

AD A098614

AFWAL-TR-80-2063

AD18623



RELIABILITY ADVANCEMENT FOR ELECTRONIC ENGINE CONTROLLERS

Volume II: Guide to Development of High Reliability
Electronic Engine Controllers

HAMILTON STANDARD
DIVISION OF UNITED TECHNOLOGIES CORPORATION
WINDSOR LOCKS, CONNECTICUT 06096

AUGUST 1980

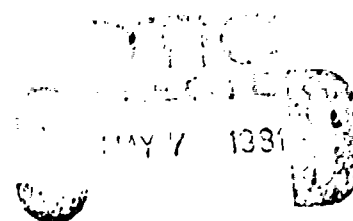
FINAL REPORT FOR PERIOD AUGUST 1977 TO APRIL 1980

TECHNICAL REPORT AFWAL-TR-80-2063

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

DTIC FILE COPY

AERO PROPULSION LABORATORY
AIR FORCE WRIGHT AERONAUTICAL LABORATORIES
AIR FORCE SYSTEMS COMMAND
WRIGHT-PATTERSON AIR FORCE BASE, OHIO 45433



A

81 5 04 162

NOTICE

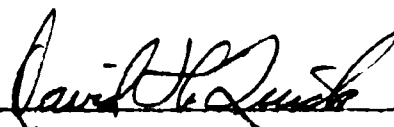
When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely related Government procurement operation, the United States Government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture use, or sell any patented invention that may in any way be related thereto.

This report has been reviewed by the Office of Public Affairs (ASD/PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public, including foreign nations.

This technical report has been reviewed and is approved for publication.

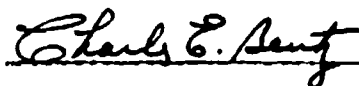


CHARLES E. RYAN, JR.
PROJECT ENGINEER



DAVID H. QUICK, LT COL, USAF
CHIEF, COMPONENTS BRANCH
TURBINE ENGINE DIVISION
AERO PROPULSION LABORATORY

FOR THE COMMANDER



CHARLES E. BENTZ
ACTING DEPUTY DIRECTOR
TURBINE ENGINE DIVISION
AERO PROPULSION LABORATORY

"If your address has changed, if you wish to be removed from our mailing list, or if the addressee is no longer employed by your organization please notify AFWAL/POTC, W-PAFB, OH 45433 to help us maintain a current mailing list".

Copies of this report should not be returned unless return is required by security considerations, contractual obligations, or notice on a specific document.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFWAL-TR-80-2063-101.11	2. GOVT ACCESSION NO. AD-A098614	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) RELIABILITY ADVANCEMENT FOR ELECTRONIC ENGINE CONTROLLERS. Volume II: Guide to the Development of High Reliability Electronic Engine Controllers		5. TYPE OF REPORT & PERIOD COVERED Final August 1977 - April 1980
7. AUTHOR(s) C. Rabinowitz K. Walworth R. Otterberg P. Cote K. Boucher M. McGlone (P&WA) J. Vernon		6. PERFORMING ORG. REPORT NUMBER HSER-7668
9. PERFORMING ORGANIZATION NAME AND ADDRESS Hamilton Standard Division United Technologies Corporation Windsor Locks, Connecticut 06096		8. CONTRACT OR GRANT NUMBER(s) F33615-77-C-2055
11. CONTROLLING OFFICE NAME AND ADDRESS Aero Propulsion Laboratory, Air Force Wright Aeronautical Laboratories, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio 45433		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Project 3066, Task 306603 Work Unit 30660375
12. REPORT DATE August 1980		13. NUMBER OF PAGES 252 Pages
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) NAFIST		15. SECURITY CLASS. (of this report) Unclassified
16. DISTRIBUTION STATEMENT (of this Report) Approved for Public Release: Distribution Unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Electronic Engine Controller Fault Tolerance Reliability Accelerated Stress Test - Reliability Program Integrated Circuits Redundancy Management Reliability Growth		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) Based upon the work done in evolving the preliminary design of Volume I: Final Report this document has been prepared to serve as a guide for developers of future high reliability gas turbine engine controls. After defining the control modes and requirements for a Variable Cycle Engine various options are considered regarding system configuration, redundancy management, system simplification, and fault handling.		

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Principles for optimizing component mix and circuit design, along with possibilities for alternative implementations are presented.

To successfully control the environmental exposure of the EEC, aspects of thorough packaging design are described.

The entire Reliability Program of an organization plays a key role in the development of high reliability controls. Major elements of a successful program are discussed.

Particular emphasis is placed upon implementation of reliability tests and screens designed to enhance electronic hardware reliability.

Reliability mathematical modeling techniques are utilized to evaluate control options during system trade studies and to predict and enhance reliability growth during the design and development program and the production program.

A heavy reliance on reliability mathematical modeling and redundancy management, along with careful consideration of fault tolerant concepts is required for the successful development of future high reliability electronic engine controllers.

PREFACE

This volume of Reliability Advancement for Electronic Engine Controllers is intended to serve as a guide for the development of a high reliability, full-authority electronic engine control based upon the study of Vol. I, "Final Report". This work was conducted by Hamilton Standard Division of United Technologies Corporation under the sponsorship of the Aero Propulsion Laboratory, Turbine Engine Division, Wright-Patterson Air Force Base, Ohio (Air Force Contract No. F33615-77-C-2055), Project No. 3066, Task No. 306603, Work Unit No. 3066 03 75. Sincere thanks are due the Project Officer, Charles E. Ryan, Jr., AFWAL/POTC for his direction, guidance, and encouragement during the course of this program. Mr. Ryan established a team of advanced technology advisors to add their considerable experience to appropriate parts of this effort. Hamilton Standard Division also expresses its sincere appreciation to these organizations and individuals listed below for their invaluable contributions:

Bell Telephone Laboratories

Conrad H. Fierdt, Jr.
D. Stewart Peck
Irwin Schmidt

Delco Electronics Division, General Motors Corporation

Kenneth W. Doversberger
R. M. Siefken
W. Brown

Rome Air Development Center

Joseph B. Brauer
Clyde Lane

AFWAL Avionics Laboratory

Captain Roger E. Little
Captain Lawrence C. Hollatz

U.S. Army Electronics Command

U.S. Army Material Systems Analysis Activity

Dr. L. H. Crow

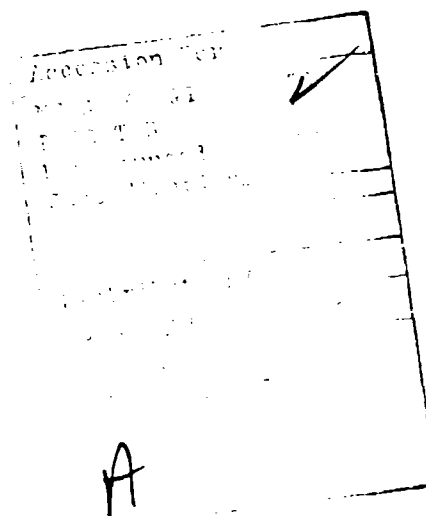


TABLE OF CONTENTS

<u>SECTION</u>		<u>PAGE</u>
I	INTRODUCTION	1
II	SYSTEM CONSIDERATIONS	2
2.1	General Requirements	2
2.1.1	Aircraft Definition	2
2.1.2	Mission Definition	4
2.1.3	Maintenance Objectives	4
2.2	Engine Characteristics and Control Modes	8
2.3	Reliability System Configuration Development	9
2.3.1	System Reliability Objectives	9
2.3.2	General Configuration	11
2.3.3	Redundancy Management	15
2.3.4	Verify Availability Requirements	23
2.3.5	Conclusions	25
2.4	Control Architecture	26
2.4.1	General	26
2.4.2	Single Channel EEC	26
2.4.3	Multichannel EEC Configurations	36
2.4.4	Self Test (BIT)	51
III	COMPONENT AND CIRCUIT IMPLEMENTATION CONSIDERATIONS	66
3.1	Methodology of Circuit and Component Technology Study	66
3.2	Reliability Evaluation Factors	66
3.2.1	Part Level Evaluation	66
3.2.2	Functional Fabrication Level Evaluation	71
3.2.3	Circuit Technology Reliability Tradeoff	74
3.2.4	Passive Component Selection	75

TABLE OF CONTENTS (Continued)

<u>SECTION</u>		<u>PAGE</u>
IV	PACKAGE CONSIDERATIONS	77
4.1	Introduction	77
4.2	Environmental Factors	78
4.2.1	General Discussion	78
4.2.2	Sources of Exposure	79
4.3	Environmental Design	86
4.3.1	Thermal Considerations	86
4.3.2	Vibration Consideration	89
4.3.3	Acoustics	90
4.3.4	Shock	92
4.4	Interconnect Trades	92
4.4.1	Circuit Integration	93
4.4.2	Interconnect and Packaging (I/P) Structure	93
4.4.3	Terminations	96
4.4.4	Cabling	105
4.4.5	Testing	105
4.5	Material Consideration	106
V	RELIABILITY PROGRAM	108
5.1	Reliability Philosophy	108
5.2	Reliability Design Analysis	111
5.3	Mathematical and Statistical Support	114
5.4	Failure Mode, Effects and Criticality Analysis (FMECA)	115
5.4.1	General	115
5.4.2	Item Number and Item Description	118
5.4.3	Failure Mode	119
5.4.4	Probable Cause	119
5.4.5	Failure Effects	119
5.4.6	Detection Method	119
5.4.7	Compensating Features	119
5.4.8	Criticality Classification	119
5.4.9	Probability of Failure	120
5.4.10	FMECA Report	121
5.5	Failure Analysis	121
5.5.1	Establish Failure Analysis Purpose	121
5.5.2	Develop Failure Analysis Techniques	121

TABLE OF CONTENTS (Continued)

<u>SECTION</u>		<u>PAGE</u>
5.5.3	Failure Analysis Requirements	121
5.5.4	Conduct Failure Analysis	122
5.5.5	Document Failure Analysis Results	123
5.5.6	Corrective Action Loop	124
5.6	Maintainability Design Concepts	124
5.6.1	Maintainability Parameters	124
5.6.2	Maintenance Concepts	125
5.7	Training	126
5.8	Derating	128
VI	TESTS TO ENHANCE RELIABILITY GROWTH	129
6.1	Introduction	129
6.2	Piece Part Screening	131
6.2.1	Integrated Circuits	131
6.2.2	Discrete Semiconductors	136
6.2.3	Tantalum Capacitors	138
6.2.4	Multilayer Epoxy or Polyimide Printed Circuit Boards	143
6.3	Accelerated Stress Testing	147
6.3.1	Introduction	147
6.3.2	Sample Test Program	147
6.3.3	Conclusion and Results of Accelerated Test	154
6.4	Subassembly Level (Module) Screening	157
6.4.1	Preproduction	157
6.4.2	Production	160
6.5	Final Assembly Level Screening	162
6.6	Reliability Development Testing	171
6.7	Reliability Growth Modeling	176
6.7.1	Generalized Statistical Analysis	176
6.7.2	Early Failure Growth Evaluation	192

TABLE OF CONTENTS (Continued)

<u>SECTION</u>		<u>PAGE</u>
APPENDIX A	VARIABLE CYCLE ENGINE (VCE) CHARACTERISTICS AND CONTROL MODES	195
APPENDIX B	REDUNDANCY OPERATING PLANS FOR VARIOUS CHANNEL CONFIGURATIONS	211
APPENDIX C	PARAMETRIC AND FUNCTIONAL DEVICE TESTING	213
APPENDIX D	CONSTRUCTION EVALUATION FOR SAMPLE ACCELERATED LIFE TESTS	219
	REFERENCES	221

LIST OF ILLUSTRATIONS

<u>FIGURE</u>		<u>PAGE</u>
1	TACTICAL FIGHTER WITH TWO VARIABLE CYCLE ENGINES (VCE)	3
2	VARIABLE CYCLE ENGINE	5
3	ADVANCED TACTICAL FIGHTER MISSION PROFILE: BATTLEFIELD INTERDICTION MISSION	6
4	ADVANCED TACTICAL FIGHTER MISSION PROFILE: DEEP STRIKE MISSION	6
5	AVAILABILITY - FLIGHT SAFETY CONFLICT	10
6	COVERAGE VALUES	13
7	CONFIGURATION COMPARISON PERFECT COVERAGE	14
8	CONFIGURATION COMPARISON IMPERFECT COVERAGE	16
9	FAILURE LIKELIHOOD SENSITIVITY TO SECOND FAILURE COVERAGE	18
10	SECOND FAILURE COVERAGE SENSITIVITY	19
11	FAILURE LIKELIHOOD COMPUTATIONS FOR DIFFERENT REDUNDANCY CONFIGURATIONS	22
12	INCREASED AVAILABILITY THRU FAULT TOLERANCE	24
13	SINGLE CHANNEL EEC	27
14	FAILURE MODE SYNTHESIZATION CURVES	35
15	TRIPLE CHANNEL EEC SYSTEM	40
16	DUAL CHANNEL EEC SYSTEM WITH SELECTIVE REDUNDANCIES	52
17	INHERENT FIT (FAILURES IN TIME) TECHNOLOGY CURVES	72
18	FAILURE RATE VS TEMPERATURE GRAPH	87
19	ENGINE CASE VIBRATION	91
20	CHIP PACKAGING METHODS	98
21	DIE CONNECTION TECHNIQUES	99
22	SEPARABLE AND NONSEPARABLE CONNECTORS	102
23	ESTABLISHMENT OF ACCELERATED BURN-IN CONDITIONS (DESIGN AND DEVELOPMENT PHASE, FOR INTEGRATED CIRCUITS)	133
24	100% SCREENING OF INTEGRATED CIRCUITS DURING PRODUCTION PHASE	134
25	100% ACCELERATED SCREENING FLOW FOR DISCRETE SEMICONDUCTORS	137
26	STEP-STRESS TEST OF SOLID TANTALUM CAPACITORS (PREPRODUCTION PHASE)	140
27	STEP-STRESS TEST OF NON-SOLID TANTALUM CAPACITORS (PREPRODUCTION PHASE)	141
28	100% ACCELERATED SCREENING OF TANTALUM CAPACITORS (PRODUCTION PHASE)	142

LIST OF ILLUSTRATIONS (Continued)

<u>FIGURE</u>		<u>PAGE</u>
29	100% SCREENING OF MULTILAYER POLYIMIDE LAMINATE PRINTED CIRCUIT BOARDS (PREPRODUCTION AND PRODUCTION)	145
30	PRINTED CIRCUIT BOARD PLATED THRU HOLES	146
31	TEST PROGRAM FLOW	149
32	MC14163B BIAS CIRCUIT	152
33	100% SCREENING OF POLYIMIDE P.C. BOARD MODEL DURING PREPRODUCTION PHASE	158
34	TEMPERATURE EXTREMES AT DWELL TIME	159
35	100% PREPRODUCTION SCREENING OF MODULES INCOR- PORATING LCC AND CERAMIC SUBSTRATES	161
36	100% SCREENING OF MODULES INCORPORATING POLYIMIDE PC BOARDS DURING PRODUCTION PHASE	163
37	100% SCREENING OF PRODUCTION MODULES INCORPORATING LCC AND CERAMIC SUBSTRATES	164
38	PRODUCTION ACCEPTANCE TEST OF END-ITEM EQUIPMENT	165
39	GENERALIZED TEMPERATURE CYCLING FAILURE RATE CURVES AS A FUNCTION OF EQUIPMENT COMPLEXITY	166
40	DETERMINATION OF NUMBER OF TEMPERATURE CYCLES AS A FUNCTION OF EQUIPMENT COMPLEXITY	168
41	TEMPERATURE RATE OF CHANGE OF EQUIPMENT IN ITS USE ENVIRONMENT BY SEVERITY RANK	169
42	CERT OBJECTIVES	173
43	CERT TEST CONDITIONS	174
44	RELIABILITY GROWTH CYCLE	175
45	GENERALIZED STATISTICAL ANALYSIS FLOW CHART	177
46	CUMULATIVE FAILURES	179
47	AVERAGE FAILURE RATE	179

LIST OF TABLES

<u>TABLE</u>		<u>PAGE</u>
1	GENERAL AIRCRAFT ASSUMPTIONS SUMMARY	2
2	SINGLE CHANNEL EEC SYSTEM DEFINITION	28
3	BUILT-IN-TEST (SELF-TEST) SUMMARY	33
4	TRIPLE CHANNEL EEC SYSTEM DEFINITION	41
5	FIRST FAILURE FLAG ACTION TRIPLE CHANNEL SYSTEM	49
6	DUAL CHANNEL SYSTEM DEFINITION	53
7	FIRST FAILURE FLAG ACTION: DUAL CHANNEL SYSTEM	59
8	TECHNOLOGY INHERENT FAILURE RATES (FAILURES IN TIME)	70
9	COMPARISON OF HIGH-PERFORMANCE LAMINATES AND THICK-FILM SUBSTRATES	95
10	NONSEPARABLE CONNECTIONS	104
11	FAILURE MODES	107
12	FAILURE MODE EFFECTS AND CRITICALITY ANALYSIS TABLE	117
13	BIAS CIRCUIT EVALUATION SUMMARY	153
14	PARAMETRIC TEST SUMMARY	155
15	CONFIDENCE INTERVALS FOR MTBF FROM TIME TERMINATED TEST	185
16	CRITICAL VALUES FOR CRAMER-VON MISES GOODNESS OF FIT TEST	187
17	CONFIDENCE INTERVALS FOR MTBF FROM FAILURE TERMINATED TEST	189

GLOSSARY

ACCELERATED STRESS TESTING - Testing in which the applied stress level is chosen to exceed that stated in the reference conditions in order to shorten the time required to observe the stress response of the item or magnify the response in a given time.

AVAILABILITY - A measure of the degree to which an item is in the operable and committable state at the start of the mission.

COVERAGE - The conditional probability that given the existence of a failure in an operational system, the system is able to recover and continue operation with no permanent loss of function.

CROSS CHANNEL MONITORING - The process by which the signals or outputs of the channels are compared and any disagreement, outside of a tolerance range, is classified a fault.

CROSS-STRAPPING - The physical hardwiring of an element in one channel to elements in other channels.

FAULT TOLERANCE - The ability of the system to experience a finite number of failures and continue operation, in either a fully operational or degraded mode.

FLIGHT SAFETY RELIABILITY - The probability, per flight, of not losing the aircraft due to failures in the engine control.

IN-LINE CHANNEL MONITORING - The process by which the signals or outputs of a single channel are checked (for faults) by the processor of the channel. Also referred to as BIT.

MAINTENANCE RELIABILITY - The probability that the device will not require a maintenance action in the manner and under the conditions of intended use.

MISSION RELIABILITY - The probability that the device will successfully complete its defined mission.

OPERATIONAL READINESS - See AVAILABILITY.

REDUNDANCY MANAGEMENT - The process of improving the coverage of failures with the purpose of making the system fault tolerant.

SYNTHESIS - The substitution of data calculated from the physical relationships of the system using other parameters for a failed element.

ABBREVIATIONS, ACRONYMS, AND SYMBOLS

A4 - High Pressure Turbine Inlet Area
A41 - Low Pressure Turbine Inlet Area
A/D - Analog-to-Digital Converter
AFAPL - Air Force Aero Propulsion Laboratory
AFCRL - Air Force Cambridge Research Laboratories
AGE - Auxiliary Ground Equipment
AGREE - Advisory Group on Reliability of Electronic Equipment
AIC - Air Inlet Control
AJD - Duct Stream Exhaust Nozzle Area
AJE - Core Stream Exhaust Nozzle Area
AMSAA - Army Material Systems Analysis Activity
AQL - Acceptable Quality Level
ASSY - Assembly
AST - Accelerated Stress Testing
AUG - Augmentation
BIT - Built-In-Test
CMVT - Constant Match Varying Temperature
COS - Cost of Ownership Study
CPU - Central Processor Unit
CSVA - Compressor Stator Vane Angle
D/A - Digital-to-Analog Converter

Delta (Δ):

ΔP_3 - Compressor Discharge Differential Pressure

ΔP_{13} - Fan Discharge Differential Pressure

DIP - Dual In-Line Package

DMA - Direct Memory Access

DPRAM - Dual Port Random Access Memory

DPCTRAM - Dual Port Cross Talk Random Access Memory

EAROM - Electrically Alterable Read Only Memory

ECM - Electronic Counter Measures

ECS - Environmental Control System

ECU - Electronic Control Unit

EEC - Electronic Engine Control

E_f - Fan Excitation Order

E_H - High Rotor Excitation Order

EMC - Electromagnetic Compatibility

EMI - Electromagnetic Interference

EMP - Electromagnetic Pulse

EOC - End of Conversion

EPR - Engine Pressure Ratio

FADEC - Full Authority Digital Electronic Control

FET - Field Effect Transistor

FIFO - First In First Out

FIGV - Fan Inlet Guide Vane Angle

FIT - Failures In Time

FMEA - Failure Mode Effects Analysis

FMECA - Failure Mode Effects and Criticality Analysis

FTF - Fly To Failure

GOMAC - Government Microcircuits Application Conference

HCC - Hermetic Chip Carrier

HTOT - High Temperature Overstress Testing

HTRB - High Temperature Reverse Bias

I/O - Input/Output

JAN (JN) - Joint Army Navy

JANS - Highest Procurement Level

JANTX - Extra Testing

JANTXV - Extra Testing and Internal Visual

KOPS - Thousand Operations Per Second

LCC - Leadless Chip Carrier

LOD - Light Off Detector

LRU - Line Replaceable Unit

LSB - Least Significant Bit

LSC - Logistic Support Cost

LSI - Large Scale Integration

MIMD - Multiple Instruction Multiple Data

MOS - Metal Oxide Semiconductor

MSB - Most Significant Bit

MSFC - Marshal Space Flight Center
 MSI - Medium Scale Integration
 MTBF - Mean Time Between Failures
 MTBS - Mean Time Before Shutdown
 MTBUR - Mean Time Before Unscheduled Removal
 MUX - Multiplexer
 N_1 (NL) - Low Rotor Speed
 N_2 (NH) - High Rotor Speed
 NHA - Next Higher Assembly
 NOCS - Non-Operational Control System
 P2 - Fan Inlet Total Pressure
 P3 - Compressor Discharge Total Pressure
 P5 - Low Pressure Turbine Discharge Total Pressure
 P5/P2 - Engine Pressure Ratio
 P12 - Fan Inlet Total Pressure
 P13 - Fan Discharge Total Pressure
 P_{am} - Ambient Pressure
 PAT - Production Acceptance Test
 P_b - Burner Pressure
 PIND - Particle Impact Noise Detection
 PLA - Power Lever Angle
 PLADH - Duct Augmentor Power Lever Angle
 POR - Power On Reset
 PROM - Programmable Read Only Memory

PSR - Power Supply Reset
PS3 - Compressor Discharge Static Pressure
PS13 - Fan Discharge Static Pressure
PT2 - Total Fan Inlet Pressure
PT3 - Total Compressor Discharge Pressure
PT5 - Total Low Pressure Turbine Discharge Pressure
PT13 - Total Fan Discharge Pressure
Ptd - Fan Duct Total Pressure
PWM - Pulse Width Modulation
QPL - Qualified Products List (Mil)
RAM - Random Access Memory
R/D - Resolver-to-Digital Converter
RF - Rocket Fire Signal
RI - Receiving Inspection
RM - Redundancy Management
ROM - Read Only Memory
SDFTP - Self Diagnosing Fault Tolerant Microprocessor
SEM - Scanning Electron Microscope
SIMD - Single Instruction Multiple Data
SISD - Single Instruction Single Data
SOS - Silicon On Sapphire
SOV - Solenoid Operated Valve
SPM - Scratch Pad Memory

SSI - Small Scale Integration

T_3 - Compressor Discharge Total Temperature

T_{22} - Compressor Inlet Total Temperature

TAB - Tape Automated Bonding

T_{am} - Ambient Temperature

TBT - Turbine Blade Temperature

Thr. Bal. - Thrust Balance

TPS - Turbine Pump Speed

TT_2 - Fan Inlet Total Temperature

T_{td} - Fan Duct Total Temperature

TTL or T^2L - Transistor to Transistor Logic

UART - Universal Asynchronous Receiver/Transmitter

VCE - Variable Cycle Engine

VLSI - Very Large Scale Integration

V/STOL - Vertical/Short Take-Off and Landing

WA_{13} - Duct Air Flow

W_{ad} - Fan Duct Airflow Rate

W_f - Fuel Flow

W_{fd1} - Duct Augmentor Fuel Flow, Zone 1

W_{fd2} - Duct Augmentor Fuel Flow, Zone 2

W_{fd3} - Duct Augmentor Fuel Flow, Zone 3

WFDH - Fuel Flow, Duct Heater

W_{fep} - Gas Generator Primary Zone Fuel Flow

W_{fes} - Gas Generator Secondary Zone Fuel Flow

WOW - Weight On Wheels Signal

W_{td} - Duct Heater Fuel Flowrate

W_{te} - Core Fuel Flowrate

XNH - High Rotor Speed

XLN - Low Rotor Speed

θ_{t2} - Ratio of fan inlet air temperature to standard ambient temperature
at sea level

SUMMARY

The employment of electronics technology in the full-authority control of aircraft turbine engines offers many advantages over the traditional hydro-mechanical technology: increased accuracy, improved control modes, better maintenance, and substantially reduced life cycle cost. In terms of the key element of reliability, however, considerable study and investigation of means to improve the reliability potential of electronic engine controllers is necessary to the end that, at maturity no reliability penalty need attend their use on military engines. Reliability Advancement For Electronic Engine Controls (RAEEC), Volume I: "Final Report," AFWAL-TR-80-2063, summarizes the work done toward achieving controller characteristics capable of projecting a maintenance MTBF of 25,000 hours after 500,000 controller flight hours. This compares favorably with the high reliability levels of mature hydromechanical systems. Volume II: "Guide to the Development of High Reliability Electronic Engine Controllers", has been prepared to serve as a guide for developers of future electronic engine controllers in the achievement of the high reliability levels cited in the "Final Report".

As in the "Final Report", the subject EEC's are situated on an advanced tactical fighter with two variable-cycle engines (VCE). The control modes, characteristics, and rating limits have been presented in detail as well as a discussion of the philosophy and ground rules for maintenance.

The control architecture and configuration have been considered in light of engine requirements and control modes. The configuration must accommodate the engine/control handling procedures, self-test requirements, failure annunciation ground rules, and maintenance requirements. A number of options regarding system organization, system simplification, redundancy management, failure modes, and failure detection were summarized.

The single-channel EEC and its limited provisions for self-test could not be expected to meet reliability and safety requirements. Multichannel systems, however, properly designed, can overcome the limitations of the single-channel configuration by permitting the use of full or partial redundancy to improve self-test effectiveness; by providing failure recovery or acceptable back-up control; and by permitting deferred maintenance. The implications of these systems on size, weight, and total life cost must be carefully considered.

The reliability objectives are high system availability and high flight safety. An important concern in control architecture is that while redundancy will increase flight safety reliability, it also decreases system availability due to increased maintenance requirements. A heavy reliance on reliability math modeling and redundancy management techniques is necessary to develop a system configuration capable of meeting these co-existent goals.

The increase in flight safety associated with the use of redundant channels is dependent not only on channel MTBF but also on the concept of coverage and the redundancy operating plan. Methods and criteria for determination of the optimum combination of coverage values and redundancy operating plans were explored. Flight safety is extremely sensitive to changes in coverage values.

In order to offset the decrease in availability caused by application of redundancy techniques to increase flight safety, the concept of fault tolerance, as applied to maintenance alerts, must be explored. The application of fault tolerant techniques reduces the number of maintenance alerts issued and therefore increases availability.

The use of the fault tolerant approach allows the flight safety to remain within its requirement as the availability is increased. Therefore the conflict in the achievement of both high flight safety and high system availability can be resolved.

Optimized component mix and circuit design is also necessary to achieve reliability goals. Once system functions have been defined, the guidelines and methods presented here can be used to evaluate the reliability of alternative implementations. Reliability evaluation factors are assigned for different features at the part level (e.g., production volume, years of production, and past performance) and at the functional fabrication level (e.g., number of active devices, junction temperatures, and board area). This facilitates tradeoffs of the considered circuit technologies.

The intent of the packaging design section was to emphasize the primary environmental design parameters to consider in the development of a package to house and protect a high reliability EEC. This involves careful consideration of environmental factors (primarily temperature and vibration), environmental design, interconnect/design tradeoffs, and material selection. The mechanical components investigated include: interconnects, wire/cables, connectors, printed circuit boards, fasteners, vibration isolators, and the physical structure.

Interconnects and package structure have a great impact on the EEC package reliability. Among the methods considered to increase reliability levels are: maximizing circuit integration, minimizing component count and connections, and providing good mechanical support for components and wires. Failure modes and causes were investigated for various materials.

Elements of the environment have been reviewed for conditions on and off the engine: from storage and shipping to flight service and repair. A complete definition of the total engine environment is absolutely crucial to successfully control the total exposure of the EEC and to achieve maximum reliability.

The Reliability Program of an organization is a vital area in the development of high reliability controls. Success requires management and technical involvement in the overall reliability operation associated with company activities such as engineering, training, testing, manufacturing, quality control, packaging, and mathematical and statistical support.

Failure modes, effects, and criticality analyses (FMECA) are important techniques for evaluation of a system. Elements of FMECA have been described with the objective of highlighting potentially critical failure areas.

This "Development Guide" has placed particular emphasis upon the implementation of reliability tests and screens designed to enhance the reliability of electronic hardware intended for use in an environment identified as hostile due to its high vibration and temperature levels; conditions germane to an aircraft engine mounted application. The testing program structured herein emphasizes the performance of reliability tests at the key points of development and production cycles. Among the key points identified are: the selection and screening of piece parts; fabrication and test of both polyimide and ceramic substrate multilayer printed circuit boards; subassembly or module level screening; and end-item level acceptance testing.

During the development, or preproduction, phase emphasis is placed upon the establishment of those screening and testing conditions which will be the most effective in ferreting out defective and/or marginal parts and assemblies during the production cycle. From various industrial reports on the subject of reliability testing, the single most effective screen at all levels of assembly is thermal cycling. All agree, however, the optimum conditions of the thermal cycle screen (its rate of change, temperature range and number of cycles) are dependent upon the packaging and component mix of the equipment to be screened; the processes involved with its manufacture as well as the facilities where it is manufactured influence the behavior of the equipment to a degree sufficient to also affect the selection of thermal cycle parameters.

CERT testing has been described which will allow corrective actions to be rapidly incorporated in the total control population during 50,000 hours of CERT testing. This will allow a substantially improved reliability growth rate resulting in a higher reliability level at the time of introduction to service and a projected reduction in time to mature reliability of two to four years accompanied by reduced aircraft delays and scrubbed missions.

The value of accelerated stress testing was emphasized; detailed procedures and results of a sample test program have been presented. Such tests are designed to identify failure modes and mechanisms in order to establish failure rates and median life; and to develop screening methods that could be used for the procurement of high reliability components for an EEC.

Reliability growth modeling and trend tests, as detailed here, are vital for planning corrective actions and determining their impact on a system.

No single reliability activity or improvement measure will result in a high degree of reliability enhancement for an electronic engine controller; but a family of improvement means and techniques described in this guide can result in a full-authority EEC with a level of reliability suitable for future high-performance turbine engines.

In summation, the entire purpose and goal of this Development Guide is to increase EEC reliability through a variety of design/development/production actions, and not simply to measure reliability.

SECTION I

INTRODUCTION

The prospective application of full-authority electronic control technology in future high-performance turbine engines has necessitated investigation of means to increase the reliability of these controls to a level which approaches the reliability of traditional hydromechanical controls. This Volume II of Reliability Advancement for Electronic Engine Controllers is based upon Volume I, "Final Report", which summarizes the work done toward achieving controller characteristics capable of projecting a maintenance MTBF of 25,000 hours after 500,000 controller flight hours. This document is intended to serve as a comprehensive guide to future developers of electronic engine controllers in attaining the required high levels of reliability.

Principal concepts and procedures have been delineated; particularly those areas critical to the achievement of these increased reliability goals.

Following establishment of basic ground rules, control modes, and maintenance requirements for an electronic controller mounted on a variable cycle engine (VCE), various control system configurations are considered to accommodate the engine/control handling procedures, self-test requirements, and failure annunciation ground rules.

Criteria for conducting tradeoffs to optimize component mix, circuit design, and material selection are presented.

In addition to component and system considerations the importance of key elements of an organization's overall Reliability Program are discussed, along with failure analyses, reliability growth modeling and trend testing.

Particular emphasis is placed upon tests and screens at key points of development and production to enhance the reliability of electronic hardware.

Throughout this Development Guide, the goal is to increase reliability - not to simply measure it.

Section II

SYSTEM CONSIDERATION

2.1 General Requirements

Control system design starts with the "plant" definition which in this case means the engine mounted in its intended airframe and flying its intended missions. It proceeds then to study and define the control modes, the environment, the reliability characteristics, the maintenance characteristics, the control architecture and the performance of the plant/control combination.

In this program, a number of assumptions (Table 1) have been made with regard to aircraft type, engine control configuration, control modes, quality, handling procedures and availability; concerning maintenance and repair procedures; and with regard to the types of missions to be flown.

2.1.1 Aircraft Definition

The type of aircraft to which this development guide was applied is an advanced tactical fighter with two variable cycle engines (VCE) located on the aft fuselage as shown in Figure 1.

TABLE 1 GENERAL AIRCRAFT ASSUMPTIONS SUMMARY

Aircraft	-	Advanced Tactical Fighter
Engine Type	-	Variable Cycle Engine
Engine Quantity	-	Two
Engine Location	-	Aft Fuselage
Mission Definitions	- *	Battlefield Interdiction
	*	Deep Strike Mission
Takeoff Distance	-	< 3000 Ft
Acceleration Time	(Mach 0.85 to Mach 1.5) -	< 70 Sec
Maneuver Capability	-	3g
Mission Rate	-	2 Per Day

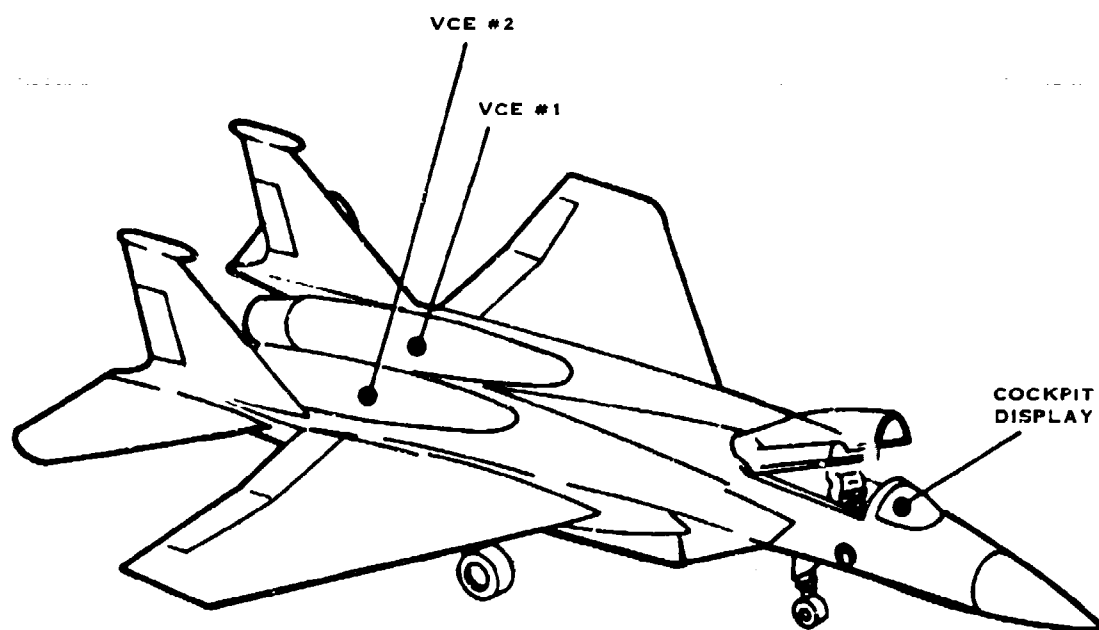


FIGURE 1 TACTICAL FIGHTER WITH TWO VARIABLE CYCLE ENGINES (VCE)

2.1.1 Continued

The variable cycle engine addressed in this study is shown schematically in Figure 2, and is discussed in paragraph 2.2 and Appendix A.

For this design guide it is assumed that the controller is mounted on the outer engine case downstream of the fan and upstream of the duct augmentor flameholders. This location is preferred in order to minimize engine envelope dimensions while avoiding the elevated temperatures in the aft part of the engine.

2.1.2 Mission Definition

A battlefield interdiction mission (Figure 3) and a deep strike mission (Figure 4) are typical requirements for an advanced tactical fighter and were the basis of this study. Both missions have a 300-nmi subsonic radius which consists of takeoff, climb, and subsonic cruise, with a 30-min loiter at return to base. In addition, the battlefield interdiction mission has a 15-min high altitude loiter before penetration. The altitude and Mach number of the subsonic cruise out and back are optimized to provide maximum range per pound of fuel consumed.

The battlefield interdiction mission has a 100-nmi penetration radius at low altitude and low supersonic Mach number (20,000 ft, Mach 1.5). The deep-strike mission is directed at enemy supply lines, resulting in a greater penetration radius: approximately 265 nmi. After an acceleration to Mach 2.2, the aircraft climbs to an altitude that provides the maximum range per pound of fuel consumed. The altitude of the return leg at Mach 2.2 is also optimized for maximum range per pound of fuel.

In addition to these mission requirements, the aircraft must have a takeoff distance of less than 3,000 ft and an acceleration time from subsonic to supersonic flight speeds (Mach 0.85 to Mach 1.5) of less than 70 sec. Maneuver capability of 3g is also required at a representative combat condition.

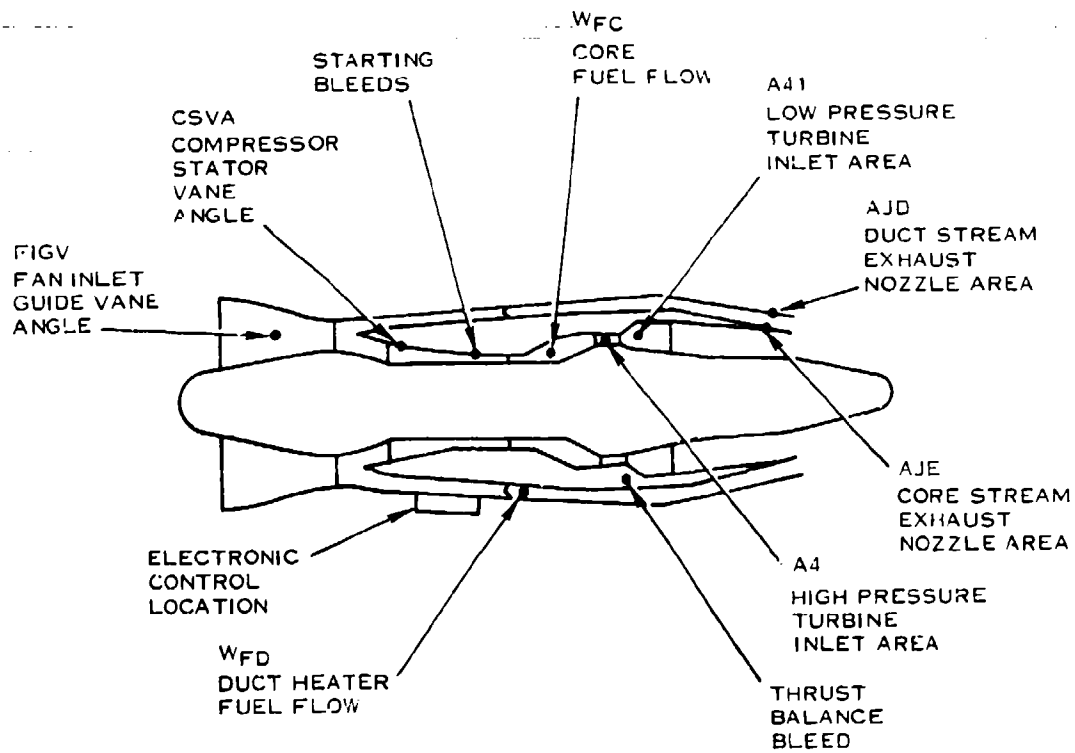
The aircraft must also be capable of carrying out at least two missions per day equally divided.

