". The basic system reliability equation is then formed by multiplying the product of the serial reliabilities by the product of the redundant groups reliabilities. It may be desirable or necessary to develop a distinct basic system equation for each significant function and/or operating mode. The basic system reliability equation takes the form of the following.

$$R(t) = \pi_i R_{si}(t)\, \pi_k R_{pk}(t) \qquad \text{(Equation 13)}$$

where R_{si} = ith serial element

R_{pk} = kth group of redundant elements.

(2) Step 2 - Establish the Mathematical Model for the Serial Elements. State each R_{pk} in terms of the appropriate statistical failure descriptor. A constant failure rate is generally characteristic of electronic equipment; and, in most other cases, an "average" failure rate can be used over a restricted, defined period of time. For this constant failure rate case, then, the reliability of the serial elements in the system becomes the following.

$$\pi_i R_{si}(t) = \pi_i e^{-\lambda_{si} t} = e^{-t\Sigma_i \lambda_{si}} \qquad \text{(Equation 14)}$$

where λ_{si} = failure rate of the ith serial element.

(3) <u>Step 3 - Establish Reliability Equations for the Redundant Group of Elements</u>. As with the preceding, state each R_{pk} in terms of the failure descriptor for each element of the group. And, if repair is initiated before system failure, R_{pk} will also be a function of the maintenance parameters.

(a) <u>Non-repairable Redundancy</u>. Here, restoration is not initiated until the group fails in its function. The reliability statement is developed simply by defining the failed state in terms of likelihood of occurrence. Take the common form of redundancy, where all elements are operating and only one is required for success. Specifically, consider the example of three such elements. The group fails only when all three units fail in the time period considered. Hence, the UNRELIABILITY of the group is equal to the product of the UNRELIABILITIES of the elements. In terms of the Reliabilities, this is stated by the following equation.

$$R_{pk} = 1 - (1-R_1)(1-R_2)(1-R_3) \qquad \text{(Equation 15)}$$

For elements with constant and equal failure rates, the reliability equation becomes the following.

$$R_{pk} = e^{-3\lambda_k t} - 3e^{-2\lambda_k t} + 3e^{-\lambda_k t} \qquad \text{(Equation 16)}$$

It is of interest to note that the group no longer has a constant failure rate characteristic; and, therefore, does not have a failure rate which is additive in obtaining total failure rate.

(b) <u>Repairable Redundancy</u>. In this case, maintenance is initiated as soon as an element of the redundant group fails. The group continues performing its function while the failed element is being restored or replaced. The derivation of the mathematical expression for reliability is no longer as simply performed as for the first case. The time required to restore the failed element is now a factor in the reliability of the group. The equations tend to become complex. An excellent source for exact equations, and working approxi-

mations, for a variety of cases is the RELIABILITY HANDBOOK; B.T. Kozlov and I.A. Ushakov; 1970; Holt, Rinehart and Winston, Inc. The details are beyond the scope of this Handbook.

(4) Step 4 - Define the Equipment Mathematical Model for Reliability. The mathematical (analytic) model for the equipment is obtained by inserting the formulations obtained by Step 2 and Step 3 into the basic system equation defined in Step 1.

b. System Simulation Model. A system simulation may be defined as any representation of the variables and constants which form the physical system. The analytical model developed in the preceding could thus be interpreted as a simulation of the reliability parameters of the equipment of concern. As such it relates statistical AVERAGES and the results represent statistical averages. However, the equations cannot be considered to truly simulate the system and its variables. A true SIMULATION represents (simulates) the ACTUAL variables; and not simply their statistical averages.

(1) Computerization. Prior to the ready availability of digital computers, simulation for the reliability of a large-scale system was not feasible because of the sheer magnitude of the calculation task. The simulation is now feasible. The computer is used to digitally simulate random events (or system phenomena), generally using "Monte Carlo" techniques to manipulate the events. Since ALL variables affecting reliability (such as maintenance and logistics) can be simulated and manipulated in the same model, the digital simulation model can generally more realistically evaluate expected reliability (than can the analytic approach). Digital simulation is thus an extremely powerful tool in evaluating operational system reliability, and the effect of design and/or support changes. Specific simulation programs, available for use on time-share computer systems, are described in Appendix 2.

(2) When to Consider using Simulation. It is worthwhile considering the use of a Simulation Model for any of the following conditions.

(a) Complex equipment with complex redundancies and/or with redundancies of the repairable category. In this case, it may not even be possible to formulate the closed, analytical statement for the total reliability. Or, if such statement is possible, an analytical solution or other manipulation may not be feasible.

(b) Multi-faceted maintenance support; as, for example, having to consider the not uncommon situation of having both significant scheduled maintenance and significant "as-required" maintenance on the same groups of elements.

(c) Significant restrictions and/or limitations in maintenance available for redundant elements; such as limited numbers of maintenance personnel and/or limited availability of maintenance equipment.

29. APPORTIONMENT (ALLOCATION) OF RELIABILITY REQUIREMENTS (S3.5.1.2). Reliability apportionment (or allocation) is the process of establishing reliability goals (or requirements) for subdivisions of the contract equipment item. The objective of the allocation process is to arrive at reasonable subdivision goals to assure achievement of the overall reliability requirement for the equipment.

a. Applications to Reliability Programs. Allocations are, basically, used as a forcing function on, first, "system" (configuration) design; then, on circuit design; and finally, on part selection and/or control. The allocations should not be treated as a static, fixed assignment of reliability goals. They should be continually reviewed, and readjusted as required, as the design progresses and the reliability potential becomes fixed for particular areas.

(1) In a development program, it is essential that initial allocations be completed and reviewed before commitment to the basic design approach. The allocations may indicate the need for applying redundancy in particular areas. Later stages of allocations readjustments may indicate that special parts and/or controls will be needed in the prototype program. Final allocations may indicate the need for changing the equipment reliability requirement for the

prototype. During the early development, allocations will be based on similar equipment and/or similar modules reliability predictions. At later states, average stress predictions will become available - which may force reallocations.

(2) In the prototype (preproduction) program, initial allocations are again made and reviewed. These may indicate the need for a re-assessment of redundancy needs, as a result of new reliability requirements and/or other changes from the development model. At this stage, the allocations act as a forcing function on configuration design primarily. Later stages of the dynamic allocation process are intended to act as forcing functions on specific circuit designers; and possibly even on parts selection and/or control. The earliest allocations will have to be based on predictions for similar modules. Then average stress predictions will become available to use as a base. Finally, stress-analysis predictions will become available. After stress-analysis predictions have become available on all equipment elements, allocations are intended primarily as forcing functions on parts controls.

(3) Dissemination. Allocated goals must be imposed as reliability REQUIREMENTS on the responsible engineers; and they must be held to account by the program management. If this is not done, allocations become a relatively ineffectual exercise.

b. Basic Allocation Procedure. The following are the basic steps required to perform an allocation. It is essentially the same as that used by the FAA in arriving at the reliability requirement for the conract item (see paragraph 13. of this Handbook).

(1) Step 1 - Translate the equipment Reliability Requirements to required failure rate, if the specification has not already done so.

(2) Step 2 - Perform a reliability prediction for the equipment, using a consistent approach for all elements. The specific technique will depend on the stage of development.

(3) Step 3 - Make initial allocation of reliability goals. Allocate to at least the level of design-responsibility packages and/or procurement packages. Goals are allocated to elements on the basis that the ratio of allocated-to-predicted failure rate of the element is the same as for the total equipment. For equipments with planned redundancy, the allocation first treats the redundant group as a single equipment element. Goals are then allocated within the redundant group, if required.

(4) Step 4 - Review the initially allocated goals for feasibility and reallocate goals if required. A determination of feasibility is based on such factors as similar equipment history, state- of-art, costs, weight or space implications, and schedule restrictions. Where the feasibility is indicated as no better than just "conditional", review the allocations to see if a reallocation of goals can ease the feasibility problem. Repeat steps 2, 3, and 4 as the design progresses and/or certain areas become fixed for some reason and/or reliability predictions change for any reason.

30. RELIABILITY PREDICTION TECHNIQUES AND APPLICABILITY (S3.5.1.3 - S3.5.1.3.1.4). Reliability predictions provide the capability for quantifying reliability; and are therefore essential to making reliability an engineering discipline. A prediction is an indicator of the design's inherent reliability capability. Predictions therefore have significant applications throughout all phases in the evolution of a system. Specific task categories for application of reliability prediction are discussed in the following sub-paragraph.

a. Application of Reliability Predictions. System (equipment) development tasks involving significant prediction activity can be classified into seven general task categories: feasibility study, allocation study, design comparison, proposal evaluation, trade study, design review, and design analysis. These task categories differ in principal objective, and are performed at different stages of the equipment's evolution. However, the associated reliability predictions are performed using essentially the same basic procedure for any task category; the major difference in procedure being dictated by the particular development phase of the equipment rather than by the task. The purpose and characteristics of each task category, and the

relationship of the reliability prediction to the task objective, are summarized by the following.

(1) Feasibility Studies. In general, feasibility studies are directed toward evaluating the feasibility of given technological approaches in meeting operational objectives within the practical constraints of time and cost. However, in most systems, severe operational requirements generate additional constraints in the area of system effectiveness. Therefore, an evaluation of the probable level of system reliability that will be achieved by the approach in question is a critical factor in the feasibility analysis. Such evaluations of system reliability involve reliability predictions based on extremely gross system performance and environmental data.

(2) Allocation Study. A series of progressive studies are performed for the purpose of allocating system effectiveness requirements among the several elements of the system. System effectiveness includes system reliability as a major parameter. Therefore, a significant portion of allocation studies involves the allocation of system reliability. During such studies, reliability prediction procedures are applied as the primary analytical tools of reliability allocation.

(3) Design Comparison. Alternate designs of established feasibility are compared in selecting the specific approach(es) to be considered for further development. Reliability is a major parameter in the effectiveness of a given design; and must be considered in any comparison of alternate designs. Thus, the probable level of system reliability, as determined by means of reliability predictions, becomes an important aspect of comparing alternate designs.

(4) Proposal Evaluation. In general, proposals are evaluated in terms of many interrelated factors. One of these factors is an evaluation, usually by means of a reliability prediction, to verify the reliability of the proposed design. Such evaluation requires a reliability prediction which is directed toward assuring that at least a minimum acceptable reliability level will be realized. This is not normally as rigorous as a

prediction performed for the purpose of estimating the actual value of reliability, as might be required in design comparison studies.

(5) Trade-off Studies. Trade-off studies can involve any of many sets of interrelated design factors. However, in most cases, physical and functional design characteristics are traded against each other within constraints of system operational effectiveness, operational requirements, and physical restrictions. Thus, reliability predictions, as the trade-off areas are varied, are important aspects of any trade-off study because of the relationships between system effectiveness and reliability.

(6) Design Review. Formal design reviews are performed at appropriate stages of system development to assure that the design is progressing according to the baseline requirements. These design reviews include an assessment of every aspect of design, including the achieved level of reliability. Therefore, a reliability prediction, performed at a level of detail that considers details of hardware design, forms an important part of analysis performed in support of a design review.

(7) Design Analysis. As a system design progresses through the development, periodically updated reliability predictions are invaluable for identifying the reliability problems that may be generated, assessing the effect of design change, and otherwise measuring the progress of the design with respect to the achieved reliability. In addition, specialized design analyses involving reliability predictions are performed for such purposes as supporting maintenance, logistics, and test program planning studies.

b. Reliability Prediction Techniques. A system (equipment) reliability prediction is started by determining the reliability (or failure rate) of the elements in the reliability block diagram and/or mathematical model. The model is then used to obtain the system reliability. The validity of the system prediction is thus a function of the reliability prediction technique used for the system model elements.

(1) Specific Techniques for Predicting Element Reliability. Several reliability prediction techniques are in common use. These allow system predictions to be performed with varying degrees of accuracy; depending on the stage of system evaluation under consideration. Three basic reliability prediction techniques are adequate to cover the spectrum of program phase and design detail. These are summarized in the following subparagraphs. (Appendix 2 describes some available time-share computer programs applicable to prediction.) The specific procedures for implementing these techniques are described in the following paragraphs.

(a) Similar Equipment Technique. The equipment (and/or elements thereof) under consideration is compared with similar equipments (and/or elements) of known reliability in estimating the probable level of achievable reliability.

(b) Part Count/Average Stress. Equipment reliability is estimated as a function of the number of parts, in each of several part classes, to be included in the equipment; and average stresses for each class.

(c) Stress Analysis Technique. The equipment failure rate is determined as an additional function of all individual part failure rates; and considering part type, specific stress level, and derating characteristics of each part.

(2) Basic Characteristics and Applications. Table 4 summarizes the basic characteristics of these prediction techniques, and their reliability task applicability.

31. RELIABILITY PREDICTION REQUIREMENTS (PERFORMANCE/ SUBMITTAL) - (S3.5.1.3.5). Equipment reliability assessments must be maintained current with design evolution, selection, and/or change. Furthermore, the reliabilty predictions shall incorporate the failure information gained from the FAILURE REPORTING SYSTEM. Observed reliability achievement for equipment elements shall also be incorporated into the reliability predictions as learned.

a. Prediction Submittals. A preliminary prediction for the contract equipment reliability shall be submitted with the proposal for the contract. This shall include full disclosure of the models, analysis techniques, environment and stress assumptions, and failure rate sources used. Full detailed prediction disclosures shall also be prepared for each Formal Design Review and submitted to the FAA, in a full RELIABILITY ALLOCATIONS, ASSESSMENTS, AND ANALYSIS REPORT (per DID R-2 of Appendix 3). These latter disclosures shall additionally give specific part failure rates, environment, and stress - with a description of the basis and/or method for the determined environment and stress.

b. Results Submittals. Summary presentations of the results of reliability predictions, and comparisons with observed and allocated values, shall be presented in the monthly RELIABILITY PROGRAM STATUS REPORTS (per DID R-7 of Appendix 3). Full disclosure of details is not required, unless there is some significant difference, in methods or sources, from the previously submitted full disclosure.

32. DETAIL-STRESS RELIABILITY PREDICTION PROCEDURE (S3.5.1.3.1.4). Several reliability prediction techniques have been developed that permit a detailed part-by-part analysis of a system design - to the extent that the effects of specific degrading stresses are considered in determining the failure rates of individual parts. These techniques are all similar in application, the major difference being the source of failure rate data; and the corresponding differences in the procedures used in extracting data from the data source, and translating these data for application to a specific system. Since details of the equipment design are required in determining stress ratios, temperature, and other application and environmental data, these techniques are only applicable during the late stages of design. Also, because of the high level of complexity

of modern systems, the application of the procedure is time consuming; and should only be used when such detailed part-by-part analysis is warranted. The following are the basic steps in a general procedure for performing a detail-stress reliability prediction.

a. Step 1 - Establish a parts list for each element of the Reliability Block Diagram and/or Mathematical Model. The list must include definition of the part, its specification(s), and circuit reference indicators.

b. Step 2 - Determine the ambient operational air temperature in which the parts operate.

c. Step 3 - Perform a stress and thermal analysis to establish the operational and environmental stresses on each part. This specific parameters and characteristics that must be defined and/or evaluated vary with the type of part. (The requirements may also vary with the particular failure rate source being used.)

d. Step 4 - Determine the resultant base failure rate for each part. This is taken from the appropriate table or graph of the source being used; and is generally a function of part type and specification, operating temperature, and relative level of operational stress.

e. Step 5 - Determine the adjustment factor(s) required for each part base failure rate. These are generally multiplicative on, but may also be additive to, the base failure rate. They define the failure effect of the specific application being considered (such as ground-fixed vs. ground-mobile vs. airborne).

f. Step 6 - Calculate the operational failure rate of each part. This will be a function of the base failure rate (Step 4) and the adjustment factors (Step 5). Again, this relationship varies with part type and the specific failure rate source being used.

g. Step 7 - Add the part failure rates to obtain the failure rate of the equipment element. This procedure is valid only when there is no redundancy between parts. Redundant part groups should be treated as distinct system elements in the reliability block diagram/mathematical model. (See Paragraph 30, Step 3.)

h. Step 8 - Combine the failure rates of the equipment elements to obtain the reliability prediction for the equipment. The previously established Mathematical Model (and/or Simulation Model) is used to obtain the required reliability measure: which may be in terms of failure rate, MTBF, or Probability of Success.

33. PART-COUNT/AVERAGE-STRESS RELIABILITY PREDICTION PROCEDURE (S3.5.1.3.1.3). The Part Count/Average Stress prediction technique makes use of average failure rates established for general part classes. This reliability prediction technique is applied when estimated part inventories are available, but the design details necessary for a stress analysis are not known. The procedure for performing a Part Count/Average Stress prediction is very similar to that for the Stress Analysis Technique. The differences lie in the type of parts listing required and in the manner of establishing the part failure rates. The Average-Stress technique involves establishing part classes and their population; and establishing generic (i.e., average) failure rates for the classes. The following are the basic steps in a general procedure for the part-count/average-stress prediction technique.

a. Step 1 - Define the part classes for which generic failure rates are to be established.

b. Step 2 - Define/Establish the expected "average" operational/environmental stresses for each part class. The specific parameters/characteristics for which averages must be established are those discussed in Step 3 of the Stress Analysis technique. It is common practice to establish two sets of averages - one for parts in digital circuits; and the second for parts used in analog circuits. Generally, the average stresses to be used are derived from part application policies; or experience with part application in other equipments. This step is unnecessary when generic failure rates are established directly on the basis of observed data.

c. Step 3 - Establish generic failure rates for each of the part classes. Generally, this is done by using the "average" stresses of the previous step to develop the generic failure rates (following the procedures of Steps 4, 5, and 6 of the Stress Analysis Technique). As was noted in the previous step, generic failure rates may be established on the basis of experienced failure data.

d. Step 4 - Establish a listing of the part classes, and their quantities in each element of the Reliability Block Diagram and/or Mathematical Model. The part classes must be the same as those established in Step 1.

e. Step 5 - Determine the predicted failure rate of the equipment element. This is done by first assigning failure rates, as established in Step 3, for each part class in the equipment element. This is then multiplied by the number of the part class used. After this is done for each class, the results are added to obtain the failure rate of the equipment element of concern.

f. Step 6 - Combine the failure rates of the equipment elements to obtain the reliability prediction for the total equipment.

34. RELIABILITY PREDICTION BY SIMILAR FUNCTIONAL EQUIPMENTS AND/OR MODULES (S3.5.1.3.1.1, S3.5.1.3.1.2). This prediction technique makes use of the failure rates (or reliabilities) determined for, or experienced with, similar previously developed or used equipments. Obviously, the prediction results will be more meaningful and accurate if field results on similar equipments are used. The "similar element" technique is used in making very early predictions of reliability before any significant characteristics of the equipment design have been established. In most cases, the technique is used to estimate the feasibility of meeting a reliability objective within the current "state-of-the-art". However, it may sometimes be necessary to extrapolate beyond the state-of-the-art. A general procedure for performing a "similar-element" prediction is given by the following basic steps.

a. Step 1 - For each element of the Reliability Block Diagram, identify the similar elements for which reliability data is available. The identification of similar elements is generally done on a one-to-one basis with the contract equipment functional-elements (such as similar computers). However, the identification may be at a lower level; i.e., the available "similar" element may be similar to the components (such as cards/modules/assemblies) which form the equipment element. Identification as "similar" is based on consideration of such factors as: function, operating modes, "state-of-the-art", type of design and/or construction, use and/or application, and complexity. It is preferable, where possible, that the "similar" elements be of

the same manufacturer intended for the new equipment element.

b. Step 2 - Define the failure rate observed, or otherwise determined, for each of the "similar" elements. In addition to the failure rate value itself, it is necessary to identify the data source, data quality and type, and the attendant environmental conditions (where different from that expected for the new equipment).

c. Step 3 - Adjust each of the "similar" failure rates to the conditions of the new equipment. It is generally not possible, or necessary, to adjust the failure rates for all of the differences in equipment points of similarity. In almost all cases, it is adequate to adjust the failure rate of the "similar" element for: 1) estimated complexity differences; 2) more severe expected environments; and 3) estimated effect of "state-of-the-art" differences. The last is the most difficult adjustment to make; hence, wherever possible, it is desirable to select the "similar" element within the same state-of-art expected, or required, of the new equipment.

d. Step 4 - Using the adjusted similar element failure rates, establish the expected failure rate of each equipment element.

e. Step 5 - Obtain the Reliability estimate for the new equipment by using the element failure rates in the previously developed Mathematical Model for the equipment.

35. PART FAILURE RATE DATA SOURCES (S3.5.1.3.2). In the Stress Analysis and Part Count/Average Stress Prediction Techniques, the specific failure rate source used is a decisive factor in the validity of the resultant reliability prediction. The following section defines the recommended failure rate sources. These are acceptable to the FAA without further justification by the contractor. The use of any other sources or specific failure rates requires justification by the contractor; and their acceptance in a specific program is subject to approval by the FAA.

a. Recommended and Acceptable Data Sources. Only two failure rate sources for electronic parts are acceptable to the FAA without further justification. These are: 1) the RADC "RELIABILITY NOTEBOOK," RADC-TR-67-108, Vol. II; and 2) RELIABILITY STRESS AND

FAILURE RATE DATA FOR ELECTRONIC EQUIPMENT," MIL-HKBK-217A. For micro-electronic failure rates, only the RADC Reliability Notebook is acceptable, without justification, to the FAA. The RADC Notebook is, in general, the most up-to-date government-controlled source of electronic part failure rates. Hence, the RADC Notebook, RADC-TR-67-108, is in all cases the preferred failure rate source for electronic parts. The RADC "NONELECTRONIC RELIABILITY NOTEBOOK", TR-69-458, is the preferred failure rate source for nonelectronic parts.

b. Other Data Sources. Other possibilities as failure rate sources are listed below. Their listing does not imply any recommendation by the FAA. And, their use in any specific instance is therefore subject to approval by the FAA.

(1) FARADA. FARADA (Failure Rate Data) is a collection of failure rates from a variety of sources. It gives the number of test hours, the number of observed failures, and the measured failure rates for each source. There will be several entries, usually with different failure rates, for a given type of part. FARADA also includes contractor compendiums of failure rates - often significantly more optimistic than those of the two recommended sources. FARADA is therefore not a good source for consistent data. It should be used only with extreme caution; and, then, only as a source for parts not contained in the two recommended sources.

(2) GIDEP. GIDEP (Government-Industry Data Exchange Program) is a source of part test data. However, the tests covered are usually short-term qualification procedures; and, are therefore not directly useful in making reliability predictions.

(3) RAC. The RAC (Reliability Analysis Central) is an RADC sponsored, IIT-Research-Institute operated, DOD information center. Its scope is limited to being a source of failure rates only for microelectronics. The RAC data is ultimately incorporated into the RADC Reliability Notebooks. In the interim, it can provide current information. RAC analyzes its data inputs to provide useful reliability prediction information.