2.1.3 Maintenance Objectives

2.1.3.1 Philosophy

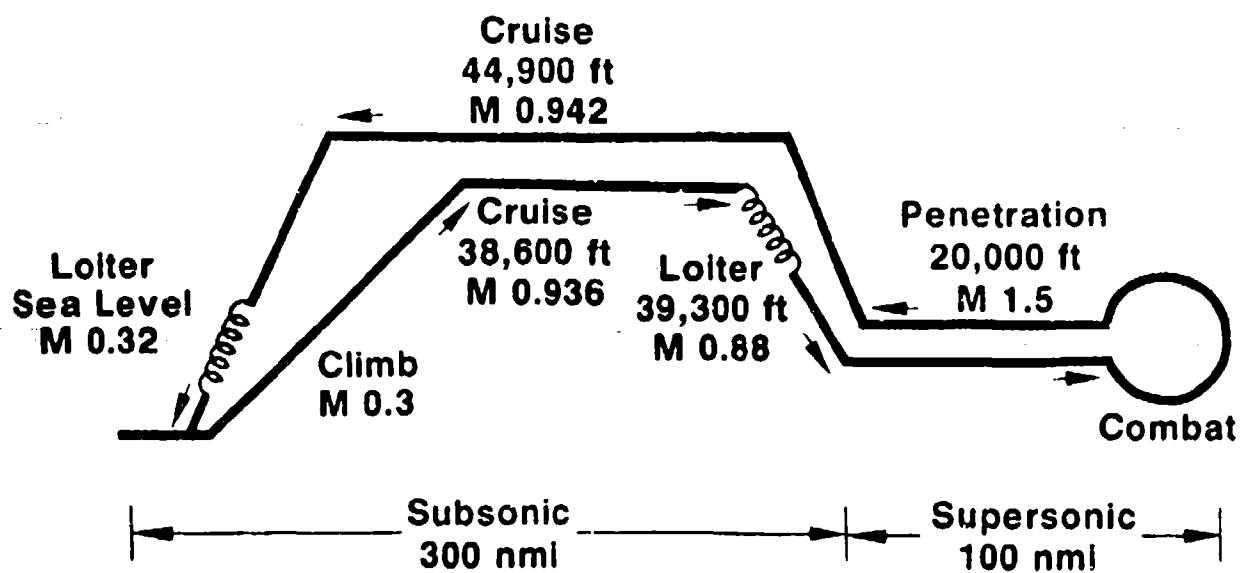
The current Tactical Air Command (TAC) maintenance concept is "Fly To Failure" (FTF), i.e., no scheduled maintenance, trims, or adjustments are allowed at the forward front line base. Maintenance action is initiated only after faults are detected. No ground support equipment is to be required to detect and isolate failures. The Electronic Engine Control (EEC) must be provided with self-contained health monitoring capability (self-test) enabling it to automatically detect and flag system failures. The ground rules for failure alerts are as follows:

1. Any single failure which degrades engine performance or requires an engine shutdown must be flagged.



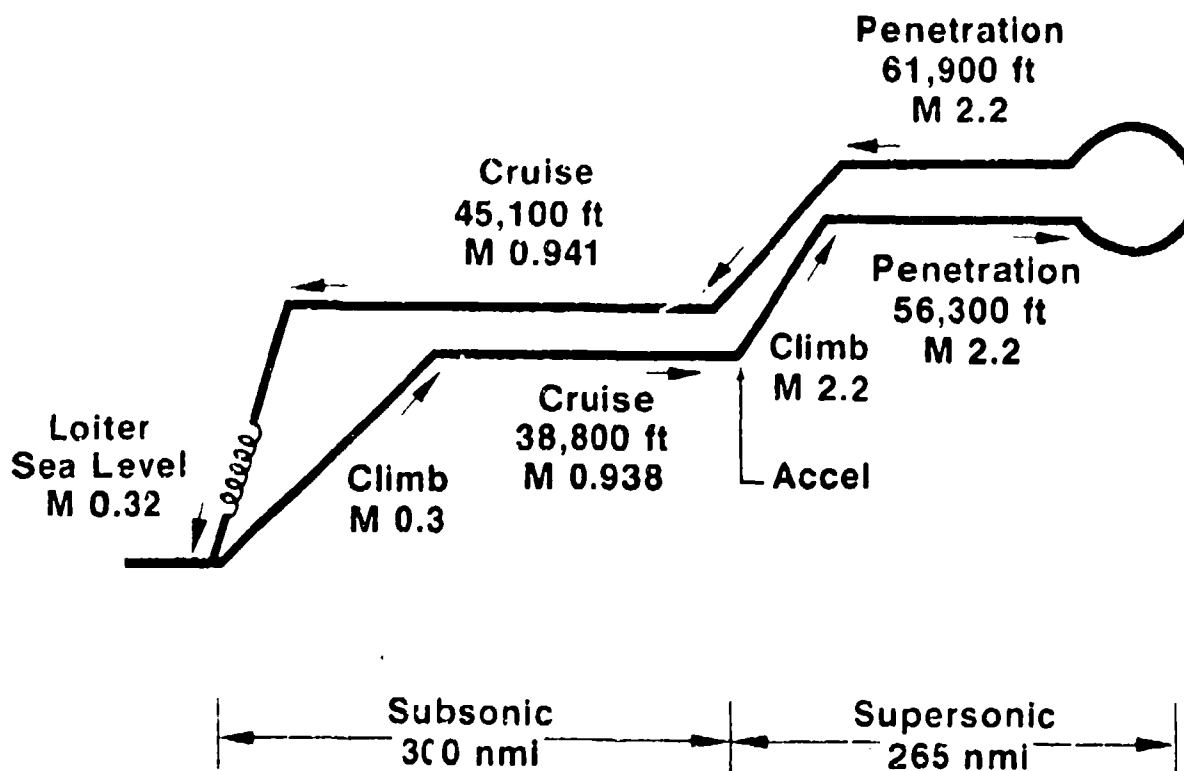
E - 5655

FIGURE 2 VARIABLE CYCLE ENGINE



E - 4807

FIGURE 3 ADVANCED TACTICAL FIGHTER MISSION PROFILE - BATTLEFIELD INTERDICTION MISSION



E 4806

FIGURE 4 ADVANCED TACTICAL FIGHTER MISSION PROFILE - DEEP STRIKE MISSION

2.1.3.1 Continued

2. Any single failure which diminishes flight safety to the extent that the next failure might result in a major loss of engine performance, or require an engine shutdown, must be flagged.

System failure is indicated in the pilot's cockpit display. The EEC box must also display an automatically latched, manually reset, fault flag to indicate its own failure. The maintenance reliability goal for the EEC is 25,000 hrs. M¹BF.

If a back-up control mode is provided to reduce the incidence of in-flight shutdowns, it must be capable of ensuring safe engine operation at useful levels of thrust over the entire aircraft flight profile. The back-up control must also be compatible with the FTF maintenance concept and must not require scheduled maintenance, trims, or adjustments.

2.1.3.2 Procedures Following Failures

Upon receiving a fault alert, during takeoff or in flight, the pilot is expected to abort the mission. The pilot will check his instruments to determine if shutdown is necessary in order to prevent engine damage. A desirable mission failure rate for the EEC falls between one in-flight shutdown in 10⁶ hrs. of operation and two in-flight shutdowns in 10⁷ hrs. of operation.

2.1.3.3 Maintenance Levels

(Guidance for various maintenance level actions was derived from "Maintainability Design Criteria Handbook for Designers of Shipboard Electronic Equipment" March 1965, Navships 94324).

Level I

Level I maintenance action takes place at the forward front line base out of which a squadron operates. On receiving a cockpit fault indication, the pilot is expected to abort the mission and execute an emergency landing at the nearest air base. A maintenance action is required before the aircraft is again available for operation. The most desirable action is to replace the failed LRU out of spares. The faulty LRU is returned to the nearest level II maintenance base for repair. The repaired LRU is returned to spares.

Level II

Level II maintenance action is carried out at a designated air base equipped to provide intermediate repair actions. In the case of EEC failures, this involves replacement of circuit boards, pressure sensor transducers, and other subassembly modules with spares. For this task, Level II designated bases are provided with test equipment not usually available at the Level I front line base; i.e., AGE (Auxiliary Ground

2.1.3.3 Continued

Equipment) computer test sets which are capable of diagnosing and isolating faults to the module level. Once a fault has been isolated, the defective module is replaced from the spare parts inventory and the repaired EEC unit is returned to the Level I base. The faulty module is then returned to the nearest Level III depot for repair.

Level III

Level III maintenance action is carried out at a central repair depot fully equipped to repair EEC modules at the component level. Turn-around time for Level III maintenance action is about 45 days if equipment is to an intermediate (Level II) base located within the United States. As long as 90 days may be required if the repaired module must be returned to an intermediate base located outside the United States. Turnaround time includes the time to ship and repair the failed unit, plus the time to return it to service once repairs are completed.

2.2 Engine Characteristics and Control Modes

Variable cycle engines such as the configuration shown in Figure 2, incorporate variable fan stator vanes, variable compressor stator vanes, variable high- and low-pressure turbine vane areas, and variable primary and fan duct exhaust nozzle areas in a two stream exhaust configuration. This degree of variable geometry provides the propulsion system designer with improved flexibility for controlling engine operating pressures, thrust - turbine temperature - airflow relationships, engine by-pass ratio, and transient response. Probably the single most important source of performance benefit for this engine configuration over a fixed-area turbine configuration is the capability to operate at constant inlet airflow over not only the augmented power range, but also over a significant portion of the nonaugmented high power range.

It should be apparent that these performance gains noted for a variable cycle engine are not obtained without an appreciable increase in control mode complexity, relative to a fixed-area turbine engine, due to the additional control variables. A simplified version of the control mode block diagram is presented in Appendix A for the purpose of describing basic control mode operation for the nonaugmented variable geometry turbine engine. This is basically a closed-loop, or integral controller, which implies that each control variable is determined as a function of an error between a scheduled and sensed value of an engine parameter.

A detailed description of VCE control modes, engine ratings, and operational limits is presented in Appendix A. Also discussed are minimum back-up control modes for continuing VCE operation at reduced, yet safe, levels following failures of various control loops. Actions taken are intended to satisfy the criteria for acceptable back-up control outlined in Section 2.1.3.2.

2.3 Reliability System Configuration Development

2.3.1 System Reliability Objectives

The first step in the design of a high reliability electronic engine control is to develop the system configuration based on the two most basic reliability objectives:

- o High Flight Safety Reliability
- o High System Availability

In the most general terms, flight safety is defined as the minimum suite of equipments necessary to insure no loss of life. The classical definition of availability is the probability of being operationally ready at any point in time. Before proceeding any further, these general concepts of safety and availability should be defined in terms of the electronic engine control and the requirements set. The definition of system safety should include the minimum hardware complement to assure meeting a defined failure likelihood.

The concept of high availability implies infrequent maintenance actions and therefore a high Mean Time Between Failures, or a correspondingly low series failure likelihood. This approach to defining and measuring availability is probably the most easily understood method.

This method of viewing availability highlights the conflict in the achievement of both high flight safety and high system availability. Flight safety is best achieved by several levels of redundancy while high availability (high series MTBF) is achieved by simplicity. This concept is illustrated in the following example.

Assume a system has a complement of equipments whose total failure rate is 100×10^{-6} F/Hr. The system has a mission time of 2 hours. Also, assume only a portion of the equipments in the system are required for flight safety (80×10^{-6} F/Hr.). This system has a series failure likelihood of 1.9998×10^{-4} or an MTBF of 10,000 hrs. and a flight safety failure likelihood of 1.5999×10^{-4} . (See Figure 5). To increase the flight safety failure likelihood, two levels of redundancy are added to the system. This new system has a series failure likelihood of 5.9982×10^{-4} or an MTBF of 3333 hrs. and a flight safety failure likelihood of 4.0950×10^{-12} . (See Figure 5). As can be seen, the flight safety failure likelihood has been increased at the expense of MTBF. The methodology used to derive these results will be explained in depth later in this section. This example is a simple illustration of the conflicting nature of the two goals.

These co-existent goals require the careful development of a system configuration with heavy reliance on reliability math modeling and Redundancy Management (RM) techniques. The attainment of these goals is also likely to require an iterative trade-off design process.

A)

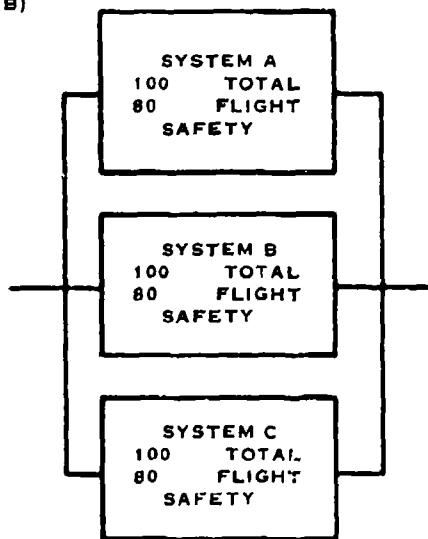


$$FL(SERIES) = Q = 1 - R = 1 - e^{-(100 \times 10^{-6})(2)} \\ = 1.9998 \times 10^{-4}$$

$$MTBF = \frac{1}{100 \times 10^{-6}} = 10,000 \text{ HR}$$

$$FL(FLIGHT SAFETY) = Q = 1 - R = 1 - e^{-(80 \times 10^{-6})(2)} \\ = 1.5999 \times 10^{-4}$$

B)



$$FL(SERIES) = Q = 1 - R = 1 - e^{-(300 \times 10^{-6})(2)} \\ = 5.9982 \times 10^{-4}$$

$$MTBF = \frac{1}{300 \times 10^{-6}} = 3333 \text{ HR}$$

$$FL(FLIGHT SAFETY) = Q^3 = (1 - R)^3 = \\ 1 - e^{-(80 \times 10^{-6})(2)} \\ = 4.0950 \times 10^{-12}$$

FIGURE 5 AVAILABILITY FLIGHT SAFETY CONFLICT

2.3.2 General Configuration

Once the quantitative reliability goals have been defined and identified, the next step is to determine the general system configuration necessary to achieve an estimate for flight safety failure likelihood in the same "ball park" as the requirement. The following steps are necessary to determine the general system configuration.

- o Define Baseline Channel
- o Determine Channel Coverage
- o Determine Number of Channels Required

2.3.2.1 Define Baseline Channel

At this point the equipments necessary to perform the mission should be defined. This becomes the baseline channel for the electronic engine control. Consider the following simplistic engine control. A channel is defined to consist of a power supply ($\lambda = 20$), a pressure sensor ($\lambda = 17$), an A/D converter ($\lambda = 10$), a resolver ($\lambda = 3$), an R/D converter ($\lambda = 7$), a processor ($\lambda = 38$), and a torque motor ($\lambda = 5$). The total failure rate for the channel is 100λ .

2.3.2.2 Determine Channel Coverage

Once the channel has been defined, the channel coverage value may be determined. The concept of coverage is an important one in a fault tolerant system. As stated by Wulf (1), it is much more important to recover from failures than to prevent them since perfect reliability is not attainable. Coverage is defined as the conditional probability that, given the existence of a failure in the system, is able to recover and continue operation with no permanent loss of function (2).

The calculation of coverage values includes only those failure modes which degrade functional performance. The total failure rate for a system is composed of nonfunctional failure modes plus functional failure modes. Nonfunctional failure modes are those failures having no effect on system operation and which do not reduce the level of coverage. The functional failure modes are those failures which degrade system performance. The group of functional failure modes can be split into two subgroups: a group whose failure modes are covered (detectable, isolatable, and recoverable) and a group whose failure modes are uncovered (undetectable, unisolatable, or unrecoverable).

$$\lambda T = \lambda NF + \lambda F$$

$$\lambda F = \lambda U + \lambda C$$

- λT = Total failure rate
- λNF = Nonfunctional failure rate
- λF = Functional failure rate
- λU = Uncovered functional failure rate
- λC = Covered functional failure rate

2.3.2.2 Continued

From the above equations, coverage for a single piece of equipment, can be defined as:

$$C = 1 - \frac{\lambda U}{\lambda F}$$

For a channel the coverage can be defined as:

$$C = \frac{\sum C_i \lambda_i}{\sum \lambda_i}$$

where

C_i = ith equipment coverage
 λ_i = ith equipment failure rate

Consider the previous example. For the power supply assume the entire failure rate is functional and the uncovered functional failure rate is 1λ . Therefore the coverage for the power supply is $C = 1 - 1/20 = 0.95$.

For the pressure sensor assume the entire failure rate is functional and the uncovered functional failure rate is 2λ . Therefore the coverage for the pressure sensor is $C = 1 - 2/15 = 0.88$. For the processor assume 12λ is the nonfunctional failure rate associated with the capability for in-flight recording of data to be used for post-flight analysis. The failure of this portion of the processor does not degrade system performance during flight; hence its designation as nonfunctional. Assume the uncovered functional failure rate is 0.5λ . Therefore the coverage for the processor is $C = 1 - .5/(38-12) = 0.98$. The coverage values for the rest of the equipments were arrived at in the same manner and displayed in Figure 6. The value for the channel coverage is then calculated.

For an actual analysis the values for the functional failure rate and the uncovered functional failure rate would be determined by analysis of the circuit diagrams and built-in-test routines. An FMEA would also be of necessity in the determination of coverage values.

2.3.2.3 Determine Number of Channels Required

The next step is to determine the number of required baseline channels for the engine control to meet its flight safety requirement. Figure 7 can be used as a design guide for this purpose. This figure illustrates the best results for different configurations. For a two-channel configuration, where the coverage value is entirely determined by in-line BIT, the realistic coverage value is 0.96. All of the present literature suggests this is a reasonable value for in-line BIT. In a three-channel system, recovery after the first failure is most often achieved using cross-channel monitoring. The coverage value of 1.0 for the first failure is within the realm of present engineering and hardware expertise. The coverage value for the second failure was assumed to be 0.96 for the same reasons presented for the two-channel configuration. In a

Equipment	λT	λF	λU	C
Power	20	20	1	0.95
Pressure Sensor	17	17	2	0.88
A/D Converter	10	10	0.1	0.99
Resolver	3	3	0.1	0.97
R/D Converter	7	7	1.75	0.75
Processor	38	26	0.5	0.98
Torque Motor	5	5	0.1	0.98

Coverage

0.99
0.98
0.97
0.95
0.88
0.75

Failure Rate

10
31
3
20
17
7

$$C_{\text{Channel}} = \frac{\sum C_i \lambda_i}{\sum \lambda_i}$$

$$C = \underline{\underline{0.94}}$$

FIGURE 6 COVERAGE VALUES

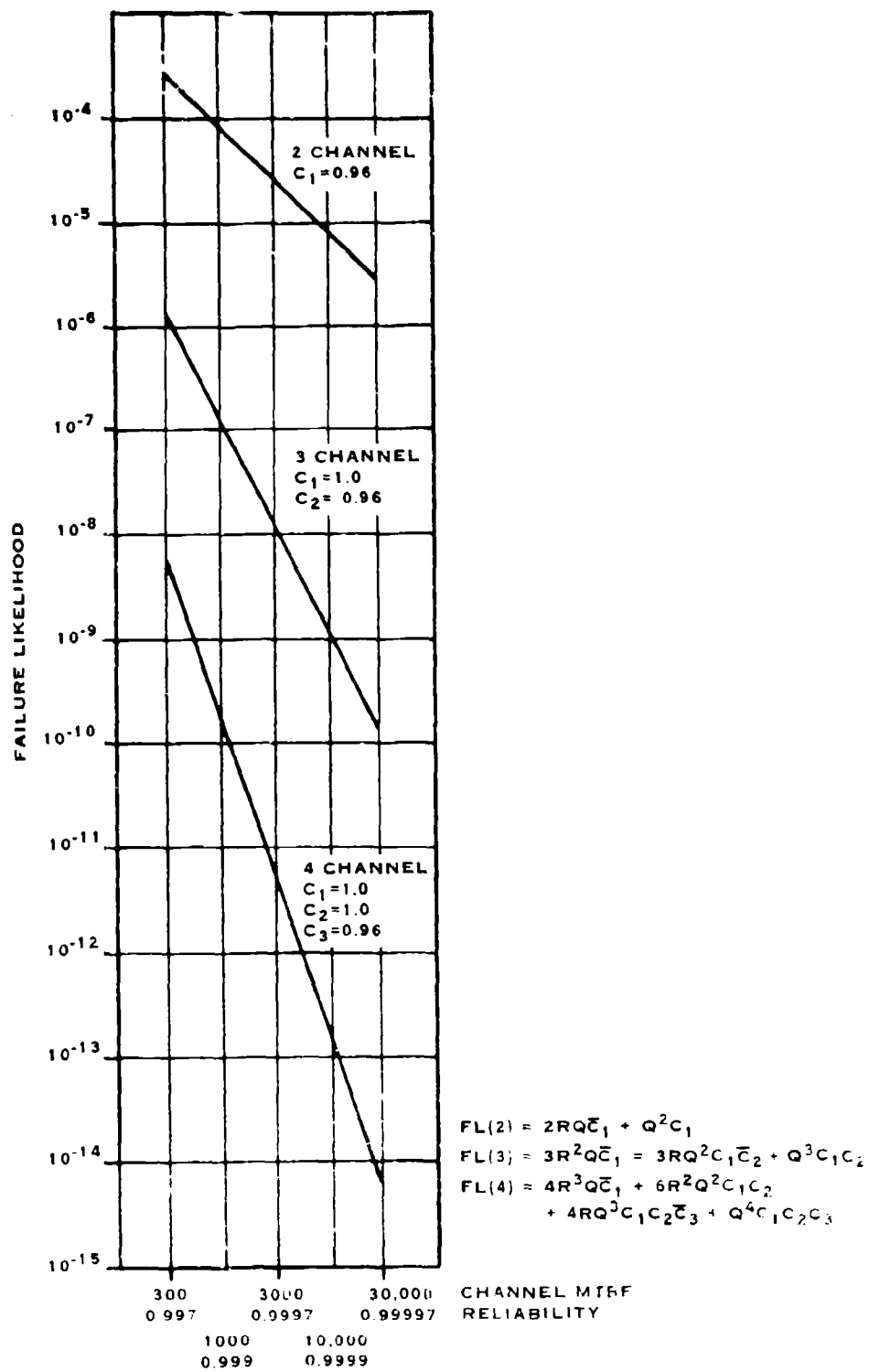


FIGURE 7 CONFIGURATION COMPARISON PERFECT COVERPAGE

2.3.2.3 Continued

four-channel system, recovery after the first two failures is achieved by cross-channel monitoring techniques, therefore the coverage value is 1.0. The coverage value for the third failure was assumed to be 0.96 because recovery is accomplished through in-line BIT techniques.

At this point it becomes necessary to discuss an important characteristic of the coverage value associated with cross-channel monitoring. It turns out that the failure likelihood of a system is extremely sensitive to minute changes in this coverage value near 1.0. For example, consider Figure 8. The same equations used for Figure 7 were plotted in Figure 8 except that the first failure coverage value was changed from 1.0 to .999. Notice that the failure likelihoods for the respective configurations have increased drastically, and even the relative position of the three-channel and four-channel lines have changed. It is obvious that care must be taken when quantifying the C_1 . It is not sufficient to say that C_1 is "approximately one".

Consider the continuing example. The engine control must meet a flight safety failure likelihood requirement of 1×10^{-7} . The baseline channel, as defined, exhibits an MTBF of 10,000 hrs. If the mission length is assumed to be one hour, then by using Figure 7, it can be seen that a three-channel (1.20×10^{-9}) and a four-channel (1.6×10^{-13}) system both exceed the requirement (1×10^{-6}), but that a two-channel system (8.00×10^{-6}) fails to meet the requirement. Therefore, for the engine control in the example, a three-channel configuration was selected.

The final system configuration cannot be determined until the detailed Redundancy Management Policy has been formulated.

2.3.3 Redundancy Management

Once the number of channels has been determined for a given system, the redundancy operating plan can be determined. For two channels the number of different plans is limited: the channels may be operated in a parallel configuration with one channel designated as primary; or in a standby configuration (3). In either case, a failure is detected by BIT and switching is initiated.

For three or more channels per system, the number of different plans is many and varied. Most of these plans are based on the Von Neuman (4) method of redundancy. Detection and switching, after at least the first failure, is accomplished by cross-channel monitoring techniques (majority logic voting). After detection of the failure, the system may be reconfigured so that a different redundancy operating plan applies. This failure/detection/reconfiguration cycle can continue until the last operating channel remains.

After the redundancy operating plan has been selected, the exact flight safety failure likelihood equation can be formulated. This equation is then evaluated and the result compared to the requirement. If the redundancy operating plan does not enable the system to meet its requirement, there are four options open: (1) select a different redundancy operating plan and repeat the analysis; (2) increase the coverage value(s) for the channels and repeat the analysis; (3) increase the channel MTBF and repeat the analysis; or (4) add another channel

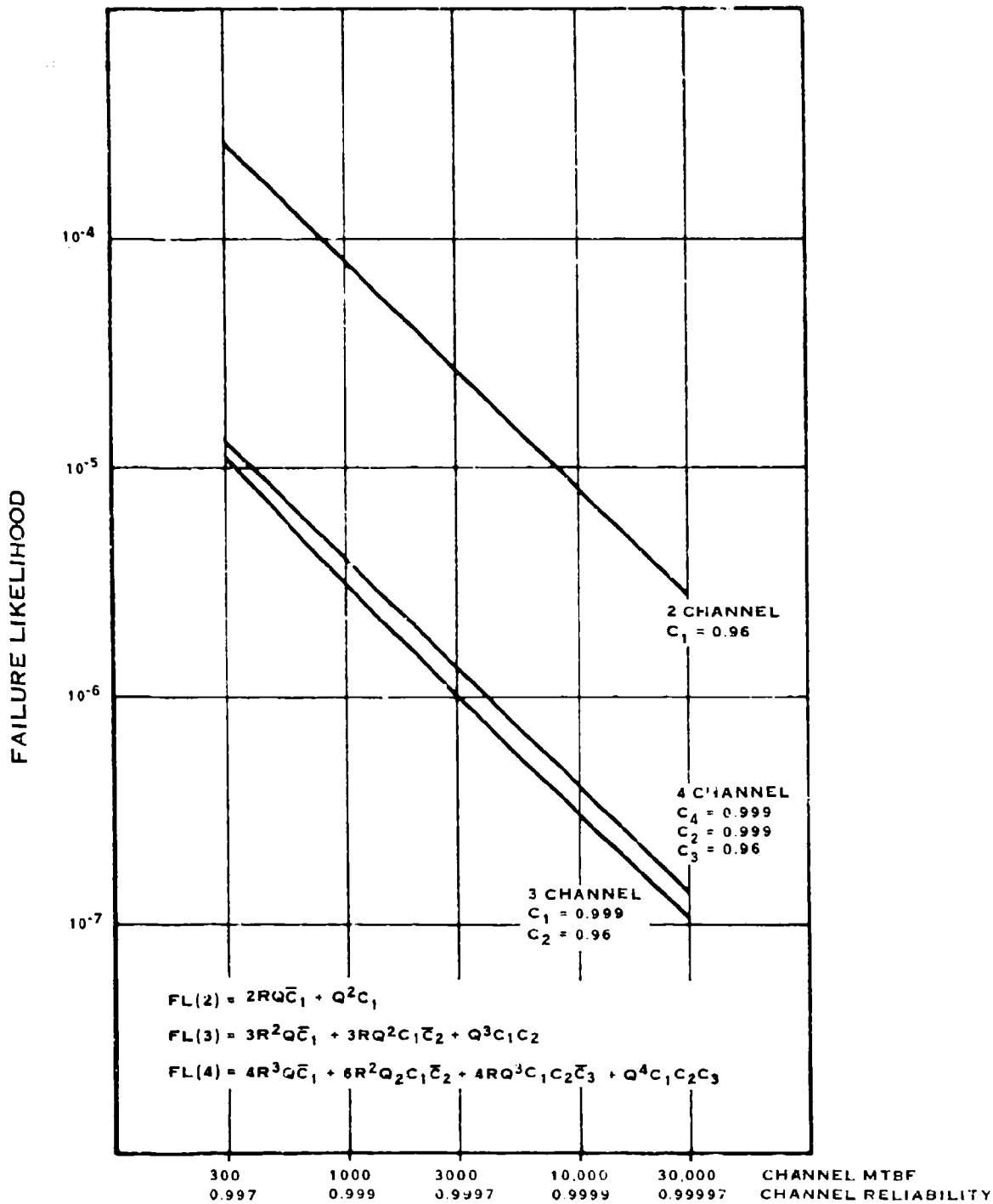


FIGURE 8 CONFIGURATION COMPARISON IMPERFECT COVERAGE

2.3.3 Continued

to the system and repeat the analysis. This is one point at which the iterative nature of the design process becomes apparent.

Of the four options, selecting a different redundancy operating plan requires the least hardware changes. The equipment and the channel remain the same, only the hardware associated with system reconfiguration is altered. This represents a small portion of the total system. A description and partial listing of possible redundancy operating plans are located in Appendix B.

Increasing the coverage values for the channel generally requires improvement in failure detection and recovery design. Increasing the coverage value associated with cross-channel monitoring, should this value be less than 1.0, requires the implementation of more efficient/reliable voting techniques/hardware. Insight for increasing the coverage value associated with in-line BIT is provided by the definition of coverage. ($C = 1 - \lambda U / \lambda F$). If the value of the uncovered failure rates was reduced, coverage would increase. Each piece of equipment in the channel should be reviewed to determine which uncovered failure modes could be eliminated the easiest. These uncovered failure modes can be eliminated either by: hardware redesign; applying redundancy techniques at the component level (Shannon-More Redundancy Method(5)) or at the circuit level (Tryon Redundancy Method (6)); or by a BIT redesign (hardware and/or software).

Increasing the second failure coverage factor associated with in-line BIT may not always decrease the failure likelihood. Refer to Figure 9. The failure likelihood for a three-channel system was plotted using a first failure coverage of 0.999 while the second failure coverage was varied through a range of values ($C_2 = 0.7$ to 0.999). The results show that for high channel reliability ($R_C > .999$), as defined by $R_C = e^{-\text{time/channel MTBF}}$, increasing C_2 has negligible effect upon failure likelihood. Second failure coverage has the greatest impact upon failure likelihood when the channel reliability is between 0.717 and 0.997. This phenomenon can be explained by analyzing the failure likelihood equation:

$$FL = 3R^2QC_1 + 3RQ^2C_1C_2 + Q^3C_1C_2$$

For channels with high reliabilities, R is very close to 1 and Q is very close to zero. Therefore the terms containing RQ^2 and Q^3 are insignificant and the failure likelihood is determined by the dominant R^2Q term, which is not dependent upon C_2 . For channels with lower reliabilities the terms containing RQ^2 and Q^3 are no longer insignificant and the failure likelihood is dependent upon all three terms. Therefore it is also dependent upon C_2 .

The failure likelihood can be made more dependent upon C_2 if the value of C_1 is increased. Figure 10 displays this phenomenon. In this graph the failure likelihood is graphed as a function of C_2 while C_1 was varied through a range of values ($C_1 = 0.95$ to 1.0) and the channel reliability was held constant. The results show that for $C_1 = 0.95$, at the assumed channel reliability, there is no change in failure likelihood for $C_2 = 0.65$ to 1.0 . However, as C_1 is increased towards 1, the failure likelihood begins to show greater dependency on C_2 ,

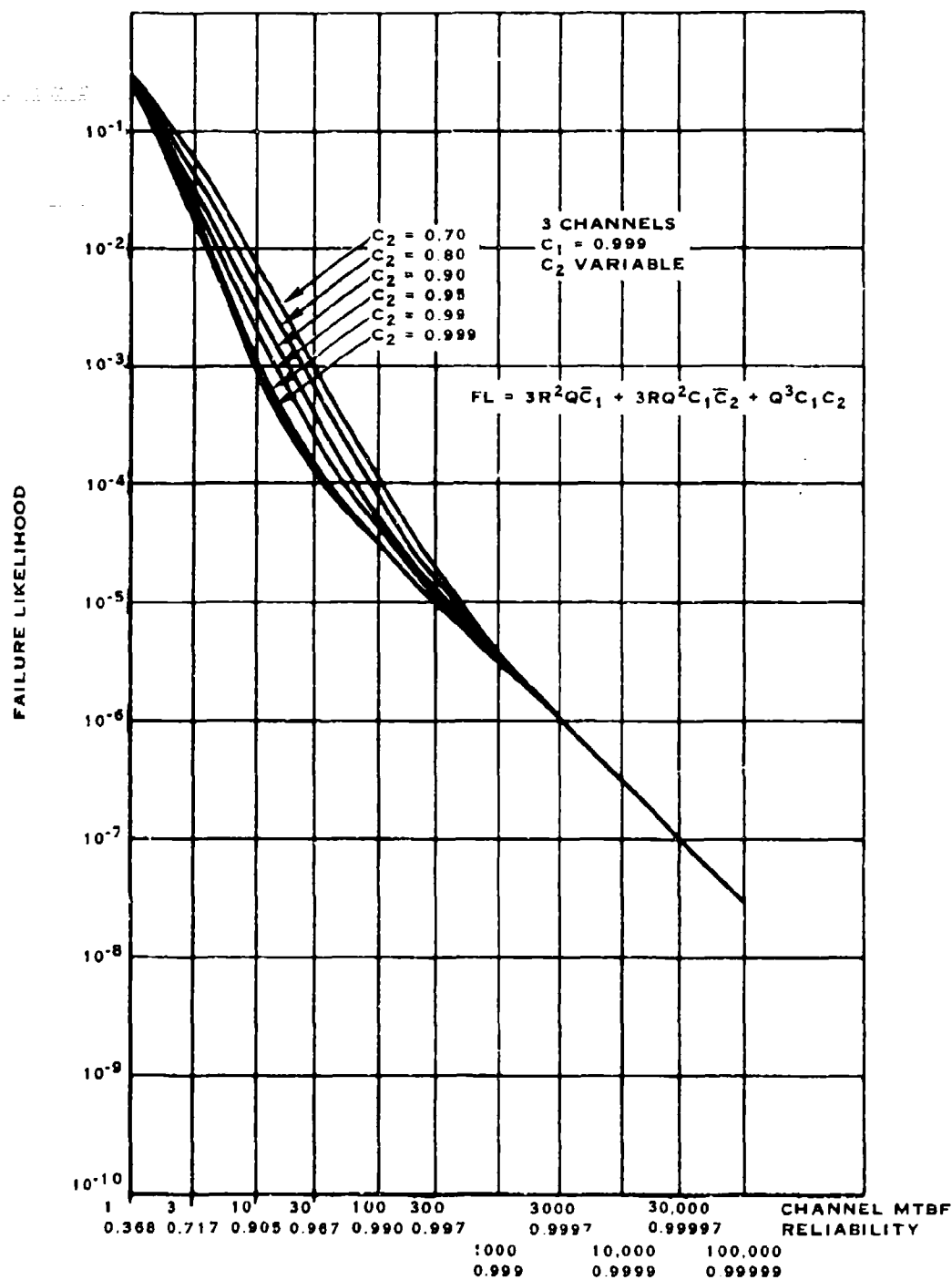


FIGURE 9 FAILURE LIKELIHOOD SENSITIVITY TO SECOND FAILURE COVERAGE

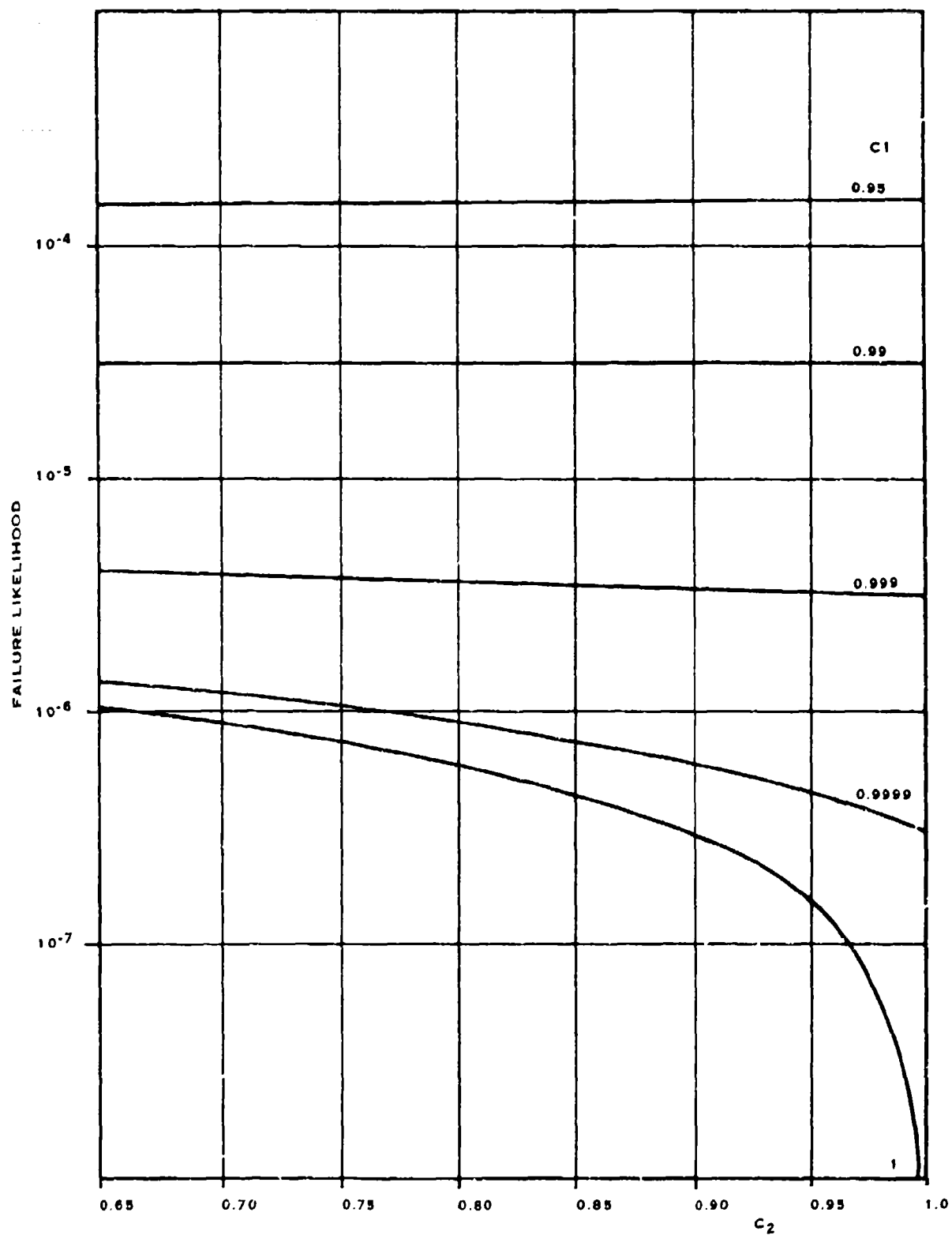


FIGURE 10 SECOND FAILURE COVERAGE SENSITIVITY

2.3.3 Continued

at the assumed channel reliability. For $C_1 = 1.0$ the change in failure likelihood is more than 2 orders of magnitude as C_2 varies from 0.65 to 1.0.

This phenomenon can also be explained by analyzing the failure likelihood equation:

$$FL = 3R^2Q\bar{C}_1 + 3RQ^2C_1\bar{C}_2 + Q^3C_1C_2$$

From the previous analysis it was found that the first term ($3R^2Q\bar{C}_1$) is the dominant term for high channel reliabilities. However as C_1 approaches 1, $\bar{C}_1$ approaches zero and the first term begins to lose its dominance and the failure likelihood becomes more dependent upon C_2 because of the contributions of the other terms.

The conclusion drawn from this analysis is that the blanket statement: "Increasing C_2 will decrease failure likelihood", does not always hold true, and that some preliminary analysis must be done before making such a statement. In some cases C_2 will have little or no effect upon failure likelihood, but by increasing C_1 the sensitivity of failure likelihood to C_2 can be improved.

The third option available to revise the system so as to meet its requirement is to increase the channel MTBF. Referring to Figure 7 it can be seen that increasing the channel MTBF only a few percentage points does not significantly decrease the failure likelihood. For a dual channel system (Figure 7), an increase in channel MTBF of ten results in an order of magnitude decrease in likelihood of failure of the control. Such an increase in channel MTBF is costly and difficult to obtain.

The fourth option available to revise the system to enable it to meet its requirement is to add another channel. This method will always yield a decrease in failure likelihood when going from two channels to three channels, because the three-channel system can employ cross-channel monitoring, which has a higher inherent coverage value, for first failure detection and recovery. However this method may not always yield the same result when going from a three-channel system to a four-channel system. If the coverage value associated with cross-channel monitoring is perfect ($C_1 = 1.0$), then going from three channels to four channels will reduce the failure likelihood. (See Figure 7). If the coverage value associated with cross-channel monitoring is less than perfect (e.g., $C_1 = 0.999$), then going from three channels to four channels may actually increase the failure likelihood (see Figure 8). The addition of a fourth channel with imperfect coverage increases the number of possible failures from which recovery cannot be initiated. Hence the failure likelihood increases.

Consider the continuing example. Assume that initially a standby redundancy operating plan was chosen. In this operating plan one channel is on-line and the other two channels are in standby. When the on-line channel fails, one of the two standby channels is switched on-line. This failure/detection/reconfiguration continues until the last good channel is placed on-line. The detection and reconfiguration is initiated by in-line BIT for both the first

2.3.3 Continued

and second failure. Therefore the coverage value is 0.94 as previously determined (Figure 6). The failure likelihood equation is

$$FL = 3R^2Q\bar{C}_1 + 3RQ^2C_1\bar{C}_2 + Q^3C_1C_2$$

Evaluation of the equation for the engine control in question (channel MTBF = 10,000 hrs., mission time = 1 hr., $C_1 = C_2 = .94$) yields a failure likelihood of 1.8×10^{-5} . This value does not meet the requirement of 1.0×10^{-6} .