(4) Vendor or Supplier Data. Vendor or Supplier data may represent only the selected, best reliability test results, rather than the typical. The data may include invalid conversion factors for converting the failure rates from the test (or observed) stresses to the operational stresses. Finally, there is a tendency to omit details on test conditions which, if known, might disadvantageously alter the conclusions drawn. Unfortunately, however, the vendor may have the only existing data on a unique new part. In this case, it is desirable that the raw test data, where it exists, be available to support the claimed failure rates.

36. ENVIRONMENT AND ELECTRICAL STRESS LEVELS FOR RELIABILITY PREDICTIONS (S3.5.1.3.3). Invalid assumptions or calculations of the operating environment and/or part stresses will result in an equally INVALID reliability prediction.

a. Environment. In using any of the prediction techniques to predict operational reliability, the determination of failure rates shall be based on operation in the "worst-case" expected (or specified) for the equipment in FAA field use. Reliability engineering efforts shall be predicated on operation in this environment. Unless otherwise specified by the FAA, the definition of worst-case environment shall be based on the levels specified in the FAA Specification, FAA-G-2100, GENERAL REQUIREMENTS FOR ELECTRONIC EQUIPMENT. When a reliability prediction is specific to a demonstration test requirement, the environment specified for the demonstration shall be used. (The specified demonstration test environment is not necessarily a true or complete reflection of the total operation environments.)

b. Electrical Stress Levels. The effect of electrical stress on the reliability of specific part types is specifically defined in the recommended failure rate data sources previously identified (paragraph 38). In NO case shall actual part application exceed the policies established in FAA-G-2100, GENERAL REQUIREMENTS FOR ELECTRONIC EQUIPMENT. In performing reliability predictions by the similar equipment or part-count/average-stress techniques, the failure rates shall be based on stressing policies established specific to the program. Where these have not yet been established, the stress levels of FAA-G-2100 shall be used. In performing a

reliability prediction using the stress-analysis technique, the specific actual stresses, as determined by measurement or stress analysis, shall be used.

37. PREDICTIONS FOR RELIABILITY IMPACT STUDIES (S3.5.1.3.4 - S3.5.1.3.4.6). A full range of reliability impact studies is normally required only in study, not equipment, programs. Selected impact studies may be specified as part of an equipment contract. Under an equipment contract, the studies are intended to serve as reliability analysis inputs into the trade-offs considered at the formal design reviews.

a. Submittals. When impact studies are required, the specific approach and coverage shall be described in the submitted RELIABILITY PROGRAM PLAN (DID R-1 of Appendix 3). The results of such studies shall be submitted as part of the RELIABILITY ALLOCATIONS, ASSESSMENTS, AND ANALYSIS REPORT (DID R-2). Progress in the studies is of course also indicated in the RELIABILITY PROGRAM STATUS REPORT (DID R-7).

b. Specific Study Requirements. The following are the six Impact Studies, any one of which or all may be required. The individual study is intended to investigate the effect of varying a particular parameter on the predicted reliability. When more than one study is required, in addition to investigating the reliability effect of the individual parameter, the combined effect shall also be investigated.

(1) Design Variations. A reliability prediction shall be made for each design variation and/or option in the study contract. In the equipment contract, this requires that a prediction be made for all options and that it be SUBMITTED. The cost impact of each variation shall be defined.

(2) Stress Variations. A range of stress policies shall be defined, from minimum values affecting reliability to full rate stress. The part classes in the subject equipment shall be defined. Reliability predictions shall then be made to indicate the reliability effect of varying the stress on specific part classes; and the effect of varying the stress on all parts. In the latter, the same relative stressing may be assumed for all parts.

(3) Ambient Temperature Variations. The ambient temperature for the subject equipment shall be varied from the minimum operating temperature affecting reliability to the maximum value at which the majority of parts will operate. A reliability prediction is made to indicate the effect of the varying temperature. Where the contract equipment consists of distinct cabinets, each cabinet shall be so investigated individually.

(4) Impact of Part Quality. The part classes in the subject equipment shall be defined. Then the available part qualities (including established reliability as a part quality class) for each part class shall be determined. Reliability predictions shall then be made to indicate the reliability effect on the equipment of varying the quality of the individual part classes; and the effect of simultaneously varying all part classes in the same "quality direction". For each variation, the cost impact shall also be determined.

(5) Impact of Quality Control Programs. A full range of applicable parts quality control programs shall be defined for part classes, with special stress on semiconductors, integrated circuits, and hybrid microcircuits. The quality control program definition shall include consideration of parts inspection, testing, and "burn-in". The effect of each quality control variation on part failure rate shall be determined. And reliability predictions shall be made to determine the effect of part quality control on the equipment reliability. In all cases, the cost of the quality control program shall be defined.

(6) Cost Study. Under this study, reliability predictions shall be made as required to define the relationship between cost and reliability requirement. As a minimum, this study shall include consideration of redundant design, part quality, and part quality control in the cost factor.

38. DEGRADATION ANALYSIS OF CIRCUITS (S3.5.1.4 - S3.5.1.4.4). Where not otherwise specified by the procurement documentation, the required degradation analysis is performed on all unique circuits in the equipment.

a. Submittals. When a degradation analysis is required, the approach to establishing models or equations, selection of input parameters to be varied, and selection of "unique" circuits shall be described in the RELIABILITY PROGRAM PLAN (DID R-1 of Appendix 3). These are subject to the approval of the FAA. The RELIABILITY ALLOCATIONS, ASSESSMENTS, AND ANALYSIS REPORT (DID R-2) shall define the models or equations, the input parameters, and the selected circuits to be analyzed. This REPORT shall also document the results of completed studies. Predictions shall reflect the information gained in performing the degradation analyses. The RELIABILITY PROGRAM STATUS REPORT (DID R-7) shall reflect the progress being made in the analyses.

b. Specific Degradation Studies. The degradation analysis considers part characteristics as the variable, independent, input parameters; and circuit performance characteristics as the output parameter. Where more than one of the degradation analysis methods is required, they shall be performed individually. The following are the four methods, any one or more of which may be specified as a requirement.

(1) Parameter Variation Analysis. As a minimum, each input parameter shall be varied over the range of its possible values, while holding all other input parameters at their DEFINED nominal values. The analysis shall determine the effect on the circuit output parameters; circuit failure points shall be defined; and maximum ALLOWABLE input parameter variation established.

(2) Worst-Case Analysis. All input parameters shall be varied simultaneously, with each being varied in the direction which increases the output parameter above the DEFINED nominal. A Worst-Case output value shall be established; i.e., the output parameters values when each input parameter reaches the limit of its tolerance or expected drift range. Circuit failure points for the input parameters shall be defined. The input parameters shall then be varied in the direction decreasing the output parameter BELOW nominal; and the worst-case values and circuit failure points defined.

(3) Variance (and Mean) Analysis. Determine the mean and variance for each input parameter distribution. Correlation coefficients must then be defined for the set of distributions. From these data, the mean and variance of each output parameter shall be determined. Circuit failure points shall be defined for the output parameters, individual input parameter distributions, and combined input parameter set.

(4) Monte Carlo Simulation. Establish a true simulation of the circuit and its input parameters. This requires a full determination of the distribution for all input parameters. The simulation shall randomly select from these distributions, individually and in random combination. The output of the simulation shall establish the fully defined distribution except for each output parameter. Again, circuit failure points shall be defined.

SECTION 4. PARTS, ASSEMBLIES, MATERIALS, AND PROCESSES

39. THE PARTS, MATERIALS, AND PROCESSES PROGRAM (S3.5.2, S3.5.2.4 - S3.5.3). There are two basic aspects, or phases, to a total Parts, Materials, and Processes program. The first phase is to control selection and application. The second phase is to assure proper handling of the items. Basic requirements and goals for each of the phases are discussed in the following subparagraphs. When a parts, materials, and processes program is imposed as part of the required reliability program, the plan for implementation shall be submitted as an element of the RELIABILITY PROGRAM PLAN (DID R-1 of Appendix 3).

a. Parts, Materials, and Processes Control. For reliability, the goal of the parts, materials and processes control program is the assurance that the required reliability is achieved in the designs. This is achieved by controlling proper selection and application of the parts, materials, and processes. The elements of this control program shall include at least the following items.

(1) A Standardization effort to minimize the number of different parts and materials used.

(2) A Preferred Parts and Materials list development maximizing the use of MIL parts and/or parts with proven reliability histories, and monitoring the use thereof.

(3) FAA Specification, FAA-G-2100, GENERAL REQUIREMENTS FOR ELECTRONIC EQUIPMENT compliance.

(4) Use of Procurement Specifications to impose reliability requirements, and monitoring compliance.

(5) Monitoring and Guidance of Design to assure proper application of parts and materials.

b. Parts, Assemblies, and Material Handling. The goal of the handling requirements and procedures is to assure that the fabricated equipment does not contain degraded parts, assemblies, or material. Or, in other words, the goal is to assure that the equipment design reliability is not degraded by the handling of parts, assemblies, or materials. Requirements and controls shall therefore be established to: 1) prevent the use of questionable-condition parts, assemblies, or materials by

manufacturing; and 2) prevent the degradation of the parts, assemblies, or materials by the manufacturing process.

c. Deficient Item Notifications and Responses. A deficient item is one which is found to NOT meet its procurement specification.

(1) Notification by Contractor. The contractor shall investigate for deficiency all items suffering repeated failures and/or whose failures have had a critical impact on the program. Confirmed deficiencies shall be reported to the FAA via a DEFECTIVE OR INADEQUATE PARTS AND/OR SPECIFICATIONS NOTIFICATION (DID R-3). The notification shall define the deficient item, the confirmation analysis, the determined deficiency cause, actual and/or potential effect on equipment reliability, and corrective action taken.

(2) Response to Deficiency Notice by FAA. The contractor shall respond to Deficiency Notices which may be issued by the FAA. The response shall be in the manner prescribed by the DID SUSPECT MATERIAL DEFICIENCY NOTICE RESPONSE (DID R-9 of Appendix 3). As a minimum, the response shall identify the number of the deficient item used, their location in the equipment, an analysis of the reliability effect of the deficiency, impact on the reliability program, and corrective action taken.

40. THE RELIABILITY DESIGN GUIDE (S3.5.2.1, S3.5.2.1.1). A Reliability Design Guide shall be prepared which is specific to the program. The Guide shall be designed to fulfill three basic objectives: 1) assign allocated Reliability goals, 2) establish a preferred parts list, and 3) provide specific guidance in reliability design. Before being imposed on equipment designers as a program requirement, the Reliability Design Guide shall be reviewed and approved as part of the Preliminary Design Review (the first Formal Design Review of the program). The approved Design Guide shall then be submitted as part of the DESIGN REVIEW REPORT (DID R-12 of Appendix 3) for that design review.

a. Scope of the Reliability Design Guide. The Reliability Design Guide shall contain the following elements as a minimum.

(1) Reliability requirements for the equipment.

(2) Environmental envelope for the equipment.

(3) Reliability Model (block diagram and/or mathematical model) of the equipment.

(4) Allocated Reliability requirements assigned to lower levels.

(5) Reliability Design Techniques recommendations and guidance.

(6) Reliability Check Lists for design reviews.

(7) Preferred Parts List, prepared to the minimum requirements defined by the following sub-paragraph b.

b. The Preferred Parts List. The preferred parts list establishes the parts recommended for use on the program. The part selection shall first comply with the requirements of the FAA Specification, FAA-G-2100, GENERAL REQUIREMENTS FOR ELECTRONIC EQUIPMENT. Whenever available, parts having established quantitative reliability levels shall be selected for the list. The part selection shall also be directed toward STANDARDIZATION of parts. To this end, priority shall be given to the use of parts already included in government-issued preferred parts documents. The preferred parts list included in the Reliability Design Guide shall contain the following information.

(1) Parts Listing for the preferred parts, fully identifying each part.

(2) Stress/Temperature Policies. Maximum allowed and recommended nominal stress and temperature shall be defined for each listed part. A particular part can carry more than one nominal recommendation, as a function of the circuit type. In any case, the stresses and/or temperatures shall not exceed the limitations of FAA-G-2100.

(3) Failure Rates. At each of the stress/temperature conditions established by the above, a failure rate shall be specified for the listed part. (A record of the data source should be maintained, but not necessarily in the design guide.)

(4) Application/Selection Criteria. Specific areas of application shall be defined for each listed part: and/or criteria shall be given for selecting the part most suited for a particular application.

41. PARTS, MATERIALS, AND PROCESS APPLICATION REVIEW AND VERIFICATION (S3.5.2.2 - S3.5.2.3). The Application Review is intended to verify the correct selection of parts, materials, and/or processes for the specific application; and to verify that the acceptable limits on stress and temperature are not exceeded. Justification must be provided for deviations from the preferred parts lists and/or recommended stresses and/or temperatures. All such deviations shall be evaluated for reliability impact. The Application Reviews covering a Contract End Item shall be completed sufficiently prior to the Critical Design Review (CDR) to serve as input to the CDR; and to be reflected in the Reliability Assessments presented at the CDR. (Predictions of the equipment reliability shall be kept current with the findings of the application reviews.) Stress Verifications and/or thermal analyses, when required, shall be performed prior to, and serve as inputs to, the appropriate Application Review. The program check-points selected for holding Application Reviews, or the plan for performing the selection, shall be reflected in the Reliability Program Plan, as documented in the RELIABILITY PROGRAM PLAN (DID R-1 of Appendix 3). The proceedings and summary results of the Application Review shall be fully documented in the PARTS, MATERIALS, AND PROCESSES APPLICATION REVIEW REPORT (DID R-13 of Appendix 3).

a. Verification of part application stresses and temperatures. The objective of this task is to determine, by actual measurements on the equipment, whether the MAXIMUM stresses and temperatures allowed by the Design Guide (which is within the limits set by FAA-G-2100) are EXCEEDED by the implemented designs. The plan for selecting measurement samples, and the associated confidence levels, shall be reflected in the submitted RELIABILITY PROGRAM PLAN (DID R-1 of Appendix 3). Results shall serve as inputs to the appropriate Application Review.

b. Thermal Analysis. The requirement for a thermal analysis of parts is NOT the same thermal analysis required for a Detail-Stress Reliability Prediction Procedure (see paragraph 34.). The thermal analysis in the prediction procedure is carried out only TO the part, normally only to the point of defining

AMBIENT temperatures. Full Thermal Analysis OF (or FOR) each part requires that the thermal analysis be performed on each individual part - with the goal of determining internal thermal profiles. As a minimum, thermal analysis of parts shall provide the following.

(1) Passive device HOT-SPOT temperatures.

(2) Semiconductor JUNCTION temperatures.

(3) Monolithic Integrated Circuit HOT-SPOT (and/or Maximum Junction) Temperatures.

(4) Vacuum and Gas Tube MAXIMUM BULB temperatures.

(5) Hybrid Microcircuits treated as made up of parts, with the above provided for EACH PART.

SECTION 5.
FAILURE MODE AND EFFECT ANALYSIS, AND CRITICAL ITEMS

42. EFFECTIVE FAILURE MODE AND EFFECT ANALYSIS IN THE RELIABILITY PROGRAM (S3.5.4). Basically, a Failure Mode and Effect Analysis (FMEA) studies an equipment element, its interfaces, and the interfaces of its components in order to: 1) define the possible failure modes; 2) determine the effect of each failure on the equipment element being studied; and 3) investigate the probable consequences on the equipment function(s). The FMEA effort should be treated as a dynamic, iterative reliability task performed through all phases of equipment development. Coupled with the reliability predictions, the FMEA effort provides the primary reliability information for use in design and/or configuration trade-off decisions.

a. Application in a Reliability Program. The FMEA effort is potentially one of the most beneficial contributors of the reliability program to the overall equipment program. The first program function of the FMEA is to identify and highlight all first-order (i.e., catastrophic) failure modes, develop proposed design corrections, and present the findings to the design review team. Second, for failure modes outside the first-order category, the FMEA develops probability-of-occurrence data for use in making management trade-offs on the extent of time and/or effort to be invested in corrective action. Lastly, the FMEA results should provide criteria for use in planning and designing tests for the equipment.

b. Effective Implementation of an FMEA Effort. To be effective in the reliability program, the FMEA must of course competently detect, analyze, and evaluate all SIGNIFICANT failure modes at the pertinent levels. Equally important, however, is the need for the FMEA findings to be reported in a TIMELY manner and in a form to be of use at the over-all program decision points. Some level of FMEA can, and should, be initiated as soon as functional interfaces are defined, before the design becomes fixed. The design impact of FMEAs becomes significantly less at later stages of development. FMEA findings must be recognized for their value and actively used in improving equipment reliability. The following sub-paragraphs discuss some specific requirements for effectively implementing an FMEA effort in a reliability program.

(1) Integrate FMEA Effort into the Reliability Program Plan. The first requirement is to recognize the dynamic nature of the FMEA effort; and that its iterations must correspond to progress in the design effort. Therefore, the reliability program plan must schedule FMEA outputs to correspond to the design-decision milestones scheduled in the overall program plan. At each FMEA output point, the reliability program plan should clearly define the required depth of analysis, the expected findings, and the intended use of the results. These will depend on the particular element being reviewed at the decision point, the criticality of the element, and the general equipment requirements.

(2) Maintain Timeliness of FMEA Reporting. The scheduling of FMEA outputs must be maintained current with changes in the overall program schedules. Late submission of FMEA reports and/or findings must be avoided. The need for timeliness shall take precedence over the reliability engineer's desire for comprehensive analyses. Without such adherence to timeliness, the FMEA effort loses all value to the design engineer and project management.

(3) Use Specifically Appropriate Analysis Methods. The analysis method or level used at a specific FMEA point should be appropriate to the item being analyzed, the stage of development, and the intended use of the findings. The dangers of too simple an analysis are obvious - problem areas WILL be missed and the findings may be erroneous. On the other hand, overly sophisticated analyses are wasteful in time and effort; and may not be readily understandable to the design and/or project personnel (thus compounding an existing communication problem).

(4) Maintain Direct Communications with Responsible Design Engineers. Formal FMEA reporting for the formal design-decision points is of course required, and is scheduled in the reliability program plan. Equally important, however, is that direct communications be established, and maintained, between the reliability engineer and the responsible design engineers.

(a) The Need. The reliability engineer needs to obtain technical design and function information from the designer, for use in the FMEA. Also, for effective corrective action consideration, the reliability engineer must be able to DIRECTLY and immediately relay FMEA findings to the design engineer. Direct engineer-to-engineer communication also does much toward establishing designer confidence toward the value of the FMEA findings; and, therefore enhances the attitude toward the need for any indicated corrective response.

(b) Establishing Communications. Ideally, the FMEA should be performed JOINTLY by the reliability and design engineers - automatically resolving the communication problem. In most cases, however, the reliability engineer must conduct the actual FMEA by himself - coordinating with the responsible design and systems engineers. In such cases, it is the responsibility of the reliability engineer to establish communications, obtain the required technical assistance and/or input, and then relay the FMEA findings to the appropriate point.

43. LEVELS OF FMEA (S3.5.4.1, S3.5.4.2). FMEAs are of two basic types (functional or hardware) as a function of the types of failure modes being considered. The functional type of FMEA analyzes the cause and effect of function, and functional interface, failures. The hardware type of FMEA is concerned with specific electrical or mechanical failures. The level of FMEA CAN extend from the investigation of failures in basic equipment functions all the way down to analyzing failures of pieceparts. The latter is extremely detailed; and the required effort soon becomes prohibitive for the benefit gained. Hence, FMEAs performed for an FAA Reliability Program will be restricted to one, or both, of two basic categories: Functional, or Circuit-Level. These categories of FMEA are defined in the following sub-paragraphs. The level and/or type of FMEA applicable at any particular review point will depend on the stage of equipment development, and the intent of the review.

a. Functional Level FMEA. The functional level FMEA is concerned with the analysis of the failure modes of: 1) basic equipment functions; 2) functional interfaces between MAJOR equipment elements; and 3) man-machine functional interfaces. The MAJOR equipment elements shall be to at least the level of defining distinct cabinets, procurement packages, and areas to which allocated reliability goals have been assigned. The failure modes are analyzed to determine the effect on the mission or intended use of the equipment: the likelihood of occurrence; and the possible corrective actions. The Functional-Level FMEA is primarily directed toward the review, control, and improvement of the overall system configuration and/or design for reliability. However, it is also significant to establishing effective maintenance concepts; and defining circuits deserving special attention in the next lower level FMEA. The functional-level FMEA can be initiated as early as the concept phase of equipment evolution. In a formal reliability program, functional-level FMEA findings should be available for review at the Preliminary Design Review (PDR), and up-dated as equipment configuration develops.

b. Circuit Level FMEA. For FMEA purposes, equipment CIRCUITS are defined as the lowest level sets of interconnected elements with only connector electrical interfaces into the equipment, AND providing functions with specifiable performance requirements. The circuit level FMEA is then concerned with failures in the circuit functions; and with specific electrical interface failures. Again, the failure modes are analyzed to determine their effect on equipment functions; the likelihood of their occurrence; and possible corrective actions. In addition to its function of monitoring design reliability, the Circuit-Level FMEA can provide important support to the development of maintenance concepts, and fault detection and isolation requirements. The functional and electrical FMEA of a circuit is usually performed in two basic stages, as the circuit design develops. The functional circuit-level FMEA should be available for review at the PDR, for the definable circuits. The circuit-level FMEAs are updated, and evolve into electrical FMEAs, as configuration and circuit design progress. Electrical circuit-level FMEA findings should then be available for review at the Critical Design Review (CDR).

44. GENERAL PROCEDURES FOR PERFORMING FMEA (S3.5.4 - S3.5.4.2). The basic objectives for any FMEA are: 1) identification of failure modes; 2) definition of failure effect on equipment function and/or mission; 3) determination of probability of failure mode occurrence; and 4) development of appropriate corrective action(s). These objectives should be pursued on a continuing basis, as the equipment evolves into its ultimate design and configuration. Formal documentation of the FMEA and its findings is considered to be an integral part of the FMEA effort. Hence, a standardized, formal FMEA Form should be prepared and all specific analysis efforts documented therein. At appropriate points of the effort, a formal FMEA REPORT must be prepared which contains the completed Forms and summarizes the FMEA findings. (DID R-11 of Appendix 3, FAILURE MODE AND EFFECT ANALYSIS REPORT, defines the FMEA documentation requirements.) The following sub-paragraphs define the basic form and report requirements, and give a general procedure for carrying out an analysis.

a. Establish the FMEA Analysis Form. The Analysis Form should be designed to fulfill three basic functions: data collection, analysis documentation, and findings presentation. First, the Form will be used to collect the information required to perform the FMEA Analysis. To this end, the required entries should be readily recognizable to the design engineers; and not to just the reliability engineer. This will facilitate getting data from the responsible engineers. Secondly, the Form will be used to document the specific analyses and results. Finally, the Form will be used to present specific findings to responsible design engineers. In this last function, it is necessary that recommendations and their application be readily recognizable; and do not become lost in a "busy" entry space filled with non-pertinent information. The Forms should contain only the absolute minimum number of entries required to fulfill these above functions.

b. Perform and Document the Analysis. The following "steps" form a general procedure for carrying out the analysis of an FMEA. The steps are given in terms of the information required for the Analysis Form.

(1) Step 1 - Identify the engineer responsible for the Analysis and the completion of the Forms.

(2) Step 2 - Establish Dates for FMEA Initiation, Completion, and any Revisions. This serves to establish the system status during the time that the analysis was performed.

(3) Step 3 - Identify the Item Under Analysis and its Configurational Relationship to the Total System. "Item Under Analysis" is the equipment AREA which is under immediate analysis. Nomenclature and Identification Number must, of course, be given for the Item Under Analysis (IUA). In addition, however, sufficient data must be given to unambiguously identify the IUAs "indent" (or hierarchical) relationship to the rest of the system.

(4) Step 4 - Identify the Specific Part/Function Interface for which the Failure Modes will be Defined. For a Functional FMEA, the function or functional interface needs to be identified. For a circuit-level FMEA, functions and/or electrical interfaces need to be identified. For interfaces, also indicate whether they are input or output signals; and identify the source/sink as the case may be.

(5) Step 5 - Describe the Failure Mode. Description of the failure mode shall consider such conditions as open, short, out-of-tolerance, premature operation, failure to operate/cease operation when required, degraded performance, etc.

(6) Step 6 - Describe/Define the Failure Causes. Describe the likely causes of the listed failure mode. Limit these to those of a deterministic nature.

(7) Describe the Failure Effect Through the Successively Higher Levels of Equipment. Note the effect on the performance of the IUA and the ultimate effect on the performance of the end item equipment. Effect on intermediate levels of equipment can usually be indicated by reference to an appropriate higher-level FMEA. If not, these should also be briefly described.

(8) Step 8 - Determine the Probability of Failure or Failure Rate. Either the Probability of Failure or the Failure Rate must be used in all the FMEA levels. Where failure rates are available it is preferable that these be used. Failure rates

are usually given for "failure" of a part, regardless of the mode. Failure rates may be assigned to modes by considering their relative likelihood. In early stages of system development, when the functional FMEA is initiated, it is not likely that failure rates can be assigned to the failures. In this case, it will be adequate to determine the Relative probabilities of failure. (Document all sources, assumptions, and methods of analysis in the FMEA report.)

(9) Step 9 - Identify Available, or Recommended, Corrective Action. Note any recommended and/or available design changes, specification revisions, procedural changes, or other factors which would eliminate the mode of failure or reduce the probability of occurrence and/or reduce its effect. Describe any operating procedures recommended and/or available to bypass the failure, reduce the probability of occurrence, and/or reduce its effect. Identify any a-priori testing or processing which can be applied to reduce the probability of failure.

(a) Impact. Where any of the corrective actions are intended to reduce the probability of occurrence, indicate the expected improvement.

(b) Status. Identify any of the corrective actions already initiated at the time of the FMEA.

c. Prepare the FMEA Report. Each FMEA performed for a design review point shall be documented in a complete, formal report (per DID R-11 of Appendix 3, FAILURE MODE AND EFFECT ANALYSIS REPORT). The report shall contain the following substantive information as a minimum.

(1) FMEA Identification. Identify Program and review point for which Report is prepared; Report originator and dates; and Originators dates and titles for the FMEA analyses included.

(2) Introduction and Scope. Briefly describe intended use of equipment. Define the purpose of the review point for which the report is being prepared; and briefly describe the intended use of the report and the analyses contained therein. List the Items analyzed,

their indenture level descriptions, and the FMEA levels and/or types applied.

(3) Data Sources. Identify the specific indexes, drawings, schematics, predictions, and other data sources used for the analyses and report.

(4) Functional Descriptions. Prepare an over-all description of the equipment functions and interface requirements, detailing the same for the Items analyzed in the report. Prepare functional block diagrams to support this description.

(5) Analysis Methods. Summarize the assumptions used in performing the specific FMEA analyses. Define the techniques used in estimating the probabilities of failure. Define any unique terms used in the analyses.

(6) Corrective Actions. Summarize the corrective actions, the problems they were intended to resolve, and their status. Present detailed analysis and description of the particularly significant corrective action recommendations; summarizing the expected reliability impact of implementing such actions.

(7) Reliability Conclusions. Summarize the FMEA indications for operational reliability (as opposed to inherent reliability). Summarize the expected reliability impact of the recommended corrective actions.

(8) Recommendations for Further Investigations. Identify areas where more detailed FMEAs are indicated. Recommend investigative tests and test criteria. Provide recommendations for improving the data sources.

(9) FMEA Forms Attachment. Attach the completed FMEA Analysis Forms which pertain to the report. Precede with a list of definitions for any special codes, terms, or acronyms that were used in the forms. Also explain any deviations taken from standard use of the forms.

45. CRITICAL ITEMS IDENTIFICATION, CONTROL, AND HANDLING (S3.5.5). Critical items are those equipment elements which are of special significance to meeting the equipment performance (including reliability) specifications; and/or those elements with a significant

potential for preventing accomplishment of other contractual commitments. Potential candidates for the "critical items" list shall include all deliverable and diagnostic computer programs, in addition to the hardware constituting the contract equipment. The contractor shall identify all such critical items, at least prior to the Critical Design Review (CDR). Control and/or Handling procedures shall be developed, and implemented, for minimizing the criticality potential of these items.

a. Criticality Factors. At least the following factors shall be considered in the identification of critical items. Approach and/or types of analyses to be used in this identification shall be described in the submitted RELIABILITY PROGRAM PLAN.

(1) Reliability. Any item with a significant potential for preventing achievement of the required reliability is critical. Reliability predictions, models, and FMEAs are useful tools in the identification, and control, of such items.

(2) Limited Life. All items with a limited life should be considered critical (and preventive replacement schedules developed).

(3) Cost. Items of excessive cost could prevent accomplishment of the contract within dollar restrictions. Items with a potential for becoming excessive in cost should be classed as critical. They will require special attention by contract cost management and control.

(4) Acquisition lead time. Items with acquisition lead times not compatible with the contract schedule cannot, of course, be used. Hence, items with a potential for developing excessive lead times must be classed as critical items. These items will require special procurement procedures and coordination with the supplier.

(5) Safety. Items presenting an immediate hazard to personnel and/or equipment, or with a significant potential for producing such hazard, should be considered critical items. The hazard presented can be one occurring in field use and/or transportation and/or fabrication. Furthermore, the item may be "unsafe" of itself or because of its required installation in the equipment. Safety critical items will require

(as applicable) the development of special handling procedures, maintenance procedures, operating restrictions, shipping requirements, and/or attention to safety in design or configuration.

(6) Maintenance. Items with a potential for causing excessive maintenance loading are candidates for the "critical item" list. The excessive maintenance may be required because of the item's high failure rate (which, because of redundancy, may not affect equipment reliability); or, because of a need for frequent preventive maintenance and/or replacement. The FMEA is an important tool in the identification of such items and in their control. (This criticality has obvious connections with the reliability-and limited-life-critical items.) Items requiring unique maintenance skills and/or equipment must also be considered critical. Procedures and/or requirements must be established to make sure such maintenance skill or equipment is available. Design attention should also be directed toward eliminating the "unique" requirements.

b. Critical Item List Documentation. The list of critical items shall be fully documented and available for review at the Critical Design Review (CDR). Documentation shall be per the requirements of the CRITICAL ITEMS REPORT (DID R-10 of Appendix 3). The formally documented report shall include at least the following information items.

(1) Identification of the Critical Items.

(2) Quantity of each item used in the equipment.

(3) Equipment Functions affected by the critical item.

(4) Criticality basis, including a summary of pertinent analyses.

(5) Procedures and requirements for the control, handling, and/or management of the critical item; and possible techniques and/or approaches for reducing their criticality level.

SECTION 6. DESIGN REVIEWS

46. THE DESIGN REVIEW PROGRAM (S3.5.6). A total design review effort is a planned, continuous monitoring and evaluation of an equipment design effort (or a study) to assure that it meets all requirements, including that of reliability. Such an effort periodically appraises the progress being made in achieving the design objectives; and systematically brings to bear pertinently-specialized talent on specific problem areas. Design reviews appropriately scheduled and properly performed, provide one of the potentially most powerful and effective tools available for an effective Reliability Program.

a. Basic Objectives of a Review Program. For the contractor, the design review program should ensure that the designer considers and takes into account ALL pertinent factors. The programmed Design Reviews also provide an important interface with the FAA.

(1) Contractor Project Control Objectives. The total Design Review effort should be organized and programmed toward the achievement of the following basic contractor objectives.

(a) Qualified personnel applied to design review and evaluation.

(b) Integrity of equipment interfacings.

(c) Trade-offs based on all pertinent factors.

(d) Formal recording of problems, corrective actions, and bases for any decisions.

(e) Fully mature design, achieved with maximum likelihood.

(2) FAA Interface Requirements. The design review program must be designed to provide, or facilitate, at least the following interfaces to the FAA.

(a) Progress toward requirements, including reliability.

(b) Contractor OPR's, both personnel and organizational.

(c) Specific Review Plans for Formal Design Reviews and general approach for detailed design reviews.

(d) Reliability Design Guide review.

(e) Preview of Data Packages developed for use in the Formal Design Reviews.

(f) Formally Documented Design Review minutes.

b. Types of Design Reviews. The Design Review effort generally consists of two distinct types of reviews. The first is the Formal Design Reviews, the scheduling of which is contractually required. The other type is the informal Detailed Design Reviews.

(1) The Formal Design Reviews. These are generally conducted at the Contract End Item level; and the basic intent is an over-all review of design progress. There are four basic types of Formal Design Review: the Study Design Review (SDR); the Preliminary Design Review (PDR); the Critical Design Review (CDR); and the First Article Configuration Inspection (FACI). Each of these is conducted with specific objectives. The general intent of each of these Formal Design Reviews, and the more significant Reliability objectives of each, are discussed in the following paragraphs of this Section. Detailed direction and guidance for conducting SDRs, PDRs, CDRs, and FACIs may be found in the following documents.

(a) ESDP 375-10, INSTRUCTIONS FOR CONDUCTING FORMAL TECHNICAL REVIEWS, INSPECTIONS, AND DEMONSTRATIONS.

(b) AFSCM 375-1, CONFIGURATION MANAGEMENT DURING DEFINITION AND ACQUISITION.

(c) AFSCM 375-5, SYSTEMS ENGINEERING MANAGEMENT PROCEDURES.

(d) AFR 80-28, ENGINEERING INSPECTIONS.

(2) Detailed Design Reviews. These are directed toward the review and evaluation of specific circuits within the contract equipment. Findings are generally summarized in the next following Formal Design Review. The specific objectives for the detailed design reviews, and

the involved reliability activity, will depend on their time relationship to the Formal Design Reviews defined in the preceding paragraph.

c. The Design Review Program Plan. A Design Review Program Plan should be prepared as an integral element of the total reliability program plan. The first objective of the plan is to define the time-phased contract milestones at which the Formal Design Reviews will be held. The definition for each such point should include scheduled time, description of contract event at the milestone, basic reliability objectives in the review, and the technical skills or disciplines required at the review. To the extent possible, the program for the detailed design reviews should be similarly defined. Normally, it is not possible to pre-define the specific informal detailed design review. The program plan should at least define the review objectives over a given period in the contract.

d. Notifications. All participants in a design review should be given adequate notification to allow for adequate preparation. The FAA requires formal notification at least 10 working days prior to each Formal Design Review. The FAA should be provided similar notification for more significant informal Detailed Design Reviews. Invited contractor personnel should be given at least 10 working days advance notification for all design reviews they are to attend. The Formal Design Review notification should be accompanied with a review data package, which is comprehensive enough to allow all attendees to be thoroughly prepared at the review. The advance package should always include an agenda and a list of all invited attendees and their responsibilities. Similar advanced packages should also be provided to the attendees of the detailed design reviews.

e. Minutes Documentation. A formal, standardized format shall be established for the documentation of all design review actions and/or findings. For Formal Design Reviews, the documented minutes must be submitted to the FAA, per DID R-12, DESIGN REVIEW REPORT (Appendix 3). The content of the design review minutes should be representative of at least the following information items.

(1) Technical and/or Functional Description of the design or equipment or study under review.

(2) Review Board actions listing, for Formal Design Review.

(3) Approved Design Changes listing and description, with effective dates.

(4) "Open" problems listing, with corrective actions and their status.

(5) OPR identification for listed problems and actions.

(6) Bases for all decisions.

47. THE DESIGN REVIEW BOARD AND REVIEW PARTICIPATION (S3.5.6 - S3.5.6.2). The TECHNICAL Effectiveness of the design review effort can be no better than the combined technical competence supplied by the Design Review Board. However, to have any real impact on the PROGRAM, the Design Review Board must be vested with adequate authority, and given full top-management support.

a. Review Board Structure. The Design Review Board organized for a particular program is composed of a panel of PERMANENT members, supported by specialized, AS REQUIRED, talent in specific technical areas. The permanent Review Board should consist of: the Project Engineer, a Reliability Engineer, a Maintainability Engineer, a Value Engineer, and one or more Senior Design Engineers. Specialists should then be made available to the Permanent Board as the need arises. (The supporting specialists should participate only when actually needed; and should be dismissed as soon as possible.) The full Permanent Design Review Board shall preside over all Formal Design Reviews. The entire permanent board will not normally preside over the informal, detailed design reviews. However, in the latter case, all decisions shall be submitted to the permanent Design Review Board for approval.

b. Basic Participation Requirements. Design reviews, particularly the Formal Design Reviews, too often are merely staged affairs that simply reflect the results of previous meetings. This approach should be avoided. The design reviews should be treated as active engineering; and the reviews should indicate

thorough preparation and attention to detail by all active participants.

(1) The design engineer must be prepared to defend all decisions reached by him, by presenting any required studies, calculations, and/or test data.

(2) A thorough pre-review analysis of potential problem areas should be performed by all engineers invited to attend the Review.

(3) All change recommendations by participating engineers should be accompanied by detail indication of the expected impact on equipment characteristics.

(4) A-priori Design Disagreements. When the Review Board has a-priori information on areas of disagreement with the designer, the designer should be notified of such in sufficient time before the formal meeting to allow assembling of any required supporting reference material.

c. Design Review Primary Responsibilities.

(1) Program (Project) Manager. The Program (Project) Manager shall be the Office of Primary Responsibility (OPR) for the Design Review Program. As such, the program manager shall be directly responsible for the conduct of the Formal Design Reviews; and for all Review documentation preparation and distribution. Depending on the complexity of the contract, similar responsibilities for detailed design reviews may be delegated to lower levels of management.

(2) Reliability Program Manager. The reliability program manager shall be the OPR for the reliability aspects of the design review program. This shall include the responsibility for reliability preparation, reliability participation, and all post-review analysis or other followup pertaining to reliability. The reliability program manager also normally acts as a member of the Permanent Design Review Board.

48. GENERAL RELIABILITY REVIEW CONSIDERATIONS (S3.5.6, S3.5.6.3).

a. Basic Reliability Review Factors. Following are the more basic reliability review factors, and/or considerations, applicable to the general Design Review. Some will not be applicable to specific reviews on a specific equipment or design. And, the required stress to be placed on the factors will depend on the objectives of the specific Design Review.

(1) Performance requirements and definitions of failure.

(2) Apportionment and modeling techniques; and allocated reliability requirements.

(3) Prediction of current specific design reliability, relation to goal, and impact on over-all equipment reliability.

(4) Reliability growth potential.

(5) Failure Mode Analysis (FMEA) of the specific design. In design stages, reduction of marginal failure modes is stressed, with error and/or tolerance studies where indicated.

(6) Reliability Design Guidelines review and compliance verification. Guidelines reviewed at PDR, compliance then followed.

(7) Use Environments to which the subject item will be subjected (including consideration of operational, storage, transport, and production-process environments).

(8) Design optimization trade-offs considering reliability, maintainability, performance, weight, space, power, cost, and schedule.

(9) Tests, plans and results of tests conducted to date (including reliability, performance, environmental, and stress test data).

(10) Specifications for reliability requirements on tests and hardware.

(11) Plans (including identification of OPR's) for reliability improvement and problem resolution.

b. The Design Review Check List. To ensure that the Design Review is carried out expeditiously and that all pertinent factors are considered, a Design Review Check List should be prepared prior to the Review. The applicable check list should form a part of the pre-review data package delivered to invited Design Review participants. The Reliability Design Guidelines (see paragraph 42.), which are reviewed at the PDR, should contain the Reliability Review Check List(s) to be applied in the following Formal Design Reviews and detailed design reviews.

49. THE FORMAL STUDY REVIEWS (S3.5.6.1). The Study Design Review (SDR) is applied to the "study contract". The subject "study" may range from broad concept or feasibility investigations to reliability analyses on specific designs and/or existing equipments. SDRs are applied to at least two Study Contract milestones. The objectives for SDRs are very specific to the particular study; and can only be defined here in very broad terms. The basic, over-all objective for the SDR effort is to monitor technical progress and assure valid completion of the required investigations.

a. The Initial SDR of a study has the following general objectives.

(1) Ensure adequate consideration is given to reliability as a study factor (in a multi-discipline study).

(2) Evaluation of the preliminary reliability study results and methods used.

(3) Identification of "holes" in data and/or analyses, and review of proposed resolution.

(4) Validate applicability of planned analysis methods for continuing study; and define expected and/or required results.

b. Intermediate SDRs, if held, have essentially the same objectives as the initial SDR - differing primarily in the specific subjects. Thus, the intermediate SDRs would have the following general objectives.

(1) Evaluation of the reliability study results to date.

(2) Re-evaluation of the previously identified "holes" and review resolution status.

(3) Review the analysis, and/or data input, requirements for study completion; and plans for fulfillment.

c. The Final SDR is held some time before submittal of the final report for the study; and the objectives are therefore directed to that end. The general objectives for the final SDR are the following.

(1) Final Review of reliability study results, and the documentation thereof.

(2) Review study requirements against results, and plans for removal of any "holes" or inadequacies.

(3) Review final report requirements and planned inputs.

50. RELIABILITY IN THE PRELIMINARY DESIGN REVIEW (PDR) (S3.5.6, S3.5.6.2). The Preliminary Design Review (PDR) is the first defined Formal Review point following initiation of the equipment contract effort. The PDR must be performed before final commitment to the basic design approach for the Contract End Item. This formal technical review is performed by the contractor based on review criteria and agenda submitted to, and approved by, the FAA.

a. Basic Requirements. The basic objective of the PDR is the evaluation of the engineering design approach to assure that the specified reliability requirements for the End Item can be satisfied. In general, separate design reviews are not justified for each separate engineering discipline. Instead, reliability specialists should be included on the Design Review Board; and reliability design evaluated as an integral part of the equipment design. However, a distinct evaluation of the reliability design is generally required prior to the PDR in order to establish the necessary Review inputs.

b. PDR Reliability Activity. The following items are representative of the reliability engineering activity required to prepare for, and participate in, the PDR.

(1) Identification of reliability design factors for consideration in establishing the review agenda.

(2) Assessment of Functional FMEA impact; and implications of unresolved findings.

(3) Reliability Block Diagram and Mathematical Model preparation and validation.

(4) Assessment of reliability prediction (based on design approaches) in relation to specified requirements and allocations.

(5) Identification of "high-risk" areas in reliability design and evaluation of design approaches.

(6) Reliability Design Guide preparation and evaluation. (See paragraph 42. of Handbook.)

(7) Evaluate adequacy of Reliability Program Plan.

(8) Review adequacy of Reliability Test Program, and compatibility with over-all test programs.

51. RELIABILITY IN THE CRITICAL DESIGN REVIEW (CDR) (S3.5.6, S3.5.6.2). The next Formal Review point following the PDR is the Critical Design Review (CDR). The CDR is performed at the time when the detailed design is essentially complete.

a. Basic Objectives and Requirements. The CDR is performed to evaluate the final design prior to committing the design to fabrication. The Review includes a critical evaluation of "build to" detailed specifications that will eventually form the technical input to the Configuration Baseline for production. Reliability engineering participation follows essentially the same general procedures as for PDR; except that they should be more critical.

b. CDR Reliability Activity. The following are representative of the reliability engineering activities required to prepare for, and participate in, the CDR.

(1) Identification of reliability design factors for consideration in establishing the CDR agenda, concentrating on "high-risk" areas identified in PDR.

(2) Identification of reliability factors critical in fabrication (such as handling requirements, process controls, testing requirements, etc.).

(3) Evaluation of reliability effectiveness of designs in "high-risk" areas identified in PDR.

(4) Review of Compliance with Reliability Design Guide, and assessment of impact of deviations.

(5) Assessment of Circuit-level FMEA impact; and implications of unresolved findings.

(6) Appraisal of Reliability Program general effectiveness.

(7) Assessment of up-dated, stress-analysis, detailed reliability predictions (supported by any available test data) in relation to requirements and allocations.

(8) Review of proposed production specifications; and validation of completeness and accuracy of reliability inputs.

52. RELIABILITY IN THE FIRST ARTICLE CONFIGURATION INSPECTION (FACI) (S3.5.6, S3.5.6.2). The First Article Configuration Inspection (FACI) is the final Formal Design Review point. At this point, the first equipment produced is compared with the verified requirements of the production specification. The FACI establishes the Product Configuration Baseline; and forms the basis for formal acceptance of the final production specifications.

a. Basic Requirements. The production specifications reviewed in CDR do not contain explicitly defined reliability performance requirements. The assumption is that the required level of reliability will be achieved if the production specification requirements are met. However, it is still necessary to verify achievement of the required reliability by the production process.

b. FACI Reliability Activity. In support of FACI, the basic task of reliability engineering is to assure that the required level of reliability is NOT DEGRADED by differences between specifications and the actual produced hardware. The following are some of the specific reliability analyses required to support this evaluation.

(1) Assessment of the reliability impact indicated by the results of all tests preceding FACI.

(2) Evaluation of the attention paid to the Reliability Factors Critical in Fabrication (identified in CDR).

(3) Review of design and/or configuration changes for production, to assure that design reliability is not degraded.

53. DETAILED DESIGN REVIEW ACTIVITY. The detailed design reviews are directed toward the detailed review and evaluation of specific circuit designs. The findings of these reviews are used to institute immediate corrective action; and, to prepare the required inputs for the following Formal Design Review. The specific number of such detailed reviews, and their scheduling, will vary as a function of equipment complexity, types of circuits and hardware, and schedule and personnel limitations.

a. Basic Objectives. The detailed design reviews can be categorized as a function of their time relationship to the Formal Equipment Design Reviews. Thus, detailed design reviews are classed as occurring Pre-PDR, Post-PDR and Pre-CDR, or Post-CDR and Pre-FACI. All have two basic objectives. The first is to evaluate the progress toward allocated reliability goals and identify the need for re-allocation. The second basic objective is the identification of problem, or "high-risk", areas. The type of problem pursued in the second objective will depend on the phase category of the review.

b. Pre-PDR Design Reviews. These detailed design reviews are performed on a continuing basis, as the basic design approaches are developed. Some of the associated reliability engineering activities are given by the following items.

(1) Estimates of achievable reliability for design review subjects, and impact on overall reliability requirements.

(2) Evaluation of allocated reliability goals feasibility.

(3) Functional FMEAs directed toward identification of potential equipment design problems.