Assume that a new redundancy plan is selected: Triple Modular Redundancy (TMR/Simplex/Simple). In this operating plan the three channels are used in a voting configuration. After the first failure, detection and reconfiguration is accomplished through cross-channel monitoring. Assume that the first failure coverage is less than perfect, $C_1 = 0.999$. The system selects one of the two remaining channels and places it on-line. The other remaining good channel is placed in standby. If the on-line channel should fail, detection and reconfiguration is initiated by in-line BIT. Therefore the second failure coverage value is 0.94. The remaining one good channel is placed on-line.

Evaluation of the equation for this engine control (channel MTBF = 10,000 hrs., mission time = 1 hr., $C_1 = 0.999$, $C_2 = 0.94$) yields a failure likelihood of 3.02×10^{-7} , which exceeds the requirement (See Figure 11). Therefore changing the redundancy operating plan from Standby to TMR/Simplex/Simplex enables the three-channel system to meet the requirement.

For the sake of argument, assume that 3.02×10^{-7} still does not meet the requirement, and to decrease the failure likelihood still further an increase of C_2 is contemplated. However by looking at Figure 9 it can be seen that for $C_1 = 0.999$ and a 10,000 hr. channel MTBF, increasing C_2 has almost no effect upon failure likelihood. Therefore trying to decrease failure likelihood by increasing C_2 is a futile effort, and if the TMR/Simplex/Simplex system is to meet this new, lower requirement then C_1 must be increased or the channel reliability increased.

Suppose that instead of changing the redundancy operating plan, an attempt was made to increase the coverage value of the channel. By iteration, it was found that a coverage value of 0.997 would be required if the standby redundancy three-channel system was to meet the requirement (See Figure 11). The attainment of such a high coverage factor by in-line BIT would require a design well beyond the current state-of-the art. Therefore it is highly improbable that the standby redundancy three-channel system will meet the requirement.

Another method of reducing the failure likelihood of the original standby system would be to increase the channel MTBF. By iteration it was found that the channel MTBF would have to be increased to 180,000 hours for the requirement to be met. This would correspond to a reduction of from 100λ to 5.5λ . This reduction is obviously not within the realm of present technology.

- STAND-BY REDUNDANCY THREE-CHANNEL SYSTEM

$$FL = 3R^2QC_1 + 3RQ^2C_1C_2 + Q^3C_1C_2$$

$$R = 1 - e^{-1/10,000}$$

$$Q = 1 - R$$

$$C_1 = .94$$

$$C_2 = .94$$

$$FL = 1.8 \times 10^{-5} \text{ Fails to meet requirement of } 1.0 \times 10^{-6}$$

- TRM/SIMPLEX/SIMPLEX SYSTEM

$$FL = 3R^2QC_1 + 3RQ^2C_1C_2 + Q^3C_1C_2$$

$$R = 1 - e^{-1/10,000}$$

$$Q = 1 - R$$

$$C_1 = .999$$

$$C_2 = .94$$

$$FL = 3.02 \times 10^{-7} \text{ Exceeds requirement of } 1.0 \times 10^{-6}$$

- STAND-BY REDUNDANCY THREE-CHANNEL SYSTEM - IMPROVED COVERAGE

$$FL = 3R^2QC_1 + 3RQ^2C_1C_2 + Q^3C_1C_2$$

$$C_1 = C_2 = .96$$

$$FL = 1.2 \times 10^{-5}$$

$$C_1 = C_2 = .98$$

$$FL = 6.0 \times 10^{-6}$$

$$C_1 = C_2 = .99$$

$$FL = 3.0 \times 10^{-6}$$

$$C_1 = C_2 = .995$$

$$FL = 1.5 \times 10^{-6}$$

$$C_1 = C_2 = .997$$

$$FL = 9.0 \times 10^{-7} \text{ Exceeds requirement of } 1.0 \times 10^{-6}$$

FIGURE 11 FAILURE LIKELIHOOD COMPUTATIONS FOR DIFFERENT REDUNDANCY CONFIGURATIONS

2.3.3 Continued

Once the final configuration has been determined and the flight safety requirements met, the next step is to define the crew alert policy using the failure effects for each failure mode. A warning should be communicated to the crew when one additional fault of a critical function or a major function will cause a catastrophic system loss or mission abort. A warning should be communicated to the crew when a minor function has completely failed and full system performance is not available.

2.3.4 Verify Availability Requirements

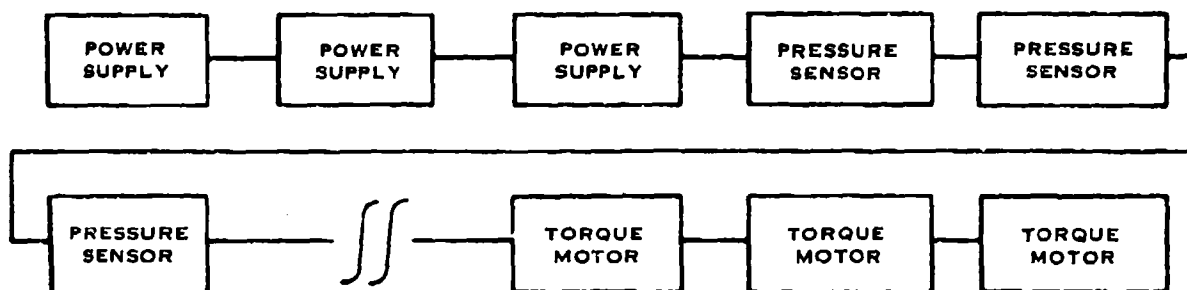
From the final system configuration, the series MTBF or the series failure likelihood can be determined from the system. Consider the continuing example. For the configuration and redundancy operating plan that has met the requirement (3 channel - TMR/Simplex/Simplex) there is 100λ per channel for a total of 300λ in series. The MTBF of the series string is 3333 hr. or a series failure likelihood of 3.0×10^{-4} . This is a significant change from a one channel system (MTBF = 10,000, FL = 1.0×10^{-4}).

The conflict in the achievement of both high flight safety and high system availability is emphasized by the above example. What is needed is a methodology to increase availability after the system has been organized to meet its flight safety requirement. The present method assumes that a maintenance alert is generated with the first failure, therefore the series string of equipment is used to determine the MTBF.

An alternative method incorporates the concept of fault tolerance. Instead of generating a maintenance alert after the first failure, the maintenance alert is generated after the second or third failure. This fault tolerant concept extends the period of trouble-free service life and thus increases system availability. The new methodology changes the Availability Model from a series string of equipments to a series string of modules, where the modules are composed of N equipments in parallel for an N-channel system and module failure is defined as failure of N equipments or N-1 equipments, etc. (See Figure 12). The failure of a module generates a maintenance alert. The number of equipment failures tolerated per module is dependent upon the Maintenance Alert Policy. The Maintenance Alert Policy is formulated using basically the same criteria and guidelines uses in the design of the Crew Alert Policy.

With the use of the fault tolerant approach for flagging maintenance actions, it is conceivable that at the beginning of a given mission there may be one or more equipments in the system in the failed state with no crew or maintenance alert given. This possibility of the system not being in the "full-up" state at the start of the mission will lead to a lower flight safety failure likelihood than calculated. The calculated value assumes the system is "full-up" at the start of any mission. This reduction in flight safety failure likelihood can be offset by the use of information cross-strapping between channels and software synthesis of parameter values. Information cross-strapping provides for the transfer of the appropriate raw data to a channel with the failed

• NON-FAULT TOLERANT AVAILABILITY MODEL

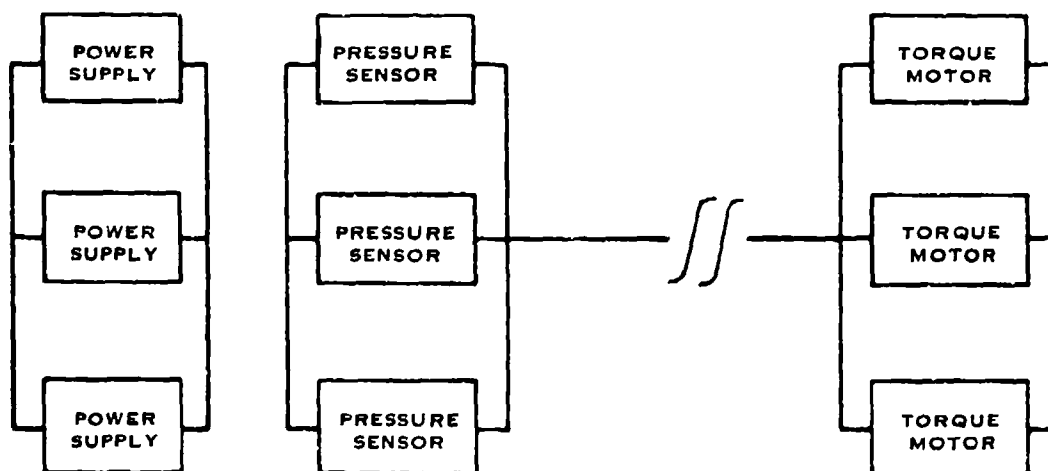


SERIES = 300

MTBF = $1/300 = 3333$ HRS

FL = 3×10^{-4}

• FAULT TOLERANT AVAILABILITY MODEL



2 FAIL OF 3

3 FAIL OF 3

2 FAIL OF 3

$-2(20)(1)$ $-3(20)(1)$ $-(17)1$ $-2(10)(1)$ $-3(10)(1)$

$$FL = 1 - (3e^{-2(20)(1)} - 2e^{-3(20)(1)}) (1 - 1e^{-(17)1})^3 (3e^{-2(10)(1)} - 2e^{-3(10)(1)}) \\ (3e^{-2(3)(1)} - 2e^{-3(3)(1)}) (3e^{-2(7)(1)} - 2e^{-3(7)(1)}) (3e^{-2(38)(1)} - 2e^{-3(38)(1)}) \\ (3e^{-2(5)(1)} - 2e^{-3(5)(1)}) = 7 \times 10^{-9}$$

FIGURE 12 INCREASED AVAILABILITY THRU FAULT TOLERANCE

2.3.4 Continued

piece of equipment from a channel with operational equipment. This allows the channel with the failed piece of equipment to operate in a "full-up" mode. Software synthesis of parameter values provides this same capability.

2.3.5 Conclusions

The achievement of both high system availability and high flight safety, is difficult due to the conflict of different system configurations required. A heavy reliance on reliability math modeling and redundancy management techniques is necessary to develop a system configuration capable of meeting these co-existent goals.

The increase in flight safety associated with the use of redundant channels is dependent not only on channel MTBF but also on the concept of coverage and the redundancy operating plan. Methods and criteria for determination of the optimum combination of coverage values and redundancy operating plans were explored. Flight safety is extremely sensitive to changes in coverage values.

In order to offset the decrease in availability caused by application of redundancy techniques to increase flight safety, the concept of fault tolerance, as applied to maintenance alerts, must be explored. The application of fault tolerance techniques reduces the number of maintenance alerts issued and therefore increases the availability.

The use of the fault tolerant approach allows the flight safety to remain within its requirement as the availability is increased. Therefore the conflict in the achievement of both high flight safety and high system availability is resolved.

2.4 Control Architecture

2.4.1 General

The control architecture must fit the engine requirements and control modes. It must accommodate the engine/control handling procedures, self-test (or Built-in-test - BIT) requirements, failure annunciation groundrules and maintenance requirements. A number of options regarding system organization, system simplification, redundancy management, failure modes, and failure detection are summarized below.

2.4.2 Single Channel EEC

2.4.2.1 Configuration and Self-Testing

The simplest, most direct approach to implementing an EEC capable of providing the control modes required by the engine is the single channel configuration given in Figure 13. The single channel EEC is capable of interfacing with engine/airframe transducers and effectors. Input signals from the transducers are converted by the input interfaced into digital data words which are supplied to the digital central processor unit (CPU). The CPU is programmed to execute the gas generator (core engine) control logic, and the augmentor control logic (Appendix A), from which it computes the correct outputs to the effectors. The output interfaces convert the CPU digital data output words into the required effector drive signals. The EEC unit receives raw AC power from its own alternator. A detailed system definition of the single channel EEC concept is given in Table 2.

In addition to control mode functions, the single channel concept must also include self-test and fault annunciation compatible with the requirements in Section 2.1.3. Self-test is preferably implemented by software, except when the nature of the test requires hardware implementation, since this approach has the least impact on system cost, size, weight, and reliability. The CPU usually provides sufficient memory and processor time to include self-test routines as well as other "housekeeping" functions not directly related to control mode functions. Even if additional memory is required to include the self-test routines in the program, its impact on system cost, size, weight, and reliability is significantly less than hardware implementation of the tests.

The self-test routines available for application to EEC systems are listed in Table 3. All of these tests are applicable to the single channel EEC except for tests 3 and 17. Test 3 can be applied only to triple (or greater) redundant functions (not used in the single channel EEC), while test 17 applies only to multichannel systems. Test 2 is applicable in the single channel system to input parameters that are measured by dual transducers (as in the case of PLA), or are synthesized by software in

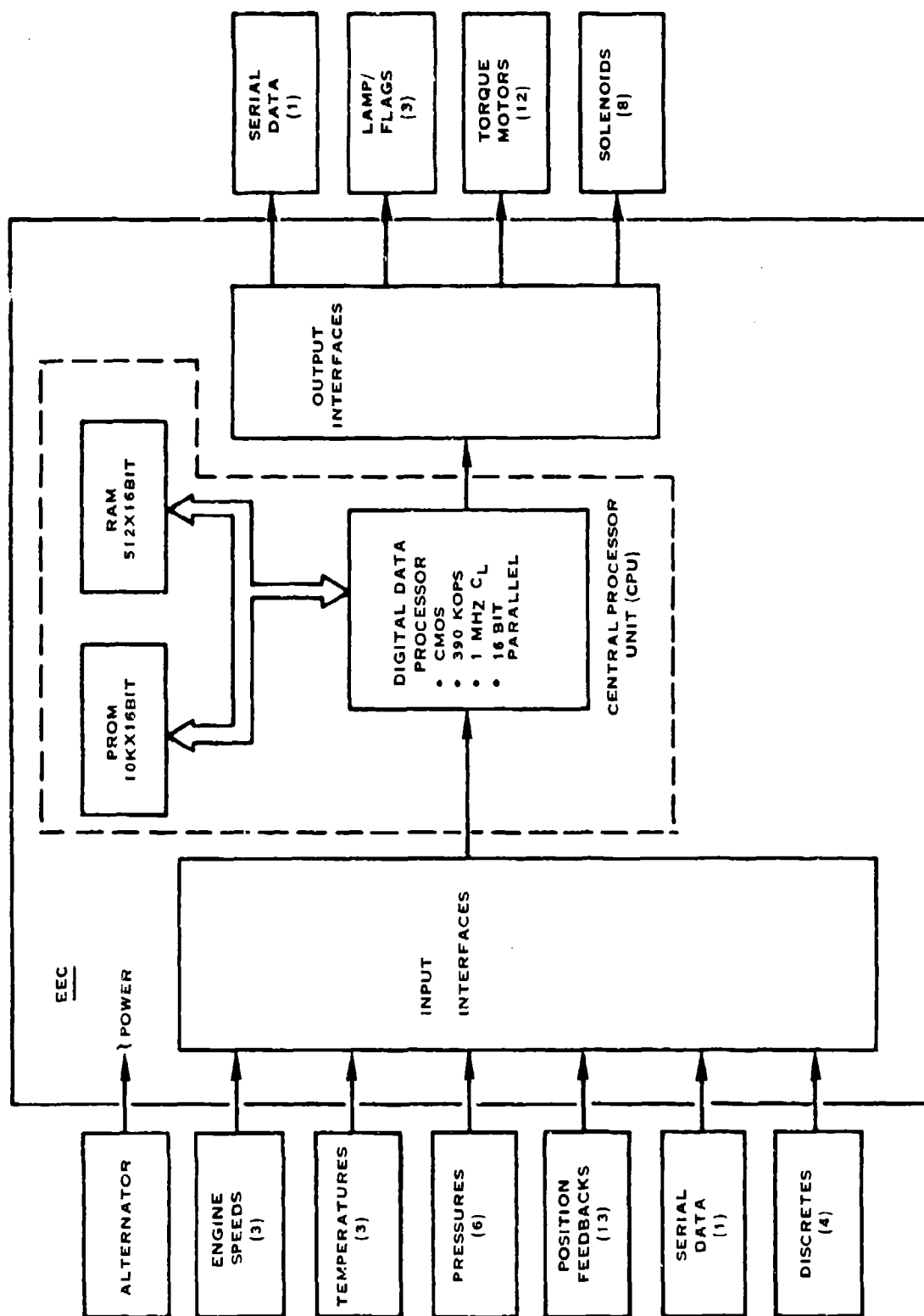


FIGURE 13 SINGLE CHANNEL EEC

TABLE 2

SINGLE CHANNEL EEC SYSTEM DEFINITION

FUNCTION	COMPLETE LOSS OF FUNCTION	PARAMETER	DEFINITION	INCLUDED IN:	
				HARDWARE (NUMBER)	SOFTWARE
POWER SUPPLY	SHUTDOWN	ALTERNATOR	SUPPLIED FROM DEDICATED ALTERNATOR WINDINGS	1	NO
SIGNAL INTERFACE	MINOR	<u>ENGINE SPEED:</u> TPS NH	TURBO PUMP SPEED	(3) 1	NO
	MAJOR		HIGH ROTOR SPEED	1	YES
	MAJOR	NL	LOW ROTOR SPEED	1	SYNTHESIZED NO
	MAJOR	<u>TEMPERATURE:</u> TT2	FAN INLET TOTAL TEMP.	(3) 1	YES
	MINOR		TURBINE BLADE TEMP.	1	SYNTHESIZED YES*
	MAJOR	T22	COMPRESSOR INLET TOTAL TEMP.	1	SYNTHESIZED YES
	MAJOR	<u>PRESSURE:</u> PT2	FAN INLET TOTAL PRESSURE	(6) 1	YES
	MAJOR		COMPRESSOR DISCHARGE TOTAL PRESSURE	1	SYNTHESIZED YES
	MINOR	Δ P13	FAN DISCHARGE DIFFERENTIAL PRESSURE	1	SYNTHESIZED NO
	MINOR	PT5	LOW PRESSURE TURBINE DISCHARGE TOTAL PRESSURE	1	NO
FOR CORE ENGINE CONTROL	MINOR	PT13	FAN DISCHARGE TOTAL PRESSURE	1	YES
	MAJOR	Δ P3	COMPRESSOR DISCHARGE DIFFERENTIAL PRESSURE	1	SYNTHESIZED YES
					SYNTHESIZED
					SYNTHESIZED

TABLE 2 (Continued)

FUNCTION	COMPLETE LOSS OF FUNCTION	PARAMETER	DEFINITION	INCLUDED IN:	
				HARDWARE (NUMBER)	SOFTWARE
FOR CORE ENGINE CONTROL	SHUTDOWN MAJOR SHUTDOWN MAJOR MAJOR MAJOR MAJOR MINOR SHUTDOWN SHUTDOWN	<u>POSITION:</u> PLA	-	(13) 2	NO
		FIGV	POWER LEVER ANGLE	1	NO
		CSVA	FAN INLET GUIDE VANE	1	NO
		A4	COMPRESSOR STATOR VANE ACTUATOR	1	NO
		A41	HIGH PRESSURE TURBINE INLET AREA	1	NO
		A4J	LOW PRESSURE TURBINE INLET AREA	1	NO
		A4E	CORE STREAM EXHAUST NOZZLE AREA	1	NO
		A4D	DUCT STREAM EXHAUST NOZZLE AREA	1	NO
		WFEP	GAS GENERATOR PRIMARY FUEL FLOW	1	NO
		WFES	G.G. SECONDARY FUEL FLOW	1	NO
FOR AUGMENTOR CONTROL	MINOR MINOR MINOR	WFD1	DUCT AUGMENTOR FUEL FLOW TO ZONE 1	1	NO
		WFD2	DUCT AUGMENTOR FUEL FLOW TO ZONE 2	1	NO
		WFD3	DUCT AUGMENTOR FUEL FLOW TO ZONE 3	1	NO
FOR CORE ENGINE CONTROL	MINOR	SERIAL DIGITAL	-	(1)	NO
		DATA STREAM	-	-	-
		INCLUDES:	-	-	-
		AIR INLET CONTROL FLT. CONTROL ECM MISSION COMPUTER	- - - -	- - - -	- - - -

TABLE 2 (Continued)

COMPLETE LOSS OF FUNCTION		PARAMETER	DEFINITION	INCLUDED IN:			
FUNCTION	FUNCTION	DISCRETE:		HARDWARE (NUMBER)	SOFTWARE		
FOR CORE ENGINE CONTROL	{ MINOR MINOR MAJOR }	R.F.	ROCKET FIRE	(4) 1	NO		
		W.O.W.	WEIGHT ON WHEELS	1	NO		
		PILOT ENABLE	PILOT SWITCH ENABLES/ DISABLES EEC	1	NO		
FOR AUGMENTOR CONTROL	MINOR	LOD	AUGMENTOR LIGHT OFF DETECTOR	1	NO		
OUTPUT DRIVE INTERFACE							
FOR CORE ENGINE CONTROL	{ MINOR MAJOR SHUTDOWN MAJOR MAJOR MAJOR MINOR SHUTDOWN SHUTDOWN }	TORQUE MOTOR:					
		TPS	TURBO PUMP SPEED CONTROL	(12) 1	NO		
		FIGV	SAME AS FOR POSITION	1	NO		
		CSVA	" " " "	1	NO		
		A4	" " " "	1	NO		
		A41	" " " "	1	NO		
		AJE	" " " "	1	NO		
		AJD	" " " "	1	NO		
		WFEP	" " " "	1	NO		
		WFES	" " " "	1	NO		
		FOR AUGMENTOR CONTROL	{ MINOR MINOR MINOR }	WFD1	" " " "	1	NO
				WFD2	" " " "	1	NO
WFD3	" " " "			1	NO		
FOR CORE ENGINE CONTROL	{ MAJOR MAJOR SHUTDOWN SHUTDOWN SHUTDOWN }	SOLENOID:					
		START BLEED	(8) 1	NO			
		STAGING	1	NO			
		THRUST BALANCE	1	NO			
		BLEED	1	NO			
	WFEP			1	NO		
GAS GEN. PRIMARY FUEL FLOW SHUTOFF VALVE							

TABLE 2 (Continued)

FUNCTION	COMPLETE LOSS OF FUNCTION	PARAMETER	DEFINITION	INCLUDED IN:	
				HARDWARE (NUMBER)	SOFTWARE
FOR AUGMENTOR CONTROL	MINOR	SOLENOID: Wfd1	DUCT ZONE 1 FUEL FLOW SHUT-OFF VALVE	1	NO
	MINOR	Wfd2	DUCT ZONE 2 FUEL FLOW SHUT-OFF VALVE	1	NO
	MINOR	Wfd3	DUCT ZONE 3 FUEL FLOW SHUT-OFF VALVE	1	NO
	MINOR	AUGMENTOR IGNITOR RELAY	-	1	NO
FOR ANNUNCIATION	MINOR	LAMPS/FLAGS: EEC ENABLED	COCKPIT LAMP INDICATES EEC ENABLED	(3) 1	NO
	MINOR	EEC FAULT FLAG (LATCHED)	LRU FLAG INDICATES EEC FAULT	1	NO
	MAJOR	NOCs FAULT FLAG (LATCHED)	NON-OPERATIONAL CONTROL SYSTEM FAULT FLAG LOCATED IN ASP	1	NO
	MINOR	SERIAL DIGITAL DATA STREAM SAME AS FOR INPUT	-	(1)	NO
FOR DATA OUTPUT	SHUTDOWN	CPU	CENTRAL PROCESSOR UNIT IMPLEMENTS EEC CHANNEL PROGRAM	1	NO

TABLE 2 (Continued)

FUNCTION	COMPLETE LOSS OF FUNCTION	PARAMETER	DEFINITION	INCLUDED IN:	
				HARDWARE (NUMBER)	SOFTWARE
CONTROL LOOP COMPUTATION	SHUTDOWN	WFEP & WFES	GAS GENERATOR PRIMARY AND SECONDARY FUEL FLOWS	NO	YES
	MAJOR	AJE	CORE STREAM EXHAUST NOZZLE AREA	NO	YES
FOR CORE ENGINE CONTROL	MAJOR	A4	HIGH PRESSURE TURBINE INLET AREA	NO	YES
	MAJOR	A41	LOW PRESSURE TURBINE INLET AREA	NO	YES
	MINOR	AJD	DUCT STREAM EXHAUST NOZZLE AREA	NO	YES
	MAJOR	FIGV	FAN INLET GUIDE VANE POSITION	NO	YES
	SHUTDOWN	CSVA	COMPRESSOR STATOR VANE ACTUATOR POSITION	NO	YES
	MAJOR	START BLEED	STARTING BLEED ON/OFF	NO	YES
FOR AUGMENTOR CONTROL	SHUTDOWN	THRUST BALANCE	THRUST BALANCE BLEED ON/OFF	NO	YES
	MINOR	TPS	TURBO PUMP SPEED CONTROL	NO	YES
	MINOR	WFD1, WFD2, and WFD3	DUCT AUGMENTOR FUEL FLOWS	NO	YES

* SYNTHESIZED FOR FAULT DETECTION ONLY.

TABLE 3 BUILT-IN-TEST (SELF-TEST) SUMMARY

<u>BIT Test Number and Name</u>	<u>In-Flt Tests</u>	<u>Pre-Flt Tests</u>	<u>Software (S) or Hardware (H)</u>
1 Input Range Limit Check	X	X	S
2 Parameter Correlation Check	X	X	S
3 Parameter Majority Logic Check	X	X	S
4 Read Only Memory (ROM) Check	X	X	S
5 Computer Cycle Time Test	X	X	H
6 Output Wraparound Test	X	X	H & S
7 Injected Input Test		X	S
8 Canned Output Computation		X	S
9 Loop Dynamic Check	X	X	S
10 Reference Signal Check	X	X	H & S
11 Power Supply Test	X	X	H
12 Processor Instruction Test	X	X	S
13 Read-Write (Scratch-pad Memory Check)	X	X	S
14 End of Conversion (EDC) BIT Not Detected	X	X	S
15 Hardware Parity and Code Verifier Checks	X	X	H
16 Clock Loss Detect Circuit	X	X	H
17 UART Sync Word Detected	X	X	H

2.4.2.1 Configuration and Self-Testing (Continued)

addition to being measured by a transducer. (See Table 2.) The curves from which the program synthesizes these parameters are given in Figure 14. Synthesized parameters are somewhat less accurate than sensed parameters; however, their accuracy is sufficient to permit comparison checking with the parameter transducer measurement. The remaining self-test routines are termed "in-line tests" because they can be carried out on nonredundant parameters.

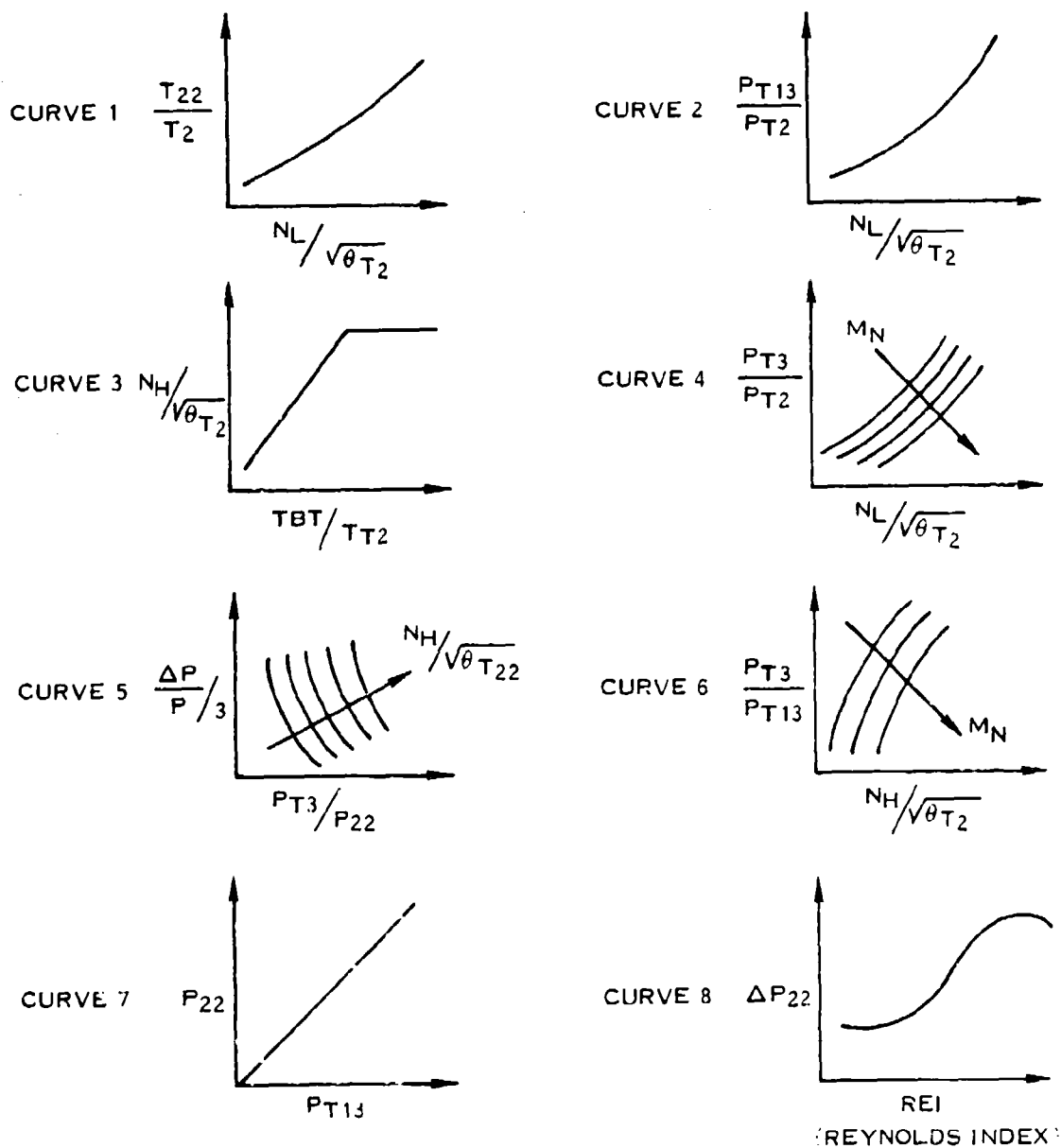
Section 2.1.3 requires that the self-test routines, in their totality, alert the pilot to any single failure which degrades engine performance or requires an engine shutdown. This ground rule does not require that the fault causing the malfunction be isolated and/or repaired. When alerted, the pilot is expected to abort the mission and, if necessary, shut-down the malfunctioning engine to prevent its damage. Self-test 2, where it is applicable, is 100% effective in detecting a fault, but is not able to isolate the failed component and is therefore unable to effect a recovery by using the redundant component. The "in-line tests" are less than 100% effective in detecting a fault; however, once detected, the fault is isolated since there is only a single component implementing the function. Recovery with a single component is, of course, impossible.

In summary then, the totality of self-tests in a single channel EEC allows for 100% self-test effectiveness only for single failures in redundant parameters, and recovery only to the extent of the self-test effectiveness of "in-line tests" (eg. tests 1, 4, 5, 6, 9, etc.) applied separately to each component of the redundant combination.

2.4.2.2 Limitations

Despite its simplicity, the limitations imposed by the single channel concept on self-test effectiveness, and fault recovery, severely restrict its ability to meet EEC maintenance and reliability goals in several areas.

The large number of nonredundant parameters in which faults can be detected only by "in-line tests" means that some faults under certain flight conditions may go unalerted due to the less than 100% effectiveness of this type of self-test. This is particularly hazardous when the complete loss of a parameter function results in a major degradation in performance, or requires shutdown to prevent engine damage. To avoid this condition requires that nonredundant parameters be implemented so that only "detectable" failure modes are possible for all flight conditions. This does not appear feasible, and in any case, places too severe a constraint on design. It should be noted that PLA was provided with dual hardware redundancy because the only in-range test applicable to this parameter is test 1, which alone is too limited in effectiveness



NOTE:

FAIL 1 $\Rightarrow$ CURVE 1
 FAIL 2 $\Rightarrow$ CURVE 2
 ETC.

E 5656

FIGURE 14 FAILURE MODE SYNTHESIZATION CURVES

2.4.2.2 Limitations (Continued)

to adequately protect against engine damage resulting from a nonalerted failure of this parameter function.

Another limitation is that every failure must be flagged resulting in a mission abort or engine shutdown. This is because faults in nonredundant parameters result in performance degradation (since recovery is impossible), while faults in redundant parameters reduce flight safety because the next like failure will result in a major loss in performance or require an in-flight shutdown. Since a maintenance action is required following each mission abort, it is necessary to limit the total failure rate of all components which affect performance to 40λ in order to achieve a maintenance reliability goal of 25000 hr MTBF. With present technology, a single channel EEC capable of providing VCE control would have a total failure rate at least 5 times as great. Improvements in single channel EEC reliability would have to be made at the device level, and would most likely require breakthroughs in several technical areas such as inherent device reliability, vibration isolation, cooling, reliability testing, etc. Procurement cost and cost of spare parts can be expected to be very high because of the required high device reliability.

In a single channel configuration, mission reliability can be no greater than maintenance reliability since single faults cannot be tolerated and result in a mission abort. Even if it is possible to achieve a maintenance reliability of 25000 hr MTBF the mission reliability, in terms of failure likelihood for a 1 hr. flight, would be 4×10^{-5} . If mission reliability is defined in terms of engine shutdowns, failure likelihood is somewhat reduced because the single channel control is capable of switching to a back-up control mode. This allows the engine to continue to operate safely at a reduced, but useful, level of thrust during mission abort. Minimum back-up control modes for a single channel EEC are described in Appendix A and are restricted to a failure which can be isolated to a single variable geometry loop other than CSVA, or to a minor function. The limitations on acceptable back-up control modes and self-test effectiveness permit shutdowns to be avoided in not more than half the incidences of failure. Mission reliability, with respect to engine shutdowns, cannot be expected to exceed 50,000 hr MTBS which is only 5% of the minimum desirable value of 1.0×10^6 hours. Mission reliability goals cannot, therefore, be achieved without a hardware back-up control. Since the requirement for acceptable back-up control is to provide core engine control (Appendix A) this is tantamount to providing a dual channel EEC configuration.

2.4.3 Multichannel EEC Configurations

The limitations imposed by a single channel EEC on meeting the health monitoring (self-test), reliability, and maintenance goals set for the EEC suggest the application of multiple channel configurations for control

2.4.3 Multichannel EEC Configurations (Continued)

system implementation. Multiple channel configurations, properly designed, can overcome the limitations of the single channel EEC by allowing the use of full or partial redundancy to improve self-test effectiveness; to provide failure recovery or acceptable back-up control; and to permit deferred maintenance.

2.4.3.1 Application of Redundancy for High Reliability

On the surface, the achievement of both high mission reliability, and high maintenance reliability through redundant channels are conflicting goals in that, while mission reliability significantly improves with one or more redundant channels, maintenance reliability is significantly degraded by the multiplicity of components. This contradiction is apparent because it is based on a maintenance concept which requires that a failure be flagged the moment it occurs, and repaired before the start of the next mission. This maintenance concept ensures high mission reliability at the cost of increased unscheduled maintenance actions.

The deferred maintenance concept allows a repair to be delayed if it does not degrade performance or impair flight safety. In this concept, the addition of a level of redundancy to extend maintenance MTBF is just as legitimate as the application of redundancy to improve mission reliability; however, the same level of redundancy cannot provide both improvements. Deferring a maintenance action requires that the EEC not signal a maintenance alert when a deferrable fault occurs. However, the EEC must still conform to these previously mentioned failure alert ground rules:

- 1) Any single failure which degrades engine performance or requires an engine shutdown must be flagged.
- 2) Any single failure which diminishes flight safety to the extent that the next failure might result in a major loss in engine performance, or require an engine shutdown, must be flagged.

To avoid flagging the first failure, the above ground rules obviously require triple redundancy for all those EEC parameters (Table 2) in which the complete loss of function results in a major loss of performance or in engine shutdown; and they require dual redundancy for those parameters in which the complete loss of function results only in minor degradation of performance. Faults which can result in major loss of performance (or engine shutdown) are all associated with core engine (gas generator) control, while most of the faults producing only minor degradation in performance are associated with augmentor control. Therefore, the minimum multichannel EEC configuration for extending maintenance MTBF through redundancy is a triple redundant core engine control combined with a dual redundant augmentor control. Mission reliability in the

2.4.3.1 Application of Redundancy for High Reliability (Continued)

minimum multichannel configuration is established by dual redundancy in the core engine control since the first failure is not flagged and, therefore, goes unrepaired for succeeding missions.

Higher levels of redundancy can, of course, be established for multichannel EEC systems. Their objective may be to further extend maintenance MTBF by allowing deferred maintenance on second, as well as first, failures; or to increase mission reliability by providing triple redundancy in the core engine control following the first (unflagged) failure. The limit on the level of redundancy is established in practice by its impact on system size, weight, power dissipation, and above all, on life cycle cost (LCC).

Size, weight, and power dissipation are increased significantly by each additional redundant channel, and in themselves set an upper limit on the number of channels that can be included in the EEC package. Power dissipation is limited by the heat transfer capability of the EEC cooling system over the aircraft's entire flight envelope. Size and weight increases place additional constraints on the ability to isolate the EEC package from vibration and shock.

The impact on life cycle cost is the primary consideration involved in the determination of the practical level of redundancy because extending maintenance MTBF is not viable unless it results in lower life cycle cost. Extending MTBF through multichannel redundancy reduces the frequency of maintenance actions at the forward front line base (Level I), and therefore reduces maintenance labor cost and increases aircraft availability. The procurement cost of a multiple channel EEC can be expected to be high, but this increased cost is to a large extent offset by the need for fewer spare units at the Level I base.

At the intermediate base (Level II) the redundant EEC unit will multiply the number of replacement circuit boards, pressure sensors, etc. that must be made available. It will also increase labor costs because of the additional time required to isolate the failed board or pressure sensor using conventional test equipment. Substantial reductions in maintenance cost at the intermediate repair level can be realized by utilizing the increased self-test effectiveness of the redundant multichannel EEC to isolate and flag failures at the board level. This will eliminate the need for costly test equipment and will reduce labor cost at the Level II base. This offsets, to a large extent, the cost of additional replacement boards.

No reductions can be made at the Level III depot since redundant multichannel EEC design increases the number of boards that have to be repaired at the device level. Level III maintenance cost can be expected to be

2.4.3.1 Application of Redundancy for High Reliability (Continued)

roughly multiplied by the number of redundant EEC channels.

2.4.3.2 Triple Channel EEC

The triple channel EEC system block diagram is given in Figure 15; Table 4 provides the system definition. This EEC configuration meets the minimal design requirements for deferring a maintenance alert for the first failure as follows:

- o Core engine control is included in all three channels; therefore, all parameters whose failure can result in major performance degradation, or engine shut down, are provided with triple redundancy. Augmentor functions which result in only minor degradation are included in two of the three channels.
- o Redundancy is provided, as much as possible, at the parameter function level. This means that a failure of a parameter in one channel does not prevent the other "good" parameters of the failed channel from continuing to provide back-up for like parameters in the other channels. Redundancy at the parameter level significantly improves both maintenance and mission reliability because only the failure of "like" parameters in all three channels fails the EEC.
- o Parameter redundancy is implemented in software by inter-linking the primary, secondary, and back-up CPU's with UART (Universal Asynchronous Receiver/Transmitter) data channels. This provides the advantages of providing better electrical isolation, and substantially reducing the impact on hardware complexity resulting from redundancy at the parameter level. However, this configuration has the disadvantage that failure of the CPU not only fails the channel, but also deprives the remaining "good" channels of their parameter back-ups since UART data transmission is dependent upon the correct operation of the CPU program. Hardwired fault discrete logic is provided as a back-up to each UART data channel to ensure that EEC operation is switched over from the "failed" to the "best health" channel.
- o Software synthesis of pressure parameters is used together with "like" dual redundant hardware pressure transducers to provide triple redundancy for pressure parameters whose failure results in major performance loss. This approach significantly affects system economics because of the relatively high cost, size, and weight of vibrating pressure transducers.