(4) General preparation for PDR.

c. Pre-CDR/Post-PDR Design Reviews. These are performed as the detail designs develop. Emphasis is placed on those areas previously defined as having potential design problems and those identified as "high-risk" in PDR. Special attention is also paid to follow-up on any other open problems defined by the PDR findings. The following are representative of the associated reliability engineering activities.

(1) Review designs for Reliability Design Guide compliance.

(2) Detail-stress reliability predictions for the review subjects.

(3) Evaluate predicted reliability against allocation, define impact on equipment reliability requirement, and identify any need for goal reallocation.

(4) Detailed, Circuit-level, FMEAs, concentrating on previously identified "high-risk" areas; and directed toward identification of potential circuit design problems and Critical Reliability Factors for special fabrication attention.

(5) Follow up on resolution of "open problems" identified by PDR.

d. Pre-FACI/Post-CDR Design Reviews. In this phase, the basic reliability activity is directed toward preparing inputs to the FACI by monitoring design changes for production, and by monitoring test results. Particular attention is directed to the CDR-identified Critical Reliability Factors (for special production attention). Specific reliability review activities should include the following.

(1) Follow up on resolution of "open problems" identified by CDR.

(2) Evaluate each design and/or component change for impact on overall equipment reliability requirements.

(3) Monitor configuration development and changes, and evaluate potential effect on reliability.

(4) Analyze test data for equipment reliability impact.

(5) Prepare final prediction of reliability, taking into account information gained in above.

SECTION 7. EFFECTS OF STORAGE, SHELF-LIFE, PACKAGING, TRANSPORTATION, HANDLING, AND MAINTENANCE

54. EFFECTS OF STORAGE, SHELF-LIFE, PACKAGING, TRANSPORTATION, HANDLING, AND MAINTENANCE. Storage, shelf-life, packaging, transportation, handling, and maintenance are very real life-cycle factors with a potential for degrading equipment reliability in the field. Hence, the potential reliability effect of these factors must be evaluated; required limits on the factors must be defined; and procedures must be established for minimizing their reliability effect. The determined effects, limits, and procedures shall be documented in the submitted RELIABILITY ALLOCATIONS, ASSESSMENTS, AND ANALYSIS REPORT (DID R-2 of Appendix 3.). The analyses and/or considerations required for this effort shall include at least the following.

a. Age and/or Environment Sensitivity. Identify the major or critical characteristics of equipment elements which deteriorate with age and/or environment. For these elements, establish environmental limits for the life-cycle phase of the element (including storage, transportation, and operation); and relate these to the environments defined, or expected, for the contract equipment. Also, establish the storage, shelf-life, and operational life limits for these elements. Define any special tests, inspections, preventive maintenance, or other procedures required for the storage phase to minimize the effect of storage and assure element reliability.

b. Maintenance Effects. Define the maintenance philosophy required to obtain, and retain, the required equipment reliability. Relate deviations from this philosophy to their potential effect on operational reliability. Specifically define any special maintenance and restoration procedures which must be followed to avoid reliability degradation.

c. Packaging, Transportation, and Handling. Determine the aspects of packaging, transportation, and handling with a significant potential for degrading the equipment reliability. Define the equipment elements specifically affected, the effect, and the reliability impact. Define the special procedures recommended or required to overcome the potential problems, minimize their occurrence, and/or lessen their reliability effect.

SECTION 8. DESIGN SPECIFICATION, DRAWING RELEASE, AND DESIGN CHANGES

55. DESIGN SPECIFICATION INPUTS (S3.5.1.5). As part of the "system" design task, the contractor will develop performance requirements for equipment elements. These are then imposed through design specifications or procurement specifications.

    a. Design Specifications. Design specifications are issued for those elements to be designed and developed by the contractor. The allocated reliability goals must be made a part of each design specification. Where applicable, each goal must be accompanied by specified reliability verification, or assurance, test requirements.

    b. Procurement Specifications. When the equipment element is to be procured from, and/or developed by, an outside source, a procurement specification is issued. Direct procurements, with no development involved, require only the specification of an explicit or implicit reliability requirement. Where the procurement involves development, acceptance criteria and/or a reliability program shall also be specified. Requirements for SUPPLIER AND SUBCONTRACTOR CONTROL are fully discussed in paragraph 25. of this Handbook.

    c. Reliability Review. All design and procurement specifications shall be reviewed by a reliability engineer to ensure that the allocated reliability goals and test requirements are indeed imposed. The procurement specifications shall be reviewed to ensure that any required reliability programs are also, indeed imposed.

56. DESIGN APPROVAL (S3.5.7). A reliability engineer shall review, and APPROVE by signature, all design drawings, schematics, and associated material lists before they are released to fabrication. A minimum design approval review consists of the following elements.

    a. Design Review Compliance. Verify compliance with findings of previously held detailed design review, and evaluate the effect of any deviations.

    b. Part Selection. Verify acceptability of the specified parts.

c. Packaging or Configuration. Evaluate the drawing for potential packaging and/or configuration problems, with special attention to thermal aspects.

d. Reliability Assessment. Compare the up-dated reliability prediction for the design against its allocated reliability requirement.

57. ENGINEERING DESIGN CHANGES (S3.9). All engineering design (and part) changes made after release to fabrication shall be monitored for possible reliability degradation. Changes in an equipment element are evaluated for their reliability effect relative to the allocated reliability requirement for that element. Changes causing a degraded element reliability, or with a high potential for such degradation, shall be identified; their specific effect on the element reliability determined; and the impact on achievement of the equipment reliability requirement evaluated. The identification, reliability determination, and impact evaluation shall be fully documented and presented to the Change Control Board for the project.

SECTION 9. RELIABILITY TESTING

58. THE RELIABILITY DEVELOPMENT TESTING PROGRAM (S3.7.1.1). Achievement of high inherent reliability in the product is dependent on the degree to which the design has been guided and verified by reliability testing during development. Development testing is an empirical technique used to generate information that is not otherwise available - because of the inadequacy and/or difficulty of a purely analytical approach. Development testing is also used to satisfy a management need for "proof" of results being achieved, before commitment to production.

a. Test Objectives in Development. Development tests are employed by the designer to evaluate the adequacy of his design, and to point out its weaknesses. Such tests may be thought of as DESIGN TECHNIQUES, in that the test results are applied directly to the problem of design refinement. At the same time, development tests provide management with direct evidence of design status with respect to over-all requirements. Relative to the Reliability Program, the following are the basic development test objectives.

(1) To measure the reliability of a new item, with unknown characteristics.

(2) To verify the predicted, and/or specified, reliability of an equipment element.

(3) Selection of design approaches for reliability.

(4) Determine relationships between parameters which influence reliability.

(5) Provide "status" inputs to the management monitoring of the reliability program.

b. Effective Tests. Reliability test methods in development are, in general, "designed experiments". The test conditions and methods of data analysis are pre-planned on the basis of engineering and statistical considerations. To obtain the desired, effective results, each of the following steps must be considered and completed for each test. Each of the steps should be sufficiently documented to allow total repetition of the test.

(1) Define the Specific Test Objective(s).

(2) Establish the Required Test Conditions (including consideration of environment, failure definitions, acceptable risks, discrimination ratio, etc.).

(3) Design or Select the Test Plan (including definition of decision criteria, sample requirements, length of test, etc.).

(4) Define the Test Configuration and Procedures for implementing the Plan.

(5) Implement the Test and collect the required data.

(6) Analyze the data to fulfill the test objectives.

c. Test Design Considerations. When properly planned for, much of the development testing conducted for performance information can be designed to simultaneously yield the desired reliability information; with very little alteration in test plans. In other instances, there is no alternative but to design and conduct a test purely for reliability investigation or verification purposes.

(1) Basic Test Requirements and Limitations. The design and implementation of a development program must weigh and balance the engineering and statistical requirements for accomplishing the test objective, and the administrative limitations.

(a) Engineering requirements dictate the environmental stress levels, duty cycles, range of applications, and performance limits to be used in defining success or failure of the item under test.

(b) Statistical requirements relate to the desired accuracy of results, the order and manner of selection and testing, and the confidence which can be placed in the decisions made.

(c) Administrative limitations pertain to the practical limitations on time, funds, and facilities which may necessitate compromises in the engineering and/or statistical requirements.

(2) Test Design Options. To optimize test design with respect to the above requirements and limitations, it will be necessary to either trade-off within test parameters without compromising results validity; or trade-off test parameters against results validity.

(a) Sample size and test time. Consideration may be given to using smaller sample sizes with longer test times versus larger sample sizes with shorter test times.

(b) Accelerated tests. Consideration may be given to the feasibility of using accelerating test conditions in order to induce more failures, when the effects of such accelerated conditions on failure modes are KNOWN. Although the effects of accelerated conditions on parts failure modes and rates are known in certain instances, it is generally not feasible to translate these effects into predictions of the equipment failure behavior.

(c) Test Confidence. Consideration may also be given to sacrificing test confidence level, thus permitting a reduction in sample size or test time, in order to conform to existing administrative limitations.

59. TYPES OF RELIABILITY DEVELOPMENT TESTS (S3.7.1.1). Reliability tests in development fall into two basic categories: Investigative Tests and Decision-Making Tests. Certain fundamentals of test design must be understood and translated into "reliability test" design criteria. Tests and Test Objectives within the two basic categories of development testing are described in the following sub-paragraphs.

a. Investigative Tests. Investigative Tests are TESTS OF INQUIRY, and are thus intended to provide data for FORMULATING HYPOTHESES. In the reliability investigative test, an experiment is designed to FORMULATE a hypothesis about the reliability of a product or a process. On the basis of the test results, a hypothesis of cause and effect relationships is formulated for design guidance (pending VERIFICATION by the second type of test). Investigative tests applied to reliability problems are of two types: Measurements Tests and Relationship Evaluation Tests.

(1) Measurement Tests. These are designed to MEASURE the reliability of an item (with confidence limits applied). Reliability measurement tests should be conducted under known, controlled operating conditions - simulating expected field conditions. The operating times accumulated and the number of failures observed provide the basis for calculating failure rate or MTBF. Confidence limits are directly related to the number of failures observed. This investigative test does NOT presuppose, or predict, a reliability; but rather depends upon the analysis of test data to DETERMINE the reliability.

(2) Relationship Evaluation Tests. These are designed to evaluate relationships between environments or stresses and parameters which influence failure rate (i.e., reliability). Part-to-part variations and changes in environmental conditions cause corresponding changes in circuit or equipment parameters (such as output power or voltage, frequency stability, and failure rate). Knowledge of the relationship between variables can be obtained through a planned relationship evaluation test program, utilizing REGRESSION ANALYSIS techniques. Regression analysis is a statistical technique which quantitatively defines the "best" fit or relationship between a set of variables, based on the observed test data.

b. Decision-Making Tests. Decision-making tests are intended to VERIFY HYPOTHESES about reliability, and are therefore called TESTS OF HYPOTHESIS. The decision-making test is designed to verify whether or not a predetermined hypothesis about reliability behavior is in fact met. Decision-making tests applied to reliability decisions fall into two broad categories: Reliability Verification Tests and Reliability Comparison Tests.

(1) Decision Risks. A statement or hypothesis is first made concerning the items to be tested. Decision criteria are then established; so that simple inspection of test results will determine whether to ACCEPT or REJECT the a-priori hypothesis. Two types of risk are always associated with the accept or reject decisions - faulty acceptance and faulty rejection.

(a) Rejection Risk. This is the risk of rejecting a hypothesis when in fact it should have been accepted. This is normally denoted by α . (Note that in Demonstration or Acceptance testing, this is referred to as the PRODUCER'S RISK.)

(b) Acceptance Risk. This is the probability, or risk, of accepting a hypothesis when in fact it should have been rejected. This is normally denoted by β. (Note that in Demonstration or Acceptance Testing, this is referred to as the CONSUMER'S RISK.)

(2) Reliability Verification Tests. Verification tests are used to verify whether a desired (predicted or specified) reliability result has, or has not, been obtained. The test is usually used to provide the development team with "proof" (with confidence limits) that the design has in fact achieved the specified, or allocated, reliability. As a secondary objective, estimation of observed reliability is also obtained.

(3) Reliability Comparison Tests. A problem frequently confronting the designer is to select the more reliable of two options. These may be options of parts, of design approaches, of processes, or of environments. Usually the choice is on the basis of which is the more reliable; and the test is designed to determine the acceptability of the hypothesis that there is no reliability difference. In some cases, the choice will be made on the basis of a specified degree of difference.

60. THE RELIABILITY DEMONSTRATION TEST (S3.7.1.2). The reliability demonstration test is intended to evaluate the acceptability of the hypothesis that the equipment meets the specified reliability performance requirement (usually in terms of a specified MTBF).

a. Important Test Parameters. The following parameters are used to define the test (usually sequential) required for demonstration. These will normally be imposed, or specified, in the procurement documentation.

(1) Specified MTBF. The MTBF specified as a performance requirement is normally the nominally acceptable value in the demonstration test. It is denoted by θ_o.

(2) Minimum Acceptable MTBF. This is used to define the unacceptable range of MTBF's, and is denoted by θ_1.

(3) Discrimination Ratio. This is simply the ratio of the Specified MTBF (θ_o) to the Minimum Acceptable MTBF (θ_1).

(4) Producer's Risk. This is the probability (normally stated in percentage) of rejecting an equipment whose true MTBF is actually equal to the θ_o value. It is the risk taken by the contractor in the demonstration test. The producer's risk is denoted by α.

(5) Consumer's Risk. This is the probability of an equipment being accepted whose true MTBF is equal to the θ_1 value. It is the risk taken by the FAA when it determines acceptability on the basis of a demonstration test. The consumer's risk is denoted by β.

b. Test Requirement. The required demonstration test, test conditions, and definition of test subject are normally imposed on the contractor by specification in the procurement documentation. The imposed test plan will normally be one selected from MIL-STD-781, RELIABILITY TESTS: EXPONENTIAL DISTRIBUTION. The imposed test shall be performed.

(1) Alternate. Where the test plan is not specified (and/or the test requirement is otherwise not fully defined) in the procurement documentation, the contractor shall select a test plan from MIL-STD-781, and fill all other "holes", following Handbook paragraph 17, SELECTION AND SPECIFICATION OF THE RELIABILITY TEST, for guidance as to requirements. The selection and completion shall be submitted as a proposed RELIABILITY TEST AND DEMONSTRATION PLAN (per the requirements of DID R-5 of Appendix 3).

(2) Plans and Procedures. The contractor is required to submit an initial Demonstration Plan with his proposal; and a final Plan soon after contract award. The requirements for a RELIABILITY TEST AND DEMONSTRATION PLAN are fully described in

DID R-5 of Appendix 3. Some time before the actual conduct of the test, the contractor will be required to submit ACCEPTANCE TEST PROCEDURES, whose contents shall be in accordance with the requirements of DID R-6 of Appendix 3.

61. RELIABILITY ACCEPTANCE TESTS IN PRODUCTION (S3.7.1.4). Whereas the Demonstration Test is intended to QUALIFY an equipment design, Production Acceptance Tests are intended to indicate continuing PRODUCTION of ACCEPTABLE equipment (of a previously qualified design). Production Reliability tests are performed periodically, on SAMPLES from production lots.

a. Test Requirement. The required test plan, environment, basic test conditions, sample size, and production "lots" to be tested are normally all specified in the procurement documentation. If they are not specified, the contractor shall fill any "holes", proceeding as described for the reliability demonstration test in sub-paragraph b.(1) of the preceding paragraph 62.

b. Lot Acceptance. Lot acceptance shall be based on reaching an ACCEPT decision in the Production Acceptance Test applied to the lot. In the event of a REJECT decision, all shipments shall be stopped until any required corrective action is ACCOMPLISHED and the equipment accepted. If the corrective action is NOT a DESIGN CHANGE, the Production Acceptance Test shall be repeated as specified originally. If the required corrective action IS a DESIGN CHANGE, a full Reliability Demonstration Test shall normally be required before Production Acceptance Testing is allowed to resume.

c. Plans and Procedures. With regard to requirements for Test Plans and Procedures, Production Acceptance Tests shall be treated in the same manner as the Demonstration Test; and the documentation shall be as described in subparagraph b. (2) of the preceding paragraph 62.

62. RELIABILITY TESTING PLANS, PROCEDURES, AND REPORTS (S3.7.2 - S3.7.4, S3.7.7.5). Test Plans, Procedures, and Reports constitute the basic deliverable documentation on reliability tests. The following subparagraphs relate required documentation to the types of reliability tests that must be covered.

a. Reliability Demonstration Plan. When a Reliability Demonstration Plan is specified (paragraph 3.7.3 of FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT), plans shall be provided for all required Reliability Demonstration Testing and Production Acceptance Tests (paragraphs 3.7.1.2 and 3.7.1.4, respectively, of the FAA Specification). The Plans shall be prepared per the requirements for the RELIABILITY TEST AND DEMONSTRATION PLAN as defined by DID R-5 of Appendix 3.

b. Reliability Test Program Plans. When a Reliability Test Program Plan is required (paragraph 3.7.2 of the FAA RELIABILITY PROGRAM REQUIREMENTS Specification), it shall incorporate any requirement for a Reliability Demonstration Plan per the preceding. Two separate documentations are NOT required. Thus, specification of a Reliability Test Program Plan imposes required documentation of all specified reliability tests and test program - including Development Testing, Reliability Demonstration Tests, Conditioning Tests, and Reliability Production Acceptance Tests (paragraphs 3.7.1.1, 3.7.1.2, 3.7.1.3, and 3.7.1.4 respectively of the FAA Specification). The Reliability Test Program Plan shall be documented per the requirements for the RELIABILITY TEST AND DEMONSTRATION PLAN as defined by DID R-5 of Appendix 3.

c. Reliability Test Procedure. The specification of a documented Reliability Test Procedure (paragraph 3.7.4 of the FAA RELIABILITY PROGRAM Specification) is intended to apply to Reliability Demonstration Testing, Conditioning Tests, and Reliability Production Acceptance Tests. Deliverable Documentation of Test Procedures is NOT required for the Development Tests (paragraph 3.7.1.1 of the FAA Specification). Documentation of the required Reliability Test Procedures shall fulfill the requirements for the ACCEPTANCE TEST PROCEDURE as defined by DID R-6 of Appendix 3, as applicable to the specific test.

d. Reliability Test Report. The requirement for a fully documented Reliability Test Report (paragraph 3.7.7.5 of the FAA RELIABILITY PROGRAM Specification) is intended to apply to ONLY the Reliability Demonstration Tests and the Reliability Production Acceptance Tests. Delivered Documentation of the Reliability Test Report shall fulfill the requirements for the RELIABILITY TEST

AND DEMONSTRATIONS REPORTS as defined by DID R-8 of Appendix 3.

SECTION 10. FAILURE DATA COLLECTION, ANALYSIS, AND CORRECTIVE ACTION

63. DESIGN OF A FAILURE REPORTING AND DATA COLLECTION SYSTEM (S3.8). The design and implementation of an effective failure reporting and data collection system is the backbone of the Failure Data Collection, Analysis, and Corrective Action Program. Failure reporting and data collection is an essential link in the events controlling reliability growth of the product to achievement of the reliability requirements. Design of an effective reporting and data collection system requires consideration of the following factors. (Corrective Action and Failure Analysis will be treated in following paragraphs.)

a. Objectives of the Failure Reporting and Data Collection System. A clear statement of the ultimate objectives is necessarily the first step in the design of the failure reporting and data collection system. The basic reliability objectives are to provide or establish the following.

(1) Failure frequencies and failure patterns.

(2) Failure cause and effect relationships.

(3) Equipment effectiveness evaluations.

(4) Corrective Action priorities.

(5) Timely and Appropriate Distribution of data, results, and assignments.

b. Data Processing Techniques. Data processing in support of the objectives may be performed manually and/or by computer. The procedure to be used will be a function of the data volume expected, schedule restrictions, computer service availability, and economical factors. The specific processing procedure to be used within each objective should be defined prior to establishing the Data Requirements and Data Collection Forms.

c. Data Requirements. The type of data INPUT required is dictated by the objectives (and the analyses required in fulfilling the objectives). Since reporting of findings is an integral part of the failure reporting and data collection system, it is equally important to define the type of data OUTPUTTED from analyses. The minimum data element (input and output) coverage of the Data Collection

System shall be as defined in Data Item Description R-4 (FAILURE DATA REPORTING AND FEEDBACK, FAILURE SUMMARY REPORTS) of Appendix 3. It is also necessary to define the required FORMAT for inputted data; as dictated by the specific processing techniques to be applied.

d. Establishment of Data Collection and Distribution Procedures. Data collection procedures may now be established, once the data requirements have been defined. A major element in implementing data collection is the failure report form on which the raw data are recorded. This is the major link between the operational activities and the analysis activities. Procedures must also be established for getting the appropriate raw data to the appropriate analysis activity; and for documenting the analysis results. Finally, it is important that a specifically pertinent distribution be established. Personnel requiring data and/or analysis results should be able to get the specific information required, and NO MORE.

(1) Failure Report Form Considerations. A well-designed report form is a key element in establishing an effective failure reporting and data collection system. The data form should, therefore, meet the following general criteria.

(a) No Superfluous Data. No data should be required which is not needed. Avoid requiring data which is "interesting" but has no application to the objectives of the data system.

(b) Analysis Compatibility. The format should permit recording of all essential data in a format compatible with the analyses to be performed.

(c) Processing Compatibility. The data should be presented in a format suitable for direct use in the specific processing procedures to be used. This includes appropriate coding for computer processing, when such is the case.

(d) Reduction of Human Error. To encourage accurate data recording, sources of human error should be minimized. The format should not be confusing. The instructions must be adequate. The form itself should be

as self-explanatory as possible, minimizing the use of coded, or keyed, explanations.

(2) Central Data Activity. A central data activity shall be assigned the responsibility for data collection and distribution. This shall include the raw failure reports, subsequent analyses, and responsibility for the generation and distribution of failure summary reports. The central data activity shall maintain a Central Data File for the project. The Central Data File shall contain all original failure reports, analysis reports, failure summary reports, and a problem vs. corrective action historical file.

e. Subcontractor Interface. The subcontractor interface must be defined and requirements for compatibility established. If a Failure Data Collection, Analysis, and Corrective Action program is required of the contractor, he shall allocate that requirement to his subcontractors. If economically feasible, the subcontractor should be required to use the same forms as those used by the contractor. This is especially important if computerized processing is to be used.

64. THE FAILURE REVIEW BOARD AND CORRECTIVE ACTION (S3.8.2, S3.8.4). Cost-effective reliability growth is possible only by instituting selective, controlled corrective action, based on the indications of the Failure Reporting and Data Collection System. Corrective action procedures, and the related responsibilities of the Failure Review Board, must therefore be clearly established.

a. Corrective Action Procedures. The following are the basic elements of an over-all corrective action program. Procedures must be defined for implementing and/or controlling each of these elements.

(1) Establish Corrective Action Candidates. Candidates for corrective action are established on the basis of the failure reports. It is not necessary or desirable to institute corrective action investigations on all failures. A priority order should be established for attacking suspect problems. One approach is to use the predicted (or "expected") failure rates of each part as a baseline; and then establish a priority by dividing the measured (via the failure reports) failure rate by this baseline.

(2) Assign responsibility(s) for Corrective Action. This shall include the responsibility for determining the cause of the problem, proposing corrective action, and implementing the required "fix".

(3) Define the Failure Analysis Requirements. The objective of failure analysis is to pin-point the cause of the failure problem. Specific Physical Failure Analyses may be required. Analytical investigations will be required to define the cause.

(4) Determine and Propose the Required "Fix". The "fix" for an observed problem may consist of design changes, part changes, test changes, and/or procedural changes. A proposal for a "fix" should be accompanied with the associated time, cost, and effectiveness estimates. The proposal is evaluated by the Design Review Board.

(5) Implement the "Fix". Implementation shall give consideration to questions of the need for retrofitting and the possible need for purging parts from the equipment.

(6) Determine Effectiveness of the "Fix". Until the effectiveness of the fix has been determined, the problem must still be considered to be "open". At this point, it may be desirable to re-evaluate questions of retrofitting and/or part purging.

b. The Failure Review Board. The basic responsibility of the Failure Review Board is to monitor and control the Corrective Action Procedures with the goal of cost-effective Reliability Growth for the equipment.

(1) Responsibility and sole authority for initiating Corrective Actions based on failure data should rest with the Failure Review Board. The Board shall monitor the failure summary reports, supplemented as required by individual reports, to detect the possible need for corrective action. Requests for corrective action, originating outside of the Board, shall be submitted to the Board for approval. The Failure Review Board shall be responsible for establishing the priorities for corrective action candidates.

(2) Proposed "Fixes" shall be reviewed and approved by the Board, prior to active implementation.

(3) Specific Responsibility for each corrective action investigation shall be assigned by the Failure Review Board. Usually, a single responsibility should be assigned for the total resolution of the detected suspect problem - including determination of cause, proposal of "fix", and implementation of "fix".

65. FAILURE ANALYSIS (S3.8.3). A Failure Analysis effort is required to support the Corrective Action program, in verifying the suspect problem and pinpointing the cause. The total failure analysis effort consists of two basic phases: 1) Failure mode analysis on the failed component and 2) Determination of the failure cause. Normally, both phases are required to pinpoint the cause of a failure problem.

a. Failed Component Analysis. This phase is required to verify that the component itself has in fact failed, and to determine the manner or mode of failure. The contractor should have at least a basic laboratory facility for carrying out such investigations. The following are RECOMMENDED capabilities for a basic facility.

(1) Electrical test capability at temperature extremes. Frequently, the observed failure of the component is evidenced only at the temperature extremes. The supposedly failed device should be tested over the full range of temperatures to verify that it was indeed a true failure (and not simply replaced because of bad connections).

(2) Hermeticity testing. Where applicable, package tests for hermeticity integrity should be considered a basic test - performed prior to opening the package. Once the package is opened, evidence of a leaky case is destroyed. Rather than guess at its existence, the investigation can verify the presence or absence of a leak in a supposedly sealed device by the use of available and relatively inexpensive test devices.

(3) X-ray testing. An X-ray capability is also a basic analysis tool - to be employed before opening a package. The presence or absence of foreign particles, broken leads, or cracked

material may be obscured when the package is opened. The equipment need not be expensive.

(4) De-cap and Sectioning Equipment. To examine the inside of a part, such as capped semiconductors and microcircuits, de-cap and sectioning equipment are required - including a variety of appropriate solvents. The specific equipment requirements depend on the type of part to be investigated.

(5) Microscopic Examination. Once the part is opened for inspection, microscopic examination is used to provide insight into the manner of failure. This capability should have a photographic recording accessory.

(6) Options. The preceding provide a basic failure analysis capability. Optionally, more sophisticated and expensive equipment such as infra-red scanners, electron beam microprobes and scanning electron microscopes can be obtained. Outside failure analysis laboratories may be used for special capabilities, not often required. In no case, however, should the vendor of the suspect item be depended on for a failure analysis.

b. Failure Cause Analysis. The first phase of the analysis simply determines the manner of failure. This must then be completed by an investigation directed to determining the CAUSE of the failure. The basic investigation may be of a design analysis or empirical inspection nature. In most cases, this will have to be supported by a statistical analysis. And, in some cases, specific tests may have to be performed to finally pinpoint the cause of the problem.

SECTION 11. DOCUMENTATION AND DATA REQUIREMENTS

66. DELIVERABLE AND NONDELIVERABLE DATA OR DOCUMENTATION (S-general documentation). The documented data items associated DATA OR DOCUMENTATION. The documented data items associated with the Reliability Program are of two contractual categories: Deliverable or Non-Deliverable. Deliverable data items are formally documented and delivered to the FAA as required by the procurement documentation. Certain other data items, although their documentation is imposed by the required Reliability Program, are not delivered to the FAA. However, the latter Non-Deliverable items are subject to review by the FAA - even though they are not formally documented.

a. Data Requirements in the Procurement Documentation. A data requirement in the procurement documentation is not intended to generate any reliability engineering or analysis tasks. The data requirement is intended to document the results and/or procedures of otherwise required reliability tasks.

(1) Deliverable Data Items are specifically required as distinct contractual items, in the "Delivery and Performance Requirements" part of the procurement documentation. The specific data item will be defined here, along with the required delivery schedule. The data item requirement will be related to a full, formal, DATA ITEM DESCRIPTION.

(2) Non-Deliverable Data Items are specified only to the extent of being an element in the imposed Reliability Program (for example, the maintenance of test operation sheets and logs). Delivery schedules and formal DATA ITEM DESCRIPTIONS will NOT be imposed.

b. Data Requirements in the Reliability Program Plan. Data requirements (whether deliverable or non-deliverable) ARE reliability program tasks; and must be so treated in the submittal of the Reliability Program Plan (as described in paragraph 24). Plans for obtaining the required data and accomplishing the required documentation shall be integrated into the Reliability Program Plan. These shall include a detailed schedule for the delivery of Deliverable Data Items, and subsequent up-dates. Where the program requires extensive data and/or documentation, the reliability program plan shall include a description of the Data Control Procedures to be employed.

67. STANDARD DELIVERABLE DATA ITEMS (S-deliverable documentation). Certain items of data will be required on most contracts. Others will ALWAYS be required on particular types of contracts. These are considered to be Standard Data Items. Appendix 3 contains the full DATA ITEM DESCRIPTIONS for thirteen such Standard Deliverable Data Items. The following sub-paragraphs identify each of the thirteen Data Item Descriptions; and summarize the purpose of, and requirements for fulfillment of, the Data Item. References to the FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT, and the present HANDBOOK are also indicated in the following.

a. DID R-1, Reliability Program Plan.

(1) Purpose. Basic documentation of the contractor's planning for implementation of the required Reliability Program. Used by FAA to monitor contractor's reliability effort.

(2) Summary of Requirements. Full description of plans for accomplishing each task of the required Reliability Program, including time-phasing and manloading involved. Definition of techniques for requirements allocation, reliability predictions, reliability demonstration, and Failure Reporting program.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.4.1.1.

(b) FAA RELIABILITY HANDBOOK, paragraph 24.

b. DID R-2, Reliability Allocations, Assessments, and Analysis Report.

(1) Purpose. Used by FAA to (1) evaluate contractor's estimate of equipment reliability; (2) evaluate the current and potential reliability of the equipment; and (3) identify critical design features.

(2) Summary of Requirements. Full disclosure of reliability estimate and analyses used. Description of trade studies involving reliability. Definition of major or critical characteristics of items deteriorating with age. Allocated reliability goals.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraphs 3.5.1.1 through 3.5.1.4.4, 3.5.6.3, and 3.5.8.

(b) FAA RELIABILITY HANDBOOK, paragraphs 28 through 40, 50, and 56.

c. DID R-3, Defective or Inadequate Parts and/or Specifications Notification.

(1) Purpose. Used to notify the FAA of defective parts and/or specifications encountered in the program.

(2) Summary of Requirements. Full definition of defective or inadequate parts, materials, and/or specifications encountered in the program; and their usage in the contract equipment.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.5.2.4.

(b) FAA RELIABILITY HANDBOOK, paragraph 41.

d. DID R-4, Failure Data Reporting and Feedback, Failure Summary Reports.

(1) Purpose. Summary reports used by FAA to monitor contractor's failure data collection system; to monitor the types, severity, and frequency of failures; and to monitor the status of remedial action.

(2) Summary of Requirements. The Data Item defines the scope of the Data Collection system required to obtain the desired Summary Reports. The summaries shall identify the failures; describe the failure symptom, mode, and effect; provide trend analysis data; and define corrective actions and status.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraphs 3.8 through 3.8.2, and 3.8.5 through 3.8.5.2.

(b) FAA RELIABILITY HANDBOOK, paragraph 65.

e. DID R-5, Reliability Test and Demonstration Plan.

(1) Purpose. Provides documentation of contractor's Reliability test program plan and Demonstration plan. Used by FAA to review and evaluate the plans and for subsequent surveillance.

(2) Summary of Requirements. Full disclosure of plan for demonstration of reliability requirements, and plans for implementation of all other imposed reliability testing.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraphs 3.7.2 and 3.7.3.

(b) FAA RELIABILITY HANDBOOK, paragraph 64.

f. DID R-6, Acceptance Test Procedure.

(1) Purpose. Reviewed by FAA for adequacy in compliance with applicable specification requirements; and subsequently used for surveillance of the Acceptance Tests.

(2) Summary of Requirements. Full description of acceptance test objectives, equipment, preconditions, conditions, detailed procedures, and accept/reject criteria and failure definitions. "Acceptance" Tests include - Demonstration, Production Acceptance, and Conditioning Tests.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.7.4.

(b) FAA RELIABILITY HANDBOOK, paragraph 64.

g. DID R-7, Reliability Program Status Reports.

(1) Purpose. Used by FAA for monitoring and evaluating contractor's progress and accomplishments in the required Reliability Program.

(2) Summary of Requirements. General status relative to the Reliability Program Plan. Listing of "open" reliability problems. Comparison of reliability observed, predicted, and required - with trend presentation.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.10.1.

h. DID R-8, Reliability Test and Demonstration Report.

(1) Purpose. These provide the FAA with formal records of required reliability tests and/or demonstrations. Used in evaluating degree of success in the tests.

(2) Summary of Requirements. Full identification of tests, results obtained, and corrective action anticipated. Also imposes a requirement for "hot-line" reports to notify FAA of test emergencies. Normally imposed on only Demonstration and Production Acceptance Tests.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraphs 3.7.7.5 and 3.8.5.3.

(b) FAA RELIABILITY HANDBOOK, paragraph 64.

i. DID R-9, Suspect Material Deficiency Notice, Response.

(1) Purpose. Provides for contractor's RESPONSE to notification by FAA of defective parts, materials, and/or specifications.

(2) Summary of Requirements. Define usage of suspect item and potential effect on equipment.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.5.2.5.

(b) FAA RELIABILITY HANDBOOK, paragraph 41.

j. DID R-10, Critical Items Report.

(1) Purpose. Provides FAA with identification of items deemed critical. Used by contractor for control and/or handling of such items.

(2) Summary of Requirements. Listing of Critical Items, basis for criticality, and definition of control and/or handling requirements.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.5.5.

(b) FAA RELIABILITY HANDBOOK, paragraph 47.

k. DID R-11, Failure Mode and Effect Analysis (FMEA) Report.

(1) Purpose. Used by FAA in review and evaluation of contractor's approach to achieving assured equipment reliability. Used by contractor in design trade-offs, reliability upgrading, and planning of development tests.

(2) Summary of Requirements. The Data Item Description defines the requirements for individual analyses to fulfill the report requirements. The report shall include the individual FMEAs; description of analysis methods and assumptions; summary of corrective actions and status; implications for equipment reliability; and recommendations for further analysis, tests, and/or improved data sources.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.5.4.

(b) FAA RELIABILITY HANDBOOK, paragraphs 44 and 46.

l. DID R-12, Design Review Report.

(1) Purpose. Furnishes formal documentation of proceedings, actions, and results of Formal Design Reviews.

(2) Summary of Requirements. Definition of items reviewed; listing of all review board actions; listing of all "open" problems and corrective actions, with status thereof; and identification of OPR's.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraphs 3.5.6 through 3.5.6.3.

(b) FAA RELIABILITY HANDBOOK, paragraph 48.

m. DID R-13, Parts, Materials, and Processes Application Review Report.

(1) Purpose. Provides formal documentation of contractually required Application Reviews; and serves to identify use of non-standard and/or non-approved parts.

(2) Summary of Requirements. Document application review findings. Identify deviations from allowed (or policy defined) stresses and the reliability impact. Identify and justify the use of nonstandard and/or non-approved parts, materials, processes, or techniques.

(3) Reference Data.

(a) FAA RELIABILITY PROGRAM REQUIREMENTS Specification, paragraph 3.5.2.3.

(b) FAA RELIABILITY HANDBOOK, paragraph 43.

APPENDIX 1. GLOSSARY

1. <u>ABBREVIATIONS AND SYMBOLS</u>. The following are the abbreviations and symbols, with definitions, used in this Handbook.

A ----- Inherent Availability.

A ----- Operational Availability.

CDR ---- Formal Critical Design Review.
DID ---- Data Item Description.
FAA ---- Federal Aviation Administration.
FACI --- Formal First Article Configuration Inspection.
FARADA - Failure Rate Data (Program).
FMEA --- Failure Mode and Effect Analysis.
GIDEP -- Government-Industry Data Exchange Program.
MDT ---- Mean Down Time.
MTBF --- Mean Time Between Failures.
MTBM --- Mean Time Between Maintenance Actions.
MTTR --- Mean Time to Repair.
NAS ---- National Airspace System.
OPR ---- Office of Primary Responsibility.
PDR ---- Formal Preliminary Design Review.
RAC ---- Reliability Analysis Center.
R(t) --- Reliability Function (of time).
SDR ---- Formal Study Design Review.
------ Producer's Risk (also used as parameter in Weibull Reliability Function).
------ Consumer's Risk.
θ ----- Specified MTBF, for Demonstration.

θ ----- Minimum Acceptable MTBF, for Demonstration.

------ Failure Rate (also used as parameter in Weibull Reliability Function).
----- Hazard Rate, Instantaneous Failure Rate.

2. DEFINITIONS OF TERMS. The definitions in MIL-STD-280 and MIL-STD-721 apply to this Handbook, except as they may be added to, or modified by, the following list of definitions for the more significant terms used in this Handbook.

Availability - Probability that an item will be operationally ready when needed at any point during a specified mission or duty time.

Availability, Inherent - "Designed-in" Availability, a function of MTBF and MTTR.

Availability, Operational - "In-use" Availability, a function of MTBF and MDT.

Block Diagram, Reliability - Pictorial, block-diagram, representation of the equipment "success" paths.

Circuits, Equipment - Lowest level sets of interconnected elements with only connector electrical interfaces into the equipment, and providing functions with specifiable performance requirements.

Consumer's Risk - In demonstration testing, the probability of accepting an equipment whose true MTBF is equal to the Minimum Acceptable MTBF.

Development Model - An equipment model used for experimentation and/or testing to: (1) demonstrate the technical feasibility of a design; (2) determine its ability to meet existing performance requirements; (3) secure engineering data for use in further development; and (4) establish technical requirements for prototype contract definition.

Discrimination Ratio - Ratio of the Specified MTBF (θ) to the Minimum Acceptable MTBF (θ).

Equipment - A general term characterizing a broad category of electronic items (as system, subsystem, set, that perform a complete function(s).

Failure Rate - The number of failures of an item per unit measure of life (cycles, time, etc.).

Mathematical Model, Reliability - Mathematical representation of the equipment's "success" paths.

Mean Down Time - Mean Time required to restore an inoperative equipment (or element thereof); including consideration of active maintenance time and logistics delays and administrative delays.

Mean Time Between Maintenance Actions - Mean Time Between Failures of an equipment's elements (regardless of whether or not the equipment's function fails).

Mean Time To Repair - Mean ACTIVE maintenance time required per corrective maintenance action.

MTBF, Minimum Acceptable - Lower bound on the acceptable MTBF in demonstration.

MTBF, Specified - Performance requirement for MTBF, and nominal value for demonstration.

Producer's Risk - In demonstration testing, the probability of rejecting an equipment whose true MTBF is equal to the Specified MTBF.

Production Model - An equipment in its final form of final production design; made by production tools, jigs, fixtures, and methods; and employing approved parts.

Prototype (Preproduction) Model - An equipment model suitable for complete evaluation of form, fit, and performance. It is in final form in all respects; employs final approved parts; and is completely representative of final equipment.

Redundancy - The existence of more than one means, or "path", for accomplishing a given function; i.e., more than one "success" path.

Redundancy, Active - That redundancy where all redundant elements are actively functioning in the equipment; rather than being connected in when needed.

Redundancy, Non-Repairable - That redundancy where corrective maintenance is NOT initiated until failure of the function provided by the redundant elements.

Redundancy, Repairable - That redundancy where corrective maintenance is initiated BEFORE failure of the function provided by the redundant elements, and the function continues during such maintenance.

Redundancy, Stand-by - That redundancy where the alternate is not actively functioning in the equipment, and must be connected in when needed. When not being used, the alternate element may be non-operating, fully-operating, or partially-operating.

Reliability - The probability that an equipment will perform satisfactorily for a specified period of time, when used under specified conditions.

Reliability Requirement - The required or specified level of reliability performance; and given in terms of MTBF, Failure Rate, or Reliability for a specified time.

APPENDIX 2. COMPUTER PROGRAMS

1. EXISTING CIRCUIT ANALYSIS PROGRAMS. A number of circuit analysis programs which are useful to the reliability engineer exist. A list of the most useful ones follows:

NAME	TYPE OF ANALYSIS	SOURCE (See a.)
SCEPTRE	D-C and Transient Analysis of non-linear circuits.	CSC
CIRCUS	Transient Analysis of non-linear circuits.	GE
TRAC	Transient Analysis of non-linear circuits.	GE/CSC
ECAP	Steady state and transient analysis of linear and piece-wise linear circuits.	GE/CSC
MICAP	Analysis of Micro-wave circuits.	TYM

In addition, a comprehensive library of reliability-oriented time-sharing programs is available from Computer Sciences Corporation. These programs are available to Government Agencies through a GSA Service Contract. Program Abstracts of these programs are given in the following paragraphs.

a. Program Sources.

CSC - Computer Sciences Corporation
8278 Colesville Road
Silver Spring, Maryland

GE - General Electric Time Sharing
3550 Wilshire Blvd.
Los Angeles, Ca.

TYM - TYM Share
336 East Kelso
Inglewood, Ca.

2. SYSTEM MODELING PROGRAMS.

a. SYSREL. Simulates a system of components (each having a distribution on time to failure) and determines the distribution on time to failure for the total system. Provides the mean time to failure, the standard deviation, and the highest and lowest simulated times to failure for the specified number of trials. Options include histograms of the simulated failure data.

b. RELAT. Provides the probability of a system accomplishing its mission; when the probability of each component accomplishing its mission and the circuit diagram of the system are specified. The program also provides for sensitivity analysis on any component or group of components.

c. CUSTOM. Provides the capability of modeling the reliability of a system whose outputs or performance can be functionally related to randomized inputs and parameters. Use options include histograms of the simulated data.

d. SENSAN. Provides sensitivity analysis for the model constructed for CUSTOM.

e. BYSREL. Uses new sample data, with the help of Bayes' rule, to modify a given probability assignment for the MTBF for a device.

3. LIFE TESTING PROGRAMS.

a. MTBFS1. Evaluates life testing plans when the user wants to test a number of devices for a relatively short time. The user specifies the number of items to be tested, the length of time each device must operate, and the number of failures that will cause rejection. The program then calculates and plots the probability of acceptance (operating characteristic curve) as a function of the mean time between failure (MTBF).

b. MTBFM1. Evaluates multiple-level life testing plans when the user wants to test a number of devices for a relatively short time, and accepts, resamples, or rejects, based on the number of devices that fail. The user specifies the proposed multiple-level sampling plan; and the program calculates and plots the probability of

acceptance (operating characteristic curve) as a function of the MTBF of the device. User options include a printout of the average number of devices tested as a function of the MTBF.

c. MTBFS2. Evaluates life testing plans when the user tests a fixed number of devices to failure and accepts or rejects based on the total operating hours. The user specifies the number of devices to be tested to failure and the total number of operating hours required for acceptance. The program then calculates and plots probability of acceptance (operating characteristic curve) as a function of the device's mean time between failure (MTBF).

d. MTBFM2. Evaluates multiple-level life testing plans when the user tests a fixed number of devices to failure; and accepts, resamples, or rejects on the basis of total operating hours. The program calculates and plots the probability of lot acceptance as a function of the lot's MTBF. User options include a printout of the average number of devices tested as a function of the MTBF.

e. MTBFS3. Evaluates sampling plans when the user specifies a fixed-length test (for example, 100 hours). The program accepts or rejects, based on the number of failures during this time. The user specifies his life testing plan, and the program calculates and plots the probability of acceptance (operating characteristic curve) as a function of the device's MTBF. User options include the average test time as a function of the MTBF.

4. TEST DATA ANALYSIS PROGRAMS.

a. MTBFL1. Calculates confidence limits in the MTBF when the test specifies running a fixed number of devices to failure. User options include histograms of the test results.

b. MTBFT1. Calculates tolerance limits on time to failure when the test consists of running a specified number of devices until they fail. For example, the program would analyze the test data and tell you that you can be 90 percent confident that less than 5 percent of the devices will fail during the first 100 hours of

operation. User options include histograms of the test data.

c. MTBFL2. Calculates confidence limits on the Mean Time Between Failures (MTBF) from fixed- length test data.

d. MTBFT2. Calculates tolerance limits on the time to failure when the fixed-length test consists of running a specified time (for example, 1000 hours) and recording the number of failures.

5. MIL STANDARDS PROGRAMS.

a. TABFM1. Determines the correct sample size and the acceptability constant according to MIL-STD-414 Standard Deviation Method, Form 1. The program does all table analysis.

b. FM1414. Analyzes the sample data; calculates the quality index, and indicates acceptance or rejection of the lot according to MIL-STD-414 Standard Deviation Method, Form 1. The program does all calculations and table analysis. User options include histograms of the data.

c. TABFM2. Determines the correct sample size and allowable percent defective according to MIL-STD-414 Standard Deviation Method, Form 2. The program does all table analysis.

d. FM2414. Analyzes the sample data, calculates the quality index (single or double specification); determines the estimated percent defective (single or double); and indicates acceptance or rejection of the lot according to MIL-STD-414, Standard Deviation Method, Form 2. The program does all calculations. User options include histograms of the data.