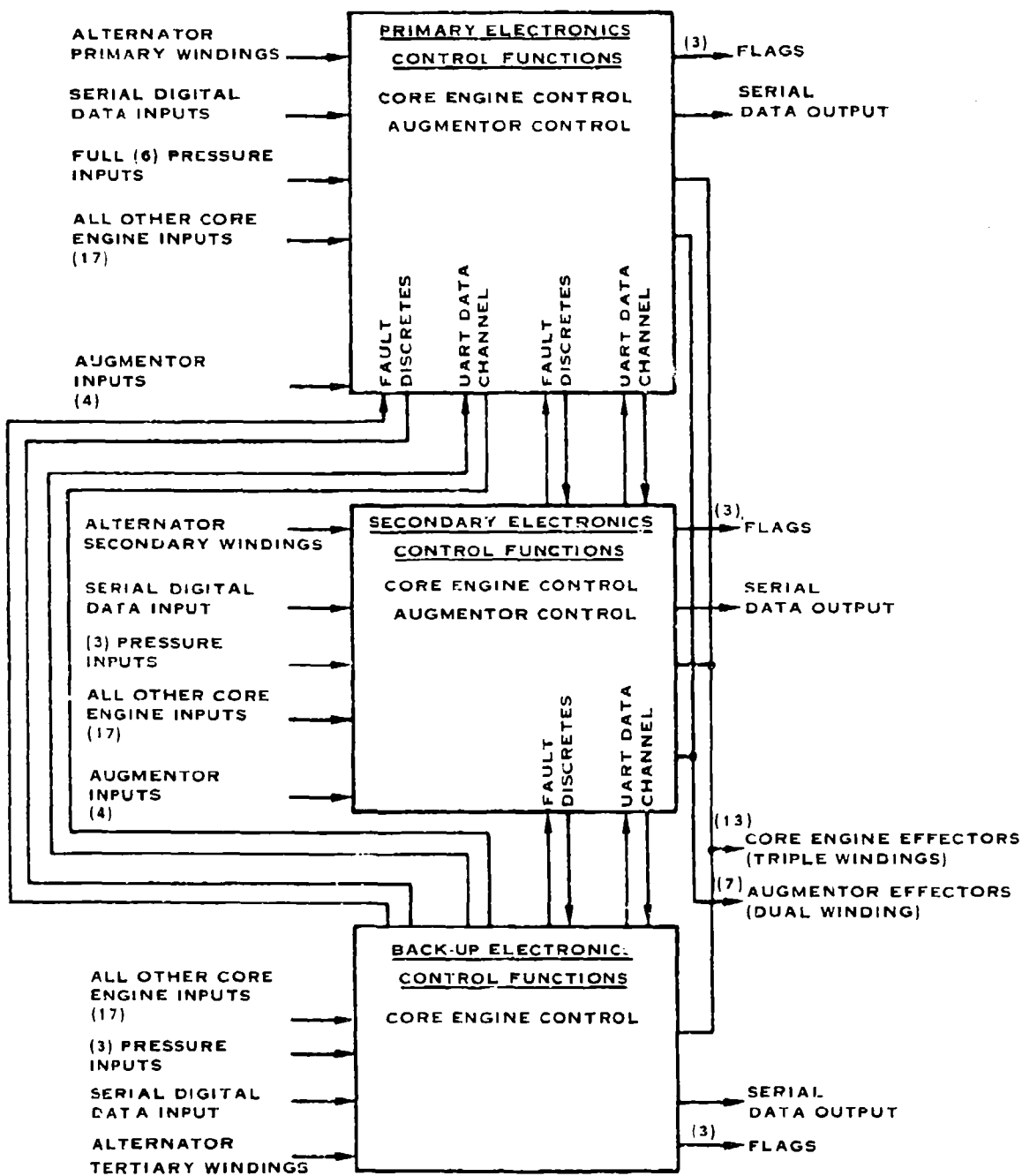


FIGURE 15 TRIPLE CHANNEL EEC SYSTEM

TABLE 4 TRIPLE CHANNEL EEC SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	NUMBER INCLUDED IN HARDWARE:		
			SECON-DARY	BACK-UP	PRI-MARY
For Augmentor Control	WFD1	Duct Augmentor Fuel Flow to Zone 1	1	0	1
	WFD2	Duct Augmentor Fuel Flow to Zone 2	1	0	1
	WFD3	Duct Augmentor Fuel Flow to Zone 3	1	0	1
For Core Engine Control	Serial Digital Data Stream Includes:	---	---	---	---
	Air Inlet Control	---	(1)	(1)	(1)
	Fit. Control	---	---	---	---
	ECM	---	---	---	---
	Mission Computer	---	---	---	---
	Discrete:	---	---	---	---
	R.F.	---	(4)	(3)	(4)
	W.O.W.	Rocket Fire	1	1	1
	Primary/Secondary Enable	Weight On Wheels	1	0	1
	Back-up Enable	Pilot Switch Enables/Disables Primary/Secondary EEC	0	1	0
For Augmentor Control	LOD	Pilot Switch Enables/Disables Back-up EEC	1	0	1
Output Drive: For Core Engine Control	Torque Motor:	---	(12)	(9)	(12)
	TPS	Turbo Pump Speed Control	1	1	1
	FIG V	Same as For Position	1	1	1
	CSVA	Same as For Position	1	1	1
	A4	Same as For Position	1	1	1
	A41	Same as For Position	1	1	1
	A4E	Same as For Position	1	1	1
	A4D	Same as For Position	1	1	1
	WFEP	Same as For Position	1	1	1
	WFES	Same as For Position	1	1	1

*Note: Single cockpit double pole primary/secondary enable switch.

TABLE 4 TRIPLE CHANNEL EEC SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	NUMBER INCLUDED IN HARDWARE:		
			SECON-DARY	BACK-UP	PRI-MARY
For Augmentor Control	WFD1	Same as For Position	1	0	1
	WFD2	Same as For Position	1	0	1
	WFD3	Same as For Position	1	0	1
For Core Engine Control	Solenoid:	---	(8)	(4)	(8)
	Start Bleed	---	1	1	1
	Staging	---	1	1	1
For Augmentor Control	Thrust Balance Bleed	---	1	1	1
	WFEP	Gas Gen. Primary Fuel Flow Shutoff Valve	1	1	1
	WFD1	Duct Zone 1 Fuel Flow Shutoff Valve	1	0	1
For Augmentor Control	WFD2	Duct Zone 2 Fuel Flow Shutoff Valve	1	0	1
	WFD3	Duct Zone 3 Fuel Flow Shutoff Valve	1	0	1
For Augmentor Control	Augmentor Ignitor Relay	---	1	0	1
	Lamps/Flags	---	(3)	(3)	(3)
	* Primary/Secondary On	Cockpit Lamp Indicates Primary/Secondary EEC Enabled	1	0	1
For Annunciation	Back-up On	Cockpit Lamp Indicates Back-up EEC Enabled	0	1	0
	Primary/Secondary Fault Flag (Latched)	LRU Flag Indicates Primary/Secondary EEC Fault	1	0	1
	Back-up Fault Flag (Latched)	LRU Flag Indicates Back-up EEC Fault	0	1	0
For Data Output	NOCS Fault Flag (Latched)	Non-Operational Control System Fault Flag Located on ASP	1	1	1
	Serial Digital Data Stream	---	(1)	(1)	(1)
	Same as For Input	---	(1)	(1)	(1)
For Digital Processing	CPU	Central Processor Unit Implements EEC Channel Program	1	1	1

*Note: Single cockpit lamp for Primary/Secondary On

TABLE 4 TRIPLE CHANNEL EEC SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	NUMBER INCLUDED IN SOFTWARE:		
			SECON-DARY	BACK-UP	PRI-MARY
Control Loop Computation: For Core Engine Control	---	---	---	---	---
	WFEP & WFES	Gas Generator Primary and Secondary Fuel Flows	Yes	Yes	Yes
	AJE	Core Stream Exhaust Nozzle Area	Yes	Yes	Yes
	A4	High Pressure Turbine Inlet Area	Yes	Yes	Yes
	A41	Low Pressure Turbine Inlet Area	Yes	Yes	Yes
	A4D	Duct Stream Exhaust Nozzle Area	Yes	Yes	Yes
	FIG V	Fan Inlet Guide Vane Position	Yes	Yes	Yes
	CSVA	Compressor Stator Vane Actuator Position	Yes	Yes	Yes
	Start Bleed Thrust Balance TPS	Starting Bleed On/Off Thrust Balance Bleed On/Off Turbo Pump Speed Control	Yes	Yes	Yes
	WFD1, WFD2, & WFD3	Duct Augmentor Fuel Flows	Yes	No	Yes
Synthesization: (See Figure 14 For Curves Used in Synthesizing Parameters)	NH	High Rotor Speed Synthesized From Curves 3, or 6	Yes	Yes	Yes
	TBT	Turbine Blade Temp Synthesized From Curve 3	Yes	Yes	Yes
	T22	Compressor Inlet Total Temp. Synthesized From Curve 1	Yes	Yes	Yes
	P12	Fan Inlet Total Pressure Synthesized From Curves 2, or 4	Yes	Yes	Yes
	P13	Compressor Discharge Total Pressure Synthesized From Curves 4, or 6	Yes	Yes	Yes

TABLE 4 TRIPLE CHANNEL EEC SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	NUMBER INCLUDED IN SOFTWARE:		
			SECON-DARY	BACK-UP	PRI-MARY
Synthesization (Continued)	PT13	Fan Discharge Total Pressure Synthesized From Curves 2, or 6	Yes	Yes	Yes
	$\Delta P3$	Compressor Discharge Differential Pressure Synthesized from Curve 5 Using Curves 7 and 8	Yes	Yes	Yes
FUNCTION	PARAMETER	IMPLEMENTED BY:	INCLUDED IN:		
			SECON-DARY	BACK-UP	PRI-MARY
Self Test	1: Input Range Limit Check	Software	Yes	Yes	Yes
	2: Parameter Correlation Check	Software	Yes	Yes	Yes
	3: Parameter Majority Logic Check	Software	Yes	Yes	Yes
	4: Read Only Memory Check	Software	Yes	Yes	Yes
	5: Computer Cycle Time Test	Hardware	Yes	Yes	Yes
	6: Output Wraparound Test	Hardware & Software	Yes	Yes	Yes
	7: Injected Input Test	Software	Yes	Yes	Yes
	8: Canned Output Computation	Software	Yes	Yes	Yes
	9: Loop Dynamic Check	Software	Yes	Yes	Yes
	10: Reference Signal Check	Hardware & Software	Yes	Yes	Yes
	11: Power Supply Test	Hardware	Yes	Yes	Yes
	12: Processor Instruction Test	Software	Yes	Yes	Yes
	13: Scratch Pad Memory Check	Software	Yes	Yes	Yes
	14: EOC Bit Not Detected	Software	Yes	Yes	Yes
	15: Hardware Parity & Code Verifier Checks	Hardware	Yes	Yes	Yes
	16: Clock Loss Detect Circuit	Hardware	Yes	Yes	Yes
	17: UART Sync Word Detected	Hardware	Yes	Yes	Yes

TABLE 4 TRIPLE CHANNEL EEC SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	INCLUDED IN:		
			SECON- DARY	BACK- UP	PRI- MARY
Cross Talk	UART/Dual Port RAM	Universal Asynchronous Receiver Transmitter Combined with Dual Port RAM Provides Data Link Between Primary/Secondary and Back-up CPU's for the Interchange of Input, Output, Parameter Synthesis, and Fault Data.	Yes	Yes	Yes
EEC Channel Switchover	Fault Discretes	Provides Hardwired Back-up for UART/Dual Port RAM. Used to select, on the basis of Fault Discretes received from all channels, the "Best Health" EEC. The other EEC's are automatically disabled.	1	0	1

2.4.3.2 Triple Channel EEC (Continued)

These arrangements provide for a fully functional, "stand alone" primary channel which is capable of controlling the VCE independently of the other two channels. The secondary channel alone is not fully functional in that it must receive pressure parameter data from the back-up channel in order to provide full VCE control at normal performance levels. The back-up channel is limited to core engine control only and must also receive pressure parameter data from the secondary to provide normal performance levels. The secondary channel, together with the back-up channel, and with no failures in either, provides fully functional, "stand alone" capability for VCE control.

During normal operation, with the pilot enable switch on "primary/secondary", the EEC supplies drive current to the effectors through its primary channel. However, all three channels are in operation: receiving input data through their respective interfaces; carrying out control mode, synthesis, and self-test logic; and exchanging data with each other through their UART data links. Majority logic checks are carried out for triple redundant parameters and, if passed, the average parameter value of the three inputs is used in control mode and synthesis computations. Failure of the majority logic check identifies the failed parameter. Recovery is then provided by simply rejecting the data from this parameter and averaging the input parameter on the basis of the data received from the two "good" input parameters. In this manner, the control avoids severe switch-over transients when failure detection and recovery occur.

With respect to dual redundant augmentor input parameters, parameter correlation checks are used and, if passed, the average parameter value of the two inputs is used in augmentor control mode computations. On failure of the parameter correlation check, the self-test routine resorts to "in-line" tests to isolate the failed parameter, and continues to compute augmentor control modes from data received from the remaining "good" input parameter.

With respect to output drive interfaces, only a wraparound test on the operating interface (primary for normal operation) can be carried out since the redundant channels are not supplying drive current to the effectors. If this test fails, output drive is switched from the failed primary output interface to the redundant secondary output interface while the remaining "good" primary output interfaces continue to drive their effectors. Some transient response may occur when this switch over takes place.

Failure of the primary power supply or CPU detected by hardware/software self-tests, or majority logic checks of the CPU control output data word for each effector results in automatic transfer of all effector drive currents from the primary to the secondary channel. Except for switch-over transients, normal operation is restored by this action and the

2.4.3.2 Triple Channel EEC (Continued)

faulted primary channel is effectively isolated from EEC operation. Failures of this type in the secondary or back-up channel are recorded by the software of the remaining good channels but otherwise they have no impact on VCE operation since these channels are not supplying effector drive currents. Similarly, failure of one of the UART data links is recorded by the software of all operating channels but does not, in itself, affect VCE control.

Examination of Figure 15 and Table 4 indicates that in the event of a second like input core engine failure, the two remaining inputs, through the parameter correlation check, can detect the fault and signal a fault alert to the pilot. By use of "in-line tests" the fault can be isolated in most cases and the data from the failed parameter eliminated from core engine control mode calculations, thereby restoring normal operation. If necessary, as in the case of a second like failure in the PLA inputs, the pilot, once alerted, can check his instrument panel and manually switch over to the back-up control to ensure safe mission abort.

In the case of a second channel failure, a pilot fault alert is signaled. If the failures are in the secondary and back-up channels, the pilot can abort the mission without loss of performance in the affected engine. If the primary channel is already down due to a first channel failure, and a failure has occurred in the back-up channel, the pilot can safely abort the mission with minor performance degradation, but with all engine functions, including augmentation, still available. The minor degradation in performance is due to the substitution of less accurate parameter synthesis data for parameter sensor data in the control mode calculations. On the other hand, failure of the secondary channel following the loss of the primary channel, automatically switches effector control over to the remaining back-up channel. This channel provides satisfactory back-up control by restoring, with minor performance degradation, core engine operation, but without augmentor capability. The loss of all three UART data links requires a pilot alert, even though they themselves have no effect on engine performance, since the ability of the EEC self-test routines to detect and recover from the next failure, if it should occur, is severely limited (Section 2.4.2).

From the above evaluation of possible failure modes in the triple channel EEC, it is clear that the first failure in any function does not affect engine performance nor jeopardize engine safety. Its repair, using the ground rules in Section 2.1.3, can therefore be deferred; as a result it need not be flagged for either pilot or maintenance alert. These results are summarized in Table 5 on a functional basis.

TABLE 5
FIRST FAILURE FLAG ACTION TRIPLE CHANNEL SYSTEM

FUNCTION IDENTIFICATION		LOSS OF COMPLETE FUNCTION	NO. OF ELEMENTS	FIRST FAILURE PILOT FLAG	MAINT. FLAG
I. POWER		SHUTDOWN	3	NO	NO
II. SPEEDS:	TPS	MINOR	3	NO	NO
	NH	MAJOR	3 + S	NO	NO
	NL	MAJOR	3	NO	NO
III. TEMPERATURES:	TBT AVG	MINOR	2 + (S)*	NO	NO
	TT2	MAJOR	3	NO	NO
	TBT PEAK	MINOR	2 + (S)*	NO	NO
IV. A/D CONVERTER		MAJOR	3	NO	NO
V. PRESSURES:	PT2	MAJOR	2 + S	NO	NO
	PT3	MAJOR	2 + S	NO	NO
	PT5	MINOR	2	NO	NO
	Δ P13	MINOR	2	NO	NO
	PT13	MINOR	2 + S	NO	NO
	Δ P3	MAJOR	2 + S	NO	NO
VI. RESOLVERS:	PLA	SHUTDOWN	3	NO	NO
	FIG V	MAJOR	3	NO	NO
	CSVA	SHUTDOWN	3	NO	NO
	A4	MAJOR	3	NO	NO
	A41	MAJOR	3	NO	NO
	Aje	MAJOR	3	NO	NO
	Ajd	MINOR	2	NO	NO
	Wfep	SHUTDOWN	3	NO	NO
	Wfes	SHUTDOWN	3	NO	NO
	Wfd1	MINOR	2	NO	NO
	Wfd2	MINOR	2	NO	NO
	Wfd3	MINOR	2	NO	NO
VII. R/D CONVERTER		SHUTDOWN	3	NO	NO
VIII. SIGNALS:	WOW	MINOR	3	NO	NO
	RF	MINOR	3	NO	NO
	LOD	MINOR	2	NO	NO
	ECU ENABLE	MAJOR	3	NO	YES
	AIC DATA	MINOR	3	NO	NO

TABLE 5 (Continued)

FUNCTION IDENTIFICATION		LOSS OF COMPLETE FUNCTION	NO. OF ELEMENTS	FIRST FAILURE	
				PILOT FLAG	MAINT. FLAG
IX.	PILOT FAULT FLAG SWITCH	MINOR	1	YES	YES
X.	CPU	MAJOR	3	NO	NO
XI.	CROSSTALK (CPU'S)	MINOR	3	NO	NO
XII.	TORQUE MOTORS: TPS	MINOR	3	NO	NO
	FIG V	MAJOR	3	NO	NO
	CSVA	SHUTDOWN	3	NO	NO
	A4	MAJOR	3	NO	NO
	A41	MAJOR	3	NO	NO
	Aje	MAJOR	3	NO	NO
	Ajd	MINOR	2	NO	NO
	Wfep	SHUTDOWN	3	NO	NO
	Wfes	SHUTDOWN	3	NO	NO
	Wfd1	MINOR	2	NO	NO
	Wfd2	MINOR	2	NO	NO
	Wfd3	MINOR	2	NO	NO
XIII.	SOLENOIDS: START BLEED	MAJOR	3	NO	NO
	STAGING	MAJOR	3	NO	NO
	THR. BAL.	SHUTDOWN	3	NO	NO
	Wfep S.O.V.	SHUTDOWN	3	NO	NO
	Wfd1	MINOR	2	NO	NO
	Wfd2	MINOR	2	NO	NO
	Wfd3	MINOR	2	NO	NO
XIV.	AUG. IGN. RELAY	MINOR	2	NO	NO
XV.	RESOLVER EXCITATION: A	SHUTDOWN	3	NO	NO
	B	SHUTDOWN	3	NO	NO

S - FUNCTION HAS SYNTHESIS AVAILABLE

(S)* - FUNCTION HAS SYNTHESIS AVAILABLE FOR BIT ONLY

2.4.3.3 Dual Channel EEC

An alternate approach to extending maintenance MTBF by deferred maintenance action is to apply selective redundancies to a dual channel EEC configuration illustrated in Figure 16. The system definition for this configuration is given in Table 6. As can be seen from this table, selective redundancy is applied in each channel to provide triple-redundant electrical input/output interfaces for core engine control.

Pressure parameters are measured by a single transducer with dual electronic output signals, one of which is supplied to each channel. Each channel is provided with its own alternator winding and CPU. A single UART data link provides cross-channel digital data transmission. Both channels are identically programmed. Each channel is therefore fully functional, and can provide full VCE control independent of the other channel.

During normal operation, the pilot can select either channel, through the primary or secondary enable switches, to supply effector drive currents. Self-test and fault recovery routines are identical, where applicable, to those described for the triple channel EEC. Pressure transducer faults can be detected by applying majority logic checks using the dual signal inputs and the pressure parameter synthesis provided in each channel. Fault discrete logic is provided in the primary channel as a back-up to the UART data link, and operates the same as in the triple channel EEC.

The dual channel configuration significantly reduces EEC cost, size, weight, and power dissipation when compared to the triple channel approach. It can therefore provide a design more compatible with the practical limitations on these system parameters. These improvements, however, are obtained at the cost of reduced maintenance MTBF because first failures in the power supply, CPU UART data link, and pressure transducers must now be flagged for maintenance action. Table 7 summarizes first-failure pilot and maintenance flagging requirements on a per function basis. Mission reliability is not significantly affected because triple redundancy is still implemented for core engine control.

In designing a dual channel EEC it is desirable to distribute selective redundancies as evenly as possible between the two EEC channels so as to equalize channel power supply requirements. Additional care is required in circuit partitioning in order to eliminate common-mode failure effects on circuits dedicated to selective redundancy.

2.4.4 Self-Test (BIT)

Automatic reversion to back-up control paths requires the ability to determine that a failure has occurred in a primary path. Multichannel EEC configurations provide self-test techniques which detect failures and switch the control unit to an alternate control path allowing fail-operational

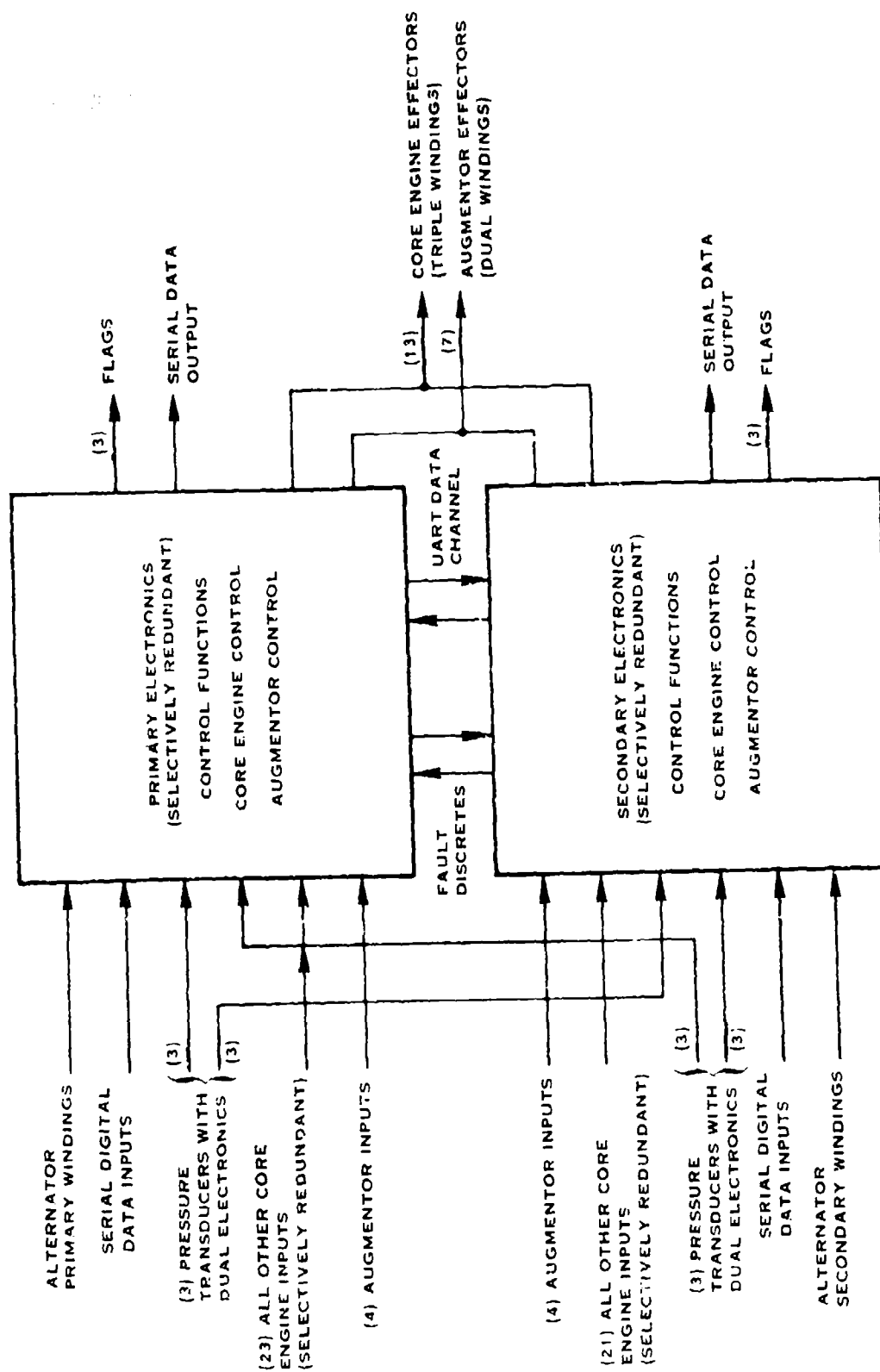


FIGURE 16 DUAL CHANNEL EEC SYSTEM WITH SELECTIVE REDUNDANCIES

TABLE 6 DUAL CHANNEL SYSTEM DEFINITION

FUNCTION	PARAMETER	DEFINITION	NUMBER INCLUDE IN:	
			PRIMARY	SECONDARY
Power Supply	Alternator	Supplied From Dedicated Alternator Windings	1	1
Inlet Signal Processing: For Core Engine Control { Single Transducer With Dual Electronics }	Engine Speed:	---	(4)	(3)
	TPS	Turbo Pump Speed	1	1
	NH	High Rotor Speed	1	1
	NL	Low Rotor Speed	2	1
	Temperature:	---	(2)	(3)
	TT2	Fan Inlet Total Temp.	1	2
	TBT	Turbine Blade Temp.	1	1
	T22	Compressor Inlet Total Temp.	0	0
	Pressure:	---	(6)	(6)
	PT2	Fan Inlet Total Pressure	1	1
	PT3	Compressor Discharge Total Pressure	1	1
	PT13	Fan Discharge Differential Pressure	1	1
	P3	Low Pressure Turbine Discharge Total Pressure	1	1
	PT5	Fan Discharge Total Pressure	1	1
	PT13	Compressor Discharge Differential Pressure	1	1
	P3	---	(17)	(15)
	Position:	Power Lever Angle	2	1
	PLA	Fan Inlet Guide Vane	2	1
	FIG V	Compressor Stator Vane Actuator	2	1
	CSVA	High Pressure Turbine Inlet Area	1	2
	A4	Low Pressure Turbine Inlet Area	1	2
	A41	Core Stream Exhaust Nozzle Area	1	2
	AJC	Duct Stream Exhaust Nozzle Area	1	1
	AJD	Gas Generator Primary Fuel Flow	2	1
	WFEP	G.G. Secondary Fuel Flow	2	1
	WFES			

TABLE 6 DUAL CHANNEL SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	NUMBER INCLUDED IN: PRIMARY	SECONDARY
For Augmentor Control	WFD1	Duct Augmentor Fuel Flow to Zone 1	1	1
	WFD2	Duct Augmentor Fuel Flow to Zone 2	1	1
	WFD3	Duct Augmentor Fuel Flow to Zone 3	1	1
For Core Engine Control	Serial Digital Data Stream	---	(1)	(1)
	Includes:	---	---	---
	Air Inlet Control	---	---	---
	Flt. Control	---	---	---
	ECM	---	---	---
	Mission Computer	---	---	---
	Discrete:	---	---	---
	R.F.	---	(4)	(4)
	W.O.W.	Rocket Fire	1	1
	Primary Enable	Weight On Wheels	1	0
For Augmentor Control	Secondary Enable	Pilot Switch Enables/Disables Primary EEC	0	1
	L00	Pilot Switch Enables/Disables Secondary EEC	1	1
		Augmentor Light Off Detector		
Output Drive: For Core Engine Control	Torque Motor:	---	(16)	(15)
	TPS	Turbo Pump Speed Control	1	1
	FIG V	Same as For Position	2	1
	CSVA	Same as For Position	2	1
	A4	Same as For Position	1	2
	A41	Same as For Position	1	2
	A4E	Same as For Position	1	2
	A4D	Same as For Position	1	1
	WFEP	Same as For Position	1	1
	WFES	Same as For Position	2	1

TABLE 6 DUAL CHANNEL SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	NUMBER INCLUDED IN: PRIMARY SECONDARY	NUMBER INCLUDED IN: PRIMARY SECONDARY
For Augmentor Control	WFD1	Same as For Position	1	1
	WFD2	Same as For Position	1	1
	WFD3	Same as For Position	1	1
For Core Engine Control	Solenoid:	---	(10)	(10)
	Start Bleed	---	2	2
	Staging	---	1	2
For Augmentor Control	Thrust Balance Bleed	---	1	1
	WFEP	Gas Gen. Primary Fuel Flow Shutoff Valve	2	1
	WFD1	Duct Zone 1 Fuel Flow Shutoff Valve	1	1
For Augmentor Control	WFD2	Duct Zone 2 Fuel Flow Shutoff Valve	1	1
	WFD3	Duct Zone 3 Fuel Flow Shutoff Valve	1	1
For Augmentor Control	Augmentor Ignitor Relay	---	1	1
	Lamps/Flags:	---	(3)	(3)
	Primary On	Cockpit Lamp Indicates Primary EEC Enabled	1	0
For Annunciation	Secondary On	Cockpit Lamp Indicates Secondary EEC Enabled	0	1
	Primary Fault Flag (Latched)	LRU Flag Indicates Primary EEC Fault	1	0
	Secondary Fault Flag (Latched)	LRU Flag Indicates Secondary EEC Fault	0	1
For Data Output	NOCS Fault Flag (Latched)	Non-Operational Control System Fault Flag Located on ASP	1	1
	Serial Digital Data Stream:	---	(1)	(1)
	Same as For Input	---	(1)	(1)

TABLE 6 DUAL CHANNEL SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	INCLUDED IN:	
			PRIMARY	SECONDARY
Digital Data Processing	CPU	Central Processor Unit Implements ECC Channel Program	1	1
Control Loop Computation: For Core Engine Control	---	---	---	---
	WFEP & WFES	Gas Generator Primary and Secondary Fuel Flows	Yes	Yes
	AJE	Core Stream Exhaust Nozzle Area	Yes	Yes
	A4	High Pressure Turbine Inlet Area	Yes	Yes
	A41	Low Pressure Turbine Inlet Area	Yes	Yes
	AJ0	Duct Stream Exhaust Nozzle Area	Yes	Yes
	FIG V	Fan Inlet Guide Vane Position	Yes	Yes
	CSVA	Compressor Stator Vane Actuator Position	Yes	Yes
	Start Bleed Thrust Balance TPS	Starting Bleed On/Off Thrust Balance Bleed On/Off Turbo Pump Speed Control Duct Augmentor Fuel Flows	Yes	Yes
	WFD1, WFD2, & WFD3		Yes	Yes
For Augmentor Control	NH	High Rotor Speed Synthesized From Curves 3, or 6	Yes	Yes
	TB1	Turbine Blade Temp. Synthesized From Curve 3	Yes	Yes
	T22	Compressor Inlet Total Temp. Synthesized From Curve 1	Yes	Yes
	PT2	Fan Inlet total Pressure Synthesized from Curves 2, or 4	Yes	Yes
Synthesization: (See Figure 14 for Curves Used in Synthesizing parameters)				

TABLE 6 DUAL CHANNEL SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	INCLUDED IN:	
			PRIMARY	SECONDARY
Synthesization (Continued)	PT3	Compressor Discharge Total Pressure Synthesized From Curves 4, or 5	Yes	Yes
	PT13	Fan Discharge Total Pressure Synthesized From Curves 2, or 6	Yes	Yes
	P3	Compressor Discharge Differential Pressure Synthesized From Curve 5 Using Curves 7 & 8	Yes	Yes
FUNCTION	PARAMETER	IMPLEMENTED BY:	INCLUDED IN:	
			PRIMARY	SECONDARY
Self Test	1: Input Range Limit Check	IN-FLY TEST	Yes	Yes
	2: Parameter Correlation Check	PRE-FLY TEST	Yes	Yes
	3: Parameter Majority Logic Check		Yes	Yes
	4: Read Only Memory Check		Yes	Yes
	5: Computer Cycle Time Test		Yes	Yes
	6: Output Wraparound Test		Yes	Yes
	7: Injected Input Test		Yes	Yes
	8: Canned Output Computation		Yes	Yes
	9: Loop Dynamic Check		Yes	Yes
	10: Reference Signal Check		Yes	Yes
	11: Power Supply Test		Yes	Yes
	12: Processor Instruction Test		Yes	Yes
	13: Scratch Pad Memory Check		Yes	Yes
	14: EOC Bit Not Detected		Yes	Yes
	15: Hardware Parity & Core Verifier Checks		Yes	Yes
	16: Clock Loss Detect Circuit		Yes	Yes
	17: UART Sync Word Detected		Yes	Yes

TABLE 6 DUAL CHANNEL SYSTEM DEFINITION (Continued)

FUNCTION	PARAMETER	DEFINITION	INCLUDED IN: PRIMARY	SECONDARY
Cross Talk	UART/Dual Port RAM	Universal Asynchronous Receiver Transmitter Combined With Dual Port RAM Provides Data Link Between Primary And Secondary CPU's For The Interchange of Input, Output, Parameter Synthesis, And Fault Data	Yes	Yes
EEC Channel Switchover	Fault Status	Provides Hardware Backup For UART/Dual Port RAM. Hardware Logic Supplied With Fault Discovers From Each EEC Determines Each Channel's Operating Status. Automatically Switches Control From Failed, Inoperative, EEC to Operative EEC.		

TABLE 7 FIRST FAILURE FLAG ACTION: DUAL CHANNEL SYSTEM

<u>Function Identification</u>	<u>Loss Of Complete Function</u>	<u>No. Of Elements</u>	<u>First Failure</u>	
			<u>Pilot Flag</u>	<u>Maint. Flag</u>
Power	Shutdown	2	Yes	Yes
Speeds:				
TPS	Minor	2	No	No
NH	Major	2*	No	No
NL	Major	3	No	No
Temperatures:				
TBT Avg	Minor	2*	No	No
TT2	Major	3	No	No
TBT Peak	Minor	2*	No	No
A/D Converter	Major	3	No	No
Pressures				
PT2 Transducer	Major	1*	Yes	Yes
PT3 Transducer	Major	1*	Yes	Yes
PT5 Transducer	Minor	1	Yes	Yes
ΔP13 Transducer	Minor	1	Yes	Yes
PT13 Transducer	Minor	1	Yes	Yes
ΔP3 Transducer	Major	1*	Yes	Yes
PT2 Electronics	Major	2*	No	No
PT3 Electronics	Major	2*	"	No
PT5 Electronics	Minor	2		No
ΔP13 Electronics	Minor	2		No
PT13 Electronics	Minor	2*	No	No
ΔP3 Electronics	Major	2*	No	No
Resolvers				
PL4	Shutdown	3	No	No
Fig V	Major	3	No	No
CSVA	Shutdown	3	No	No
A4	Major	3	No	No
A41	Major	3	No	No
Aje	Major	3	No	No
Ajd	Minor	2	No	No
Wfep	Shutdown	3	No	No
Wfes	Shutdown	3	No	No

TABLE 7 FIRST FAILURE FLAG ACTION: DUAL CHANNEL SYSTEM (Continued)

<u>Function Identification</u>	<u>Loss Of Complete Function</u>	<u>No. Of Elements</u>	<u>First Failure</u>	
			<u>Pilot Flag</u>	<u>Maint. Flag</u>
Resolvers (Continued)				
Wfd1	Minor	2	No	No
Wfd2	Minor	2	No	No
Wfd3	Minor	2	No	No
R/D Converter	Shutdown	3	No	No
Signals:				
WOW	Minor	2	No	No
RF	Minor	2	No	No
LOD	Minor	2	No	No
ECU Enable	Major	2	No	Yes
AIC Data	Minor	2	No	No
Fault Flag Switch	Minor	1	Yes	Yes
CPU	Shutdown	2	Yes	Yes
Crosstalk (CPU's)	Minor	2	Yes	Yes
Torque Motors:				
TPS	Minor	2	No	No
FLCV	Major	3	No	No
CSVA	Shutdown	3	No	No
A4	Major	3	No	No
A41	Major	3	No	No
Aje	Major	3	No	No
Ajd	Minor	2	No	No
Wfep	Shutdown	3	No	No
Wfes	Shutdown	3	No	No
Wfd1	Minor	2	No	No
Wfd2	Minor	2	No	No
Wfd3	Minor	2	No	No

TABLE 7 FIRST FAILURE FLAG ACTION: DUAL CHANNEL SYSTEM (Continued)

<u>Function Identification</u>	<u>Loss Of Complete Function</u>	<u>No. Of Elements</u>	<u>First Failure</u>	
			<u>Pilot Flag</u>	<u>Maint. Flag</u>
Solenoids:				
Start Bleed	Major	3	No	No
Staging	Major	3	No	No
Thr. Bal.	Shutdown	3	No	No
Wfep S.O.V.	Shutdown	3	No	No
Wfd1	Minor	2	No	No
Wfd2	Minor	2	No	No
Wfd3	Minor	2	No	No
Aug. Ign. Relay	Minor	2	No	No
Resolver Excit. A.	Shutdown	2	Yes	Yes
B.	Shutdown	2	Yes	Yes

* Parameter Synthesis Available

"Loss of Complete Function", indicates the impact of the function loss on engine performance. There are 14 functions where complete failure would cause the engine to shutdown. Also, there are 21 functions where control failures would have a major impact on engine performance. The loss of the remaining functions are designated as having a minor impact on engine performance.

2.4.4 Self-Test (BIT) (Continued)

performance. A summary of the tests performed within the EEC unit is shown in Table 3. As indicated in this table, some of the tests are performed only during pre-flight ground check while the remainder are performed in-flight as well. The pre-flight ground check is initiated by a command from the mission computer, with ground check continuing until signaled by the mission computer to enter the flight mode of control. The in-flight tests are performed on a continuous basis, independent of any externally generated command signals. A detailed description of each test follows.

2.4.4.1 Input Range Limit Test

The range limit test is a software BIT for detecting a failed computer input signal caused by a failure in the sensor, interconnecting cable, or input interface circuit. The range limit test is sensitive only to failures (open or short) which produce hardover signals. The range test program compares each input signal level with its normal operating range limits. Failure is indicated when the signal level exceeds its maximum or minimum limits for a given number of consecutive program cycles. The range limit test program also generates a digital failure status word indicating an input signal failure, however, it cannot identify the LRU in which the failure occurred, and can only indicate that the failure occurred somewhere in the system. The control system is switched to a redundant input signal.

2.4.4.2 Parameter Correlation Check

The parameter correlation check compares redundant parameter data words to determine if their difference in value falls within outside accuracy bounds. "Failure" in one of the two parameters is indicated when the accuracy bounds are exceeded for a given number of consecutive program cycles. However, the failed parameter channel is not isolated by this test alone. The redundant parameter data may be generated by hardware or by software synthesis.

2.4.4.3 Parameter Majority Logic Check

This is a comparison of triple redundant parameter data words to determine if their differences in value fall within outside accuracy bounds. Failure in one of the three parameters is indicated by excessive error between its value and that of the other two good parameters for a given number of consecutive program cycles. The error between the values for the two good parameter channels is, of course, within parameter accuracy limits. The failed parameter channel is thereby identified by this test which generates a digital failure status word indicating the failed parameter channel; however, it cannot identify the LRU in which the

2.4.4.3 Parameter Majority Logic Check (Continued)

failure occurred, and can only indicate the failure occurred somewhere in the system. The redundant parameter data may be generated either by hardware or by software synthesis. When failure is detected, the control is switched to a redundant input channel.

2.4.4.4 Read Only Memory (ROM) Check

The memory sum test is a software BIT for detecting a failed Read Only Memory (ROM). The test program sums each ROM location, and the sum total must equal a preset value for validity. An incorrect sum causes the program to recycle on the test thereby triggering a cycle time test failure. The memory sum test program also generates a digital failure status word indicating a ROM failure occurring in the ECU. The control system is switched to the back-up control.

2.4.4.5 Computer Cycle Time Test

Computer cycle time is a hardware BIT for detecting a hung program. This test requires the completion of each program cycle within a maximum allowable time. A computer power on reset (POR) results when program cycle time exceeds the timing limit. The POR signal reinitializes the program once and also generates a digital failure status word indicating a hung program failure occurring in the ECU. The control system is switched to the back-up control when the test is failed on the next cycle.

2.4.4.6 Output Wraparound Test

Torque motor/solenoid outputs are electrically fed back as inputs to the processor for a check by the software to detect output D/A and torque motor/solenoid drive circuit failures. Resultant action would be to indicate an ECU failure and to switch control to a redundant output channel.

2.4.4.7 Injected Input Test

This is a preflight control test which is carried out on the ECU after "engine start" but prior to "takeoff". The test is carried out under the control of the flight computer which exercises all of the ECU functions. Failure of the ECU to properly carry out each function is detected by the flight computer. Resultant action would be to indicate a LRU failure which must be repaired by unscheduled "on-line" service before the mission is dispatched.

2.4.4.8 Canned Output Computation

This is also a preflight control test except that the flight computer exercises the actuator loops. Failure of an actuator loop to respond within specifications to programmed commands is detected by the flight computer. Resultant action would be to indicate a system failure which must be repaired by unscheduled "on line" service before the mission is dispatched.

2.4.4.9 Loop Dynamic Check

The control loop error (command value minus measured value) is compared against programmed limits. Failure is indicated when the measured error exceeds the programmed error for a given number of consecutive program cycles. The loop dynamic check generates a digital failure status word indicating a failure in the control loop, but cannot alone identify in which LRU the failure occurred. When combined with the parameter correlation check the two tests can isolate the failure to either the primary or backup ECU, or to the actuator.

2.4.4.10 Reference Signal Check

Input signals are supplied to multiplexer channels at preset levels, converted into digital data words, and transmitted to the CPU. In the CPU they are compared to reference levels stored in the memory. Failure is indicated when the reference signal data word exceeds the stored references for a given number of program cycles. The reference signal test program generates a digital failure status word indicating an input channel failure occurring in the ECU, and switches control to a redundant input channel.