6. LIMIT ESTIMATION PROGRAMS.

a. BINLIM. Computes confidence limits on the reject rate. The exact binominal distribution is used so that limits are accurate for any sample size. The user imputs the sample size and the number of rejects in the sample. The program responds with 50, 75, 90, 95, 99, and 99.9 percent confidence limits.

b. FINLIM. Calculates various sample statistics and provides 50, 80, 90, 95, and 99 percent confidence limits on the lot average when the sample size is a significant portion of the lot. User options include a histogram of the sample data.

c. LINCON. Calculates natural tolerance limits. For example, the engineer would transmit the dimensions of the first 15 parts of the new model produced. The program would then provide tolerance limits that will allow the engineer to be 90 percent confident that 95 percent of the production run will be acceptable. User options include histograms of the sample data.

d. PRDLIM. Calculates prediction limits. For example, if you have tested nine parts and input the results to the program, the program calculates confidence limits on the next observation. User options include a histogram of the sample data.

e. TOLLIM. Calculates natural tolerance limits. For example, the engineer would input the dimensions of the first 15 parts of the new model produced. The program would then provide tolerance limits that allow the engineer to be 90 percent confident that 95 percent of the production run will be acceptable. User options include histograms of the sample data.

7. PROBABILITY CALCULATION PROGRAMS.

a. CHISQ. Performs a Chi Square test on data and calculates the corresponding probabilities (all table analysis is done by the program).

b. PROB. Calculates probabilities for Poisson, Binomial, Exponential, Normal, Hypergeometrics, Chi Square, Chi Square/df, and Weibull distributions.

8. DATA COMPARISON PROGRAMS.

a. COMPAR. Analyzes two sets of data to see if their averages are significantly different. The program tests the data under a number of conditions including variance known or unknown, observations paired or unpaired, variances same or different. The user enters his data and answers a series of questions.

b. MANWUT. Analyzes two sets of data using the Mann-Whitney U Test to determine if there is a significant difference between them. Non parametric tests are used (i.e., the results are good for any distribution).

c. CONTAB. Tests to see if there is significant correlation between factors. For example, do the operators attending the morning training sessions have significantly fewer rejects than those not attending the sessions?

d. MATCH. Tests for a significant difference between pairs of data. It assumes that the data from the two samples are paired (for example, the first observation from the first data set represents the output of worker XYZ before training; while the observation from the second set of data represents the output of worker XYZ after training). The program uses nonparametric tests (that is, the results are good for any distribution). User options include data plotting.

e. TESBIN. Analyzes the results of several samples to see if there is a significant difference between the reject rates. For example, assume Vendor A sent in six parts, one of which was bad; and Vendor B sent in 10 parts, four of which were bad. Is there a significant difference between vendors?

9. DISTRIBUTION TESTING PROGRAMS.

a. CHFTES. Tests data to see if the data could have been the results of a constant hazard function. User options include the plotting of sample data versus the theoretical exponential distribution.

b. NORTES. Tests data for normality. The user enters the data and the program responds by testing the data for normality. User options include plotting sample results against the theoretical normal curve results.

c. RANTES. Tests a sequence of data for having a random order.

d. WBLTES. Tests data to see if the data could be from a specified Weibull distribution. User options include plotting of sample data versus the theoretical Weibull distribution.

APPENDIX 3. DELIVERABLE DATA ITEM DESCRIPTIONS

1. This Appendix contains thirteen Standard Data Item Descriptions; of which, any or all may be called for as Deliverable Documentation in a specific procurement. The titles of the Data Item Descriptions are listed below.

   R-1. Reliability Program Plan.

   R-2. Reliability Allocations, Assessments, and Analysis Report.

   R-3. Defective or Inadequate Parts and/or Specifications Notification.

   R-4. Failure Data Reporting and Feedback, Failure Summary Reports.

   R-5. Reliability Test and Demonstration Plan.

   R-6. Acceptance Test Procedure.

   R-7. Reliability Program Status Reports.

   R-8. Reliability Test and Demonstration Reports.

   R-9. Suspect Material Deficiency Notice, Response.

   R-10. Critical Items Report.

   R-11. Failure Mode and Effects Analysis Report.

   R-12. Design Review Report.

   R-13. Parts, Materials, and Processes Application Review Report.

APPENDIX 4. REFERENCE DOCUMENTS AND SERVICES

1. REFERENCE DOCUMENTS. The following documents provide additional or supporting information with respect to the various aspects of a total reliability effort. The documents are grouped by type of information provided. Some documents provide information for several facets of reliability. However, each document is listed in this handbook as a reference for only a single subject.

   A synopsis of each document is presented in terms of the objective or purpose of the particular document with respect to the heading under which it is listed. The latest issue of a document should be used when seeking reference information.

   a. Definitions.

      (1) MIL-STD-280, Definitions of Item Levels, Item Exchangeability, Models, and Related Terms. Establishes standard terms and definitions to be used in describing the levels of military items and to designate and define item exchangeability, models, and other related terms.

      (2) MIL-STD-721, Definition of Terms for Reliability Engineering. Sets forth definitions of terms most commonly used in Reliability Engineering.

      (3) MIL-STD-1313, Microelectronic Terms and Definitions. Presents a list of terms and definitions applicable to microelectronic devices and techniques.

   b. Reliability Programs.

      (1) FAA Specification, Reliability Program Requirements for Electronic and Associated Support Equipment. Describes reliability programs to be applied to FAA procurements as a function of type of contract and equipment development status.

      (2) MIL-STD-785, Reliability Program for Systems and Equipment Development and Production. Establishes uniform criteria for a reliability program, and provides guidelines for the preparation and implementation of a reliability program plan.

      (3) NHB 5300.4, Reliability Program Provisions for Aeronautical and Space System Contractors. Provides common general requirements for all

NASA Programs to (1) design reliability into aeronautical and space systems, and (2) prevent degradation of the reliability of the design through the succeeding steps from fabrication to end use.

(4) AMCP 702-3, Reliability Handbook. Serves as a guide for Army Materiel Command project and commodity managers and professional personnel in the planning, direction and monitoring of reliability programs.

(5) RADC-TR-67-108, Vol. 1 (DDC No. AD845304) RADC Reliability Notebook, Vol. 1. Provides information in the administrative and technical areas pertinent to guiding the user toward reliability planning and making the reliability-oriented evaluations and decisions which will provide a greater degree of assurance that reliability requirements will be met.

c. Reliability Engineering.

(1) NAVAIR - 00-65-502, Handbook, Reliability Engineering. Presents step-by-step procedures for the definition, pursuit and acquisition of required reliability in Naval weapon systems, equipments and components.

(2) NAVSHIPS 94501, Bureau of Ships Reliability Design Handbook. Concentrates on providing information and guidance to engineer reliability into equipment during the basic design stage.

d. Reliability Mathematics.

(1) Reliability Handbook, B.T. Koslov and I.A. Ushakov, Holt, Rinehart and Winston, Inc., 1970. Contains computational formulas and many illustrative examples of reliability computations the engineer is confronted with in the every-day work of ensuring the reliability of equipment and complicated systems.

(2) System Reliability Engineering, G.H. Sandler; Prentice-Hall, Inc., 1963. General techniques for solving reliability problems are presented. Emphasis is on development of differential-difference equations for systems with constant failure and repair rates.

(3) Reliability Theory and Practice, I. Bazovsky; Prentice-Hall, Inc., 1963. Addresses the quantitative treatment of reliability and shows the reader how to solve reliability problems by analysis, design and testing.

(4) Mathematical Methods of Reliability Theory, B.V. Gnedenko, Yu. K. Belyayev, A.D. Solovyev; Academic Press, 1969. Mathematics of reliability are presented from the standpoints of set theory and statistics.

(5) Mathematical Handbook for Scientists and Engineers, G.A. Korn, T.M. Korn, McGraw-Hill, 1968. Provides a comprehensive reference collection of mathematical definitions, theorems and formulas for scientists, engineers and students.

(6) Models of Failure, I.B. Gertsbakh, Kh. B. Kordonskiy; Springer-Verlag, 1969. Analyzes the relationship between mathematical methods of calculating reliability and the physical nature of equipment failure.

e. Prediction Procedures and Failure Rates.

(1) MIL-STD-756, Reliability Prediction. Establishes uniform procedures for predicting the quantitative reliability of aircraft, missiles, satellites, electronic equipment and subdivisions thereof.

(2) Rolling Contact Bearing Fatigue Studies, R.A. Baughman, General Electric Company, Flight Propulsion Division, Evendale, Ohio. Describes tests for bearing fatigue and correlation of test data with actual bearing life.

(3) Methods for Predicting Combined Electronic and Mechanical System Reliability, IIT Research Institute, 1963. Describes technique for analytically combining reliability of electronic and mechanical devices to obtain overall system reliability.

(4) RADC-TR-108, Vol. II (DDC No. AD821640), RADC Reliability Notebook, Vol. II. Provides failure rates and prediction techniques for specific part types. Appendix describes radiation and space effects on parts and materials.

(5) MIL-HDBK-217, Reliability Stress and Failure Rate Data for Electronic Equipment. Presents failure rate vs. stress and temperature for various electronic parts. Also describes various reliability prediction techniques.

(6) RADC - TR-69-458, Nonelectronic Reliability Notebook. Contains failure rate data for approximately 100 nonelectronic part types in 13 different environmental applications.

(7) NAVSHIPS 93820, Handbook for the Prediction of Shipboard and Shore Electronic Equipment Reliability. Provides failure rate data for classes of equipment, functional circuits, classes of parts and individual parts. Also provides methods for predicting equipment reliability.

f. Testing.

(1) MIL-STD-202, Test Methods for Electronic and Electrical Component Parts. Establishes uniform methods for environmental, physical, and electrical testing of electronic and electrical parts.

(2) MIL-STD-271, Nondestructive Testing Requirements for Metals. Covers requirements for conducting nondestructive tests used in determining the presence of surface and internal discontinuities in metals.

(3) MIL-STD-750, Test Methods for Semiconductor Devices. Establishes uniform methods for environmental, physical, and electrical testing of semiconductor devices. Devices include such items as transistors, diodes, voltage regulators, rectifiers and tunnel diodes.

(4) MIL-STD-757, Reliability Evaluation from Demonstration Data. Presents uniform technical procedures for evaluating achieved reliability, and the necessary inputs and criteria for gathering information.

(5) MIL-STD-781, Reliability Tests: Exponential Distribution. Outlines test levels and plans for reliability qualification or production acceptance tests, and for longevity tests.

(6) MIL-STD-790, Reliability Assurance Program for Electronic Parts Specifications. Establishes criteria for a reliability assurance program to be met by manufacturers qualifying electronic parts to Established Reliability (ER) specifications.

(7) MIL-STD-810, Environmental Test Methods. Establishes uniform environmental test methods for determining resistance of equipment to the effects of natural and induced environment peculiar to military operations. The test methods apply broadly to all types of equipment and generally represent extreme conditions which usually constitute the minimum acceptable conditions.

(8) MIL-STD-883, Test Methods and Procedures for Microelectronics. Establishes uniform methods and procedures for testing microelectronic devices, including basic environmental tests to determine resistance to deleterious effects of natural elements and conditions surrounding military and space operations and physical and electrical tests. Devices include such items as monolithic microcircuits, hybrid microcircuits, microcircuit arrays, and the elements from which the circuits and arrays are formed.

(9) MIL-E-5272, General Specification for Aeronautical and Associated Equipment Environmental Testing. Presents procedures for testing aeronautical and associated equipment under simulated and accelerated climatic and environmental conditions.

(10) MIL-R-22732, Reliability Requirements for Shipboard and Ground Electronic Equipment. Prescribes procedures for evaluation of the reliability performance for shipboard and ground electronic equipment.

g. Sampling Tests.

(1) MIL-STD-105, Sampling Procedures and Tables for Inspection by Attributes. Provides sampling plans relative to attributes inspection. Attributes inspection is inspection whereby either the unit of product is classified simply as defective or non-defective, or the number of defects in the unit is counted, with respect to a given requirement or set of requirements.

(2) MIL-STD-414, Sampling Procedures and Tables for Inspection by Variables for Percent Defective. Expresses conformance as percent defective; i.e., the percent of the items falling outside specification limits. Standard is applicable when failure times are known to be normally distributed.

(3) MIL-STD-690, Failure Rate Sampling Plans and Procedures. Provides procedures for failure rate (FR) qualification; sampling plans (based on exponential distribution) for establishing and maintaining FR levels at selected confidence levels; and lot conformance inspection procedures associated with FR testing for the purpose of direct reference in appropriate military electronic parts established reliability (ER) specifications.

(4) DOD Handbook H-53, Guide for Sampling Inspection. Describes basic sampling procedures; explains basic principles underlying sampling inspection; and demonstrates how sampling plans are used in arriving at appropriate inspection and quality assurance decisions.

(5) DOD Quality Control and Reliability Handbook H108, Sampling Procedures and Tables for Life and Reliability Testing (Based on the Exponential Distribution). Contains tables of life testing sampling plans pertaining to exponential failure times. The plans are divided into three general categories: failure terminated tests, time terminated tests, and sequential tests. The mean failure time θ is used as the reliability parameter under test. Minimal and nominal acceptable values of θ, along with allowable risks, are used as the basis for specifying a satisfactory sampling plan. The sequential test procedures are outlined and the parameters of the test are tabled. Operating characteristic curves are drawn for most tabled plans.

(6) DOD Quality Control and Reliability Technical Report TR-3, Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution (Mean Life Criterion). Provides tabled plans when mean failure time is the reliability parameter to be tested and failure times have a Weibull distribution.

(7) DOD Quality Control and Reliability Technical Report TR-4, Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution (Hazard Rate Criterion). Provides tabled plans when hazard rate or instantaneous failure rate is the parameter under test.

(8) DOD Quality Control and Reliability Technical Report TR-6, Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution (Reliable Life Criterion). Provides plans when reliable life is the parameter under test. Reliable life is defined as that time beyond which a specified portion of a lot can be expected to survive.

(9) DOD Quality and Reliability Assurance Technical Report TR-7, Factors and Procedures for Applying MIL-STD-105D Sampling Plans to Life and Reliability Testing. Provides instructions for selecting life test sampling plans from MIL-STD-105D.

h. Design.

(1) FAA-G-2100, General Requirements, Electronic Equipment. Covers the general requirements for design and manufacture of FAA ground electronic equipment.

(2) MIL-E-4158, General Requirements for Ground Electronic Equipment. Presents general design and manufacturing requirements for ground electronic equipment used by the Air Force.

(3) MIL-E-5400, General Specification for Aircraft Electronic Equipment. Stipulates general requirements for design and manufacture of airborne electronic equipment for operation primarily in piloted aircraft.

(4) MIL-E-16400, General Specification, Naval Ship and Shore Electronic Equipment. Covers the general requirements applicable to the design and construction of electronic equipment intended for Naval ship or shore applications.

i. Parts/Materials/Processes.

(1) MIL-STD-242, Electronic Equipment Parts, Selected Standards. Guides contractors with respect to

the selection and use of approved parts in the design of new equipment.

(2) MIL-STD-839, Selection and Use of Parts with Established Reliability Levels. Identifies parts whose demonstrated reliability characteristics justify usage under given operational conditions.

(3) MIL-P-11268, Parts, Materials and Processes Used in Electronic Communication Equipment. Covers the selection, application and use of parts, materials and processes in the construction of electronic communication equipment.

j. Failure Reporting.

(1) FAA Order 6000.15, Maintenance of Airways Facilities. Presents general technical information needed by airway facilities maintenance personnel at the site to properly perform their maintenance duties. Included are failure reporting requirements.

(2) FAA Order 6040.5, Facility Outage and Service Interruption Report. Sets forth instructions for the preparation of Facility Outage and Service Interruption Report, FAA Form 6040-3, and Line Performance Report, FAA Form 6040-7.

(3) FAA Order 6040.7B, Daily NAS Status Report/NASCOM. Sets forth procedures for the preparation of the Daily NAS Status Report at all Air Traffic Control Centers.

(4) SP INSTR 3100.1B, Fleet Ballistic Missile Weapon System Trouble and Failure Report Program. Describes failure reporting system for the Polaris program.

(5) SP 6504, Failure Reporting and Management Techniques in the Surveyor Program. Describes failure reporting and management techniques used on the Surveyor program.

(6) ASTIA 458585, Weapon System Effectiveness Industry Advisory Committee Task Group 3 Data Collection and Management Reports. Discusses the acquisition, control, reporting, summarizing and retrieving of data as it pertains to System Effectiveness.

k. Environment.

(1) MIL-STD-210, Climatic Extremes for Military Equipment. Indicates the probable extreme climatic conditions of the normal environment to which military equipment may be exposed; and is intended to establish uniform limits not to be exceeded in normal design requirements.

(2) MIL-STD-446, Environmental Requirements for Electronic Parts. Establishes uniform levels of environments and conditions that electronic parts will be exposed to in military service.

l. Training.

(1) NAVSHIPS - 0900-002-3000, Reliability and Maintainability Training Handbook. Presents a combined reliability and maintainability training course for those who deal with contractors as well as for equipment designers. Emphasis is on contract management methods to design for required reliability.

(2) Reliability Theory and Practice Training Program, ARINC Research Corporation, 1700 K Street, Northwest, Washington, D.C. A text book supporting an in-plant reliability training program directed to both management and designers.

2. REFERENCE SERVICES. The referenced services provide information in the form of sources of failure rate data or documents. The services are grouped by type of service provided.

a. Failure Rate Data. The following sources provide data that may be used as a basis for failure rates for specific parts when the FAA-approved sources do not provide the required data (or the data provided is known to be obsolete).

(1) Micro and Hybrid Circuit Reliability. Reliability Analysis Center, RADC (RBRAC), Griffiss AFB, New York, 13441. Provides failure rate data and supporting information regarding reliability of microcircuits.

(2) Failure Rate Data (FARADA) Program. Fleet Missile Systems Analysis and Evaluation Group Annex, Naval Weapons Section, Seal Beach, Corona, California, 91720. An inter-agency sponsored effort to provide parts/components

failure rate and failure mode data to contractors and government agencies for entire spectrum of military and space equipment.

(3) Government Industry Data Exchange Program (GIDEP) Headquarters, Naval Material Command, Code 03426, Support Technology Branch, Washington, D.C., 20390. Provides test and reliability data on specific parts used by both government and industry. Inquiries may be made via computer. Participants in the program both input and obtain data and reports.

b. Obtaining Documents/Information. The following agencies provide documents that are developed within, or are the responsibility of, the specific agency.

(1) FAA Specifications and Documents. May be obtained from the Contracting Officer in the FAA office issuing the invitation for bids or request for proposals, Federal Aviation Administration, 800 Independence Ave., S.W., Washington, D.C., 20591.

(2) Military Specifications and Standards. Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, Pa., 19120.

(3) RADC Reports. Defense Documentation Center, Cameron Station, Alexandria, Virginia, 22314.

(4) NASA Publications. Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 20402.

(5) Classified and Limited Distribution Documents. Defense Documentation Center, Cameron Station, Alexandria, Virginia, 22314.

(6) Unclassified Documents Prepared Under Government Contract. U.S. Department of Commerce, National Technical Information Service, Springfield, Virginia, 22151.

APPENDIX 5

SAMPLE RELIABILITY SPECIFICATION

DEPARTMENT OF TRANSPORTATION

FEDERAL AVIATION ADMINISTRATION SPECIFICATION

RELIABILITY PROGRAM PLANS AND PROCEDURAL REQUIREMENTS FOR

ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT

1. SCOPE

1.1 Scope.- This document establishes uniform criteria for reliability programs, and provides guidelines for the preparation and implementation of reliability program plans and associated procedures.

1.2 Application.- This specification delineates reliability program requirements for ground electronic, electrical, mechanical and electromechanical equipments as a function of type of contract and equipment model in relation to its ultimate use. Multiple reliability program elements are provided to permit selecting tasks for the reliability program that are most compatible with the applicable functions. Guides for selecting reliability tasks for a specific contract are also presented. Thus, this specification provides a "shopping list" of task elements from which are selected those efforts to be applied to the procurement.

1.3 Classification.- Three types of contracts and three types of equipment are covered by this specification.

1.3.1 Contract Type.- Contracts covered by this specification are for one of the following:

(a) Studies (with or without experimental hardware)

(b) Equipment

(c) Facilities

1.3.2 Equipment Types.- The following types of equipments are covered by this specification:

(a) Development

(b) Prototype/Preproduction

(c) Production

2. APPLICABLE DOCUMENTS

2.1 Precedence of documents.- This specification shall have precedence over all specifications, standards, documents, etc., listed or referenced herein. In the event of conflict between the requirements of the equipment specification and this specification, the equipment specification shall have precedence.

2.2 Documents.- The following documents, of the issue in effect on the date of invitation for bids or request for proposal, form a part of this specification to the extent specified herein.

SPECIFICATIONS

Federal Aviation Administration

FAA-G-2100	Electronic Equipment, General Requirements

STANDARDS

FAA-STD-013a	Quality Control Program Requirements

Military

MIL-STD-280	Definition of Item Levels, Item Interchangeability, Models, and Related Terms
MIL-STD-721	Definition of Terms for Reliability Engineering
MIL-STD-781	Reliability Tests: Exponential Distribution

PUBLICATIONS

FAA Report No.	FAA Reliability Handbook (Unpublished)

(A limited number of copies of this FAA specification and other applicable FAA specifications may be obtained from the Contracting Officer in the Federal Aviation Administration office issuing the invitation for bids or request for proposals. Requests should fully identify material desired and should identify the invitation for bids, requests for proposals, contract involved, or other use to be made of the requested material. Other listed publications can be obtained as indicated.

Federal Specifications and Standards - General Services Administration Business Service Centers in Atlanta; Seattle, Washington; Boston; Chicago; Denver; Fort Worth; Kansas City, MO; Los Angeles; New York; San Francisco; and Washington, D. C.
Military Specifications and Standards - Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.
RADC Reports - National Technical Information Service, Operations Division, Springfield, Virginia 22151.

3.0 REQUIREMENTS

3.1 Summary of services and documentation to be furnished.- Services and documentation required are specified in the applicable procurement documentation.

3.2 Definitions.- The reliability definitions used in this specification are those of MIL-STD-280 and MIL-STD-721 with additions or modifications as noted below.

3.2.1 Equipment.- A general term characterizing a broad category of electronic , electrical , electromechanical , mechanical items (system, subsystem, set) that perform a complete function.

3.2.2 Facilities.-For purposes of this specification, facilities are defined as the heating, ventilating, air conditioning, prime power, auxiliary power, water, and such other furnishings or supplies that directly support the ground electronic, electrical, mechanical and electromechanical equipment used to accomplish a site function.

3.2.3 Module.- An item in a packaging scheme displaying size and regularity;and also with uniformity and nondestructive separability which may be replaced as a single entity.

3.2.4 Card.- A replaceable assembly so designed that all parts are fastened to a circuit board. A portion of a connector may or may not be one of the parts connected to the circuit board.

only. Where are delineated utilizing more than one technique and the procurement document does not stipulate the technique to be used, the contractor may at his option may select the one he deems most appropriate to the procurement.

3.3.2.1.1 Study contracts.- Design study contracts are usually concerned with the investigation of feasible designs and/or techniques for achieving desired functions and performance. The contractor shall use approved parts and design/fabrication techniques, where possible. Environmental requirements are desirable for nonstandard parts and items that are expected to be performance-limited by environmental effects; such as ferrite controls at higher temperatures. Program plan (1) is the applicable one.