2.4.4.11 Power Supply Test

The purpose of this test is to monitor the supplies for in-tolerance operation. The power supply test is a hardware BIT in which positive and negative voltages are continuously compared with reference voltage levels. A failure signal is triggered when any supply voltage exceeds its preset tolerances. A failure signal generates a digital failure status word indicating power supply failure occurring in the ECU. The control system is automatically switched to the back-up control.

2.4.4.12 Processor Instruction Test

The processor instruction test is a software BIT for detecting a failed processor hardware instruction. The instruction test program operates on each instruction with a preset data word. It compares the data word at the end of the test with the preset data word. An incorrect answer causes the program to recycle on test, thereby triggering a cycle time test failure. The instruction test program also generates a digital failure status word indicating an instruction failure occurring in the ECU. The control system is switched to the back-up control.

2.4.4.13 Read Write (Scratch Pad) Memory Check

The scratch pad test is a software BIT for detecting a failed read/write memory. The scratch pad test program operates on each read/write memory location with a preset data word. The data word is entered into the read/write memory location and then read out. The output data word is then compared with the preset data word. An incorrect answer causes the program to recycle on test triggering a cycle time test failure. The scratch pad test program also generates a digital failure status word indicating a read/write memory failure occurring in the ECU. The control system is switched to the back-up control.

2.4.4.14 End of Conversion (EOC) Bit Not detected

Failure of any digital converter to provide the processor with an EOC bit after a preset time period following the start of data conversion indicates a hang up and therefore failed digital converter. The (EOC) test program generates a digital failure status word indicating which converter failed in the ECU, and switching the control to a redundant converter.

2.4.4.15 Hardware Parity and Code Verifier Checks

This is an automatic hardware test for detecting failure in the Serial Digital Data Transmission Link.

2.4.4.16 Clock Loss Detect Circuit

This is a hardware test which automatically detects failure in either of the redundant clock oscillators provided for the processor by comparing their cycle time period with the timing period of a one shot multivibrator. Failure of either oscillator generates a digital failure status word indicating a clock failure occurring in the ECU. The control switch is to (or retains) the "good" clock for processor timing.

2.4.4.17 UART Sync Word Detected

This is an automatic hardware test of the UART cross talk channel providing communication between the primary and back-up CPU. If the UART sync word is not detected by the receiving channel within a preset maximum time from the start of data transmission, a digital failure status word is generated indicating failure of the UART channel in the ECU and flagging a maintenance alert.

SECTION III

COMPONENT AND CIRCUIT IMPLEMENTATION CONSIDERATIONS

3.1 Methodology of Circuit and Component Technology Study

The methodology of optimizing circuit design and component mix is described in this section. The methodology of this study is to examine each function in the system and identify alternate circuit implementations to achieve the same functional capability. In some instances, this entails complete redesign or direct substitution of different component technologies. To avoid a proliferation of concepts not pertinent, the following constraints should be placed upon the design:

- 1) Avoid use of custom devices.
- 2) Provide alternate design wherever CMOS is recommended.
- 3) Avoid use of devices not yet in production.
- 4) Avoid use of single source devices.
- 5) Avoid use of nonstandard, large device packages.

Once various circuit implementations are generated, a method to evaluate circuits for reliability maximization is developed. MIL-HDBK-217B is not considered as a source to perform this comparison.

3.2 Reliability Evaluation Factors

The component technology mix reliability evaluation must be approached from a combined quantitative and qualitative standpoint. The evaluation is to be performed by assessing the impact of the various component technologies at two levels. The two levels are: (1) part level, and (2) functional fabrication level.

3.2.1 Part Level Evaluation

The part level contains those factors which are related directly to the component part technology. These factors are:

- 1) Production volume and years in the market place.
- 2) Part technology and part types are identified as an industry standard.
- 3) Part technology has been proven in space or military applications.
- 4) Part type has the ability to undergo accelerated stress testing.
- 5) Component functional test characteristics.
- 6) Inherent failure characteristics.

Although each of these six categories are broad in scope, they are narrow enough when combined to adequately compare the very diverse component technologies and part types.

3.2.1 Continued

Factor 1 - Production Volume and Years in the Market Place

The purpose of this evaluation factor is to place emphasis on a part type which is currently being produced in high volume. Consideration is also given to whether the high volume is used for commercial products, military products, or a combination of both.

The justification for this emphasis on high volume is to reap the reliability and quality benefits inherent in large scale production processes. Some of the benefits are:

- 1) A large number of users have found the reliability of the component to be satisfactory.
- 2) A high yield implies that production problems have been solved.
- 3) The quality of the product is relatively high through experience and training of production personnel.

The factor used to adjudge high volume is the number of years that the component has been produced.

The various component technologies are measured against the following scale of values:

<u>Years in Manufacturing</u>	<u>Weight</u>
Over 5	50
3 - 5	35
1 - 2	30
0 - 1	10
Research (Pilot)	0

The components' years in production were determined by literature searches of industry publications, surveys, technical reports, and technical periodicals devoted to component technology and manufacture.

Factor 2 - Industry Standard

The second factor used to evaluate a component technology and a part type is its acceptance as an industry standard. The technologies are evaluated according to the following scale:

<u>Industry Standard</u>	<u>Weight</u>
Currently	40
Likely in 1 - 3 Yrs	30
Likely in 4 - 5 Yrs	10
Not Likely	0

3.2.1 Continued

The scale ranges from those technologies which are presently considered industry standards, such as the military or JEDEC, to those technologies which are not likely to become industry standards at all.

Factor 3 - Proven In Space or Military Applications

This factor is used to evaluate the part types on the basis that they have or have not proven to be satisfactory for space or military applications. The factor is dichotomized as follows:

	<u>Weight</u>
Proven	30
Not Proven	0

Inclusion of this factor is predicated on the belief that a part type and/or technology which has proven to be of value in a space or military application where the qualification reliability and quality requirements are high, is inherently more reliable than another part which has not proven itself.

Factor 4 - Accelerated Stress Testing

The accelerated stress testing factor is used to evaluate a component technology from the standpoint of developing adequate screening criteria. This factor is evaluated according to the following scale. The scale ranges from

<u>Criteria</u>	<u>Weight</u>
Accelerated stress testing (AST) performed	40
Can undergo AST at 200°C	35
Can undergo AST at 150°C	30
Can undergo AST at 125°C	15
Cannot be AST	0

those technologies which have undergone accelerated stress testing and for which a body of literature exists to those technologies which cannot be evaluated by accelerated stress testing. To produce an ultra-reliable engine control system, this ability to develop adequate component screening tests is essential to enhance reliability. If screening criteria for a component technology cannot be developed, other less effective screening methods would have to be formulated and the results verified.

3.2.1 Continued

Factor 5 - Functional Testability

This factor evaluates the current state-of-the-art with regard to the test methods and test equipment associated with a particular component type. The range of this measure is shown in the following table.

<u>Testability</u>	<u>Weight</u>
Readily available	30
Custom Program	20
Custom Program & Equipment	5

The best functional test capability is considered to be that component technology for which the test methods and test equipment are readily available. The least weight is given to those technologies which require custom test programs and special test equipment for component evaluations.

Factor 6 - Failure Rate of Technology

Inherent failure rate of a given semiconductor technology is the average failure rate achieved following thorough screening of devices made with a mature well-controlled process. Inherent failure rate varies with operating time and is different from technology to technology. The purpose of this factor is to rate the inherent component failure rate for the various technologies considered. The weights given in the following table for the ranges of failures in time (FIT x 10⁻⁹ hrs) are used as the figure of merit. The better figure of merit for a technology as presented

<u>FIT Range</u>	<u>Weight</u>
0 - 25	50
26 - 50	25
51 - 100	15
101 - 300	5
> 300	0

is for the lower values of FIT's.

Inherent failure rate data shown is taken from devices in commercial applications and is based on millions of device hours of operation. The various classes of devices considered in this study are given in the left column of Table 8. The second column gives the inherent failure rate (λ_0) for the device class. The third column contains the growth factor (α) for the technology.

Because the technologies are in different stages of maturity, it became necessary to "normalize" the inherent failure rates. The true normalization of the failure rates is the failure rates achieved at maturity of the technology. Toward this end, the Duane (7) growth curve method is applied in the following way.

TABLE 8

TECHNOLOGY INHERENT FAILURE RATES--
(FAILURES IN TIME)

DEVICE TECHNOLOGY CLASSES	λ_0 (FITS)	∞	λ (FITS)
BIPOLAR LINEAR SSI	4×10^4	0.7	63.40
BIPOLAR LINEAR MSI	4×10^4	0.7	63.40
BIPOLAR TTL (SSI AND MSI)	2×10^4	0.8	12.62
LS TTL (SSI)	1×10^5	0.8	63.10
LS TTL (MSI)	2×10^5	0.8	126.19
LS MEMORY (LSI)	1×10^5	0.8	63.10
NMOS METAL GATE (MSI)	1×10^5	0.8	63.10
NMOS METAL GATE (LSI)	1×10^5	0.8	63.10
PMOS METAL GATE (MSI)	1×10^5	0.7	158.49
PMOS METAL GATE (LSI)	$2 - 4 \times 10^5$	0.7	316.93 633.96
NMOS SILICON GATE (MSI)	1×10^5	0.8	63.10
NMOS SILICON GATE (LSI)	1×10^5	0.8	63.10 (ESTIMATE - LIMITED DATA)
CMOS METAL GATE (SSI)	2×10^4	0.7	31.70
CMOS METAL GATE (MSI)	2×10^4	0.7	31.70
CMOS (LSI)	---	---	100 (ESTIMATE)
t^2_L (MSI, LSI)	2×10^4	0.8	12.62
DISCRETE SMALL SIGNAL TRANSISTOR	2×10^4	0.8	12.62
DISCRETE SMALL SIGNAL DIODE	2×10^4	0.8	12.62

$$\lambda = \lambda_0 t^{-\infty}$$

WHERE $t = 10,000$ HOURS
 $\lambda_0 = \text{FIT @ 1 HOUR}$
 $\infty = \text{GROWTH FACTOR}$
 $\lambda = \text{MATURE FIT}$

3.2.1 Continued

The Duane postulate is stated as

$$\lambda_M = \lambda_0 t^{-\alpha}$$

where

λ_M = mature failure rate expected

λ_0 = inherent failure rate

t = expected operating time to attain maturity

α = rate of growth

The data to determine comparative mature failure rates for each technology is given in Table 8.

The data in Table 8 is plotted in Figure 17 for ease of comparing the various technologies by their inherent and mature FIT's.

3.2.2 Functional Fabrication Level Evaluation

The functional fabrication level contains those factors which are related to circuit design implementation to achieve a particular functional capability. The factors considered are:

- 1) Number of active devices.
- 2) Number of other components.
- 3) Microcircuit junction temperature.
- 4) Board area required.

These factors are used to maximize reliability by comparing the circuits generated for various fuel control functions.

Factor 1 - Number of Active Devices

The number of active devices is used as a measure of the required number of building blocks required to implement a specific function. This factor is evaluated according to the following scale of values:

<u>Number of Active Devices</u>	<u>Weight</u>
1 - 5	100
6 - 10	70
11 - 30	35
31 - 55	15
> 55	0

The scale of values favors the smaller number of active devices over a larger number. That is, preference is given to progressively higher levels of circuit integration. The 10,000 operating hours shown in Figure 17 do not represent a limit but is the approximate control life associated with 30 years in a military application.

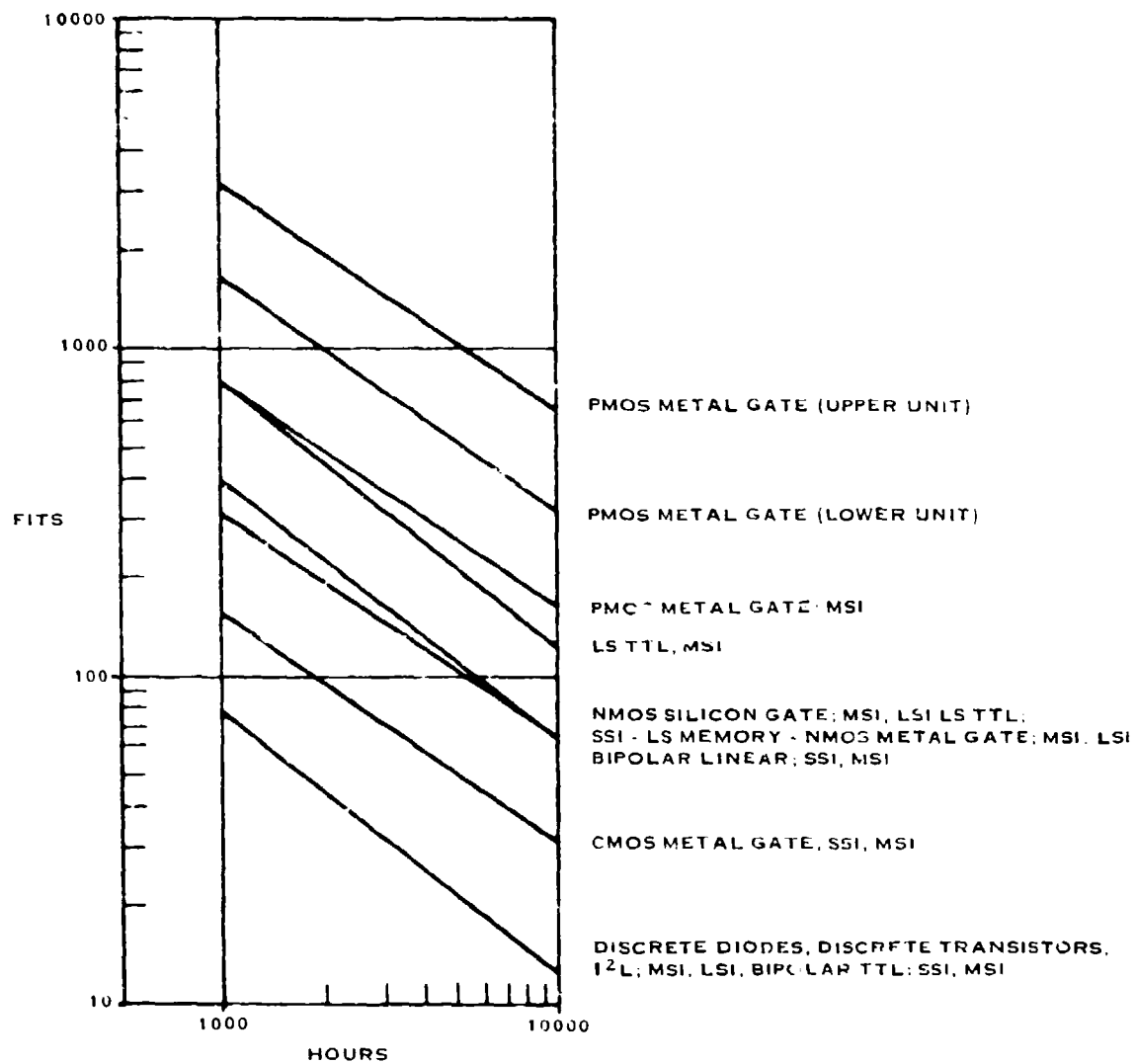


FIGURE 17 INHERENT FIT (FAILURES IN TIME) TECHNOLOGY CURVES

3.2.2 Continued

Factor 2 - Number of Other Components

This factor addresses the circuit functional complexity from the standpoint of the number of passive components required to support the active device functional building blocks. The scale used as a figure of merit is as follows:

<u>Number of Other Components</u>	<u>Weight</u>
10	15
11 - 20	12
21 - 50	8
> 50	0

The scale gives preference to those functional building blocks requiring the least number of additional passive components.

Factor 3 - Microcircuit Junction Temperature

The microcircuit junction temperature factor is based on the proposition that a technology with a lower operating junction temperature is inherently more reliable. The figures of merit for this factor are:

<u>Junction Temperature</u>	<u>Weight</u>
75°C	20
76°-90°C	15
91°-110°C	5
> 110°C	0

Factor 4 - Board Area Required

This factor is used to classify the technologies in relation to the amount of mounting space required for installation. The range of values is:

<u>Board Area</u>	<u>Weight</u>
5 in ²	20
6 - 10 in ²	15
11 - 15 in ²	10
> 15 in ²	0

The most weight is given to those technologies which require the least area to implement a given controller function, since they will require less complex interconnection and provide more homogeneous thermal dissipation.

3.2.3 Circuit Technology Reliability Tradeoff

The methodology developed in the previous sections for the part and fabrication level assessments can now be used to perform actual tradeoffs. From section 3.2, the maximum reliability point value is equal to the sum of each factor and can be as high as 240. In the evaluation of a circuit function, actual point values will be generated for each active part within that circuit. The values will then be averaged to reflect the general reliability value of the part mix/technology used. However, it is necessary to penalize the "bad actors" on low point scores, therefore each part with a score less than 170 points will require that the average be penalized by 10%. An example of this is shown below:

<u>Circuit Parts Lists</u>	<u>Weight</u>
Active Part A	195
Active Part B	200
Active Part C	130
Active Part D	175
	<u>700</u>

$$\text{Average} = \frac{700}{4} = 175$$

$$\text{Final Value} = 0.90 (175) = \underline{157 \text{ points}}$$

i.e., 10% penalty assigned due to 130 score for part "C".

In this manner a relatively few components with low score will readily affect the overall score for parts technology contribution.

From section 3.2.2, the maximum reliability point value for fabrication level assessment can be as high as 155. The final reliability assessment is the combined parts technology assessment and functional fabrication assessment.

Continuing the above example, assume the circuit has the following characteristics:

4 active parts with average junction temperature of 85°C
11 passive parts
Occupies 3.5 in² of board area

Therefore:

<u>Element</u>	<u>Weight</u>
Active Parts (4)	100
Other Parts (11)	12
Junction Temp. (85°C)	15
Board Area (3.5 in ²)	20
	<u>147</u>

3.2.3 Continued

The total reliability point value of this design approach is $157 + 147 = 304$.

The employment of the above method will readily assess, in a quantitative fashion, the expected improvement or degradation in reliability of one approach versus another. If design "A" is 304 points and design "B" is 334 points then design "B" has a reliability (MTBF) that is 10% improved over design "A". This technique assumes of course that basic performance, weight, and dissipation characteristics of all design approaches meet as a basic requirement. Thus, overall reliability improvement percentages can be assessed for each functional area and for the control irrespective of other considerations such as redundancy which may be treated separately. Where alternate designs result in only a small sensitivity to reliability, then final selection may be made upon the next most critical parameter such as cost, weight, performance growth margin, etc.

3.2.4 Passive Component Selection

As can be seen from the previous sections passive components were only included in reliability tradeoffs as they affected the general board complexity. The primary reason for this is that the quantity of these devices employed is the major reliability factor. The inherent failure rate of properly selected and applied passive devices is significantly less than active circuits and the contribution of interconnects becomes the preponderant factor for reliability evaluation. Furthermore, the technical growth and innovation in this area is nonexistent in comparison to the active element arena. Previous programs in the electronic engine control and general avionic area have demonstrated that high reliability can be attained with proper selection and application of "established reliability", passive military specifications.

The major contribution to reliability improvement then becomes one of:

- o Reduction of components
- o Standardized form factor
- o Thermal matching to circuit board
- o Increased automation in assembly

The achievement of these improvements is primarily attained through the use of resistor networks and chip capacitors.

Resistor networks, both thin and thick film, packaged in leadless carriers will: (a) reduce manual lead bending and cutting operations; (b) reduce circuit board interconnections, and area; (c) provide uniform form factor with other circuit elements lending to automated assembly; (d) obviate the need for plated through holes not compatible with ceramic substrates; (e) provide better thermal matching and heat transfer on ceramic circuit board substrates; and

3.2.4 Continued

(f) provide inherently better tracking where required.

Chip capacitors provide the same basic advantages and are available in established reliability Mil specification.

Both networks and chip capacitors have existed for several years, have found high volume commercial applications and are being incorporated in more military applications.

SECTION IV

PACKAGE CONSIDERATIONS

4.1 Introduction

The total failure rate of an electronic engine control (EEC) is comprised of electrical component plus "mechanical" component failures. The mechanical components in an EEC include all physical hardware and attachments, with the exception of the actual circuit device in its carrier. For example, an LSI circuit packaged in a leadless chip carrier is considered the electrical component. But, the leadless chip carrier termination to a circuit board is considered mechanical. In general terms, mechanical components would include:

- o Interconnects
- o Wire/cables
- o Electrical connectors
- o Printed circuit boards
- o Physical structures
- o Fasteners
- o Vibration isolators

Reliability of the package is directly related to the fulfillment of three basic tasks:

- o Defining the environment to be encountered.
- o Establishing the limits of exposure required to achieve the desired reliability.
- o Designing a mechanical package to modify the environment to within required limits.

The purpose of this section of this guide is to highlight the areas that will have the greatest impact on the mechanical package reliability and to provide basic approach techniques to combat them.

It cannot be overemphasized that complete definition of the total engine control environment is a vital prerequisite to successfully control the environmental exposure, and that it is essential to use a systems approach that simultaneously includes all criteria; including mounting location and final use.

Attempts to control the environmental exposure focus on two areas generally having the greatest impact on reliability: temperature and vibration. These and other environmental factors will be discussed in detail in the following section. Inherent capability and limitations are mostly dependent on:

4.1 Continued

(1) electrical component package configuration, especially in regard to mounting features; (2) component interconnects; (3) printed circuit laminate or other interconnect substrate; (4) cabling technique and attachment; and (5) the physical structure.

As stated, this guide will present the areas of concern and include some general recommendations, but final design features to be included for an EEC must be based upon actual requirements and environments for the specific application.

In the following paragraphs, these major topics will be discussed:

- o Environmental Factors
- o Environmental Design
- o Interconnec Design Trades
- o Material Considerations

4.2 Environmental Factors

4.2.1 General Discussion

Initial efforts to design reliable engine-mounted electronic controls were based upon the environments as specified in military specifications with installation-on-engine following previously successful techniques utilized for mechanical accessories. Since desired reliability was not achieved, investigations into failure modes and causes were initiated which have resulted in progressive improvements in early controls and major changes in design philosophy for recent controls.

While military specifications have been modified in recent years, demonstration of compliance with these specifications is inadequate by itself in determining the probable success of an electronic control. In order to achieve maximum reliability from an environmental standpoint, three basic requirements must be met:

- o DEFINITION OF EXPOSURE

Complete specification of the environments to which the control and its component parts are to be subjected.

- o DEFINITION OF ALLOWABLE EXPOSURE

Complete specification of the limits of exposure required to achieve the desired reliability level.

4.2.1 Continued

o MODIFICATION OF EXPOSURE

Mechanical package design which modifies exposures to be equal to, or less than, reliability limits.

The above is merely another way to state the standard approach to any design effort: define the problem, then effect a solution. Nevertheless, the single major factor in advancement to date has been the completeness of the problem definition. Reliance on generic engine specifications or the combination of a few worst-case parameters is wholly inadequate. The key is in complete definition. For any new or advanced application, this is admittedly difficult but it must be done in the best manner possible. Finally, complete environmental definition cannot be a unilateral effort but must include intelligence from the control designers, the engine designers, the airframe designers and the procuring agency.

4.2.2 Sources of Exposure

The various environments to be encountered by the control all contribute to functional reliability and must be defined and considered during the design. Investigations to date have revealed that the installed-in-aircraft environment is not necessarily the limiting one. Seven basic sources of exposure exist on which the life and reliability of the control are dependent. Exposure begins early in the fabrication stages and continues throughout the actual on-engine and repair service cycles. These basic sources of exposure can be categorized as follows:

- o Storage, shipping and handling of piece parts and subassemblies
- o Preparation and assembly
- o Troubleshooting and repair
- o Bench qualification testing
- o Acceptance testing or burn-in
- o Customer testing
- o Service

It is not the intent of this guide to define the controller environment, but rather to point out which parameters must be defined in order to successfully design a reliable EEC.

4.2.2 Continued

Awareness of the exposure sources to which an EEC can be subjected is the primary concern of this section. The effects of storage, shipping and handling on service reliability are not obvious. These environments are not noted for causing failures but they do produce degradation that leads to failure during service or test. This section will discuss the types of exposure introduced by these sources and recommend preventive measures.

4.2.2.1 Storage

Degradation in parts and subassemblies occurring during storage are usually the result of, but not limited to, one or more of the following:

- o Contamination from surroundings
- o Damage from stacking and packing
- o Excessive humidity or extreme dryness
- o Static discharge effects on sensitive devices
- o Corrosion

Damage resulting in detectable failures during test will lower production yield and increase rework; another source of possible degradation. Damages not leading to a detected failure during test will result in poor reliability. This point is important and will be referred to throughout this discussion.

Parts and subassemblies are routinely relegated to storage areas for various lengths of time. Storage location and configuration determine what types of exposure will be present. The following recommendations should be considered when selecting a storage facility:

- o Investigate the storage environment capabilities of parts and subassemblies during the design stages and define the requirements for storage.
- o Utilize protective packaging to modify environmental exposure.
- o Investigate the possibility of contaminants that may prove detrimental to electronics and protect accordingly.
- o Stack or pack items so as to eliminate physical stressing of cables, solder joints, components, etc.
- o Avoid storage areas having excessive humidity or extreme dryness that can make parts such as nylon insulators and printed circuit board connector housing brittle; causing minute cracks or breaks when installed.

4.2.2.1 Continued

- o Determine if component and/or board assembly packaging will create static discharge problems with sensitive component devices.
- o Investigate ammonia-base compounds, and sulfur compounds that may be stored in the vicinity of electronic connectors, since these promote corrosion of various contact materials.
- o Storage of parts and subassemblies should provide protection based on the next stage of build. For example if the next operation is to assemble and solder components to a printed circuit board, moisture protection must be provided, or pre-baking should be considered.

4.2.2.2 Shipping

EEC's are shipped via a variety of transportation modes. Depending on which mode is used, the EEC may encounter:

- o Pressure changes (altitude)
- o Extreme temperatures
- o Sustained humidity and salt air
- o Rain
- o Careless handling

The EEC shipping container must provide protection against these environments and, in general, packing per MIL-SPECS for handling is adequate for initial shipment; but all shipping configurations must be reviewed. For instance, an EEC may be shipped with an engine or engine subassembly after it reaches the customer. The shipping container at this stage must also assure adequate protection for the EEC. Further information on the cargo environment for highway and air transportation is available from the Department of Transportation and should probably be evaluated when selecting a shipping container.

4.2.2.3 Handling

In this section, handling is referred to in a somewhat different context than the previous paragraphs on shipping. This section deals with assembly floor handling of piece parts, subassemblies, and end items. Handling can be a major contributor to poor reliability. Part and assembly weaknesses occur in a variety of forms many of which go undetected. Reliability is affected since these weaknesses don't always lead to noticeable failures during test. A slightly bent component lead or connector pin, and partially damaged cable conductors are two of the more predominant handling related problems. Several

4.2.2.3 Continued

options are available that can minimize handling defects. Some of these are:

- o Design simplicity and modularization.
- o Inherent design ruggedness.
- o Avoidance of unsupported cabling.
- o Avoidance of the use of unprotected contact posts or terminals that might be susceptible to damage.
- o Fixturing to secure and protect assemblies during assembly, transport to various work stations, and testing.

4.2.2.4 Preparation and Assembly

The handling aspect mentioned in the previous paragraph is only one of the factors that affect reliability during assembly. Others include manufacturing operations and procedures such as soldering, cleaning, potting and bonding. The success of each operation is dependent on the operation previously performed, the complexity of the required task, and the skill of the operator. Human factors are a major cause of degradation, rework and repair; however, operator skill and training are also very important. The probability of human error depreciates with the increased use of automated assembly techniques but since the degree to which automation is employed is dependent upon the nature of the EEC manufacturer and the justification for automated production equipment, standardization is recommended wherever practicable to help justify capital expenses.

As mentioned earlier, the previously performed operation or set of conditions occurring just prior to these operations are very important. Thorough processing will begin with consideration of previous exposure(s) and will include the proper sequence of operations to be performed. Good process control and inspection will help produce a reliable end product; however, the nature of the operation itself can affect reliability. The use of improper tools is the biggest culprit. If crimping tools, solder iron tip size and temperature, wire strippers, serrated pliers, etc. are not chosen correctly, then the reliability of the end product will most assuredly be of low standard. The method of performing an operation is also an important consideration. Ultrasonic cleaning of printed circuit boards is a good example. Most electronic components are susceptible to high cycle fatigue damage at ultrasonic frequencies, therefore, this method of cleaning should be discouraged. Similarly, chemicals and solvents should be selected for ease of removal with cleaning agents and compatibility with hardware as they could cause long term failures as a result of corrosion or direct chemical breakdown of materials. Although

4.2.2.4 Continued

specifics about the assembly environment cannot be defined, the problems associated with assembly can be anticipated. Close liaison with manufacturing engineering and a knowledge of the various assembly operations can expose areas that may require special considerations.

4.2.2.5 Troubleshooting and Repair

Troubleshooting involves the use of manual techniques to find a problem which cannot be isolated by normal automated test cycles. Troubleshooting tends to include extraordinary procedures, especially with intermittent problems. The primary areas of concern should be:

1. Manual probing damage, the results of which can only be appreciated at high magnification, ultimately results in failure to solder connections, component leads, PCB plated thru-holes, and connectors.
2. Uncontrolled use of heat lamps, chilling sprays, ovens, vibra-tools (to locally "vibrate" the test article) and vibration shakers do damage which: a) does not cause immediate failure; b) is not easily detected; and c) degrades the unit adding to the overall failure rate.
3. Excessive "lifting" and/or removal of components or interconnects.

While not entirely avoidable, all of these can be controlled through operator training and with guidance from the appropriate functional groups such as Manufacturing and Design Engineering.

Repair is the correction of a defined problem. Degradation from repair is primarily caused by soldering irons which apply too much heat, too fast. The most common features damaged are the electrical components, and the printed circuit substrate; especially the printed circuit boards plated thru-holes, conductors and laminations (delamination).

Secondary concerns are the individual actions poorly controlled due to the impracticality of defining every possible repair action. It is, therefore, essential to have some general guidelines and high caliber personnel trained in all areas (i.e. handling components, preforming leads, component insertion, cleaning, soldering, adhesive bonding, conformal coating application and removal, etc.).

Reliability degradation can also be reduced by incorporating design features which will facilitate lower jeopardy testing techniques and by selecting materials and technology capable of withstanding the repair environment. Below are some typical examples:

- o Provide additional test points during the design phase to minimize manual probing.

4.2.2.5 Continued

- o Provide a means for "opening" circuits without unsoldering components.
- o Establish controlled standard repair procedures.
- o Include automated or semi-automated component removal/installation equipment.
- o Select interconnect technology capable of multiple repair cycles without serious degradation.
- o Assure that various subassemblies, as well as the end item, will operate at agreeable temperatures without supplemental cooling in the test environment. If this is not possible, specify the cooling required.

4.2.2.6 Bench Qualification Testing (BQT)

Traditionally the BQT is the design-controlling environment and because it is better defined than any other, it is the easiest to design too. Exposure to a BQT is not a reliability threat to production units since relatively few units get exposure, and these units do not normally see service. Sometimes, however, inappropriate BQT requirements may force the design to include features which are inconsistent with the service environment to the point of actually reducing the capability of the unit in that service environment. For this reason the BQT should be reviewed in detail relative to the projected operational exposure and modified if necessary.

4.2.2.7 Acceptance Testing or Burn-In

Acceptance or burn-in tests are designed to demonstrate the capability of the unit to operate properly and to create weak-link failures (infant mortality) prior to shipment. Failures of this nature are the most difficult to plan because of insufficient background available for advanced designs upon which to base exposure specifications. Since the ultimate goal of these tests is to cause the occurrence of failures which otherwise would appear during operation, the operational environment(s) must be used as a basis for test definition.

In order to achieve a reasonable time limit on testing, levels of exposure may be increased. However, herein lies the jeopardy of actually reducing the ultimate reliability of the control because excessive test levels may cause degradation of features, which would otherwise survive operational levels indefinitely, to the point of reduced life at those levels.

4.2.2.8 Customer Testing

Customer testing, relative to production controls, is normally non-flight control, system or engine testing conducted for the purpose of performance evaluation. Engine test facilities produce environments that certainly are different than, and may be more severe than, service or qualification tests. Communication between the EEC manufacturer and the engine manufacturer is essential to expose those elements not ordinarily included in the customer's design specification. For example, engine tests are often run in an enclosed test cell where acoustic levels may be extremely high relative to BQT and service levels. The effect these tests will have on the EEC can range from degradation to outright failure. The EEC designers should take the initiative by communicating the need for complete definition, including but not limited to:

- o Testing environments not present in the controller design specification which may result from variations in engine configuration, mode of operation, test cell conditions, etc.
- o Those areas which must be considered during EEC design and those which may be modified so as to avoid influencing major EEC design features.

4.2.2.9 Service

The environment within which the EEC must demonstrate its reliability is the most difficult to define. In addition to evaluating the EEC/engine/airframe variables, an EEC may be destined for use with little or no mechanical modification on more than one engine and each engine in more than one aircraft. Nevertheless, high reliability levels cannot be reached without thorough consideration of the final proving grounds. As stated previously, estimates of a few extremes is totally inadequate for high confidence design. All of the variables must be established, in combination, by the best means available. The relative impact, and therefore the control design, must be established by or with the aid of the control designers. It is certainly the responsibility of the control designer to outline the variables of concern and to impress upon the engine and aircraft manufacturers, as well as the final customer, the relative importance of positive participation in this effort. The variables of concern are outlined in detail in subsequent paragraphs.

When defining them, it is important that frequency of occurrence, rate of change, and time-at-condition be included. This is best accomplished by plotting each variable versus time for each projected flight profile from engine or control start up to shut down.

In addition to responding to lists generated by the control designer, each participant must be encouraged to search out and specify any extraordinary exposure the unit is likely to encounter; such as steam cleaning procedures.

4.3 Environmental Design

The environmental design of an EEC is an important consideration relative to reliability. A successful environmental design requires: 1) understanding the environmental exposure to be imposed on the electronics; and 2) a controller design with an inherent capability to accommodate that exposure. It is the intent of this section to aid in the process of understanding the environment and to present some of the options available to achieve these goals. Temperature and vibration are the two environments generally having the greatest impact on reliability and will, therefore, be the major topics covered in this section.

4.3.1 Thermal Considerations

The goal of any EEC thermal design should be to modify the temperature environment of the electronics such that each individual electronic component will operate at a temperature level commensurate with that necessary to achieve the desired reliability level. The ambient temperature surrounding the electronic components can have as much influence on the failure rates of the components as component stress ratios. It is evident, from failure rate data presented in MIL-HDBK-217B, that temperature variations may have a pronounced effect on component failure rate. The curve shown in Figure 18 illustrates this point.

The actual failure rate curve for each different component, as well as each different end item, will vary based on part capability. This data is ordinarily provided by the semiconductor manufacturer, and for reasons of conservatism, the manufacturers data is sometimes derated by the user. Because of the uncertainty in defining the environment precisely, it is not only desirable to operate at temperature "B" for generally lower failure rate, but also because the slope of the curve at that point is such that unpredicted variations in the environment, and hence component temperatures, will have minimal effect on the overall reliability. Conversely, for operation at temperature "A", even a slight change in temperature can drastically reduce reliability. There are a number of parameters that influence the thermal environment and these should be reviewed for each flight profile. They consist of, but are not limited to:

Duration and rate of occurrence	Nacelle air temperature
Nacelle pressure	Nacelle metal temperature
Nacelle air flow	Engine case temperature
Nacelle metal emissivity	Engine case emissivity

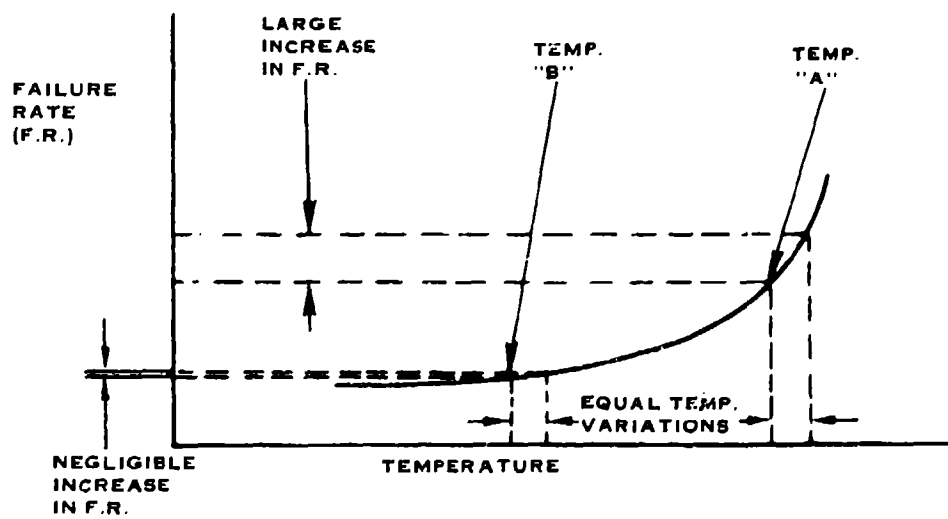


FIGURE 18 FAILURE RATE VS TEMPERATURE GRAPH

4.3.1 Continued

Local heat generators, such as engine bleeds, oil cooling and other accessories, should also be investigated. The system should be further examined for possible cooling sources. The most favorable cooling system would be one with the:

- o least complexity
- o least hardware
- o lowest and most stable component temperature

If ambient conditions are favorable, natural convection would be the most favorable since it meets the criterion of simplicity and the time constant would be relatively slow; avoid thermal shock but not excursions. Two of the available sources that can be used directly are ambient air and fuel. Tank fuel has proven to be the best source in terms of reliability because it provides a relatively constant temperature and minimal transients (aerial refueling is the major one). Other sources for direct use include ECS (Environmental Control System) air and coolant fluid.

The possibilities of available sources for indirect use are too numerous to cover completely. The approach, however, is to review all available sources of power which may be converted to cool the control:

- o Electrical Power
- o Mechanical Power
- o Bleed Air
- o Hydraulic Fluids
- o High Pressure Fuel
- o Engine Heat

The sources could be used singly or in combination to drive a variety of cooling equipment. As can be recognized with indirect usage of these engine cooling sources, the introduction of additional hardware is required to complete the system.

The disadvantage is that the cooling mechanism now becomes part of the reliability assessment in that its failure rate must be included in the calculated system failure rate.

Remote cooling sources which might be available transfer heat via two possible paths. Devices, such as heat pipes, transfer heat from the control to the ultimate heat sink; sources like ambient air, ECS air or fluid, transfer from the sink to the control. All of the cooling approaches just covered address the service environment only. The final design must be compatible with all other environments. (See Section 4.2)

4.3.1 Continued

Obviously, once the environment and basic cooling techniques have been established, the controller design must be directed toward minimizing the thermal resistance from each component to the sink to a level commensurate with its capability. It is assumed that the controller designer is familiar with the techniques for accomplishing this objective. For high confidence EEC design, a rigorous thermal evaluation must be completed which includes all thermal trades, both internal and external to the control.

4.3.2 Vibration Consideration

It is assumed that the reader of this guide is familiar with the basic approaches for designing with physical integrity within a given vibratory environment. This guide, therefore, is directed primarily at aiding in the understanding and specification of the environment.

As stated earlier, complete definition of the vibration is mandatory if the controller design is to be successful. The vibration response of the controller can only be estimated for the design, but can and should be confirmed through testing. There are numerous sources of transmitted mechanical vibration on a jet engine. Electronic equipment may be exposed to extremely complex and severe vibration which cannot be evaluated or resisted by any simple expedients. Over-design and extremely conservative design attitudes cannot be applied with any quantitative probability of success due to the complexity of exposure. Since vibration excitation of an engine mounted control is far more complex than military specifications would indicate, extensive analysis must be done to reveal the detailed nature of this complexity and to assure that all aspects are considered. The major factors that need to be covered early in the design stages are:

- o Frequencies of excitation
- o Levels of excitation
- o Input paths
- o Variables

4.3.2.1 Frequency and Level of Excitation

Physical characteristics of the rotating machinery determine the frequencies to be experienced. Frequencies which must be investigated are known to be:

- o Shaft speeds
- o Blade passing frequencies
- o Gear box speeds
- o Pump speeds
- o Other accessory speeds
- o Aircraft induced input frequencies

All of the engine frequencies will vary with engine speed.

4.3.2.1 Continued

While all of the inputs mentioned above occur simultaneously, their energy content and effect on the EEC will vary widely. The major contribution from this information to the reliability of an EEC is that vibration excitations of significant levels do occur well above the 2000 HZ limit of most military specifications, and at frequencies to which the component internal interconnects will respond.

As frequencies change with engine speed the energy associated with each frequency will also change, and in fact, the dominant frequency at each speed may be different. An example of a typical engine case vibration is shown in Figure 19.

4.3.2.2 Input Paths

The EEC package can be excited through any and all physical contacts with the engine. The primary input paths are:

- o EEC mounting brackets
- o Hydraulic and pneumatic lines
- o Electrical cables

Although the controller mounts are the most obvious vibration input path, hydraulic and pneumatic lines cannot be ignored. Relatively hard connections, such as plumbing lines, bypass the control mounting bracket isolation. The areas for concern are mechanical vibrations induced by the plumbing source (pumps, etc.) or via the engine skin vibration transmitted through the clamping points. The vibration received from the electrical cables is usually minimal because of the generally flexible construction of cable harnesses. Caution should be taken to avoid short bulky harnesses, and to properly assess the effects of relatively stiff shielding or conduit.

4.3.3 Acoustics

The effects of acoustics appear as vibration responses on printed circuit boards, components and interconnects. Items with large surfaces such as printed circuit boards and covers are the most susceptible to acoustics; whereas the effects are negligible on small individual components.

Acoustic control or attenuation must be accomplished through effective structure design since the engine control vibration isolators are bypassed. Acoustic levels vary considerably depending on engine location and location of the controller on the engine. Engine location refers to any installation within which the engine is operated. Examples wherein acoustics at the control location will vary widely are:

- o Open test cells
- o Closed test cells
- o Airframe installation

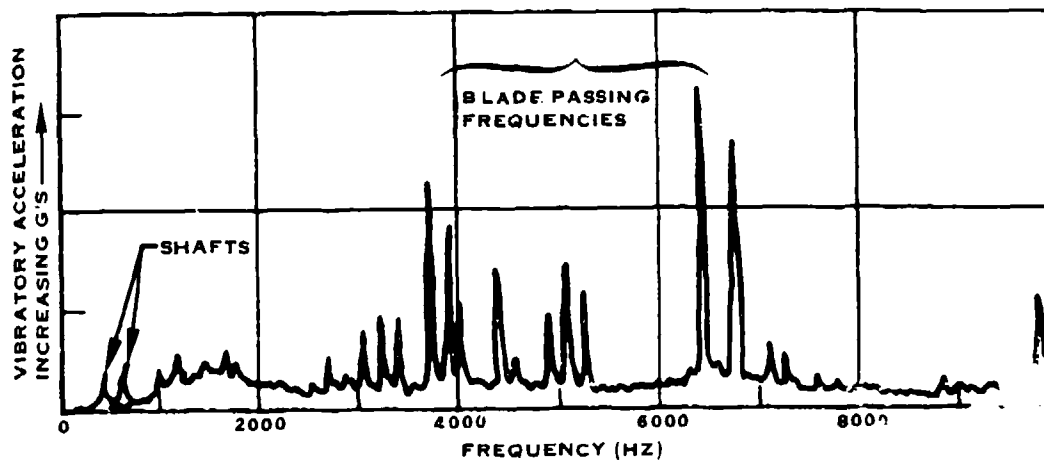


FIGURE 19 ENGINE CASE VIBRATION

4.3.3 Continued

If worst case exposure occurs in other than the airframe, a trade-off must be made to determine if the control should be designed for the worst case or if supplementary protection should be provided during that exposure.

Levels on the engine will be lower towards the forward end and will vary depending upon the "view" or exposure access to the control. Frequencies associated with acoustics include those associated with vibration because the acoustics are generated by the same physical features but are supplemented by engine pneumatics.

Reverberant chamber testing with input levels equal to those measured at the control location on engine will be more severe due to relatively efficient coupling on all sides. An installed control receives varying exposure and coupling on all surfaces due to the proximity of the engine case, baffling by other hardware and location relative to the source.

4.3.4 Shock

Designing for integrity under shock loading is, for the most part, straightforward and done with confidence since crash safety levels are usually the criteria used for design. With a vibration isolation system, the major threat is in inadequate treatment of control motion in response to shock inputs, especially with systems in which the unit center of gravity is displaced from the elastic center of the isolators. Inadequate sway space will result in periodic impacting of the unit with immediate or low cycle fatigue failures. Similarly, inadequate attention to the motion effects on cross-join features, such as plumbing and cabling, may result in unpredicted failures.

4.4 Interconnect Trades

The EEC package entity having the greatest impact on reliability is the interconnecting and packaging (I/P) structure. Terminations of various types appear at all levels of the functional interconnect scheme starting at the component chip and ending with the I/O interface connector. An EEC is comprised of hundreds of interconnects; effective implementation of those interconnects at the correct level will play a key role in overall reliability. This section will emphasize the design approach levels of interconnects and types of terminations that will result in the best reliability. Naturally, the end result will differ for each control depending on the established environment and design goals, but reliability will be the highest obtainable based on those requirements. It is possible to draw up a set of design rules for engineering a system requiring high reliability while operating in a harsh environment, by doing the following:

4.4

Continued

- o Maximize the circuit integration.
- o Maximize the electrical performance of the circuit.
- o Minimize the circuit component count.
- o Minimize and optimize joints between components, and between components and connectors.
- o Provide good mechanical support for components and wires.

4.4.1 Circuit Integration

Increasing the level of integration in the circuitry is a powerful method of achieving reliability because many operations and processes at the manufacturing stage can be eliminated, thereby removing potential failure modes. LSI (large scale integration), VLSI (very large scale integration), microprocessors, gate array, etc. technologies offer the best approach for minimizing the circuit component count, thereby minimizing the number of joints between the components and the I/P structure. It should be pointed out that even though the total number of interconnects present in the circuit won't be reduced, they will be incorporated at the chip level where a more sophisticated and reliable technology is utilized. What is required to reap the full reliability benefits is a packaging approach based on narrow and short inter-chip interconnections of low capacitance, and the elimination of all or most higher level interconnections. Such a packaging concept might be based on the extrapolation of present high-density integrated circuit interconnect technologies to the next higher packaging level. This packaging approach maximizes electrical performance, minimizes electrical component count, and greatly reduces the number of interconnects at the higher levels.

The new standard in packaging, the leadless chip carrier (LCC), offers all of these characteristics. As the lead count increases for LSI and VLSI type devices, LCC's offer significant improvements over alternative packaging systems.

For example, the ratio of longest to shortest trace on a 64-lead DIP is 7:1 compared to 1.5:1 for a comparable LCC. The shorter trace lengths inherent with chip carriers results in lower resistance and less capacitance, thus permitting faster switching times and improved systems performance. Other packages, such as the dual-in-line (DIP), flat pack and quad-in-line package (QUIP), are also used but their performance is somewhat diminished because of size.

4.4.2 Interconnect and Packaging (I/P) Structure

At a higher level, namely the I/P structure, the same important characteristics must be addressed. The newly emerging VLSI and memory circuit families are much less tolerant with regard to the electrical characteristics of their packaging environment. Such modern low power, high density circuit families as CMOS/SOS, short channel NMOS or I²L depend on small swings of the signal voltage and low signal currents.

4.4.2 Continued

Due to their high output impedance they will be slowed down to an intolerable degree when forced to drive the parasitic capacitance associated with the 15 to 20 mil wide interconnection lines of conventional printed circuit boards. These problems can be overcome in a couple of ways. Attempts can be made to utilize fine-line printing techniques on a high-performance laminate, such as polyimide or improved epoxy systems. Or, the I/P structure can be fabricated using the same type of technology presently being implemented in hybrid systems, namely thick-film multilayer substrates. The first approach is not common and carries with it several uncertainties such as: the reliability of attachment of the LCC; the acceptability by the military; and the plated through-hole integrity for smaller than standard hole sizes. On the other hand, the second approach offers technology which has had widespread usage throughout the hybrid and semiconductor industry for years. In addition, it has been determined that LCC's can be attached more reliably to a thick-film printed circuit substrate. Another consideration would be the use of "porcelain-on steel" substrates which also employ thick-film technology; although still under development, it appears to be a viable alternative to alumina. The principal advantage the porcelain-on-steel would have over alumina is size. Much larger printed circuit boards can be fabricated with porcelain-on-steel substrates. Table 9 lists comparable properties for both the high-performance laminates and thick-film substrates.

4.4.2.1 Laminates

There are certain properties which are most important to the reliability evaluation of printed board laminates:

- o Glass transition temperature
- o High temperature performance
- o Produceability

Glass transition temperature is the point at which the first significant softening of the particular resin under consideration is noted. Low glass transition temperatures are accompanied by high board coefficients of thermal expansion in the thickness, or "Z", direction. This expansion characteristic can result in direct laminate degradation through:

- o Delamination
- o Separation of external layer pads
- o Separation of internal conductors from plated through-holes
- o Separation of PTH barrels

TABLE 9

COMPARISON OF HIGH-PERFORMANCE LAMINATES AND THICK-FILM SUBSTRATES

PROPERTY	HIGH-PERFORMANCE LAMINATE				THICK-FILM SUBSTRATE	
	EPOXY G-10	TRIAZINE	POLYIMIDE	PORCELAIN ENAMEL ON STEEL	ALUMINA (96%)	
GENERAL EXPERIENCE	MOST WIDE SPREAD USAGE TO DATE	ON VERGE OF VOLUME USAGE	RECENTLY INTERNATIONALLY MARKETED	VERY LITTLE PRINTED CIRCUIT BOARD USAGE	WIDE SPREAD USAGE IN MULTI- LAYER HYBRIDS FOR MILITARY	
THERMAL CONDUCTIVITY (G/CAL/CM ² /CM/SEC/°C)	0.0007	0.0007	0.0008	0.0027	0.084	
DIMENSIONAL STABILITY	FAIR	VERY GOOD	VERY GOOD	EXCELLENT *	FAIR *	
DISSIPATION FACTOR AT 1MHZ	0.03	0.007	0.02	0.008	0.0003	
VOLUME RESISTIVITY (OHM-CM)	$> 10^9$	$> 6 \times 10^{10}$	$> 6 \times 10^{10}$	$> 10^{14}$	$> 10^{14}$	
GLASS TRANSITION TEMP. (°C)	115	250	300	N/A	N/A	
PEAK PROCESSING TEMP. (°C)	N/A	N/A	N/A	675	1000	

* APPLIES FOR BOARDS LARGER THAN 4 X 4. BOTH HAVE EXCELLENT STABILITY AT SMALLER SIZES.

4.4.2.1 Continued

Printed circuit board laminate degradation of this nature occurs predominantly during assembly processes, such as flow solder; and during testing and in-service thermal cycling. The most obvious degradation takes the form of cracks around the perimeter of the plated through-hole, but correct plated through-hole design can help prevent cracking. For example, a small plated through-hole tends to result in thinner plating and may allow entrapped etchants to remain, producing a physically weak barrel. It has been found that "non-functional" pads can help avoid some of these problems by breaking up the long spans of resin in the "Z" direction with a balanced ratio of copper to laminate thereby reducing the likelihood of copper foil cracks. An equal ratio reduces the distance of the Z-directional travel seen during hand or automatic solder thermal exposure, thermal cycle testing or field repair thermal exposure. Non-functional pads also provide more internal copper-to-copper plating surfaces resulting in a much stronger plated through-hole. Pads should be designed as large as practical, and should offer a large annular ring to provide the strongest possible barrel.

4.4.2.2 Substrates

The most important electrical performance advantages of alumina thick-film substrates have already been discussed earlier. However, there are certain other direct and indirect reliability considerations that should be ascertained, such as:

- o Low thermal coefficient of expansion
- o Very good thermal conductivity
- o High operating temperatures
- o Thick-film monolithic circuit metallization techniques

As is true with all I/P structures, whether a laminate or a substrate, the application and intent should be reviewed and a reliable approach implemented. The use of high-performance laminates such as polyimide, triazine or improved epoxies is one approach; thick-film technology using alumina or porcelain-on-steel is another. Both of these approaches have their advantages and disadvantages, and should be investigated and selected based upon the intended application.

4.4.3 Terminations

Throughout the progression of the I/P structure there are hundreds of connections and a multiplicity of termination techniques. A necessary consideration is to investigate and choose the kind of termination that will provide the highest level of confidence for the intended application. The list below shows the progression of interconnects at all levels. Details are presented in subsequent paragraphs.

4.4.3 Continued

- o Chip to carrier
- o Carrier to substrate
- o Carrier to laminate
- o Substrate/laminate to I/O connector

4.4.3.1 Chip to Carrier

The carrier which houses the active chip can take on several different configurations (i.e., DIP, flatpack, LCC, etc), but the method for terminating the chip to these packages does not differ by very much. A leadless chip carrier package can be visualized as the center portion of a DIP or flatpack with the two rows of metal leads replaced by contact pads on all four sides. Figure 20 compares the typical construction of a leadless chip carrier to that of a typical ceramic DIP and flatpack of the same lead count. As shown, the same materials, construction and termination techniques that have been used for years to fabricate the high-reliability ceramic DIP are used for fabricating the chip carriers.

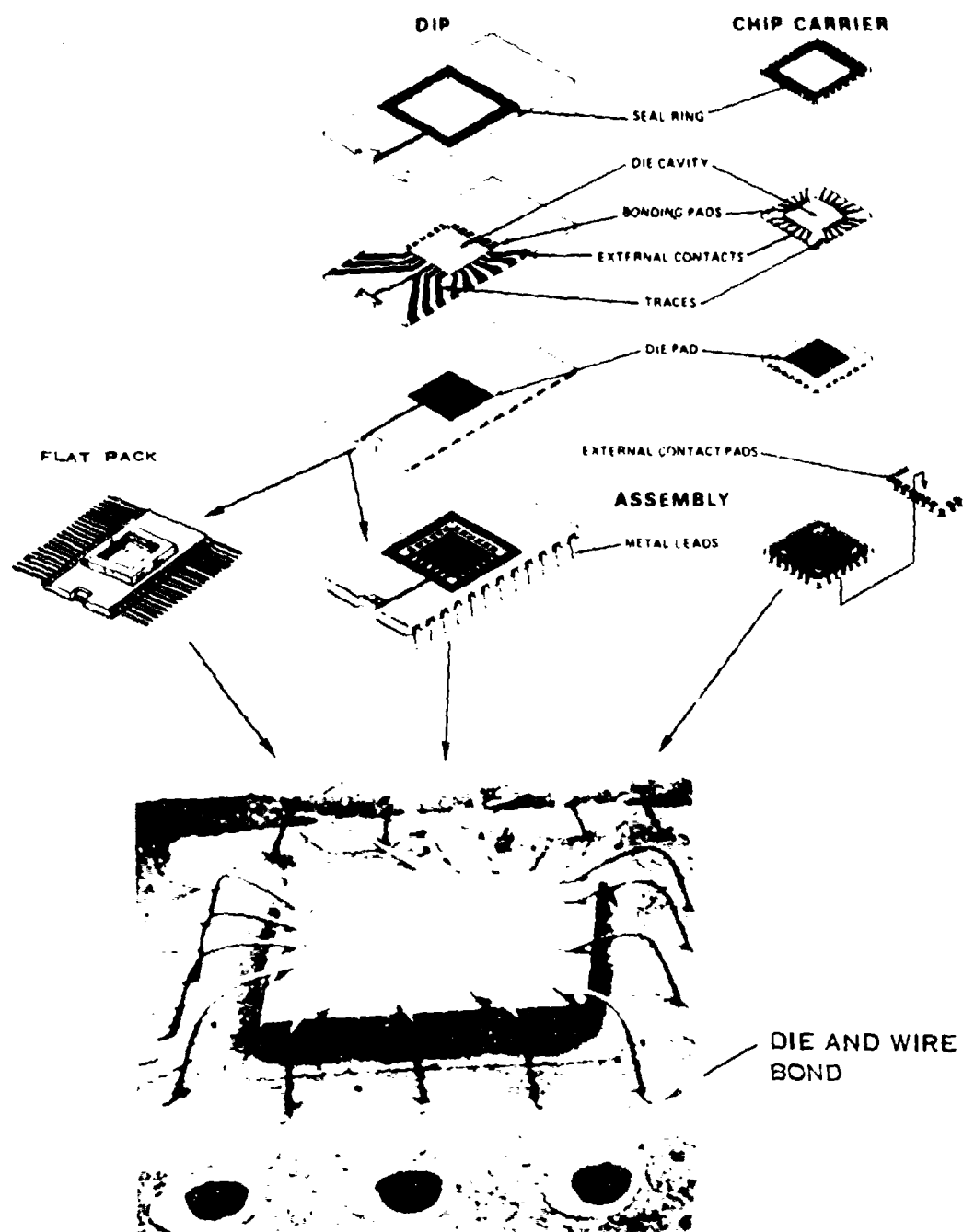
There are other approaches available for terminating the chip to the carrier other than the die and wire bonding technique shown in Figure 20. These include beam lead, flip chip and tape automated bonding (TAB). The die and wire bond is the recommended technique, however, since it is an established and proven chip termination method offering direct attachment to the ceramic carrier package for good heat transfer. Each technique should be reviewed in terms of the following parameters to determine which is most reliable for the intended application:

- o Thermal resistance
- o Availability
- o Durability
- o Automated Assembly
- o Inspectability

Figure 21 illustrates these various techniques.

4.4.3.2 Carrier to Substrate/Laminate

The reliability of the I/P structure is directly related to the type of termination that must be used for the kind of chip carrier selected. DIP packages require plated through-holes (PTH) in which to terminate, regardless of whether a substrate or a laminate is used; flatpacks and LCC's do not.



E-6735

FIGURE 20 CHIP PACKAGING METHODS

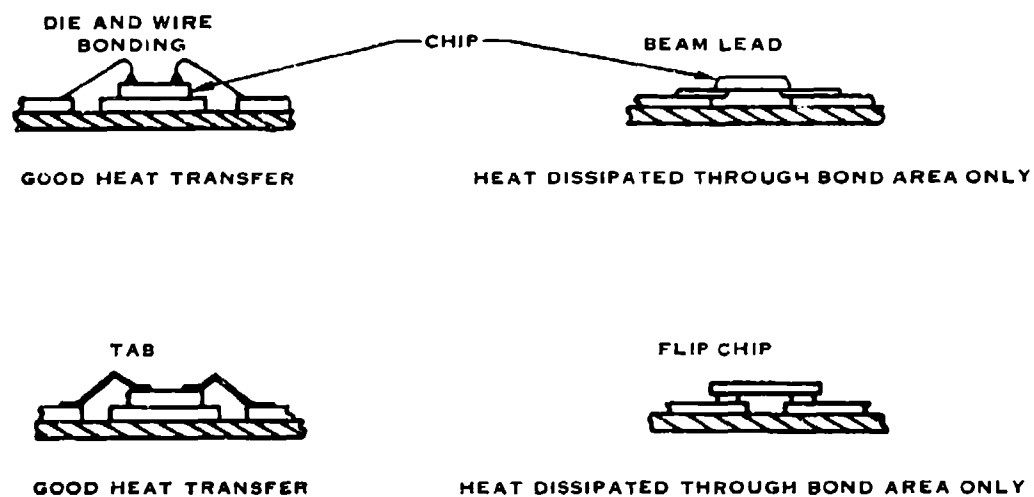


FIGURE 21 DIE CONNECTION TECHNIQUES

4.4.3.2 Continued

A through-connection of some kind is still required to connect signals to inner layers, but this is true regardless of the package configuration or the I/P structure. The thick-film substrate technology with its co-fired monolithic structure, greatly surpasses the reliability of the PTH used in conventional laminate printed circuit boards. The use of this technology for mounting and interconnecting flatpacks and LCC's is, in terms of reliability, very appealing. In general, surface soldering is better than the PTH approach because the joint is visible, is inspectable and avoids all the problems associated with PTH solder joints. The leadless chip carrier may be considered as a flatpack without leads. This concept is useful because the chip carriers are attached to the I/P structure via reflow soldering; the same basic process used to attach flatpacks. However, the problems normally associated with the use of this process for flatpack attachment are avoided since there are no flexible leads to contend with on an LCC.

The best interconnect design includes carriers to I/P structure terminations which:

- o Minimize the use of PTH's
- o Use simple attachment methods
- o Have inspectable solder joints
- o Are capable of automated assembly
- o Are repairable

4.4.3.3 Substrate/Laminate to I/O Interface

The interconnection problem modern electronic controls has generally led to large scale usage of separable connectors. It is desirable to be able to separate electronic components into functional modules or packages, and then to be able to connect or disconnect these modules without soldering. This feature is needed to facilitate: sequential testing at progressive levels; removal or replacement of defective packages; and circuit modification and growth. This also simplifies testing and assembly without degrading the I/P structure.

The tradeoffs for using a separable or nonseparable connection is an area requiring in-depth investigation and rigorous design conceptual work. If the EEC package designer can manipulate the interconnect design to provide good maintainability while at the same time maximize the use of permanent connections, it would be advantageous. In the final assessment, however, the reliability benefits of using the permanent connections must exceed the maintainability and testability benefits of having a separable one. The decision to use separable versus nonseparable connections is a difficult one but it can be based on specific objectives. In order of priority, here are some objectives to consider:

4.4.3.3 Continued

- 1) Reliability
- 2) Testability
- 3) Maintainability
- 4) Safety
- 5) Cost
- 6) Human Engineering

If the decision is made to use separable connections, there are some aspects about them that should be known. The major causes of failure in separable connectors are high contact resistance and low insulation resistance between contacts. High contact resistance occurs from factory contamination such as solder flux, lacquer or lubricant, and from field aging effects. Field aging is the most difficult to define. It can be associated with additional resistance resulting from oxide films, oils and other similar surface contaminants that invade pure metal-to-metal contact. Such films are often responsible for the highest portion of electrical resistance in a connector. The actual amount of resistance depends upon surface finish, contact pressure, and the kind of metal used in the connector.

In applications where frequent insertion and withdrawal cycles are involved, spring-applied contact force is recommended to avoid galling of contacts. Avoid using too high a contact force to decrease resistance because the contacts may wear out more quickly. Other reliability considerations related to separable connectors are:

- o Positive alignment feature to prevent bent contacts.
- o Controlled, low, stable contact resistance throughout the service life.
- o Easy insertion and removal when required, together with mechanical retention of the mated connector pair.
- o Guaranteed connection in a vibratory field.
- o Low contact wear.
- o High insulation resistance.
- o Mechanical ruggedness for handling and shipping.
- o Easy inspection of terminations.
- o Positive keying to assure mating of the correct connector mate.

If it is determined that nonseparable connections can be used without severe maintainability losses, certain advantages over separable connectors can be realized. Simply stated, a separable connector will always require at least three terminations while a nonseparable one would require no more than two. This is illustrated in Figure 22.

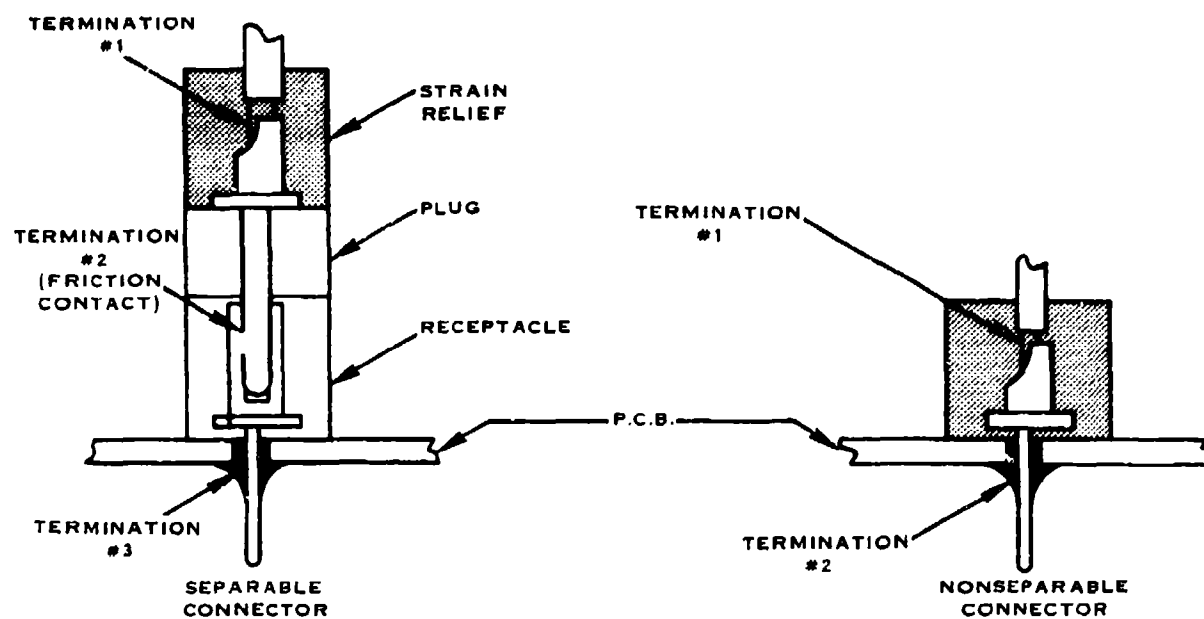


FIGURE 22 SEPARABLE AND NONSEPARABLE CONNECTORS

4.4.3.3 Continued

In terms of reliability, the interconnect design should strive to minimize the number of connections of any type. Signal commonality and grouping to reduce interconnect quantities should be a definite design objective. Generally speaking, there are three basic nonseparable attachment methods: thermal, chemical and mechanical.

Thermal terminations are made either by soldering, brazing or welding. These processes require simple equipment but usually demand high operator skill. Soldering is the most widely used thermal termination method. Brazing is similar but uses relatively infusible alloys such as silver-base materials and copper-phosphor alloys. This method is only practical when temperatures are too high for solder. Welding is occasionally used for connector terminations, but problems generally outweigh the advantages. Properly welded joints are strong and provide excellent electrical connections, but are difficult to repair and inspect. In addition, welding slightly increases the size of the joined materials.

Chemical methods are only used for specialized applications where other methods are inadequate. These include plating, conductive adhesives, and amalgam. Chemical methods are not recommended for high-current applications or high-temperature environments.

Mechanical terminations, the most widely used method for attaching wire to connectors, includes wire-wrap and crimping. Solderless wire-wrap terminations produce a reliable, gas-tight connection that has a large contact area with low contact resistance. The drawback of this method is that the required tooling is critical and must be monitored constantly to ensure reliability.

Crimping is the most widely used mechanical termination method because it requires minimal operator skill, and can produce consistent and reliable terminations at high production rates. Tooling is critical, however, and the right combination of wire, contact and crimping tool is necessary for ensuring a reliable joint. A more rugged crimp joint is possible by selecting contacts which feature two crimps: one for the wire and one for the insulation. A summary of the three most widely used nonseparable connections is presented in Table 10.

Each has its place, but with all facets considered, wire wrap and solder used with stranded wire should result in better system reliability.

TABLE 10
NONSEPARABLE CONNECTIONS

EVALUATION CRITERIA		TERMINATION		
		CRIMP	WIRE-WRAP	SOLDER
RESISTANCE TO ENVIRONMENTS	HIGH TEMP	VERY GOOD	GOOD	ACCEPTABLE
	LOW TEMP	VERY GOOD	GOOD	VERY GOOD
	THERMAL SHOCK	GOOD	GOOD	VERY GOOD
	VIBRATION	VERY GOOD	POOR	ACCEPTABLE
	SALT & HUMIDITY	VERY GOOD	ACCEPTABLE	VERY GOOD
	AGING	GOOD	GOOD	VERY GOOD
MECHANICAL PROPERTIES	PULL-OFF FORCE	VERY GOOD	GOOD	VERY GOOD
	LOW CREEP	VERY GOOD	GOOD	VERY GOOD
	STRENGTH	VERY GOOD	GOOD	VERY GOOD
ELECTRICAL PROPERTIES	LOW RESISTANCE	VERY GOOD	VERY GOOD	VERY GOOD
	RES. STABILITY	VERY GOOD	VERY GOOD	EXCELLENT
	LOW VOLTAGE	VERY GOOD	VERY GOOD	VERY GOOD
	HIGH CURRENTS	VERY GOOD	GOOD	GOOD
ACCESSIBILITY IN ASSEMBLY	LITTLE SPACE REQ'D	VERY GOOD	GOOD	GOOD
JOINING WIRE TO:	WIRE	VERY GOOD	NOT APPLICABLE	EXCELLENT
	COMPONENT	NOT APPLICABLE	GOOD	EXCELLENT
	SEPARABLE CONNECTOR	VERY GOOD	GOOD	VERY GOOD

4.4.4 Cabling

The final element of the interconnect system is the cabling required to complete the communication link internal to the control. Certain design practices should be set up that will be conducive to a reliable cabling system. These may include, but are not limited to the following:

- o Minimize the number of terminations per signal.
- o Incorporate progressive strain relief at each termination.
- o Flexibility to reduce stress on terminations.
- o Environmentally resistant.
- o Preassembly testability prior to attachment to the I/P structure.

Cabling is available in various forms and materials. Some of these are:

- o Stranded, insulated, copper wire conductors
- o Flexible, stranded, insulated, copper wire cable
- o Solid, round, insulated, copper wire conductors
- o Solid, flat, insulated, copper wire cable

The stranded types are the most reliable because of the nature of their flexibility and multiple-strand construction; where solid conductors are poor in that aspect.

Finally, the I/O connector should contain features that make it reliable. MIL-C-38999, MIL-C-5015 and MIL-C-83723 military type connectors contain most of these features and should be considered.

4.4.5 Testing

The success of any interconnect design is enhanced by the ability to test at vital stages of the assembly, starting at the component level and ending with the completed unit. The summarization defines the design features required to do these tests as follows:

- a. The electrical component must have the capability to be fully tested prior to populating the I/P structure.
- b. The active component chip in its carrier should be capable of being burned-in as part of its screening.
- c. The ability to fully test the I/P structure, whether laminate or substrate.
- d. The ability to test each module assembly, whether it be electronic or solely interconnects.
- e. The ability to test the final assembly.

4.5 Material Consideration

The relationship between material selection and reliability is part of the predetermination of which factors promote potential failures. Some of these factors have already been explored in previous sections; such as the selection of PCB material that will minimize delamination and plated-through-hole failures. Other factors can be treated generally, but should be considered during the initial design phase. Rather than attempting to cover all of the possibilities, Table 11 lists the most common failure modes, examples of their causes, and some recommendations.

It is normally assumed that all materials are of "good" quality when the EEC is sent into service; but in actuality, the pre-service environment may cause degradation before service. Degraded or marginal features will fail under exposures less severe than the design limits. Failure of features which exhibit no sign of prior degradation may be the result of inadequate design or exposures in excess of design limits.

As far as nonmetallic materials are concerned, organic materials should be avoided since these are fungus nutrient and impose age control. Connector reliability, as an example, is highly dependent on its non-metallic parts. The insulator material used in most I/O connectors has a great deal of influence on reliability because if it degrades, failures may occur. Nonmetallics are predominant as insulators and should be selected for infinite-life properties at environmental extremes.

TABLE 11
FAILURE MODES

Failure Mode	Causes	Recommendations
1. Low-cycle fatigue	- o Differential thermal expansion - o Pressure (altitude) changes - o Assembly/Disassembly - o Engine transients -start up -afterburner light-off - o Airframe transients -landings -gunfire	The primary defense against the problem of low-cycle fatigue is in anticipating and designing for its occurrence.
2. High-cycle fatigue	- o Vibration - o Acoustics	The normal design is for infinite life with a margin for testable frequencies. Want minimum practicable responses at higher frequencies.
3. Corrosion (leading to fractures)	- o Dissimilar metals - o Contaminant traps - o Inadequate protection - o Sustained high mean stress	A systems approach including design, processing and quality control for initial builds and repair cycles.
4. Corrosion (leading to electrical failure)	- o Incomplete solvent removal - o Incomplete flux removal - o Inadequate general cleaning - o Dissimilar materials - o Ingestion of fluid contaminants	Same as 3 above but in addition an appropriate mounting design and application of barrier coatings.
5. Circuit shorts and/or opens	- o Poor solderability - o Poor solder joints - o Lead/lockwire clippings - o Chips (generated at assembly)	- o Design for ease of inspectability. - o Personnel training and quality control. - o Discourage the use of lockwire internally. - o Use of proper tools and locking features.

SECTION V

RELIABILITY PROGRAM

5.1 Reliability Philosophy

The approach for ensuring that reliability is given proper consideration throughout a program is based on the philosophy that attainment of reliability objectives in products is both a management and a technical responsibility. This doctrine must be reflected in company policy establishing operational directives dedicated to the design and manufacture of equipment to the highest requisite standards of quality and reliability.

Some of the basic precepts and philosophy guides that must be understood and applied are described below.

- a. General reliability. Reliability in the general sense implies a trustworthy and predictable product. Reliability in its specific (i.e., quantitative) sense is the probability of satisfactory performance under specified conditions. The inherent reliability of a product's design tends to decrease as inevitable variations occur in manufacturing, and through the hazards of transportation, storage, operation, and maintenance.
- b. Planning reliability. Reliability is treated as a major factor in product planning, management and engineering. A product's reliability is measured, analyzed and controlled in every step of its design, development, production, logistics, and operational phases. This insures the earliest possible achievement and longest retention of the required operational reliability. One hundred percent reliability is not only unattainable for complex equipment but generally impractical, even as a design goal. Failures are normal and should be expected in testing programs, during the research and development phases and during use phases.
- c. Organizational reliability. The Reliability Organization, in addition to giving the assistance provided by its specialized discipline, monitors and assesses the effect of engineering and manufacturing activity on the reliability of a product. By means of status reports, management is informed continually of the degree of product compliance with customer requirements. The reliability group operates both as a staff and a line organization. In performing consultant-type duties, such as human factors and maintainability analysis, reliability is a staff organization. In discharging project-type responsibilities, such as design review, reliability is a line organization. Higher management levels participate in the direction of the reliability program and are aware of the status of product reliability to the same degree that they are alert to cost and performance factors.

5.1 Continued

- d. Design reliability. The inherent reliability of a product is established and determined by its basic design; maximum reliability effort is applied during this phase. Reliability cannot be improved through manufacturing or usage. Reliability can be maintained, however, at essentially its inherent peak by a planned reliability program covering the entire life of the product. The reliability of production models can be estimated from early research and development tests.

The design engineer is responsible for achieving the specified value of reliability and the reliability engineer offers specialized assistance to help the designer fulfill that responsibility.

- e. Numerical or quantitative reliability. Reliability is a product endurance capability which, quantitatively, can be set as a goal, designed into a product, and subsequently measured and analyzed. Reliability can be predicted, achieved, and maintained by controlling collectively the product elements which determine the product's reliability. The primary elements which determine a product's characteristics and capabilities are its design, manufacture and use. Achieved or ultimate reliability is a measure of the inherent product reliability which results from design and manufacture after decrements due to hazards experienced in subsequent handling, usage, and external environment are subtracted.
- f. Assurance reliability. The reliability group is designated and assigned specific responsibilities and authority for the overall reliability operation associated with company activities such as engineering, testing, manufacturing, quality control, and purchasing. The principal responsibility of the reliability group is to help achieve a level of product reliability quicker and at less cost than would be attained without this assistance.
- g. Control reliability. If the overall reliability effort is not coordinated by using the above guides, some part of the project will tend to be degraded through negligence of a section that is not doing its share to achieve and maintain reliability. To achieve reliability control, administrative operations, such as budget and schedule monitoring, must be provided.

Cooperation between all company disciplines is best obtained by defining the reliability program goals in meaningful terms, and then clearly presenting the scheme of action to all involved in the form of a Reliability Program Plan.

5.1 Continued

The operation of the Reliability Organization is directly or indirectly geared to the reliability requirements specified by the customer. The Reliability Manager formulates the policies and strategies necessary to attain those reliability requirements. The major functional activities provided during the design phase are: component and engineering standards; initial and updated reliability predictions and apportionments; reliability assurance through specialists' support, such as maintainability; and reliability design monitoring through design reviews and Failure Mode Effects and Criticality Analyses (FMECA). The Reliability Organization also provides functional services such as failure diagnosis and corrective action initiation, failure data collection and analysis, and vendor reliability surveillance.

Much of the current reliability philosophy is dictated by the military specifications referenced for a program. Some of these specifications are:

MIL-STD-785A	Reliability Program for Systems and Equipment Development and Production
MIL-STD-781C	Reliability Tests, Exponential Distribution
MIL-STD-756A	Reliability Prediction
MIL-STD-690	Life Test Sampling
MIL-STD-757	Reliability Evaluation for Demonstration Data
MIL-STD-470	Maintainability Program Requirements
MIL-STD-790	Reliability Assurance Program for Electronic Parts Specifications
MIL-STD-1635	Reliability Growth Testing
MIL-STD-1304A	Reliability Report
MIL-STD-1543	Reliability Program Requirements for Space and Missile Systems

5.2 Reliability Design Analysis

Design-reliability analysis is an embrasive term which is used to cover many reliability functions. Among two of the most important of these functions are reliability prediction analysis and reliability design review.

Reliability prediction analysis is a function for assessing the potential inherent reliability of a design. It is attempted as soon as the possible design concepts appear. The analysis reports are updated as the design matures. The reliability prediction analysis is the major reliability input to design and to design review meetings.

A typical initial reliability prediction analysis report on a functional electronics package design contains the following sections:

Introduction. The introduction describes the unit physically and functionally. The use of the unit is explained, and a picture or sketch is included.

Summary of major conclusions and recommendations. This is a vital part of the report. The purpose of reliability analysis is to identify design areas needing improvement and to propose those improvements so that corrective action will be taken.

Reliability block diagram. This diagram shows the function of the unit in the system as well as the major functions of the unit itself. Any circuit or functional redundancy is shown. (The basic drawing prints and circuit diagrams are included in attachments or appendices.)

System-reliability estimation. The analysis leads to a numerical estimate of the reliability of the unit by design and reliability personnel. The assumptions used are listed. These include required operating time, wear-out failure rates, aging characteristics, and nonstandard parts reliability.

Component reliability. Sources of failure-rate data of the unit, the application of these data to the parts of the unit, and the assumptions involved are contained in this section of the report. In addition, this section contains: information support; the failure rates used; reliability analysis of any special non-standard part; a summary of mechanical and rotational stress analyses (if applicable); a description of the method used to determine the reliability of single-shot items (such as explosive devices); identification of all calendar-time- or operating-life-limited items, along with references to provisions for their control; a statement on burn-in policy; and a statement on required procurement controls.

5.2 Continued

Failure-mode analysis. All primary failure modes are identified and described along with the effect of each on system performance. Statements are made on provisions designed to prevent progressive failures; i.e., failures which, in turn, cause other failures.

Production reliability analysis. This section of the report describes special precautions and requirements necessary to maintain product reliability during production. This includes: design definition (documentation) review requirements, use of controlled production environmental requirements (such as clean rooms); special process requirements; special testing and inspection requirements and limitations; and special handling/packaging requirements.

Maintainability analysis. This section contains fault-detection and fault-correction information, accessibility of especially limited-life items, suggested maintenance requirements, suggested service instructions, and logistic recommendations.

Conclusions and recommendations. This section is a summary of all recommendations contained in other sections of the analysis report with a reference to the specific section paragraphs where the detailed information is contained. Detailed, specific recommendations for corrective action are also included.

Design analysis is something less than an exact science, but techniques for analysis of electronic design have been worked out quite well. The mathematical and statistical techniques involved are well known. In general, analysis of electronic design involves: (1) determining the number, kind, and application of electronic parts; (2) selecting (from handbooks or from test data) reliability numbers for the parts; (3) assuming certain sets of environmental conditions; (4) making allowances for derating of parts and for redundancy of circuits; and (5) calculating the inherent reliability of the design. On moderately to very complex designs the computations are usually done on a computer. While not an exact figure, the predicted reliability number resulting from such analysis does provide a rough guide as to whether the design is anywhere near the required level of reliability. Design analyses of functional mechanical, hydraulic, and pneumatic designs are usually less exact; much less test experience is usually available on the parts used. Design analysis on structural designs is usually based upon estimation of safety factors, followed by conversion of these safety factors into reliability numbers through the use of a weighting system.

The reliability number predicted for a particular design as a result of reliability analysis is of special value in comparing alternative design

5.2 Continued

concepts when the relative inherent reliability of the designs being compared is the major purpose of the analysis. The reliability analysis report is often the only central source of complete, early design description with flow diagrams, schematics, operating theory, functional descriptions, predicted failure modes, and similar vital information. As such, it serves a valuable auxiliary communication and coordination function. The reliability prediction analysis report is, along with the design disclosure information (drawings, specifications, and procedures) a major input to the design review. A third basic input is a set of reliability design review checklists completed by the designer.

Reliability design reviews are conducted within the design organization with the reliability engineer scheduling and setting up the meetings, taking the initiative, and publishing the minutes.

The process of achieving high inherent reliability is easier and less expensive in some designs than in others. While nearly any design concept can be converted into a reliable design if enough money, time, and effort are expended, the relative ease (comparing two or more design approaches) with which reliability may be achieved can (and should) be recognized through design reviews. Conceptual design reviews have, of course, a potentially major impact on the design, with successive interim and final reviews having relatively less effect as the design becomes more fixed and less time is available for major changes.

Reliability design reviews should be combined, wherever possible, with other design reviews, such as producibility and maintainability, to minimize the demand on the designer's time and to resolve conflicting recommendations. The following are some of the design-review considerations.

- Review of customer performance requirements
- Review of customer environmental requirements
- Confirmation of use of approved parts in an approved manner
- Circuit analysis and reliability prediction
- Provisions for vibration, shock and other environments
- Provisions for heat transfer
- Provisions for maintainability
- Analysis of potential failure modes and their effects (FMECA)

To summarize, reliability design analysis is a mathematical, analytical method of estimating and predicting the inherent reliability of a design by assigning quantitative values to the components and adjusting these figures for parts population, derating, redundancy and other design factors.