3.3.2.2 Equipment contracts.- The reliability programs required in equipment contracts are primarily a function of the equipment model being procured (i.e., Developmental or Prototype/Preproduction or Production).

3.3.2.2.1 Development model.- In the development model contract, one of the basic tasks for the reliability effort is the evaluation of the possible system concept or design approaches. This must include support of the system designers. The two end goals are the analytical demonstration of the reliability achieved, and an assessment of the potential for the production model. The Program Plan to be applied is (2) as listed in Table I, Appendix A.

3.3.2.2.2 Prototype/preproduction model.- For this model, the designs are detailed into essentially final form and final parts are selected. The reliability effort is now one of part selection/application, detail design support, and detail reliability allocations and assessments. Also, a program of reliability evaluation/demonstration tests is generally implemented. Program Plan (3) of Table I is the reliability program plan to be applied.

3.3.2.2.3 Production model.- In the production model contract, the primary task of the reliability effort is to assure that reliability is not degraded by the production processes. To this end, the reliability program is concerned with process, parts, and design change monitoring and control. In many cases, some level of acceptance testing will be required. The rigorousness of the imposed program increases as a function of whether the contract is for 1) reprocurement with modifications or 2) initial production. The reliability programs for the two cases are (4) and (5) as applicable from Table I, with modifications as deemed necessary.

3.4 Quantitative Reliability Requirements.- Quantitative reliability performance requirements shall be specified in detail in the FAA detail equipment specification when appropriate. These quantitative requirements shall be directly relatable to the reliability mathematical model or models describing the reliability

performance of the design for each function under consideration as required by other performance criteria.

As delineated in the guidelines provided in Section 3.8, reliability test and demonstration requirements shall also be specified in the FAA detail specification.

3.4.1 Preliminary Definitization of Reliability Requirements.- The requirements as delineated in the FAA detail specification shall be included in appropriate sections of the proposer's proposal. The reliability modeling, apportionment and preliminary assesment shall be included to the extent necessary to validate all functions and requirements as delineated in the detail specification.

3.5 Management.- The contractor shall have one clearly identified organizational element which shall be responsible for the management and control of the reliability program for insuring its effective execution. A single reliability manager shall be responsible and accountable for the reliability effort. This manager shall have the necessary authority and resources, and report at a level having full responsibility for the contract effort, to enable him to implement and enforce the requirements specified in the contractor procurement documentation.

3.5.1 Reliability management responsibility.- The reliability manager shall be responsible and accountable for planning, implementing, controlling and reporting all reliability tasks required for this procurement. The manager shall select and utilize personnel and techniques in a manner to provide the most efficient achievement of reliability objectives and shall be responsible for development and implementation of the reliability program plan, as well as for coordination and performance of the reliability tasks on schedule and within budget. It is also the responsibility of the reliability manager to advise the FAA of reliability problems to permit remedial action at minimum cost and effect on schedule.

3.5.1.1 Program Plan.- The contractor shall provide, maintain and implement a Reliability Program Plan which describes the reliability effort to be performed as well as how the program is to be managed and controlled. The plan shall be submitted as required by the applicable procurement documentation. The minimum reliability effort to be performed shall be the specific tasks specified by contract. A summary of the reliability tasks to be performed shall be described on a single form in a time phased schedule. Milestones shall be delineated. Major milestones of the total program shall likewise be described. Requirements placed on suppliers and/or subcontractors shall be described in the program plan.

The program plan shall (1) identify the organizational elements, the reliability manager, and key personnel responsible for managing and/or implementing the overall reliability program, and (2) clearly define the related responsibilities and functions including both

policy and action. The plan shall stipulate the authority delegated to the organization to enforce its policies. The relationship between line, service, staff and policy organizations both within the reliability organization and within the company shall be identified.

The reliability program shall include:

(a) a detailed listing and description of each task together with identification of the organizational unit responsible for executing each task,

(b) summary descriptions of detailed procedures used to insure execution of each task as planned,

(c) scheduled start and completion dates for each task together with anticipated man hours required for each task,

(d) identification of known reliability oriented problems to be solved, an assessment of the impact of these problems on specified program requirements, and the proposed solutions or the proposed program to solve these problems,

(e) recording procedures used to identify problems and status of actions to resolve problems,

(f) designation of progressive reliability values and milestones,

(g) definition of task interrelationships,

(h) the method by which reliability requirements are disseminated to designers and associated personnel,

(i) periodic status recording or predicted and achieved system and equipment reliability,

(j) a description of the reliability test program, and

(k) provisions for reliability indoctrination and training as applicable to this procurement.

<u>3.5.1.2 Reliability interface compatibility</u>.- The reliability manager shall be the focal point for coordinating the reliability program with other interfacing efforts (such as listed below) to assure an integrated and effective contractual effort.

(a) System engineering

(b) Facility engineering

(c) Maintainability and maintenance engineering

(d) Safety engineering

(e) Quality assurance and quality control

(f) Standardization

(g) Human resources including human engineering, human factors, and training

(h) Configuration management

(i) Integrated logistics support

(j) Manufacturing

(k) Suppliers

(l) Subcontractors

The reliability manager shall establish data format and impose contractually allocated requirements upon suppliers and subcontractors so that all analytical data needed for reliability analysis, allocation and prediction is assured. A data exchange shall be made in accordance with procurement documentation requirements to assure requirements are being met or to allow for tradeoffs as permitted by the contract.

3.5.1.3 Reliability program control.- The contractor shall implement a system for effective management control and audit of the reliability program. This system shall provide visibility with respect to reliability progress from the standpoint of individual reliability task performance, status and budget.

To this end, individual reliability tasks shall be scheduled and budgeted. In addition, a reliability program planned versus actual expenditure schedule shall be maintained and kept current. The reliability manager shall review the total program and individual task progress and budget weekly. Submissions to the FAA shall be delineated in the contract documentation schedule.

3.5.1.4 Supplier/subcontractor control.- The reliability program plan shall stipulate methods for assuring that subcontractor's and supplier's reliability efforts are consistent with overall system requirements, that provisions are made for source selcetion of subcontractors and suppliers, surveillance of their reliability activities and assuring that reliability requirements are specified, and that the reliability efforts of suppliers and subcontractors are consistent with overall system requirements. Each subcontractor shall be required to perform specific tasks from this specification. The tasks to be performed shall result from an analysis of the particular equipment reliability, its criticality and effect on total system reliability. Each deviation in requirements from the

reliability program contractually imposed on the prime contractor shall require approval by the FAA.

3.5.1.4.1 Supplier/subcontractor design reviews.- When formal design reviews are imposed on suppliers or subcontractors as part of a supplier or subcontractor total reliability program, provision shall be made for attendance of FAA personnel. The FAA program office shall be notified 15 working days in advance of the design review meeting. The scope of each review shall be a function of what is being supplied and program status.

3.5.2 Program reviews.- The reliability program shall be planned and scheduled to permit the contractor and the FAA to review its status, including results achieved, at preplanned steps or check points. These formal reviews and assessments of reliability shall be conducted at major program points preferably in conjunction with design reviews and shall be shown on the schedule presented in the Reliability Program Plan. The FAA program office shall be notified at least 15 working days prior to each scheduled formal reliability program review. Minutes of these reviews shall be prepared by the contractor and supplied to the FAA program office within 15 working days after completion of the review. A minimum of two program reviews shall be scheduled and conducted for design and development contract efforts. The reliability manager shall be responsible for the preparation, organization and coordination of the program reviews. The contract schedule shall definitize those reviews required as a minimum.

3.6 Reliability engineering, design and analysis.- The contractor's reliability organization shall insure that reliability oriented design practices are applied in the designs of systems and equipments. These practices shall include, as required by contract, the use of reliability modeling, requirements allocation, part stress verification, parts application review, failure mode and effects analysis, and parts/materials/assemblies selection and handling. Techniques for evaluation shall include design reviews as well as analytical methods, such as reliability predictions, degradation analysis, and design of experiments, as applicable.

3.6.1 Reliability analysis.- Reliability analysis shall be performed in consonance with design development and shall be utilized to guide the design to achieve contract requirements and assure delivery of equipment with lowest life cycle cost. The technique of analysis shall vary with the data available and conform to contractual requirements. The reliability program plan shall delineate the prediction techniques to be used in performing the reliability analyses.

3.6.1.1 Reliability modeling.- Reliability models of the system shall be developed which are based on mission requirements, use environment, system design, operation and maintenance (including logistic support) as applicable. Models considering system

degradation shall also be developed. The models so developed shall be capable of demonstrating the various functional states, state probabilities or availabilities as applicable to the system under consideration.

3.6.1.1.1 Model requirements.- Models developed shall reflect:

(a) Required functions for each phase of each required mission.

(b) Critical time periods in the exercise of each function.

(c) Use environmental stresses, i.e. temperature ranges, humidity, etc., particularly if not in consonance with FAA-G-2100 Service conditions.

(d) Planned operational, maintenance and logistics concepts.

(e) System design from a hardware standpoint.

(f) The definition of system failure.

(g) Part, card, module, assembly or function failure rates.

3.6.1.1.2 Model results application.- The model shall be utilized to identify critical items or paths whose failure will either cause system or subsystem failures, major performance degradation, marginal operational conditions or departures from the required reliability. The model shall serve to identify and aid in resolving operational, safety, maintenance, and logistic problems. The model shall also be utilized in defining requirements for redundancy, built-in test, and for apportioning reliability requirements to the detail design level.

3.6.1.2 Reliability apportionment.- The reliability requirement(s) specified by the FAA shall be apportioned to lower levels within the system by allocating reliability goals to each subsystem, equipment, assembly, or subassembly to be designed or purchased as an entity. The allocations shall be based on system reliability performance and test requirements and on the reliability model for the system. Additional considerations shall be cost, schedule and state-of-the-art. When combined in accordance with the system mathematical model the initial allocated goals shall not exceed requirements specified in the FAA equipment specification by more than 10%. The initial apportionment shall be refined as the design progresses. Changes in the apportionment shall be included in the monthly progress reports. Problems in attaining the apportioned reliability levels shall be brought to the immediate attention of the FAA contracting officer for resolution.

If monthly progress reports are not required, the FAA shall be provided a report within 30 days after each new apportionment which

describes each change in apportionment together with the reason for the change.

The reliability organization shall provide each designer the allocated failure rate for the equipment for which he has design responsibility. In addition, each designer shall be provided the detailed reliability design philosophy and standard part derating policy.

3.6.1.3 Reliability predictions.- Reliability predictions shall be made based on the proposed design and mathematical model of the system element for each mission and/or mode of operation.

3.6.1.3.1 Prediction techniques.- The following techniques are applicable for predicting the reliability of FAA systems or equipment. The technique of prediction for a specific program shall be as specified by contract. If the prediction technique is not so specified, paragraph 3.5.1.3.1.4 shall apply for design and development contractural efforts.

3.6.1.3.1.1 Similar functional equipment reliability prediction.- A reliability prediction shall be made for the complete system utilizing justified reliability data for complete similar functions, e.g., computer. Justification for the reliability data shall be established through field data, test data or prior reliability predictions or combinations thereof. The reliability data shall be selected to reflect the proposed design and FAA operational use and environment. The data selected shall be subject to the approval of the FAA.

3.6.1.3.1.2 Similar card/module/assembly equivalent reliability prediction.- A reliability prediction shall be made for the complete system utilizing justified reliability data for similar cards/modules/assemblies composing the system. Justification for the reliability data shall be established through field data, test data or prior reliability predictions or combinations thereof. The reliability data shall be selected to reflect the proposed design and FAA operational use and environment. The data selected shall be subject to the approval of the FAA.

3.6.1.3.1.3 Average stress reliability prediction.- A reliability prediction shall be made for the complete system utilizing average part failure rates established for each part type according to type or circuit (e.g., digital vs. analog). These part failure rates shall be based on the average stresses established as part application policy for the equipment/system.

3.6.1.3.1.4 Detailed stress reliability prediction.- A reliability prediction shall be made for the complete system utilizing failure rates resulting from either measured or calculated stress for each part used in the system. Detailed reliability stress analyses shall be performed in accordance with the FAA Reliability Handbook. The

prediction shall be based upon the maximum temperature specified in the detail specification unless otherwise stipulated.

3.6.1.3.2 Failure rate sources/justification.- Failure rates used for predictions shall be obtained from Reliability Prediction for Electronic Equipment, MIL-HDBK-217. When the failure rate source does not contain the failure rate data required or if more recent data is available for specific parts, other justified failure rate sources may be used. Other such failure rates used shall be subject to approval by the FAA. TR-69-458, the RADC Nonelectronic Handbook, shall be used for non-electronic or non-electrical parts.

3.6.1.3.3 Use environment for predictions.- Reliability predictions for each part in a system shall be based on the expected worst case environment surrounding the part during FAA use of the system in the field unless otherwise specified in the contract.

3.6.1.3.4 Reliability studies.- Studies shall require that reliability predictions be performed for a variety and range of conditions that may affect reliability. When not otherwise specified in the procurement documentation, reliability predictions shall be made as a function of each of the following variables.

3.6.1.3.4.1 Design variations.- A reliability prediction shall be made for each design variation/option required in the study. The cost impact of each variation shall be determined.

3.6.1.3.4.2 Stress variations.- Reliability predictions shall be made as a function of varied part stress policies, ranging from the minimum values affecting reliability to full rated stress. As a minimum, the stress variation may assume the same relative stress for all parts in digital circuits.

3.6.1.3.4.3 Ambient temperature variations.- Reliability predictions shall be made as a function of ambient temperature varied from the minimum value affecting reliability to a maximum value at which the majority of parts will operate.

3.6.1.3.4.4 Part reliability/quality classes.- Reliability predictions shall be made as a function of available part reliability/quality classes. The results shall indicate the individual reliability effect of different reliability/classes of each part type; and the effect of simultaneously varying all parts in the same "reliability/class" direction. In all cases, the cost impact shall be determined. The quality or class are the reliability and quality levels as determined by a JAN vs. JANTX, or MIL-M-38510, Level A, B, or C, etc. of part quality.

3.6.1.3.4.5 Parts quality control programs.- A full range of possible Parts Quality Control Programs shall be defined. These programs shall include consideration of parts inspection, testing,

and burn-in. A reliability prediction shall be made based on the effective failure rates expected to result from each such program. In all cases, the cost impact shall be defined.

3.6.1.3.4.6 Reliability cost.- Reliability predictions shall be made as required to relate cost to achievable reliability. As a minimum, redundancy, part reliability/quality classes, and part quality control programs shall be considered in the cost factor.

3.6.1.3.5 Reliability prediction frequency.- A preliminary reliability prediction shall be submitted with the proposal together with a discussion justifying both the analysis and the reliability model or models used. Updates of this prediction shall be made as design changes occur. Complete reliability analyses of the design to date shall be available for presentation at the formal design reviews. For those portions of the system for which detail design information is not available at the time a complete system reliability prediction is required, allocated reliability values shall be used. Reliability analysis reports shall be submitted to the FAA as specified by contract. The reports shall include a comparison of predicted and allocated reliability at lower levels within the system. Modifications to this paragraph must appear in the detail specification or contract.

3.6.1.4 Degradation analysis.- A degradation analysis shall be performed on all unique circuits in the system. The analysis shall be based on part characteristics as the variable, independent, input parameters and circuit performance characteristics as the output parameters. The approach used to establish the required mathematical models/equations and selecting input parameters shall be subject to approval by the FAA. The following techniques are applicable to performing the required degradation analysis. The specific technique to be applied shall be as specified by contract. If an analysis is required and the technique is not so specified, paragraph 3.6.1.4.4 shall apply.

3.6.1.4.1 Parameter variation analysis method.- Degradation analysis shall be performed utilizing a parameter variation method. As a minimum, each input parameter shall be independently varied over the range of its possible values, while holding all other parameters at their nominal value. Circuit failure points shall be determined and maximum allowable parameter variation established.

3.6.1.4.2 Worst-case analysis method .- Degradation analysis shall be performed utilizing the worst case parameter variation method. All input parameters shall be varied simultaneously, with each parameter being varied in the direction which increases the output above nominal. A worst case output value is established when each input parameter reaches the limit of its tolerance or expected drift range. The same analysis shall be performed for parameter variations decreasing the output below nominal. Circuit failure points shall be defined for both cases.

3.6.1.4.3 Variance analysis method.- Degradation analysis shall be performed utilizing a variance analysis method. A mean and second moment (variance) shall be determined for each input parameter distribution. Correlation coefficients shall be established for all these distributions. From these data, the mean and variance of each output parameter shall be determined. In all cases, circuit failure values shall be determined.

3.6.1.5 Design specification inputs.- Reliability performance and test requirements shall be included in design specifications. The contractor's reliability organization shall review all design specifications for concurrence with the contract detail design specification and consistency with interfacing design specifications.

3.6.2 Parts/materials/process control.- A parts, materials, process control program shall be established that shall assure to the maximum extent possible the proper selection, application and use of parts, materials and processes. The program shall include the development of preferred parts from FAA-G-2100, NASA-PPL's, Military JAN, JANTX and other such parts and materials lists and a standardization effort to minimize the number and types of parts and materials required. Parts and materials selection shall comply with the requirements of specification FAA-G-2100. Specifications shall be used to describe and control parts and materials used.

3.6.2.1 Design guide.- A design guide shall be developed and disseminated to designers which presents information that guides design and insures a more reliable end product. The following information shall be included in that design guide as a minimum:

(a) Summary of contract reliability requirements.

(b) Equipment environmental envelope.

(c) Definition of equipment failure.

(d) Reliability allocations.

(e) Design recommendations.

(f) Part, material, process selection procedure.

(g) A list of parts, materials, process specialists and their telephone numbers.

(h) Preferred parts, materials, process lists reflecting FAA-G-2100 requirements.

(i) Materials and process design notes.

(j) Recommended derating for specific parts and materials.

(c) Have long lead time purchase requirements.

(d) Present a potential maintenance load problem.

(e) Have limited and finite life expectancies.

Critical items shall include all deliverable computer programs as well as those items identified through reliability and failure mode, effects analysis. The documented procedures and the critical item list established shall be subject to review and evaluation by the FAA.

3.6.6 Design reviews.- Formal design reviews shall be performed which provide comprehensive critical audits of all pertinent aspects of the design of hardware and software. The reviews shall be conducted on the system and on each design at major milestones during their evolution. Participating in the design review shall be personnel from design, fabrication, test, reliability, quality assurance, parts/materials/processes application, and other personnel as deemed necessary for a comprehensive critique. The reviews shall constitute a detailed examination of the design from the standpoint of:

(1) meeting performance requirements, including reliability,

(2) design documents, drawings and specifications adequacy,

(3) choice of part selection and application,

(4) potential production, operating or maintenance problems.

Also, to be considered at the review are:

(1) current reliability estimates and achievements for each mode of operation as derived from reliability analyses or test(s),

(2) test data obtained during design development,

(3) control measures necessary to preserve inherent reliability

(4) results of failure mode, effects analyses,

(5) corrective action on reliability critical items,

(6) supplier/subcontractor reliability programs,

(7) status of previously approved design review actions.

Supporting design data for each review shall be provided the invited attendees at least 3 days prior to the review. The FAA shall be notified and supplied supporting design data at least 10 working

days prior to each review. The results of each review shall be documented. The FAA shall be provided minutes of design review meetings within 15 days.

The program manager shall be the office of prime responsibility for the design reviews and shall be responsible for conduct of the reviews. The program manager shall also be responsible for preparation and dissemination of documentation prepared before, during, or after each review.

The program reliability manager shall be responsible for the preparation of data packages pertaining to reliability and for any reliability analyses required for each review. He shall also be responsible for follow-up on action items to ensure or verify their satisfactory completion.

3.6.6.1 Study design reviews.- Contracts for studies shall have a program review within a contracturally specified number of days after start of the program and again prior to preparation of the final report. These two reviews are considered the minimum requirements for design reviews. The initial review shall be for the purpose of assessing the study approach and the reliability approach to the effort. The review prior to the final report shall assess both the reliability and study results to date and the planned inputs to the final report. At each review the design adequacy of each major equipment/subsystem versus the reliability requirements baseline shall be presented by reliability personnel. Deviations from these requirements shall be specifically delineated in the procurement documentation.

3.6.6.2 Equipment design reviews.- Contracts which include requirements for development, prototype, or production hardware shall have design reviews prior to starting detail design (Preliminary Design Review, PDR), prior to commitment of design to fabrication (Critical Design Review, CDR), and after fabrication and test of the first article (First Article Configuration Inspection, FACI). During the Preliminary Design Review the reliability organization shall present an assessment of the reliability of the proposed concept versus requirements, delineate reliability problem areas and evaluate reliability program progress. At the Critical Design Review, reliability personnel shall show via documented analyses that the detail design and related test requirements adequately satisfy the established end-item and test requirements, including interfaces with personnel, facilities and other equipment. High risk and potential reliability production problems shall also be identified. The First Article Configuration Inspection shall serve to evaluate contract end item compliance with requirements by comparing hardware design and test results with detail specifications and drawings used during fabrication. Compliance with changes dictated by previous reviews shall also be determined. Reliability personnel shall present evaluation of test results versus predictions, production related problem areas affecting

equipment reliability and shall stipulate changes required for reliability improvement.

3.6.6.3 Design tradeoffs.- Design tradeoffs and their effect on both detail and system design shall be evaluated and documented as part of the reliability modeling and allocation activity. Tradeoffs to be considered shall be:

(a) Part operating temperature.

(b) Part derating.

(c) Choice of quality of parts, i.e., MIL-STD, established reliability, JANTX, specification control drawing parts.

(d) Extent of part burn-in.

(e) Extent and type of redundancy.

(f) On-line/off-line maintenance.

(g) Extent of built-in test.

(h) Cost.

(i) Schedule.

The results of the design tradeoffs shall be a consideration during design reviews.

3.6.7 Design approval.- As each design is completed and prior to the release of the associated drawings for fabrication, a member of the reliability organization shall review and sign each drawing. Sign off of the drawings by the reliabilty organization shall constitute a certification that the design meets or exceeds its allocated MTBF.

3.6.8 Effects of storage, shelf-life, packaging, transportation handling, and maintenance.- The reliability program shall include efforts such as test and analysis, or estimation, to determine the effects of storage, shelf-life, packaging, transportation, handling and maintenance on the reliability of the product. The efforts shall include as a minimum:

(a) Identification of major or critical characteristics of items which deteriorate with age, environmental conditions (including shock and vibration), etc.

(b) Periodic field examination, tests or stockpile reliability evaluation.

The total effort shall result in requirements and procedures which minimize the effects of storage, shelf-life, packaging, transportation, handling and maintenance on delivered items.

3.7 Production reliability.- The contractor shall implement a production reliability program which shall encompass the total production effort from purchase of parts/materials through shipment of the finished deliverable article(s). Procedures required for preventing degradation of reliability during production shall be identified and implemented. This shall include, but not be limited to:

(1) identification of the processes, fabrication techniques, and manufacturing procedures that can affect product reliability, and

(2) identification and implementation of the control procedures required in each case to prevent degradation of product reliability.

When submittal of a reliability program plan is required, the plan shall describe the specific reliability control procedures to be utilized and their expected impact on product reliability.