5.3 Mathematical and Statistical Support

Reliability engineering requires the best technical techniques and all of the labor- and time-saving devices that may be available. Quantitative support services provide advanced applied mathematics, statistical and numerical methods of analysis, curve plotting, desk calculating, and application of electronic computers to reliability problems where feasible. Centralization of these services relieves reliability engineers of routine analysis and computing and effects a reduction in cost and time required for such work.

Current reliability prediction, apportionment and measurement operations require the most advanced quantitative techniques. Because it is not reasonable to expect every reliability engineer to have knowledge in depth, a group of specialists are available for mathematical and statistical support. In providing this support, the following individual level assignments are performed:

- a. Quantitative Objectives and Goals. To assure effective and intelligent treatment of reliability data, mathematical and statistical devices are developed and applied. Techniques such as probabilities, confidence limits, distribution forms, factor analyses and correlation are often useful and necessary.
- b. Plan for Effective Quantitative Support. Individual problems must be examined and defined so that the method best suited for solution may be selected. With this best method, engineering calculations must then be solved on computers. Special analytical and mathematical studies must be systematized for current and anticipated problems related to reliability engineering operations. Preliminary categorization of data must be made so that problems of a wide scope may be solved as a whole, rather than treating individual facets of a problem in an unorganized fashion.
- c. Personnel and Facilities for Numerical Services. Techniques and programs must be developed and maintained for solving reliability problems on digital computers. Computer programming to satisfy specific requests must be provided and the library of programs in general use where used. Requests for mathematical and statistical work should be reviewed, approved, scheduled and assigned to personnel best capable of providing this service.
- d. Mathematical and Statistical Services. Advanced mathematical techniques are provided, including the specialized services of operations research, failure analysis, statistical control, and design of experiments. The results of complex mathematical analyses are often best plotted on graphs or charts, or otherwise

5.3 Continued

presented in visual form or in analytical reports. To further aid in this effort, work on quantitative techniques is performed continuously to increase the knowledge and proficiency of reliability and design engineers.

Quantitative research has developed methods by which computers and computer techniques benefit reliability prediction, apportionment, measurement and analysis. This effort is directed toward developing a computer program in anticipation of certain classes of general problems. A variety of mathematical and statistical techniques are used to suppress personal predilection toward a particular technique.

- e. Quantitative Results. Problem solving results must be interpreted with caution and reserve. Reliability efforts usually deal with samples and the conclusions drawn are valid only if the samples are truly representative. Inferences from sample data must be examined for validity in relation to the statistical technique used. Results of the mathematical and statistical specialists aid must be analyzed to insure that quantitative efforts are valid, reliable and objective. Validity refers to the extent a quantitative technique actually measures what is intended to be measured. Reliability (in a computational sense) involves the degree to which a product has the same value or rank regardless of the circumstances of the measurement. Objectivity refers to obtaining the same quantitative results when computed by different people.
- f. Reduce Product Measurement Deficiencies. Mathematical and statistical techniques must not be used to hide the absence of ideas nor to make the obvious seem profound and scientific. An essential need in reliability engineering is to formulate quantitative problems and investigations revealing functional relationships in product performance and endurance traits. Mathematics and statistics are tools to achieve an end, and are not objectives in themselves. Common sense, and even scientific insight, are required to decide when statistical methods have led to a valid answer.

5.4 Failure Mode, Effects and Criticality Analysis (FMECA)

5.4.1 General

The failure mode, effects and criticality analysis is an important technique to evaluate the potential reliability of new designs and design modifications. As such, it is an integral part of the early design process and is also a major consideration in design reviews. It is important to sustain the FMECA effort during all phases of design and development.

5.4.1 Continued

The objective of the informal FMECA is to highlight all potentially critical failure areas so that the probability of such failures is eliminated; or so that the criticality of such failures is compensated for through the basic system design. During the FMECA, each potential failure mode is considered in light of probability of occurrence and evaluated with respect to its probable effect on the safety of the pilot, aircraft and engine. The information and data developed during the FMECA is also used as an aid in proportioning the design effort for corrective action and reliability control of the system design.

For most programs, the FMECA is started during the early system-level phase and continues until the system block design has been implemented at the piece-part level.

The FMECA is usually performed on the basis of a single failure mode, but should also consider many of the cases where multiple failures may be potential hazards to system safety. For example, this effort would include the case where a component failure would not be detected until another component failure has occurred. Such failure modes might occur internal or external to the engine control.

The appropriate schematics and system diagrams are developed during the design and development phase of the program to facilitate the FMECA. To optimize the results of the analysis, supporting documentation from other design disciplines such as thermal, stress and vibration, parts application analyses, etc. are factored into the study of the potential system hazards.

An example of the typical FMECA format and analysis is shown in Table 12. The guidelines for performing an analysis, and the type of information normally found and displayed, are described in the following paragraphs.

The subject material included in the FMECA is briefly stated by the column headings shown in the example. The information used for the analysis is:

Item Number
Item Description
Failure Mode
Probable Cause
Failure Effects
Detection Method

5.4.1 Continued

Compensating Features

Criticality Class

Probability of Failure

- Class
- Source

Remarks

Each of the above categories is fully documented.

5.4.2 Item Number and Item Description

5.4.2.1 System FMECA

If the engine control is configured as two redundant control channels with separate input signals and output commands, this configuration should provide for high probability two-fail operate protection for all critical control functions. The primary objective of the system level FMECA is to ensure that common-mode system failures do not exist within individual channel equipments, between system interfaces and the system at large; i.e., one failure cannot take out more than one channel, and very high confidence that two failures cannot take out both channels. The system FMECA ensures that the two-fail operational objective has been attained to the probability of success established in the program.

The item number and item description are keyed to the schematics and system diagrams to identify the specific item which is being analyzed. If a schematic shows more than one unit of a given item number, FMECA will show a corresponding separation. Each separate item identified on a schematic or diagram will have at least one line entry on the FMECA. If an item is used in an identical application with no dissimilarities, the line entry will show the item number and reference the prior analysis. The item descriptions are correlated with the schematic or diagram descriptions.

5.4.2.2 Component Parts FMECA

Each component part which is considered during the FMECA is given at least one line entry with the item description given by a parts list. The same guidelines as described in the system FMECA are used. The remarks column is used to note the fact that several identical items are used in the assembly. If the applications differ in any way, a separate line entry is required.

5.4.2.2 Continued

The FMECA analysis should attempt to structure the logical sequence of the FMECA presentation for readability, ease in referencing and cross referencing, and for ease of understanding system performance. A decimal numbering system is used to aid analysis organization.

5.4.3 Failure Mode

The failure mode to be considered for the item analysis is stated a priori in this column. For each item, the analysis includes every reasonable, possible mode of failure. Two or more modes are usually considered for complex items. If an assumed failure mode does not apply to the complete item, the state of the exact point of failure is given. Assembly-caused failure modes will be included if they are not detectable by inspection subsequent to assembly.

5.4.4 Probable Cause

The probable cause or causes of each failure mode are identified. A separate line is used for each probable cause.

5.4.5 Failure Effects

The effect of the failure mode under scrutiny upon the component and system is identified. The description given will be as clear and complete as is practical and will take particular notice of any sequential effects induced by the failure mode under consideration. Pilot notification will also be indicated.

5.4.6 Detection Method

The method or methods by which the failure mode can be detected are stated. The methods will reflect both internal and external tests.

5.4.7 Compensating Features

Any compensating design features or system operating procedures which can counteract, nullify or override the effects of the failure mode are identified. This information includes such features as standby modes, auxiliary systems, alternate modes of operation, etc. In addition, the information will state whether the compensating features are total or partial and whether the compensating features result in reduced performance capability.

5.4.8 Criticality Classification

Failure modes will be categorized as to their probable effect on safety and mission success. The following classifications stated in MIL-S-38130 are used:

5.4.8 Continued

Class I - Safe (Minor)

This classification is used when a safe condition exists such that personnel error, design deficiencies or component malfunction will not result in a major system hazard or degradation, and will not induce system functional damage or personnel injury.

Class II - Marginal (Major)

This classification is used when a condition exists such that personnel error, design deficiencies or component malfunction will degrade system performance but which can be counteracted or adequately controlled without major damage to the system or personnel injury.

Class III - Critical

This classification is used when a condition exists such that personnel error, design deficiencies or component malfunction will degrade system performance resulting in personnel injury, substantial system damage, or in a hazard requiring immediate corrective action for personnel or system survival.

Class IV - Catastrophic (Critical)

This classification is used when a condition exists such that personnel error, design deficiency or component malfunction will severely degrade system performance and cause system loss or death or multiple injuries to personnel.

5.4.9 Probability of Failure

Parts will be analyzed as to probability of failure. If the failure rate is available, it will be used to indicate the magnitude of the potential hazard. In addition, the source of the failure rate will also be given. If failure rate data is not available, the following subjective classification will be used to approximate the failure probability:

- a. Probability of failure is not remote.
- b. Probability of failure is remote.
- c. Parts are subject to rare, random failures.
- d. Parts are not expected to fail in service.

5.4.10 FMECA Report

The FMECA records and data sheets should be accumulated as the analyses progress and maintained in a central file so that the material can be used by the systems and equipment designers to evaluate and compare alternate designs.

5.5 Failure Analysis

Failure analysis is the diagnostic examination of products for a better understanding of failure modes, failure mechanics, and failure patterns so that preventive or corrective action may be instituted. In conducting failure analyses, the following individual level assignments are performed.

5.5.1 Establish Failure Analysis Purpose

The primary purpose of failure analysis must be defined in terms of diagnosis leading to correction of departures from normal behavior in products of proven design. In some cases failure analysis may disclose the need for redesign but this should be the exception rather than the rule. If the converse were true, failure analysis simply would be a poor and untimely substitute for the correct analytic work that should take place prior to first article fabrication. As a secondary consideration, failure analysis definition must recognize the evolutionary nature of a product in that disclosure of failure patterns points the way for the most profitable areas of product improvement.

5.5.2 Develop Failure Analysis Techniques

Procedures and methods must be formulated to speedily and decisively establish product weaknesses such as improper parts selection or application, careless workmanship, or deficient operation and maintenance. Procedures must be developed not only for initially finding sources of trouble, but also for substantiating these findings through verification tests and continued surveillance of changes. Unless acceptable limits of product parameters are defined, there are not criteria for identifying a deviant condition or function; false diagnosis will result, and truly serious conditions will be overlooked. Procedure development must be directed mainly toward the massively recurring problems, but must not overlook the isolated, serious discrepancies. A failure analysis manual must be prepared for training purposes and to serve as ready reference in the conduct of failure analyses.

5.5.3 Failure Analysis Requirements

Before failure analysis is attempted, the following material must be available:

5.5.3 Continued

- a. Test, operation or maintenance procedures which detail the intended uses and stresses to which the product is subjected.
- b. Case history of the product being analyzed giving information about its design, fabrication, installation and employment.
- c. Results of previous analyses on related or similar products.
- d. Drawings, schematics, and specifications which describe the functional, structural and organizational aspects of the product.
- e. Diagnostic material, equipment and facilities such as plastic embedding compounds, microscopes, x-ray machines, and temperature boxes.
- f. Forms, checklists, analysis manuals and general instructions for conducting failure analyses and for subsequent reporting.
- g. Technicians who are trained and skilled in the procedures of nondestructive and destructive failure analysis.

The failure analysis screening committee must categorize each reported failure according to the degree of seriousness -- critical, major, or minor. Diagnostic action should desirably be initiated for all three categories, but is essential for at least the critical and major failures. If not diagnosed, minor failures must be monitored for indications of becoming more serious.

5.5.4 Conduct Failure Analysis

The purpose of analysis is to establish the cause and mechanism of failure. This is accomplished in the following sequence:

- a. Failure diagnosis begins by careful disassembly of the equipment to preserve any evidence that may prove to be of subsequent value. All unusual findings are recorded. Failed items are packed carefully and carried or sent to the failure diagnosis laboratory.
- b. In the failure diagnosis laboratory nondestructive examinations are performed by visual examinations, x-ray, Zyglo and microscopic examinations. Photographs are taken of the failed item to be used in future appraisal and subsequent documentation.
- c. Destructive analysis or testing is performed by using such practices as: immersion in dye penetrants to disclose the possibility of

5.5.4 Continued

leakage or cracks; embedding the test item in plastic and sawing the sample; or spectro-analysis. Each action and the results obtained are carefully recorded.

- d. All findings and procedures of the investigation are documented in a written report. Also included in the report is background information relating to the history of the failed equipment with special attention given to any similar or related failures on equipment of this type.
- e. A summary of possible reasons for failure is prepared and included as part of the report. Also contained in the summary are recommendations for corrective action, if considered necessary.

5.5.5 Document Failure Analysis Results

The findings of each failure analysis must be documented and placed in a serially numbered file to facilitate processing and retrieval. When additional failures are analyzed and found to be similar to a condition previously examined, the new analyses are added to the file as supplementary material. Supporting information and data, such as photographs, x-rays, recordings and spectrographic films are placed in the proper failure analysis file. The original copy of the document that triggered the failure analysis activity and the applicable drawings and specifications used in the analysis are also put in the file. Each failure analysis file is then complete and self-sufficient; this eliminates searching for material that might otherwise be lost or destroyed.

A failure analysis summary report, issued either weekly or monthly, provides a status summary of each analysis. The summary report includes the serial number of the file, a brief description of the problem, the findings to date, and the status of the analysis. The status includes failure analyses appearing for the first time, continuing current analyses, analyses referred to an outside agency, analyses deferred and waiting further inputs, and analyses completed and being closed out.

The number of man-hours and expenses spent on failure analyses must be documented and an average cost and time value per analysis calculated to serve as a reference value for management consideration.

5.5.6 Corrective Action Loop

Once the cause of and responsibility for an item malfunction has been determined, positive steps must be taken to assure that the information is used to eliminate the problem and prevent recurrence of the malfunctions. Responsibility should be assigned to an individual within the organizational element to which the corrective-action responsibility will be assigned. One useful technique used to monitor corrective action and recurrence control measures is the Corrective Action Log. The Corrective Action Log is a management report listing all known reliability (and other) problems with recommended solutions. The log identifies personnel who have been assigned responsibilities for the particular problem corrective action. The log is updated and published on a regular basis -- weekly, monthly, or even daily in some critical situations. No entry is removed until the corrective actions have been accepted.

When a significant reliability problem has been identified, as a result of an item's malfunction or failure, the problem should be logged and assigned either to the cognizant design group, or to the failure analysis group. The latter assignment is usually preferred, since malfunctions are commonly caused by defects in manufacturing and/or operator error. The analyst should consult with the design and manufacturing personnel as necessary to establish the facts. After the analyst has made his recommendations on solution of the problem, the responsibility is transferred to an "action" man in design or manufacturing. The "action" man is not bound to accept the recommendation of the analyst. His responsibility is to provide an acceptable solution.

Corrective action is not complete until the corrective action has been implemented and has been proven to be an effective problem solution. If the action is ineffective then the original problem must be reassessed, and a revised solution must be developed to correct for the inadequacy of the corrective action(s).

5.6 Maintainability Design Concepts

Reliability as represented by failure rate establishes the frequency of maintenance activity. Maintainability, however, is concerned with the time, ease, cost, manpower, facilities, etc., required to restore a system to operational status.

5.6.1 Maintainability Parameters

Because of the many facets of maintainability, the development of a single, all-encompassing figure of merit is not feasible. Instead, a series of parameters are needed to describe these multiple maintainability characteristics. This point is further verified by reviewing the various consequences

5.6.1 Continued

relating to maintenance performance. In a broad sense these include primarily: (1) cost, and (2) operational availability. These, in turn, may be related to lower-level measures such as man-hours, downtime, and spares cost. The discussion presented here will be devoted to providing some detail concerning the more important maintainability-time parameters.

A problem associated with maintenance measurement stems from its dependence upon the design, personnel, and support factors. Of these, design is the only one in the operational environment which remains essentially constant, while personnel and the support environment are susceptible to continuous change. With these variable conditions prevailing, it is not possible to cite specific values; instead, the most probable estimate made must be accompanied by statements concerning the expected variation which the parameter may take. These estimates must be further conditioned by details concerning personnel and the support environment associated with maintenance requirements.

5.6.2 Maintenance Concepts

Maintainability is a system characteristic concerning the facility with which a maintenance task may be accomplished. A maintenance task is an action or series of actions (manipulative or cognitive) required to preclude the occurrence of a failure or to restore an equipment to satisfactory operating condition. Maintenance actions may include the following:

- 1) Assembly and disassembly.
- 2) Inspecting, testing, and measuring (diagnosis and localization).
- 3) Removal and replacement (repair).
- 4) Checkout.
- 5) Cleaning and lubrication.
- 6) Securing materials (supply).
- 7) Preparation of reports.
- 8) Contingency items.
- 9) Administrative duties.

Actions identified in 1 to 5 are considered productive, and time spent in their accomplishment is classified as active; whereas the remaining elements are nonproductive and are denoted as delay-time requirements. Within the active elements, item 2, (inspecting, testing, and measuring) has been found to be the largest contribution to active time for electronic systems investigated. Hence, during the system design, features of equipments which influence this element, such as test points and indicators, must be given careful consideration.

5.6.2 Continued

A maintenance task can result for two basic reasons defined as follows:

- a. Preventive maintenance. That maintenance performed to keep a system or equipment in satisfactory operational condition by providing systematic inspection, detection, and correction of failures before they occur or before they develop into major failures.
- b. Corrective maintenance. That maintenance performed on a non-scheduled basis to restore equipment to a satisfactory condition by providing immediate correction of a failure which has caused degradation of equipment performance.

Preventive (scheduled) and corrective (unscheduled) maintenance can be performed at several locations with respect to the system deployment, depending on the maintenance concept employed. Several concepts are identified as follows:

- 1) Repair in place.
- 2) Remove, repair, replace.
- 3) Remove, replace with spare, repair at base.
- 4) Remove, replace with spare, repair at factory.
- 5) Remove, replace with spare, discard defective package.

Each of these concepts may be further modified depending on the lowest unit of repair or replacement designated by the concept; this may include part, module (component), subassembly, black box, equipment, and/or redundant system. The choice of the appropriate concept and the unit of replacement is primarily one of economics, but in certain situations strategic implications must be considered. Factors of concern in the selection include failure rate, spares cost, inventory cost, transportation cost, maintenance-facilities requirements, system deployment, test-equipment requirements, and other factors which may influence cost or strategic implications.

No specific recommendation can be made concerning which concept forms the best approach, since each situation must be examined individually by relating the cost to the strategic factors.

5.7 Training

The purpose of reliability training is to establish and carry out personnel upgrading programs for informing and orienting employees, subcontractors and vendors so they may more effectively contribute to the design and manufacture of a reliable product. The employees to whom the training program is directed

5.7 Continued

should encompass all levels of the organization: from management, down to individual production workers.

Reliability education consists of formal and informal training to improve reliability knowledge and to make everyone more reliability conscious. Education programs should present both reliability techniques and concepts. Formal methods used in reliability training are: lectures; local and national seminars, such as Government Microcircuits Application Conference (GOMAC); national symposia, such as the annual Reliability and Maintainability Symposium; newsletters; published articles; and training movies. Comprehensive and clearly written training manuals which present reliability engineering principles and practices play an important part in the training program.

Educational programs aim not only at training in reliability techniques but also in convincing personnel that these techniques should be an integral part of their everyday work. Additional, educational programs point out the benefits of increased profits, savings and corporate prestige attainable through consistent application of reliability principles and practices.

Training classes, seminars, discussion groups, movies and the display of bulletins and posters must be provided. Reliability training material must be presented clearly and patiently, with key points being stressed or repeated. Each topic should be presented as a unit and then summarized. Training programs must develop an understanding of, and consequently, a desire for a reliable product in terms of both the corporation and the customer. Misconceptions about reliability engineering often must be first cleared away before a receptive attitude is formed.

Employees must be provided the tools and techniques needed through the training program to best accomplish their portion of the overall reliability goal. Continuing educational programs must be provided to assure the absorption of existing techniques, plus training in newly developed techniques. New personnel also must receive proper training to insure proper induction into the team effort striving for the accelerated attainment of a reliable product. Individual employees must be informed about the overall concept and significance of the reliability program and about their part in the successful completion of this program. Long-range objectives must be broken down into short-range goals with each problem area treated as a unit in the training program.

5.8 Derating

Derating is defined as the operation of an item at less severe stresses than those for which it is rated. In practice, derating is accomplished by either reducing stresses, or by increasing the strength of the part, or both. Selecting a part of greater strength is usually the most practical approach.

Derating is effective because the failure rate of most parts tends to decrease as the applied stress levels are decreased below the rated value. The reverse is also true. Derating is done as necessary to assure that the required equipment reliability is within specification. As a general rule, derating should not be conservative to the point where costs rise excessively. Neither should the derating criteria be so loose as to render reliable part application ineffective. In those instances where the required degree of reliability still cannot be met after practical consideration of derating, the designer invariably resorts to redundancy.

SECTION VI

TESTS TO ENHANCE RELIABILITY GROWTH

6.1 Introduction

This section of the Development Guide addresses the implementation of reliability tests and screens designed to enhance the reliability of electronic hardware intended for use in an environment identified as hostile due to its high vibration and temperature levels; conditions germane to an aircraft engine mounted application. The testing program structured herein emphasizes the performance of reliability tests at the key points of development and production cycles. Among the key points identified are the selection and screening of piece parts, fabrication and test of both polyimide and ceramic-substrate multilayer printed circuit boards, subassembly or module level screening and end-item level acceptance testing.

During the development, or preproduction, phase emphasis is placed upon the establishment of those screening and testing conditions which will be the most effective in ferreting out defect and/or marginal parts and assemblies during the production cycle. From various industrial reports on the subject of reliability testing, the single most effective screen at all levels of assembly is thermal cycling. All agree, however, that the optimum conditions of the thermal cycle screen (its rate of change, temperature range and number of cycles) are dependent upon the packaging and component mix of the equipment to be screened; the processes involved with its manufacture as well as the facilities where it is manufactured influence the behavior of the equipment to a degree sufficient to also affect the selection of thermal cycle parameters.

From reference (47) an approximation of the categories of failures detected in mature hardware through AGREE* testing is:

Design marginalities	5%
Workmanship and Process Related	33%
Faulty Parts	62%

*Advisory Group on Reliability of Electronic Equipment

6.1 Continued

It is further asserted that the temperature soak and low level vibration (usually 2 g's sinusoidal) portion of the AGREE test cycle play a minor role in screening effectiveness causing the AGREE test method to be "... essentially equivalent to a temperature cycling test dependent on the temperature range, the temperature rate of change, and the number of cycles".

Other reports, such as those prepared by Hughes Aircraft (48), General Dynamics (49), and Lockheed (50), contain summaries heralding the effectiveness of thermal cycling in enhancing the reliability of most any type of electronic equipment. The Hughes Aircraft report, for example, cited results of thermal cycling which included "... a 50% reduction in failure rate due to board stress testing..." at the end-item level, a "... 25% reduction at AGREE test...", and a "4 to 1 reduction in failure rate at customer receiving inspection".

The General Dynamics report concluded that "fifty percent overstress testing is 5 times more effective.... than specification level testing", and "random vibration is 2 times more effective... than specification level testing", and "random vibration is 2 times more effective... than either high or low temperature testing".

Therefore, the following general rules were applied in the development of the test program defined herein.

A rational degree of flexibility must prevail throughout the test program commencing with the screening of piece parts and proceeding through the end item level acceptance test. Screens that produce no results should be discontinued while, at the same time those that continually produce meaningful results should be retained. As defect trends or failure modes are identified through testing and eliminated through follow-up recurrence control measures, it may be necessary to modify the conditions of the screen or impose an entirely different screen to assure reliability enhancement. The ability to alter the test program in a cost effective manner and essentially at will to the benefit of the ultimate customer in terms of equipment longevity and failure-free operation should exist.

The worth of a set of screens at a given component or assembly level is to be measured and evaluated directly from test results at the next higher assembly level. This approach provides the degree of interaction between test levels necessary to allow the continuity and effectiveness of the overall test program to surface. The general idea is to screen defectives out at the lowest testing level possible.

6.1 Continued

The test program should be designed to increase, not measure, reliability. This means the test conditions should provide a stress of sufficient magnitude so as to isolate "weak sisters" and be performed on a 100% basis. Any consistently failure-free test or screen is an immediate candidate for discontinuation. Further, the "test-in" reliability approach should require the shortest time feasible in order that the effectiveness of the overall program may be under constant appraisal. Measurement of reliability testing similar to that of MIL-STD-781 is extremely slow, very expensive, usually conducted on a minimum number of units and carries the stigma where, in the results, any failure poses a liability.

6.2 Piece Part Screening

The objective of 100% screening at the piece part level is to weed out infant mortality plus latent defects comprising the "freak" distribution defined in method 1016 of MIL-STD-883B. While the majority of infant mortality defects are screened out through the 100% process conditioning specified in Established Reliability procurement specifications (i.e., MIL-R-55182) and other military standards (i.e., MIL-STD-883), additional screening, generally accelerated, is required to adequately screen out those latent defects which manifest themselves as higher assembly level testing. Since these failure modes must first be identified, it is necessary to perform accelerated testing on samples of individual piece part types and families within types to establish the optimum accelerated conditions which will efficiently manifest those modes at the part screening level; i.e., through a 100% accelerated burn-in. The reliability of the balance of the lot, having been screened through these accelerated burn-in conditions, is thereby greatly enhanced.

The following paragraphs address the recommended test programs per basic piece part (reference 47) type. It must be recognized, however, that the part manufacturer may have conducted similar tests on his devices. Once ascertained, the test results should be evaluated in terms of commonality and applicability to the programs outlined herein. Should the manufacturers data adequately satisfy the requirements stated, both quantitatively and statistically (i.e., variance analyses, goodness of fit, Arrhenius plots, Eyring equations, etc.), his accelerated test conditions should be incorporated in the interest of economy.

6.2.1 Integrated Circuits

Test guidelines pertaining to piece parts emanating from the NASA sponsored studies conducted by Martin-Marietta (47) are listed below with some commentary.

6.2.1 Continued

Integrated Circuits

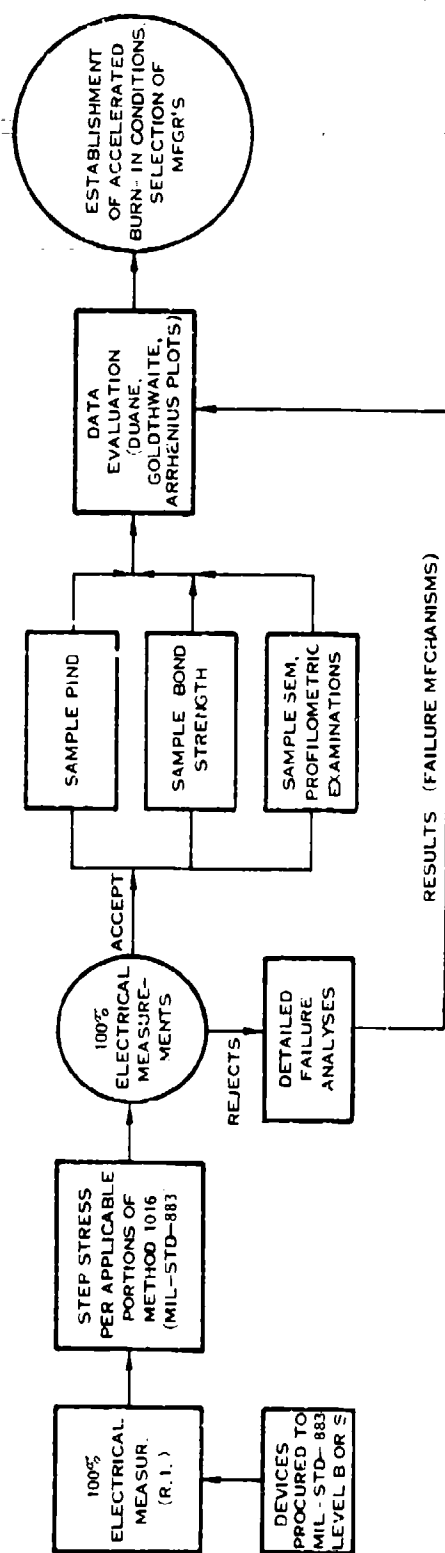
- "1. 100% electrical testing and burn-in for a minimum of 240 hours is mandatory for screening out defective devices. For programs requiring the highest reliability, consideration must be given to burn-in for longer than 240 hours, or at higher temperatures, because the internal elements of integrated circuits cannot be stressed to their rated capability."

It is their consideration to burn-in at higher temperatures that is of primary interest in this reliability enhancement study. As found in other independent studies (references (51) and (52)) accelerated or high temperature burn-in is an effective means of culling devices containing latent infant mortality related defects (termed "long term failure mechanism") from a lot or lots of integrated circuits. Again, the rule that processes, facilities, etc., involved with its manufacture influence the reliability of the end item, here, a device, applied making it necessary to evaluate each device type and/or manufacturer contemplated for use in the production of a black box systems element.

During the design and development phase, the accelerated screening criteria are to be developed on a per device level (Figure 23). Commencing with the procurement of integrated circuits screened to at least level B of MIL-STD-883, each device type is to be subjected to step stressing per applicable portions of method 1016 of MIL-STD 883 the stress conditions of which are to be selected as a function of device type/technology. The performance of PIND, Bond strength testing and Scanning Electron Microscope examinations on a sample basis plus detailed failure analyses on all step stress test rejects will identify problem manufacturers and device failure mechanisms. Collectively, these results including evaluation of step stress testing, are the tools with which the initial conditions of procurement, accelerated burn-in, and additional screening of detailed parts are to be structured for production builds.

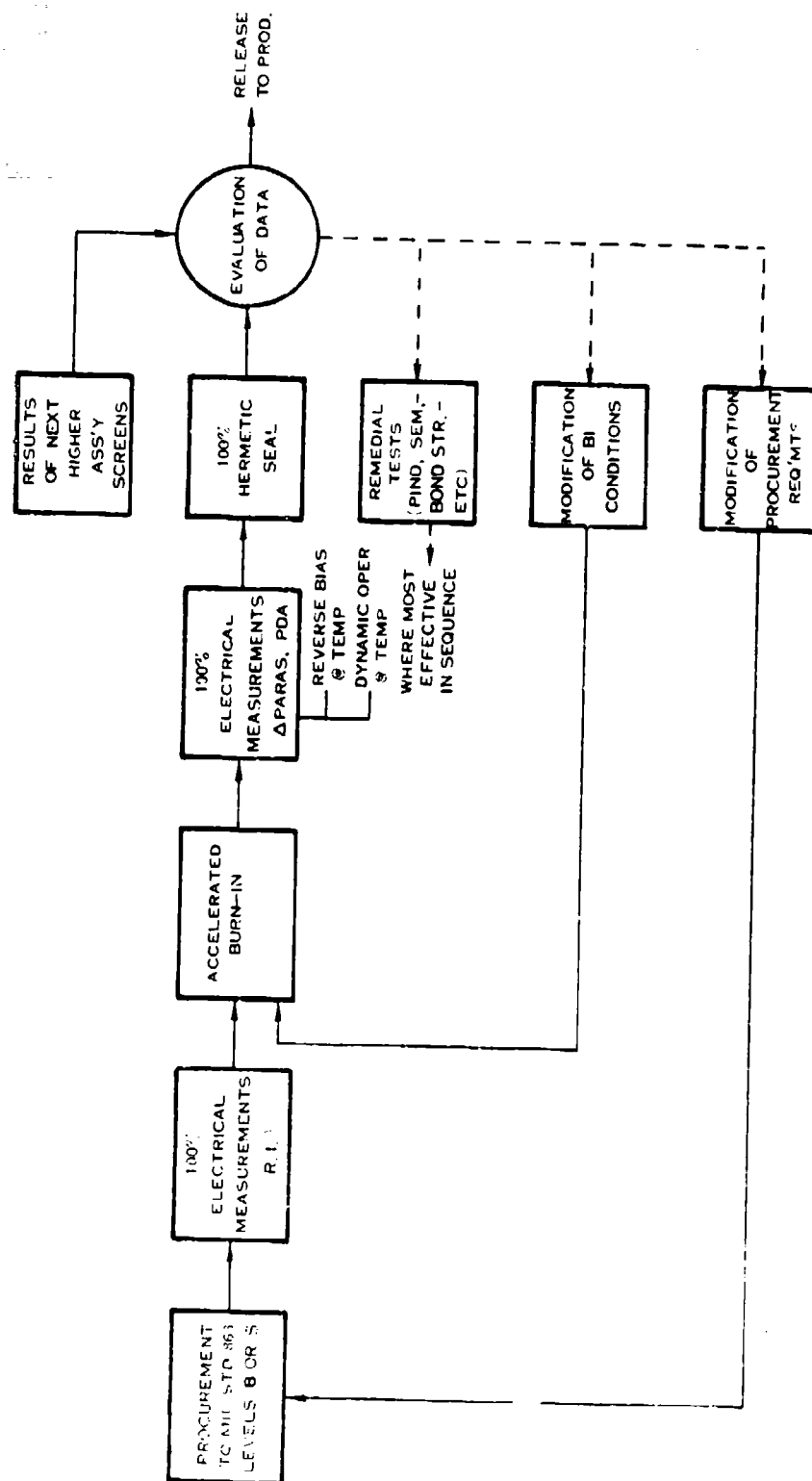
The resulting screening program applicable to integrated circuits during the production phase of the program is depicted in Figure 24. The highlights of the screening program are the continuous evaluation of the screening against yield information derived from next higher level testing, and the flexibility of the screening program in responding to changes in requirements brought about by lot variations, change in sources, etc., usually during a long term production run.

- "2. 100% Pre-cap visual inspection to standards superior to that required by MIL-STD-883 is required to detect time-dependent failure mechanisms resulting from scratches, pin-holes, residues and improperly controlled processing."



E-5675

FIGURE 23 ESTABLISHMENT OF ACCELERATED BURN-IN CONDITIONS (DESIGN AND DEVELOPMENT PHASE, FOR INTEGRATED CIRCUITS)



E-5704

FIGURE 24 100% SCREENING OF INTEGRATED CIRCUITS DURING PRODUCTION PHASE

6.2.1 Continued

The latest issue of MIL-STD-883 contains a more stringent pre-cap visual inspection than the issue in existence during the preparation of the NASA study, however, the test condition applicable to level "S" is more rigorous than that of level "B". Depending upon program needs or in-house test results it may be necessary to impose condition "A" internal visual inspection requirements when procuring to MIL-STD-883 level "B" specifications.

- "3. 100% bond pull testing is currently quite controversial, but is recommended herein because it is being successfully performed by Autonetics, Fairchild, and others, and without evidence of the possible degradation postulated by the companies that have not investigated and adopted this technique. Bond pull tests are needed since the acceleration and shock tests do not detect bad bonds because of the very small mass of the wire involved."

100% bond pull testing remains a controversial issue today and should be imposed only when considered remedial.

- "4. Submit a wafer sample from each metalization run to a detailed scanning electron microscope inspection to assure uniform and continuous metalization over window cuts and oxide steps, to avoid undercutting and water fall effects from oxide etch, to detect oversintering, and to verify mask alignment. Inspection at the wafer level is the most economical point in the process sequence for performance. Screening tests are not 100% effective in detecting these faults and further costly processing is avoided."

This is not considered cost effective at the system manufacturing level due to the fact that a single order placed may be filled by integrated circuits from a number of different metalization runs. A more effective utilization of the SEM screen by the systems house would be to conduct SEM inspections on sampled devices as part of his part/manufacturer evaluation program.

- "5. Submit a wafer sample from each metalization run to a profilometer test to verify metalization thickness and avoid electromigration problems."

Same observation as indicated for SEM above.

- "6. Perform the qualification tests of Group C in MIL-M-38510 in sequence on the same group of parts as opposed to performing the tests in parallel. This will impose the additive effects of environments that are more realistic to real life use. Also, the screening effectiveness can be evaluated."

6.2.1 Continued

As defined in MIL-M-38510, Group C is a periodic inspection not usually conducted on each lot. When conducted as part of the qualification procedure, the qualification approved status is valid for a period of 12 months, during which requalification is not required. Therefore, the value of performing the Group C tests in sequence as opposed to parallel is questionable when considering overall contribution. A further opposing argument is the limited availability and related high cost of fully qualified integrated circuit types. Systems manufacturers, due to these cost and availability considerations, tend to procure integrated circuits from reputable houses to industrial standards, process through MIL-STD-883 screening and qualify them by next higher assembly.

A more meaningful recommendation, or test guideline, would have been to include a more stringent thermal cycle test on each lot produced in light of the general finding of the study regarding the benefits of accelerated thermal cycling.

6.2.2 Discrete Semiconductors

- "1. A 100% nondestructive interconnect wire pull is recommended to eliminate defective wire bonds. Sound bonds will not be degraded."

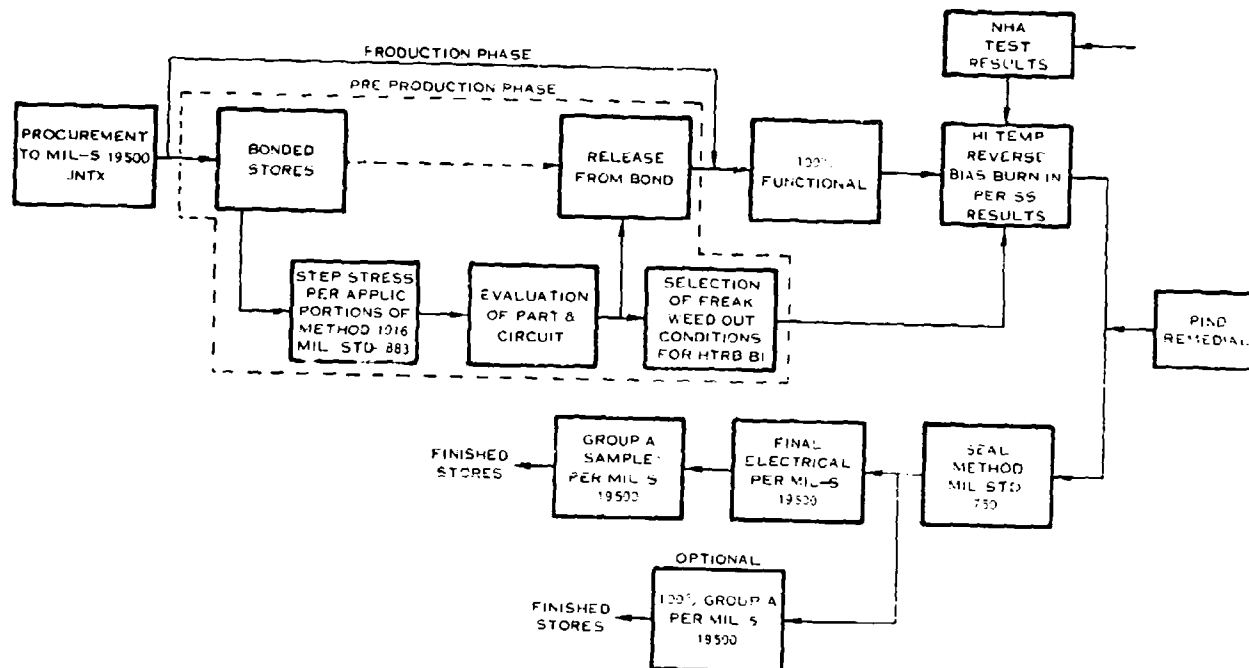
While the worth of such a screen is undisputed, an alternate approach would be to impose both forward and backward instability shock tests as required for JANS devices, due to the rather high cost of performing 100% bond tests.

- "2. A rigorous pre-cap visual inspection of the die and header assembly is essential to eliminate common assembly defects. Perform die inspection (preferably at the wafer or die level) to eliminate defective die."

Procurement to either JANS or JNTXV levels of MIL-S-19500 would fulfill this requirement. Where reliability requirements warrant, the pre-cap visual examination should be to MSFC 85M03924 criteria, incidentally, at any reliability level.

- "3. Screening tests on 100% of the parts, which include burn-in, HTRB, thermal cycling, mechanical shock, hermeticity, and parametric tests are essential to eliminate defective parts."

Procurement to JANS level of MIL-S-19500 fulfills the above; however, the above test series does not adequately address "freak" distributions, the elimination of which is essential for reliability enhancement. Figure 25 depicts the screening flow for discrete semiconductors during production and preproduction phases designed to weed out the "freak" distribution. Again, the screening conditions to be applied during the production phase are those



E 5002

FIGURE 25 100 % ACCELERATED SCREENING FLOW FOR DISCRETE SEMI-CONDUCTORS

6.2.2 Continued

identified through step stressing discretes during the preproduction phase. Results of next higher assembly (NHA) level testing, i.e., module, are to be factored into the high temperature burn-in conditions such that a high degree of efficiency may be maintained during the part screening exercise.

While procurement to JANS level of MIL-S-19500 fulfills the above requirements, cost and availability of level "S" devices may be prohibitive particularly since latent defects that may remain still must be screened out. Subjecting JNT devices to additional screening assures availability, lower initial cost, and control over the screening exercise.

6.2.3 Tantalum Capacitors

As stated in reference 47, tantalum electrolytic capacitors are less reliable than other types. In the case cited therein, of 4622 capacitors used, the 6 failures involved only tantalum. No differentiation between solid and nonsolid electrolite devices was made. The test guidelines included in reference 47 are discussed below for both solid and nonsolid tantalum types where type designations are pertinent.