3.7.1 Production failure reporting.- When a failure data collection, analysis, and corrective action task is specified, failure reporting on each deliverable article shall be initiated with the start of final assembly check-out of the article and shall continue through final acceptance. The task shall be a closed loop one, with the reliability organization serving as a focal point for follow-up and close-out action on all failures.

3.7.2 Off-the-shelf Equipments.- Commercial or off-the-shelf procured equipments shall have their reliability and test requirements stipulated in the procurement documentation.

3.8 Reliability testing.- A test program shall be established which is designed to evaluate the reliability of the system and its elements when assessed against both mission and contractual requirements. Individual tests performed as part of the total test program may not be primarily for the purposes of reliability evaluation and the reliability organization may not have prime responsibility for testing. However, it shall be the responsibility of the reliability organization to ensure that tests performed provide necessary data in a timely manner to permit reliability evaluation and feedback of information for reliabilty improvement. The reliability demonstration test(s) to be performed to demonstrate compliance with the reliability performance requirement(s) is contained in the equipment specification(s) for the item(s).

3.8.1 Test types.- The following types of reliability tests shall be performed to the extent specified in the procurement request to assure achievement of program reliability objectives.

3.8.1.1 Development testing.- A planned and scheduled program of testing of parts and/or equipment shall be performed during the development and design phases of the program to estimate achieved reliability and to provide feedback of data as a basis for making reliability improvements. The tests shall be planned using statistical design-of-experiment techniques where practical and shall be conducted under environmental stress levels and for time periods appropriate to the purpose of the test. The development testing program shall be designed to confirm adequacy of selection of parts, determine capabilities and safety margins, evaluate performance drifts with time and determine failure modes and failure rates. Reliability tests shall be combined with other development tests to the maximum extent possible. Each test shall be documented sufficiently that the test may be repeated at a later date. The reliability organization shall maintain a data file on reliability development testing.

3.8.1.2 Reliability demonstration testing.- The FAA shall specify from MIL-STD-781 the test most appropriate. The contractor's test procedure shall be approved by the FAA. The reliability demonstration test shall be performed as part of the system acceptance tests and shall be specified in the procurement documentation.

3.8.1.3 Conditioning tests.- Each equipment shall be subjected to a fixed time conditioning test. The equipment shall be operated in all its specified modes an equal percentage of time during the test unless otherwise specified. In the event of a failure, a failure report shall be prepared. The deviation of the conditioning test and the environmental conditions shall be specified by the contractor in his test procedures document. It shall be subject to FAA review and approval.

3.8.1.4 Production reliability tests.- Reliability tests shall be performed on samples taken from production lots. The frequency and conditions of test and sample size to be tested shall be as specified in the detail equipment specification. Lot acceptance shall be contingent on an accept decision resulting from the reliability test. When these tests are not specified in the applicable procurement documentation, the contractor shall select the test most appropriate from MIL-STD-781 with the test selected to be approved by the FAA. The results of each reliability production test shall be summarized in a report to the FAA.

3.8.2 Reliability test program plans.- An integrated reliability test and demonstration plan shall be prepared and submitted for approval by the FAA. The plan shall include all reliability and longevity demonstration testing to be performed during the program.

The reliability test program shall be integrated with other system/equipment test programs to the extent practical in order to avoid duplicate testing. The tests shall be statistically designed where applicable, and maximum use made of data and reliability information obtained from relevant sources.

The integrated test plan shall include all tests that contribute to reliability evaluation. The role of each test in the evaluation shall be described. Tests planned to be performed on individual microelectronic semiconductor devices shall be described. A milestone schedule of the testing program shall be presented that also shows the relationship between the reliability test program and the total program schedule.

The integrated test and demonstration plan shall be submitted as part of the reliability program plan and shall be updated as specified by contract.

3.8.3 Reliability demonstration plan.- A plan for formal demonstration of achieved reliability shall be prepared reflecting the test requirements specified by the FAA in the procurement documentation. The plan shall describe the reliability test to be performed. The test description shall include as a minimum:

(a) Number of test articles.

(b) Summary description of how the test is to be performed, including operating modes.

(c) Test duration.

(d) Criteria for test failure or success.

(e) Facilities/test equipment required.

(f) Conditions for invalidating the test.

(g) Corrective action in the event of failure.

(h) Operating environment and cyclic conditions.

(i) Power requirements.

(j) Plans for test results documentation.

(k) Preventive maintenance requirements.

The plan shall be submitted to the FAA as part of the Reliability Program Plan for critique as specified by contract. The plan shall be revised to incorporate FAA comments.

3.8.4 Reliability test procedure.- A test procedure shall be prepared and submitted for approval by the FAA. The test method requirements of FAA-STD-013a modified only as indicated below shall apply. The procedure shall apply and are shall reflect the test plan previously approved. In addition, the procedure shall include the following as a minimum:

(a) Detailed procedures for performing the test.

(b) Sample data sheets for data collection.

(c) Test equipment required.

(d) Facilities, prime power, tools, and operating/maintenance manuals required.

(e) Allowable preventive maintenance.

(g) Criteria for acceptance/rejection.

(h) Periodicity of performance checking.

(i) Test performance preconditions.

(j) Environmental requirements.

(k) Maximum preacceptance operation.

(l) Corrective action in the event of failure.

(m) Action in the event of failure to pass the test.

3.8.4.1 Definition of failure.- Inability of the equipment to meet performance requirements specified in the detail equipment specification shall be classified as a failure. Specific definition(s) of failure for the contract item for purposes of reliability demonstration shall be specified in the equipment specification.

Each failure found at the time of each performance evaluation shall be classified as relevant unless determined to be non-relevant. All failures shall be classified as relevant except those proven to the satisfaction of the FAA to be one of the following:

(a) Failures caused by an external condition which are not a test requirement.

(b) Failures of limited life items whose life is less than the test length. The life of these items shall have been previously proved via test and their use approved by the FAA prior to the test. Failures of these items prior to

the end of the stipulated period shall be classed as relevant failures.

(c) Dependent failures, i.e., failures resulting from failure(s) of another part(s).

(d) Failures caused by improper test procedures or test equipment or the improper use thereof by test personnel (human error).

(e) Failures resulting from the application of operational or environmental stresses beyond specified limits.

3.8.4.1.1 Failure confirmation.- All failures observed during the equipment reliability test shall be documented and to the extent possible confirmed. Failure to do so is insufficient grounds for deletion of such failures in the count of total failures. Lack of failure confirmation shall require close review of the test facility. If the test facility can be shown to be both at fault and completely accountable for the failure to the satisfaction of the procuring activity, then and only then can the count of such failure be eliminated.

3.8.4.2 Criteria for acceptance/rejection.- A decision to accept or reject the equipment shall be based upon the criteria specified in the detail equipment specification. The decision to accept/reject/continue testing or terminate the test shall be made every time equipment performance is measured.

3.8.4.3 Periodicity for performance checking.- The periodicity for performance checking equipment during the test shall be as specified in the detail equipment specification. If not specified, each performance parameter shall be measured and recorded at least once during each 24-hour period at approximately 24-hour intervals. If the value of any specified parameter measured is not within tolerance, a record of the failure shall be made. The failure shall be assumed to have occurred immediately after the last successful measurement of the same parameter.

3.8.4.4 Multiple operating modes.- The reliability of equipment with multiple operating modes shall be determined using a single test. During the test the equipment shall be operated in all of its specified operating modes an equal percentage of time.

3.8.4.5 Test demonstration environment.- The test demonstration environment and the cyclic variation thereof shall be as specified in the detail equipment specification.

3.8.5 Design/reliability requirements incompatibility.- If the test terminates in a reject decision, the FAA shall be notified immediately. The cause or causes of the reject decision shall be determined from an analysis of the failure data accumulated and any

design deficiency found shall be corrected. The specified performance and required characteristics of the equipment shall not be changed to achieve the reliability requirements. The contractor shall fix all failed equipment and shall retrofit all equipment, including that already delivered to the FAA, with the changes found to be necessary. The extent of retesting to be performed shall be at the option of the FAA.

3.8.6 Maximum preacceptance operation.- The equipment to be tested as part of the reliability demonstration may be operated for a period prior to the start of the reliability test. Any such operation shall be applied to all subsequently delivered equipment for the same elapsed operating time and in the same environment. Failures that occur during the equipment operation shall be considered non-relevant. All failures shall be recorded and analyzed for failure trends.

3.8.7 Test documentation.- Throughout the performance of the reliability demonstration test a complete and accurate record of measurements of equipment performance, test facility conditions, test operator observations, equipment failures and test time shall be maintained. The minimum data obtained shall be that necessary to complete the following:

(a) Operation sheet(s).

(b) Equipment log(s).

(c) Log of equipment failures and operating times.

(d) Failure report(s).

The operation sheet and equipment log may be combined as a single form if the requirements of both are satisfied. All forms used shall be structured in an orderly fashion to permit chronological entry and subsequent rapid evaluation of results.

3.8.7.1 Operation sheet(s).- The equipment operation sheet(s) shall be designed to provide a continuous history of the test sample and test facility throughout the test from the standpoint of equipment performance, maintenance actions, and unusual occurrence. The operation sheet(s) shall be maintained by the test operator in chronological order. The equipment operating time at the time of the entry shall be recorded. The heading of the operating sheet(s) shall identify the test, the specific equipments under test and the various pieces of test equipment used. Measurement of equipment and test facility performance shall be entered on numbered test data sheets. The operation sheet(s) shall be used to record the number of the test data sheets and summarize the test results. The time, date, and identification of the operation(s) shall be indicated for each operation sheet entry on each data sheet. Space shall be allowed for remarks on both the operation and data sheet(s).

Entries shall be made on the operation sheet(s) for each scheduled equipment and test facility performance measurement as well as when scheduled and/or non-scheduled maintenance actions are performed. In addition, unusual occurrences (e.g., interruption of test due to external causes) shall be recorded on the operation sheet(s).

3.8.7.2 Equipment logs.- An equipment log shall be maintained for each functional subsystem. The equipment log shall be used to record chronologically equipment performance and maintenance performed on the subsystem of any unusual occurrence associated with the subsystem during the reliability demonstration test. Each entry shall be dated and the equipment operating time at the time of the entry shall be recorded. The time and identification of the operator shall also be indicated for each entry. The equipment log shall identify the equipment for which the data is recorded. Space shall be allowed in the log for remarks.

3.8.7.3 Log of equipment failures and operating time.- The log of equipment failures and operating time shall contain the information necessary for an accept or reject decision. The heading of the log shall identify the test, the specific equipments under test, and the individual responsible for the log. The body shall contain the following information:

(a) Entry number.

(b) Date and time of entry.

(c) Identification of equipment that failed with a description of the failure.

(d) Accumulated operating time for each equipment at time of entry.

(e) Total accumulated operating time for all equipments.

(f) Normalized test time [item (e) divided by specified MTBF].

(g) Total number of failures observed for all equipments on test.

An entry shall be made at the occurrence of each apparent equipment failure. If failure diagnosis reveals that the test specimen was not at fault, the failure may be deleted. Upon accumulation of enough time or failures for either an accept or a reject decision, the test shall be concluded with an appropriate entry.

3.8.7.4 Failure reports.- An individual failure report shall be prepared for each apparent equipment failure. The failure report shall identify the failed item to the level at which maintenance action was taken and describe all pertinent circumstances attendant

to each failure. The following shall be included on each failure report.

(a) Date and time of entry.

(b) Identification of equipment.

(c) Identification of failed replaceable unit or adjustments made.

(d) Accumulated operating time at time of failure for specific equipment in which failure occurred.

(e) Failure symptoms and diagnostic action taken.

(f) How the equipment was repaired.

(g) Time required for repair.

(h) Name and signature of individual reporting failure.

Following the repair action on the equipment, the specific failure in the failed replaced item shall be determined and recorded on the failure report. A detailed analysis of the cause of each failure shall be made and recorded on the failure report to provide a complete history of the failure.

3.8.7.5 Test report .- Upon completion of the reliability demonstration test a summary report shall be prepared and submitted to the FAA as specified in the procurement documentation. The report shall present a summary description of the reliability demonstration test. A comparison of predicted versus achieved reliability and recommendations for design or operation improvement shall be presented. A summary of all failures that occurred during the test and corrective action taken, if any, shall be included in the report.

3.9 Failure data collection, analysis and corrective action program.- A controlled system for identification, reporting, analysis, corrective action of equipment performance non-conformance during test shall be instituted. Major subcontractors shall also be required to have a similar system. Reporting of performance non-conformance shall be made on both hardware and software. The contractor's existing data collection, analysis and corrective action system shall be utilized with changes as necessary to meet the following requirements.

(a) Reports all observed discrepancies in sufficient detail to permit subsequent analysis of cause.

(b) Provides timely discrepancy analysis and corrective action to prevent recurrence.

(c) Includes audits to review status of uncompleted reports, analysis and corrective actions and reports delinquencies to management.

(d) Reports accumulated operating time on major items in which discrepancy occurred.

(e) Provides visibility of failure trends.

(f) Provides timely dissemination of problem/failure reports to appropriate elements of contractor's organization.

(g) Requires subcontractor reports be submitted to the prime contractor.

The failure data collection, analysis, and corrective action program shall be described in the program plan.

Failure data reports shall be maintained in a central file.

3.9.1 Initiation of failure reporting.- The failure data collection analysis and corrective action program shall be initiated as specified in the procurement request. The following are options regarding when the program shall start.

3.9.1.1 Program initiation during design.- The failure data collection, analysis and corrective action program shall begin with the test of items using parts required in final design and final design configuration. For software, operation of the program shall begin with first application of the software.

3.9.1.2 Program initiation at acceptance.- The failure data collection, analysis and corrective action program shall begin with the start of the equipment acceptance test for both the hardware and software.

3.9.2 Failure review board.- A Failure Review Board shall be established to evaluate performance discrepancies and request corrective action. The Failure Review Board shall have representatives from the Reliability organization, Program Office, Quality Assurance, Quality Control, Purchasing, and cognizant Engineering Design. Members of the Failure Review Board shall review discrepancy summaries and individual failure reports as applicable. The Board shall request, as required, investigative and analytical action or corrective action as a result of concensus opinion. Review Board action shall be documented and follow-up shall be initiated to ensure completion of requested action.

3.9.3 Failure analysis.- Failure analysis shall include, to the extent necessary to determine the cause of failure, the following:

(a) Physical examination.

(b) Electrical and/or mechanical test.

(c) X-ray.

(d) Part dissection.

(e) Microscopic examination.

Design analysis as part of the failure analysis shall include application stress analysis and circuit analysis, including allowable part tolerance and drift. Other techniques are not precluded in the effort to determine cause of failure.

3.9.4 Corrective action.- A formal procedure for corrective action shall be instituted as a result of the findings of failure analysis or Failure Review Board action. The procedure shall have provisions for follow-up to ensure timely completion of corrective action.

3.9.5 Failure data reporting.- Failure data reports shall be prepared and submitted as required by the procurement request.

3.9.5.1 Failure summary reports.- Monthly summary reports of all failures shall be submitted to the FAA. Each report shall contain the following information regarding each failure.

(a) Identification and date of failure report.

(b) Identification of failed equipment down to the failed part level.

(c) Operating time on failed part.

(d) Description and cause of failure.

(e) Corrective maintenance time.

(f) Corrective action and its status.

A section of the summary report shall present a tabular summary of the failures reported from inception of the failure reporting to the cut-off date for the particular report.

3.9.5.2 Weekly failure reports.- Weekly reports of all failures occurring during the week shall be submitted to the FAA. Each report shall contain the following information regarding each failure.

(a) Identification and date of failure reports.

(b) Identification of failed equipment down to the failed part level.

(c) Operating time on failed part.

(d) Description and cause of failure.

(e) Corrective action in process.

3.9.5.3 Hot-line reports.- During the reliability demonstration test any failure or unusual occurrence that results in a program crisis, e.g., stoppage of test for an extended period, shall be reported immediately to the FAA via telegram.

3.10 Engineering design changes.- Each engineering design change made after the engineering documentation has been released for equipment fabrication shall be reviewed and analyzed from a reliability standpoint. The effect on system reliability shall be determined. Those changes affecting equipment reliability shall be documented. If a Change Control Board is established to rule on acceptability of design changes, a representative from the reliability organization shall be a member of the Board.

3.11 Data requirements.- Submittal requirements for documents shall be as specified in the procurement documentation.

3.11.1 Status reports.- Periodic reports and final status report shall be submitted to the FAA. These reports may be combined with other program documentation provided all reliability information is contained in a single report or section of the program report and supporting information is adequately cross referenced and readily available. The reports shall provide a complete accounting of progress on elements defined by the reliability program plan, results achieved, and status of actions to resolve major problems and correct weak links.

3.11.2 Computerized reliability predictions.- Computerized reliability predictions prepared for submittal to the FAA shall be submitted as a report containing an explanation supporting the computerized prediction. The report shall present the total system prediction results, discuss, both from an engineering standpoint and analytically, the model or models used and justify the failure rates used. Also, any conditions imposed on the prediction shall be presented and justified.

The computer printout shall present the following:

(a) Part failure rates used together with stress, environment, and failure rate source by equipment.

(b) Rank ordered part contribution to system failure rate together with part stress if applicable.

(c) Rank ordered assembly contribution to system failure rate.

(d) Part quantities, part failure rates, part stresses and environment by individual assembly and associated assembly failure rate.

(e) Group assembly quantities, assembly failure rates, and major equipment failure rate.

The computer printout shall be presented on 8-1/2 by 11 inch paper.

4.0 QUALITY ASSURANCE PROVISIONS

4.1 Quality assurance.- Requirements for sampling, inspection, and test procedures shall be as specified in the applicable procurement documentation and/or FAA-STD-013a as applicable.

5.0 PREPARATION FOR DELIVERY

5.1 Delivery requirements.- Requirements for packaging, packing, and marking for shipment shall be as specified in the applicable procurement documentation.

6.0 NOTES

6.1 Intended use.- This specification contains options regarding specific tasks to be performed. For a particular program the extent of applicability of this specification and the deviations and options desired must be specified in the applicable procurement documentation. Furthermore, the particular reliability demonstration test to which the contractor must subject his equipment for acceptnace must be specified. Section 3.3.2 of this specification presents representative reliability programs as functions of type of program and equipment being procured. The FAA Reliability Handbook presents background information and/or procedures for both selecting and performing specific reliability tasks.

6.2 Selection of the Applicable Reliability Program.- Reference should be made in the applicable procurement document to the most appropriate reliability program specified in Table I. Intended deviations from a specific program should state the inclusion or deletion of specific reliability requirements by applicable paragraph number. (See 3.2.2.3).

6.3 Generalized FMEA Format.- See Figure 1 in Appendix "B".

APPENDIX "A"

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
1.1	Scope					
2.0 through 2.3 3.1 through 3.3.2	Applicable Documents (General)	*	*	*	*	*
3.3.2.1.1	Study Contracts	*				
3.3.2.2	Equipment Contracts		*	*	*	*
3.3.2.2.1	Development Model		*			
3.3.2.2.2	Prototype/Preproduction Model			*		
3.3.2.2.3	Production Model				*	*
3.5 through 3.5.1	Management	*	*	*	*	*
3.5.1.1, 3.5.1.2	Program Plan, Rel. Interface Compatibility		*	*		*
3.5.1.3	Reliability Program Control	*	*	*	*	*
3.5.1.4	Supplier/Subcontractor Control		*	*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.5.1.4.1	Supplier/Subcontractor Design Reviews		*	*		
3.4.2	Program Reviews		*	*		
3.6 through 3.6.1.1.2	Engineering, Design and Analysis through Model Results Application	*	*	*		*
3.6.1.2	Reliability Apportionment	*	*	*		
3.6.1.3 through 3.6.1.3.1	Reliability Predictions through Prediction Techniques	*	*	*	*	*
3.6.1.3.1.1	Similar Functional Equipment Rel. Prediction					
3.6.1.3.1.2	Similar Card/Module/Assembly Equivalent Reliability Prediction	*				
3.6.1.3.1.3	Average Stress Reliability Prediction		*			
3.6.1.3.1.4	Detailed Stress Reliability Prediction				*	*
3.6.1.3.2	Failure Rate Sources/Justification		*	*	*	*
3.6.1.3.3	Use Environment for Predictions	*		*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.6.1.3.4 through 3.6.1.3.4.3	Reliability Studies through Ambient Temperature Variations	*	*			
3.6.1.3.4.4	Part Reliability/Quality Classes	*	*			
3.6.1.3.4.5	Part Quality Control Programs	*	*			
3.6.1.3.4.6	Reliability Cost	*	*	*		
3.6.1.3.5	Reliability Prediction Frequency	*	*	* or	*	*
3.6.1.4	Degradation Analysis		*	* or		
3.6.1.4.1	Parameter Variation Analysis Method		*	or		
3.6.1.4.2	Worst-Case Analysis Method	*		* or		
3.6.1.4.3	Variance Analysis Method			*		

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.6.2 through 3.6.2.1.1	Parts/Materials/Process Control through Derating Policy and Design Tolerance Values			*	*	
3.6.2.2	Verification of Part Application Stresses			*		
3.6.2.2.1	Thermal Analysis			*		
3.6.2.3 through 3.6.2.5	Parts/Materials/Process Application Review through Suspect Item Deficiencies			*	*	*
3.6.3	Parts/Assemblies/Material Handling				*	*
3.6.4	Failure Mode, Effect Analysis (FMEA)	*	*	*	*	
				or		
3.6.4.1	Functional Level FMEA	*	*			
				or		
3.6.4.2	Circuit Level FMEA			*	*	
3.6.5	Critical Items		*	*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

TABLE 1. REQUIRED RELIABILITY PROGRAMS

FAA Specification, RELIABILITY PROGRAM REQUIREMENTS FOR ELECTRONIC AND ASSOCIATED SUPPORT EQUIPMENT		Reliability Program A				
Paragraph Number	Paragraph Heading	(1)	(2)	(3)	(4)	(5)
3.9.1.2	Program Initiation at Acceptance				*	*
3.9.2 through 3.9.5.1	Failure Review Board through Failure Summary Reports		*	*	*	*
3.9.5.2	Weekly Failure Reports			*		*
3.9.5.3	Hot-Line Reports			*		*
3.10	Engineering Design Changes		*	*	*	*
3.11, 3.11.1	Data Requirements, Status Reports	*	*	*	*	*
3.11.2	Computerized Reliability Predictions	*	*	*	*	*
4.1	Intended Use	*	*	*	*	*

Notes:

A. The general applicability of such reliability program is:
(1) - Design Study
(2) - Developmental Model Equipment
(3) - Prototype/Preproduction Model
(4) - Production Model - Level 1
(5) - Production Model - Level 2

FAILURE MODES, EFFECTS AND CRITICALITY (FMECA)

System _____ Ass'y Dwg or Schematic _____

Subsystem _____ Date _____

Item Function	Failure Mode	Possible Causes	Symptons and Local Effects (Include Dependent Failures)	Existing Compensatory Provisions	Effect Upon:	Level of Severity	Failure Rate or Probability	Remarks