- "1. Tantalum capacitors should be qualified to the requirements of MIL-C-39003 or MIL-C-39006 level P, as a minimum. Additional program-peculiar requirements should be added as required."

Present QPL listings suggest level R requirements be selected as a minimum due to their availability; i.e., from more than one source. There are a few exceptions, however, where the minimum of level P would apply to avoid single sourcing.

QPL-39003 (Solid Tantalum)

Types CSR33

QPL-39006 (Nonsolid Tantalum)

Types CLR79

(Single sources only exist for the following types - CLR10, 14, 17, 69, 89 usage of which, therefore, is to be discouraged until second sources have qualified.)

- "2. Radiographic insepection on 100% of the devices should be made in accordance with more comprehensive inspection criteria such as in MSFC-STD-355 to detect anomalies more effectively."

6.2.3 Continued

(Applies only to solid tantalum capacitors.) The 100% radiographic examination criteria of MIL-C-39003 is considered adequate for aerospace programs excluding extended duration manned space expeditions. The implementation, however, of the more comprehensive radiographic inspection criteria of MSFC-STD-355 would be beneficial as a remedial action.

- "3. Burn-in should be increased to a minimum of 240 hours at rated voltage at 85°C with tight delta limit criteria. Stability is an indication of reliability and present durations are not sufficiently long to detect all parts with instabilities. Read and record measurements of capacitance, dissipation factor, and leakage should be made before and after burn-in on 100% of the devices."
- "4. Accelerated tests are applicable to solid tantalum capacitors. Caution is required in applying these techniques to foil or wet slug capacitors as electrolyte breakdown may occur at relatively low voltages creating a new failure mechanism."

The burn-in criteria of current issues of MIL-C-39003 and MIL-C-39006 remain inadequate. But to improve the burn-in and then perform accelerated testing which ultimately reflects back to the burn-in criteria is less time efficient than conducting a component evaluation program employing step stress testing to arrive at an optimum burn-in.

The fact that low temperature (circa 182°C) solder is used in the manufacture of solid tantalum capacitors and the manganese dioxide layer is extremely sensitive to temperature, particularly above 125°C, dictates an acceleration of rated voltage in lieu of temperature. It also supports the demand for stringent controls over their circuit applications.

Shown in Figures 26 and 27 are step stress test programs for solid tantalum capacitors and nonsolid tantalum capacitors, respectively, designed to establish optimum burn-in criteria which would afford reliability enhancement at minimum expense and schedule impact.

The value of applied voltage is to be established as a function of case size and capacitance value. The values shown in Figure 26 are applicable to those case sizes requiring a minimum of 110% of rated DC voltage as an applied stress. This minimum value may not exceed 130% in which case the three step stress levels would be 110%, 120%, and 130%. Caution must be exercised in the application of the voltages in that the intended value should be reached through a gradual increase instead of through a step function.

For nonsolid tantalum capacitors, the restriction of maximum applied temperature is relaxed because low temperature solder is not employed. Therefore, as shown in Figure 27, the step stress is a function of temperature as opposed to voltage. The voltage to be applied during the step stress test is 100% of the 85°C rated value.

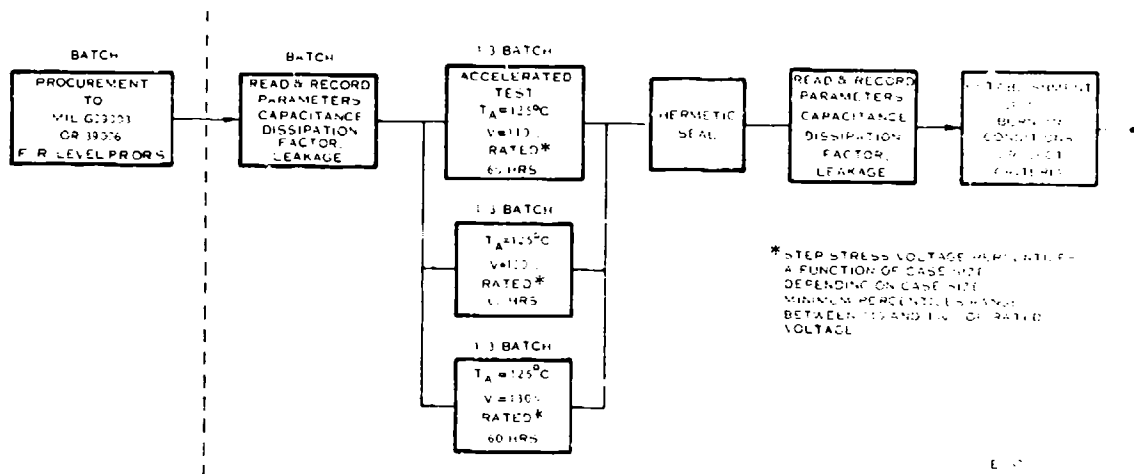


FIGURE 26 STEP-STRESS TEST OF SOLID TANTALUM CAPACITORS (PREPRODUCTION PHASE)

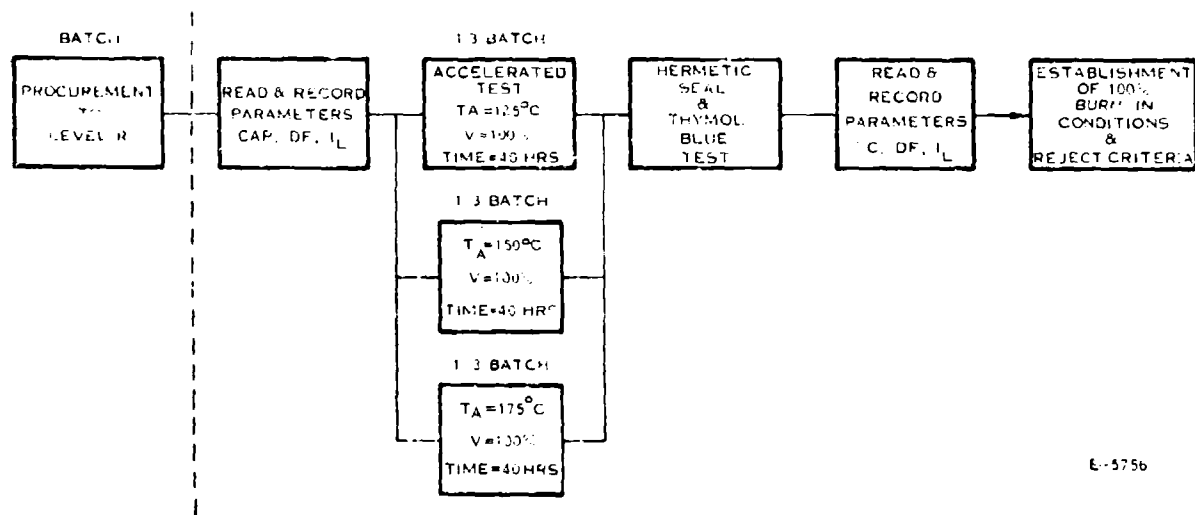
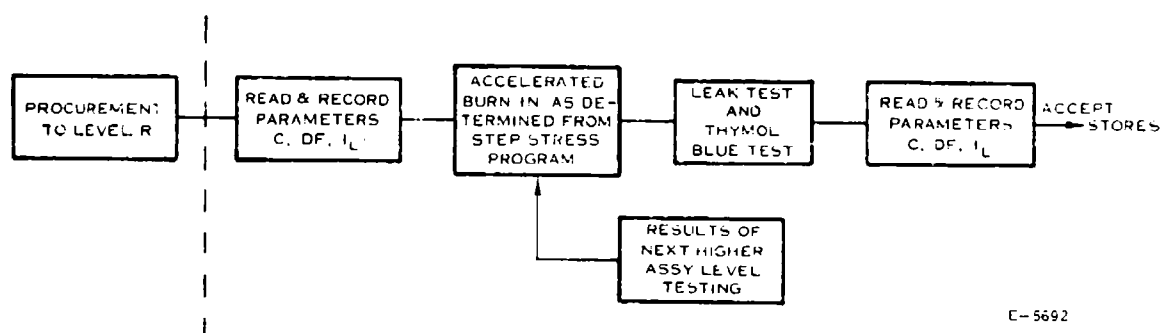


FIGURE 27 STEP-STRESS TEST OF NON-SOLID TANTALUM CAPACITORS
(PREPRODUCTION PHASE)



E-5692

FIGURE 28 100% ACCELERATED SCREENING OF TANTALUM CAPACITORS
(PRODUCTION PHASE)

6.2.3 Continued

Once the optimum burn-in conditions and associated reject criteria have been established from results of the step stress testing, 100% of the tantalum capacitors should be subjected to the accelerated burn-in as defined in Figure 28. Hermeticity per standard methods should be performed following accelerated burn-in. Where acid electrolytes are used (normally in nonsolid devices) a litmus paper or thymol blue test should be added to the usual leak test (reference 47).

The accelerated burn-in conditions should also be subject to alteration or refinement as a result of next higher level assembly screening.

6.2.4 Multilayer Epoxy or Polyimide Printed Circuit Boards

- "1. A test coupon from each production board containing 80 to 100 plated-through holes, connected in series, should be temperature cycled between -65° and 110°C, and increased electrical resistance should be cause for rejection of the production boards.

For programs with a nominally mild temperature environment 50 temperature cycles are recommended. For more severe applications, 200 temperature cycles are recommended."

From the list of failure mechanisms germane to multilayer printed circuit boards, the mechanisms having the most impact on circuit functions are either short or open circuits. While the spectrum of short circuit causes cannot be completely eliminated through in-line inspection and process control measures, it can be substantially reduced. The same statement applies to the spectrum of open circuit causes but for one subtlety - open circuit failures are, by far, more time/temperature dependent.

The majority of open circuit failures, obviously, involves the plated through hole of the multilayer board. Failures are manifested by cracks or separations of the barrel of the hole from the terminal pads of one or more layers through which the barrel passes. (As stipulated in reference (53) the primary factor affecting the long life of multilayer boards is the ductility of the copper.)

This failure mechanism also occurs during solder processing wherein the board and its plated through holes sustain the severe thermal shock associated with flow or wave soldering as well as hand soldering. In-house studies (54) have shown that a rather substantial improvement in reliability through the reduction of open circuit failures (based upon % rejects) results from the selection of polyimide/glass over epoxy/glass printed circuit board materials. While the use of polyimide over epoxy base material is encouraged, the 100% screening test outlined in Figure 29 would apply equally to either with a possible adjustment in number of thermal cycles.

6.2.4 Continued

A first article inspection to the criteria of MIL-P-55640 is recommended for each printed circuit configuration manufactured due to the fact that each board design is normally unique.

Test coupons should be specialized to best represent the complexity of the printed circuit board. A test coupon directly traceable to the board it represents and comprised of 80 to 100 plated through holes should be included.

The plated through holes should be connected in series in such a manner that the connection of the pad of one layer to the pad of a different layer is made through the barrel of a plated through hole. In no case, should a conductor path on an individual layer be connected to more than 2 plated through holes at one time. (See Figure 30).

The coupons containing the series-connected plated through holes configured per the sketch should be subjected to from 50 to 200 temperature cycles depending upon the severity of the use environment. In the case of engine mounted hardware where temperature excursions are acute, 200 cycles are recommended. The suggested temperature extremes are -65°C to 110°C (reference 47). A thermal gradient of about 20°C per minute is adequate based upon module level testing conducted by Hughes (reference 48). The selection of $175^{\circ}\text{C}/\text{minute}$ was based upon the gradient required to complete 200 thermal cycles in 72 hours with a minimum dwell at temperature extremes. (Note: The $17.5^{\circ}\text{C}/\text{minute}$ gradient is that to be experienced by the test coupon, not the temperature chamber volume.)

The accept/reject criteria to be applied is the delta resistance of the 80 to 100 plated through holes connected in series ($R_{\text{initial}} + 10\%$). Following an accept decision, the temperature cycle test should be continued for 3000 cycles simulating a 10-year life of the multilayer printed circuit board in normal aircraft usage.

A potential failure mode in high density circuitry on epoxy substrates resulting in permanent or intermittent loss of insulation resistance has been reported (67), (68). It is attributed to the growth of conductive anodic filaments (CAF) in the presence of high humidity and d.c. bias. Failure by this mechanism is manifested by a catastrophic loss of insulation resistance between conductors held at a potential difference. Insulation failure occurs due to the growth of conductive filaments in the dielectric composite. This growth results from an electrochemical process which takes place at the anode conductor and which penetrates the dielectric along the glass/epoxy interface. Prudence would dictate that this situation be carefully reviewed and the conditions for such growth and resulting failure be avoided.

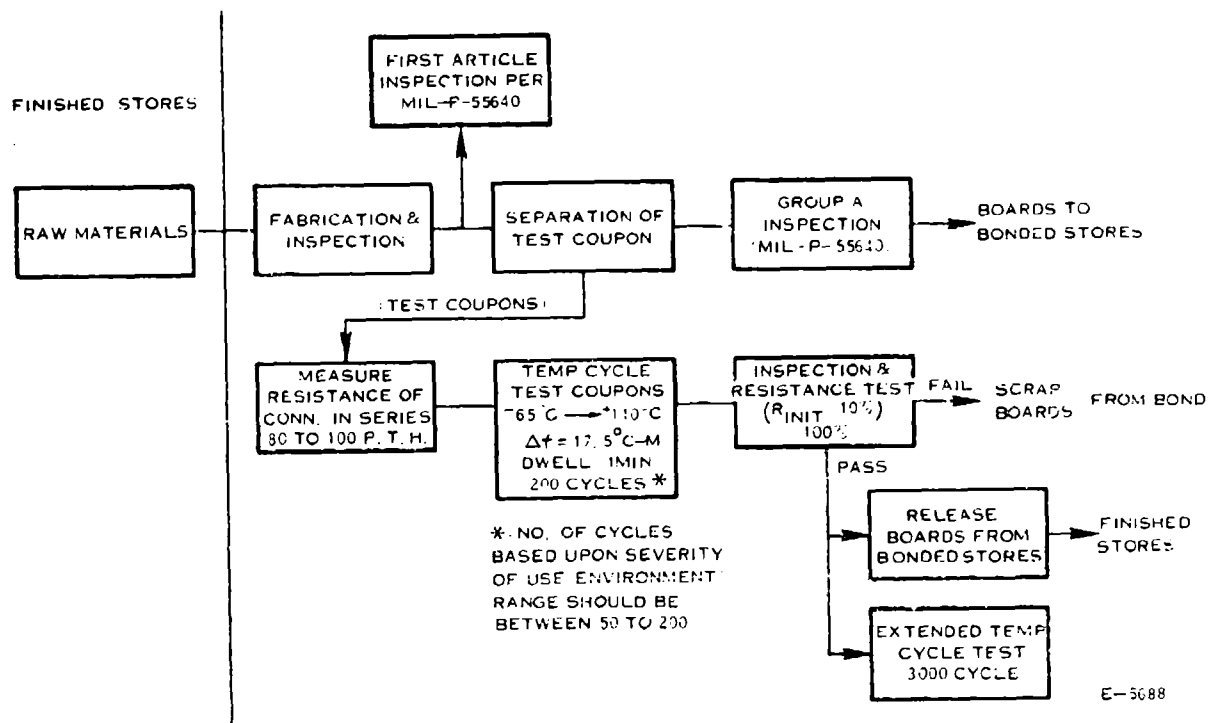
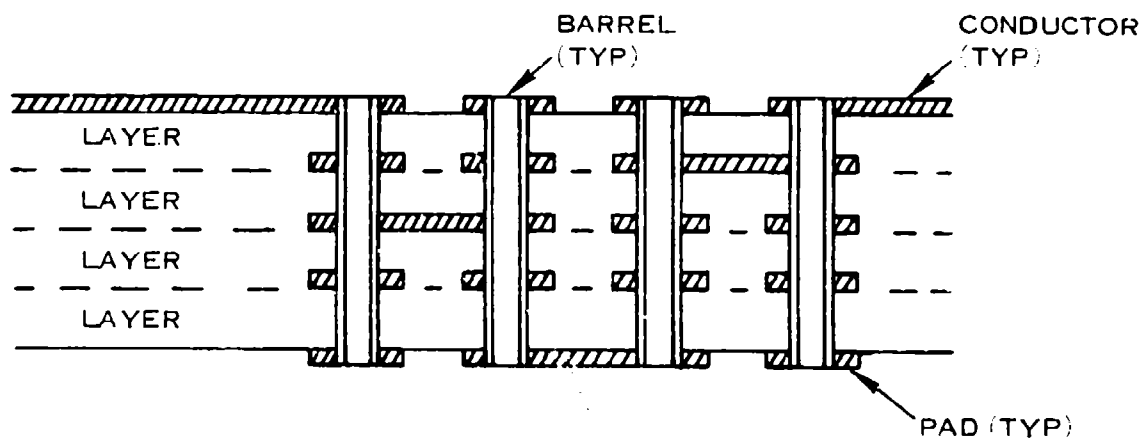


FIGURE 29 100% SCREENING OF MULTILAYER POLYIMIDE LAMINATE PRINTED CIRCUIT BOARDS (PREPRODUCTION AND PRODUCTION)



E-57 59

FIGURE 30 PRINTED CIRCUIT BOARD PLATED THRU HOLES

6.2.4 Continued

- "2. Acceptance tests should also include temperature shock tests simulating the wave, or the hand soldering operations, since thermal induced warping of the boards tends to cause cracks between the inner copper planes and the plated-through hole."

Group A inspection of MIL-P-55640 should be conducted on a tightened AQL, or better, 100% basis. In addition, thermal shock per method 107 of MIL-STD-202, test condition B should be performed.

6.3 Accelerated Stress Testing

6.3.1 Introduction

Material on the accelerated stress testing of semiconductor devices is presented here and in Section IX of Volume I because it is considered to be important guidance in the pursuit of very high reliability electronic engine controllers. The accelerated stress testing of semiconductor devices is of paramount importance in that it provides the following:

- a. Information for the determination of device failure rates.
- b. Information necessary for devising a suitable, low cost, screening method to eliminate defective devices.
- c. Parameter characterization in life use to enable recognition of sensitive parameters for reliability predictions.
- d. Life testing data indicating median life, in order to obtain highly reliable parts.
- e. Information regarding the life-limiting failure modes and mechanisms for reliability studies.

Microcircuit life testing under electrical bias and at temperatures in excess of 150°C has been shown to be a valid means of both identifying life-limiting failure modes and relating those modes to their associated use-temperature lifetimes.

6.3.2 Sample Test Program

The sample test plan described here was designed to identify failure modes and mechanisms in microcircuits in order to establish failure rates and median life, and to develop a screening method that could be used for the procurement of high reliability microcircuits for electronic engine controls.

6.3.2 Continued

The program entailed various phases performed by several separate organizations. These phases included:

- a. Procurement of test devices.
- b. Bias circuit evaluation.
- c. High-temperature accelerated life tests.
- d. Detailed analysis of failed devices.
- e. Data reduction/analysis.

The Test Program flow and sequence is shown in Figure 31.

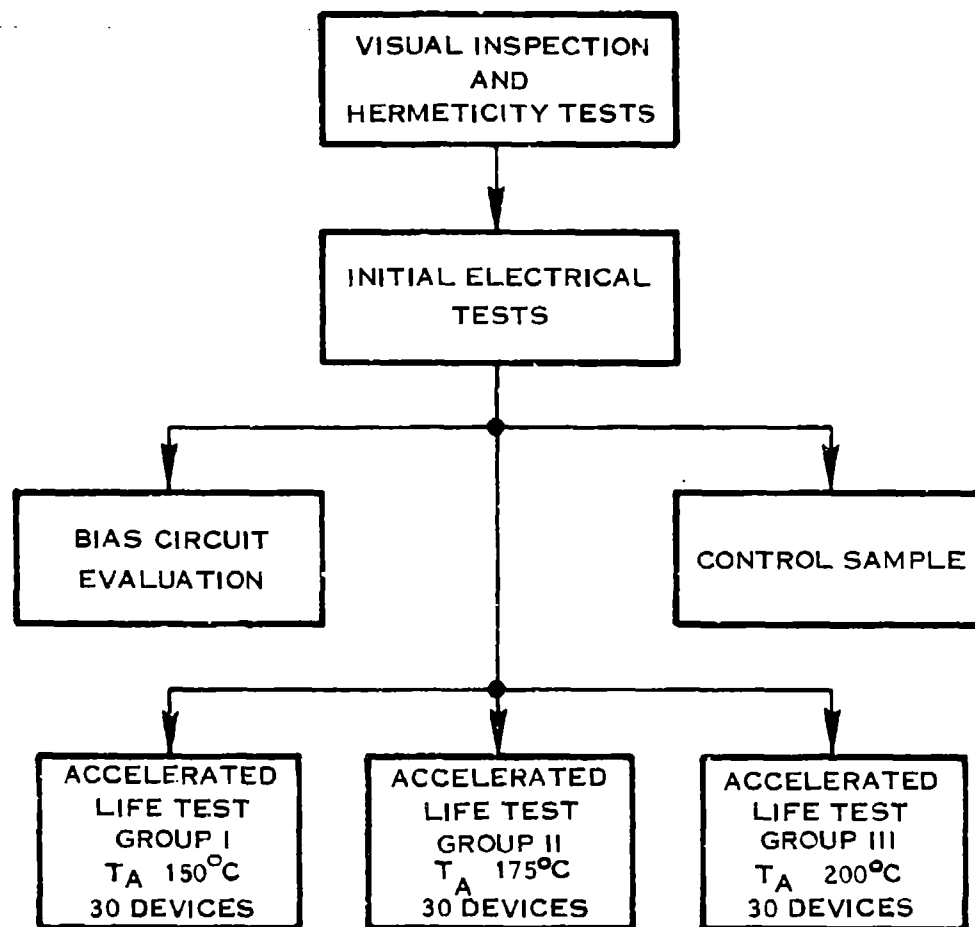
The device used for the test plan was a Motorola MC14163B CMOS counter, processed in accordance with MIL-STD-883B, Method 5004 Class B. This device is a synchronous, programmable, 4 bit, binary counter with synchronous clear. It was selected for the following reasons:

- a. It possesses a circuit complexity representative of that contained in integrated circuits incorporated in the current state-of-the-art electronic fuel controllers.
- b. The generic family has been in production for an extended period attesting to the stability of the manufacturing process.
- c. It is adaptable for accelerated test conditions.

6.3.2.1 Facility Evaluation

The facility chosen to perform the necessary testing for the program, was selected for the following reasons:

- a. The facility possessed adequate equipment and lab facilities for high temperature testing.
- b. The personnel had demonstrated from previous work in this area that they had the technical expertise to perform all phases of the program.
- c. The personnel had demonstrated familiarization with the statistical nature of data obtained from accelerated tests from past experience in this area. This would be instrumental in the correspondence of the necessary data and the reporting of results.



E-5681

FIGURE 31 TEST PROGRAM FLOW

6.3.2.1 Continued

Some of the equipment used was:

- a. A Tektronix S3260 circuit tester for automatic testing with parametric printout. This tester was calibrated at regularly scheduled intervals and operated by personnel highly qualified and familiar with this device.
- b. Special circuit boards, connectors and sockets along with interconnecting wires and resistors to enable operation at temperatures in excess of 200°C.
- c. Special high temperature chambers that utilized rack mounting of assemblies containing the devices under test.

6.3.2.2 Initial Inspections and Tests

Upon receipt devices were subjected to a visual inspection performed per MIL-STD-883B, Method 2009.1. In addition, all devices were subjected to fine and gross leak tests per MIL-STD-883B, Method 1014.2, Conditions A1 and C2, respectively. The purpose of these examinations was the elimination of devices with shipment induced damage. No damage was observed in the visual inspection and all devices passed the hermeticity tests.

All devices were then subjected to initial electrical testing at 20°C using a Tektronix S-3260 Automated Test System. The electrical tests were performed to establish a data base for the test program and to correlate the measurements obtained with the manufacturer's test data. The electrical tests included both dc parametric tests and functional tests. Appendix C contains a description of the tests including test conditions, end point limits and the truth table utilized for functional testing. No failures resulted from the initial electrical tests, and good correlation with manufacturer provided parametric data was noted.

6.3.2.3 Bias Circuit Evaluation

Prior to initiating the bias circuit evaluation, a construction evaluation was performed. This was done to determine if the devices contained materials or construction features that would preclude their operation at the temperatures specified in the Test Plan. The results of this evaluation are summarized in Appendix D. They reveal no materials nor construction features that would limit testing below 250°C.

6.3.2.3 Continued

Following the construction evaluation, a bias circuit evaluation was performed to determine the suitability of the selected bias circuit, shown in Figure 32, for high temperature accelerated life tests. This evaluation was accomplished in three parts. First, a preliminary bias circuit evaluation was performed. Next, the formal bias circuit evaluation, in compliance with the Test Plan, was conducted. Finally, the formal bias circuit evaluation was continued at higher ambient temperatures to obtain additional data.

The preliminary bias circuit evaluation utilized two test devices. This was done to limit the number of devices that would be destroyed in the event of a catastrophic failure mode at the temperatures of interest. The devices were operated at ambient temperatures from 150°C to 250°C, in 25°C increments, for approximately 30 minutes at each temperature. No problems were found that would have required a test plan change. This evaluation demonstrated that the devices remained functional at ambient temperatures up to 250°C.

The formal bias evaluation was subsequently performed. Five devices were operated in the Figure 32 bias configuration at each of the three specified ambient temperatures (150°C, 175°C, and 200°C). The power supply current and the sum of the six high input currents were monitored and recorded when the devices reached the ambient temperature, 15 minutes thereafter and at 1 hour, 2 hours and 4 hours. In addition, the outputs of each device were monitored periodically with an oscilloscope. The results of this testing are included in Table 13, Bias Circuit Evaluation Summary. All devices remained functional and none exceeded the specified supply current limit of 600 μ a, or the input current limit of 1.0 μ a. With the exception of the data points noted, the Table 13 results indicate good device stability after thermal equilibrium is reached. The devices were cooled-down under bias after each 4 hour step and underwent electrical testing. This testing indicated that the selected bias circuit was nondestructive at the specified ambient temperatures and was suitable for the high temperature accelerated life tests.

The bias circuit evaluations were continued at higher ambient temperatures until an ambient temperature was reached at which the devices would not function properly. Five devices were operated at 225°C, five at 250°C, and five at 275°C. The results of the 225°C and 250°C steps are included in Table 13. At 275°C the output signals were severely degraded and the evaluation was discontinued. Although all devices remained functional at the 225°C and 250°C ambient temperatures, three devices at 225°C, and all five at 250°C, exhibited a supply current in excess of the specified 600 μ a while the input currents remained within the 1 μ a limit. Subsequent electrical parametric and functional testing indicated negligible device degradation.

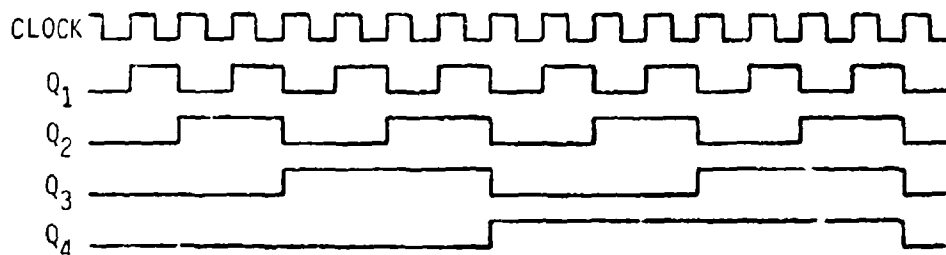
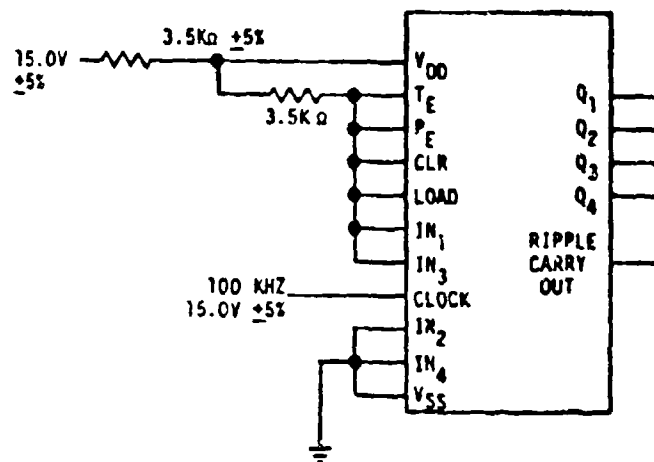


FIGURE 32 MC14163B BIAS CIRCUIT

TABLE 13 BIAS CIRCUIT EVALUATION SUMMARY

Temperature	Readout Time	Supply Current (μ A) (1)	Input Current (nA) (1)
150°C	0	67 (2)	4
	15 MINUTES	145	4
	1 HOUR	146	4
	2 HOURS	147	5
	4 HOURS	147	5
175°C	0	161	18
	15 MINUTES	171	30
	1 HOUR	175	31
	2 HOURS	175	32
	4 HOURS	175	32
200°C	0	269	97
	15 MINUTES	278	100
	1 HOUR	282	101
	2 HOURS	282	99
	4 HOURS	284	99
225°C	0	647	194
	15 MINUTES	586	262
	1 HOUR	596	268
	2 HOURS	597	269
	4 HOURS	598	272
250°C	0	1490	480
	15 MINUTES	1720	527
	1 HOUR	1750	533
	2 HOURS	1750	535
	4 HOURS	1750	395 (3)

NOTES:

- (1) Average of five devices
- (2) An adjustment in the V_{DD} and clock high level voltage was required following this measurement accounting for this low reading
- (3) This reading is in error due to an offset voltage shift in the DVM. Subsequent electrical testing indicated no input degradation.

6.3.2.3 Continued

Based on the results of the bias circuit evaluation, it was concluded that the long term (2,000 hour) accelerated life tests could be safely conducted at the specified ambient temperatures of 150°C, 175°C and 200°C. It was also concluded that life testing could be safely conducted at ambient temperatures as high as 250°C. After a review of the device characteristics with the manufacturers, it was discovered that a potential latch-up problem, and possibly others, would occur above 200°C. The 200°C maximum test temperature was determined to be adequate for the test and it insured that no test induced failure mechanisms would result.

6.3.2.4 High Temperature Accelerated Life Tests

The high temperature accelerated life tests were performed at the three selected ambient temperatures (150°C, 175°C, and 200°C) for 2,000 hours. Each test cell contained thirty devices which were biased in the Figure 32 configuration. Periodically during the life tests the devices were cooled-down under bias for interim electrical testing. The interim electrical tests were the same as the initial electrical tests and described in detail in Appendix B.

The interim electrical test times were 4, 8, 16, 32, 64, 128, 256, 512, 1,000 and 2,000 hours. A control sample of ten devices was also tested at each interim readout to verify the long term stability of the automated test equipment.

No device failures were generated by any of the accelerated life tests. In addition, no device exhibited parametric change that would indicate device degradation, as shown in Table 14.

6.3.3 Conclusion and Results of Accelerated Test

The interim electrical test data was reviewed throughout the high-temperature accelerated life tests to identify both failed devices and specific parameters that exhibited drift. As an additional data evaluation tool, summaries of the parametric data were generated for each test group and at each interim readout. The data included means, standard deviations, and maximum and minimum values for each parameter. Those measurements that were performed on several inputs or outputs were combined for this evaluation. The initial and final means and the standard deviations for the device parameters in the three test groups are included in Table 14. The initial values were computed using the specific initial data of the devices which comprise the various test groups. It can be seen that no important changes were observed as a result of the life tests. A single device (S/N 52) in the 175°C group exhibited a large I_{SS} ($\approx 1\mu A$) when measured at $V_{DD} = 15.0 V$, resulting in a high mean and sigma value for that group. This measurement was high when initially tested as well as when the manufacturer tested the device. This current remained relatively constant throughout the life test and was well within the specified end point limits.

TABLE 14 PARAMETRIC TEST SUMMARY

PARAMETER	150°C Group				175°C Group				200°C Group			
	INITIAL		2,000 HOURS		INITIAL		2,000 HOURS		INITIAL		2,000 HOURS	
	MEAN	SIGMA	MEAN	SIGMA	MEAN	SIGMA	MEAN	SIGMA	MEAN	SIGMA	MEAN	SIGMA
15V, I_{SS} (nA)	106.7	46.07	104.2	47.69	480.8	2060	484.2	2073	95.8	13.82	97.5	10.90
15V, I_{IL} (nA)	-1.359	3.950	-1.554	3.816	-1.139	0.7806	-1.320	0.8510	-1.141	0.7507	-1.311	0.8495
15V, I_{IH} (nA)	3.163	1.031	6.413	1.224	3.091	1.032	6.048	1.212	3.052	0.9818	7.072	1.280
V_{OHU} (μV)	-325.3	163.6	-304.0	159.2	-330.0	172.9	-300.0	187.3	-283.0	158.7	-342.7	163.3
V_{OL} (μV)	1055	83.54	951.3	86.39	1054	88.31	944.0	87.54	1064	81.26	952.3	82.85
15V, I_{OH} (mA)	-8.877	0.3052	-8.904	0.3028	-8.817	0.3023	-8.839	0.2974	-8.790	0.2825	-8.784	0.2736
15V, I_{OL} (mA)	9.951	0.5584	10.24	0.5577	9.997	0.4854	10.46	0.4913	9.871	0.7057	10.37	0.7030
10V, I_{SS} (nA)	38.33	30.78	92.5	22.03	91.67	30.51	88.33	32.10	82.50	32.69	75.00	40.31
10V, I_{OH} (mA)	-2.441	0.08473	-2.451	0.08277	-2.426	0.08645	-2.428	0.08301	-2.417	0.07506	-2.413	0.07602
10V, I_{OL} (mA)	2.533	0.1528	2.634	0.1566	2.549	0.1280	2.686	0.1412	2.507	0.1905	2.664	0.1983
5V, I_{SS} (nA)	80.00	35.59	90.83	26.6	74.17	40.30	81.67	32.87	70.83	42.12	88.33	27.94
5V, I_{OH} (mA)	-4.459	0.1778	-4.468	0.1757	-4.404	0.1810	-4.407	0.1780	-4.398	0.1397	-4.375	0.1406
5V, I_{OL} (mA)	1.000	0.06880	1.026	0.06895	0.998	0.07020	1.030	0.07390	0.996	0.09246	1.030	0.09711
I_{NSAT} (mA)	2.805	0.2470	2.810	0.2450	2.792	0.3267	2.807	0.3312	2.823	0.3924	2.839	0.4023
I_{PSAT} (mA)	-5.330	0.2304	-5	0.2286	-5.260	0.2350	-5.267	0.2354	-5.255	0.1800	-5.224	0.1840

6.3.3 Continued

The failures versus time data was instrumental in determining the median life and reliability level of the devices tested. No failures were obtained for up to 2,000 hours @ 200°C. This data was indicative of a highly reliable lot of devices.

In applying the failure data obtained to the lognormal distribution and Arrhenius curves, the following relationships apply.

- a. The median life of the devices under test is greater than the time obtained. With no failures on 2,000 hours, at 200°C, this extrapolates to no failures in approximately 4×10^9 hours at 25°C using a 1.0 eV slope on the Arrhenius curves (characteristic of CMOS devices). The median life is greater than 4×10^9 hours at 25°C as no failures were obtained at this point.
- b. The failure distribution of the devices can be obtained by further analysis. The standard deviation (σ) parameter was not obtained as a result of the lack of failures. However, using an assumed σ that is characteristic of CMOS devices, the median life and failure distribution can be obtained after only a few percent of failures. The slope of the lognormal cdf curve corresponding to σ will also provide the 50% median life point and other failure points. The 50%, or greater, failures data is needed to fully determine the exact values of median life and σ of each group of devices. At 125°C, the extrapolated value of 2,000 hours at 200°C is 2.5×10^5 hours.

The accelerated tests and resultant data of this program indicated that the CMOS devices used were highly reliable. Other characteristics of these devices are indicated by the values of the parameters that were actually obtained. In particular, the values of the leakage currents (approximately 100 na @ 25°C) were far below the maximum specified value of 5.0 μ a by the manufacturer. The amount of drift of this parameter was small as indicated in Table 14. The low values for leakage currents correspond to the values that would be used in MIL-M-38510 for CMOS devices.

The testing done demonstrated that the semiconductor devices subjected to test were very reliable. Clearly such testing can be very useful for semiconductor device screening purposes and for the characterization of device life distributions.

6.4 Subassembly Level (Module) Screening

The effectiveness of a comprehensive screening program at the lower assembly level of a production run has been questioned for decades. The answer inevitably was that the measurably small improvement realized did not justify the cost of implementation. The principal reason for this lack of effectiveness was recently determined to be the rather benign environmental conditions utilized. The cost of module level test equipment falls out of the argument against subassembly screening because it has become an accepted program element, particularly, where the subassembly has a high density factor and circuit complexity.

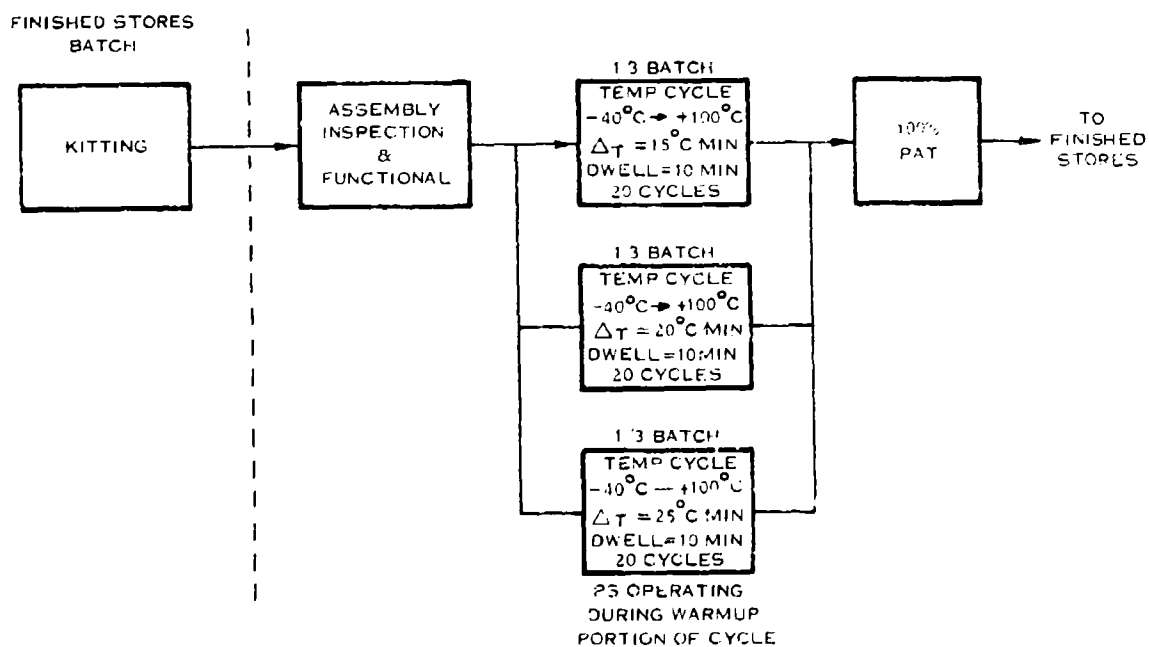
Numerous studies by independent firms (references 48, 49, 50) conducted on high-volume production modules show a definite improvement in end-item reliability attributable to subassembly thermal cycling and screening. Results indicate maximum screening effectiveness is achieved when the number of thermal cycles is between 20 and 40 and the rate of temperature change is between 15°C and 25°C per minute. Complexity plays a major role in determining the most effective rate of change for a particular module; generally, the more complex modules require smaller rates of change. (Here we could define a complex module as being a multilayer polyimide printed circuit board containing 200 piece parts the majority of which being active parts, and 2000 solder joints.)

6.4.1 Preproduction

6.4.1.1 Polyimide/Glass Printed Circuit Board Assemblies

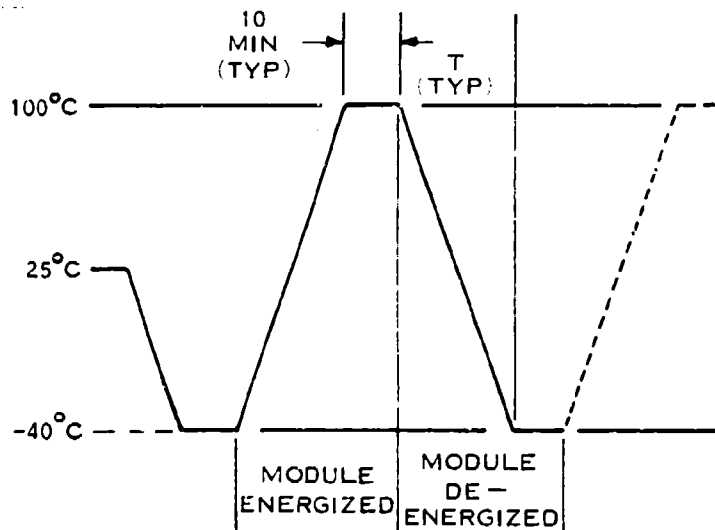
During the development phase of the program the determination of the stresses and levels which will provide optimum screening effectiveness (measured at the next higher assembly level) is to be accomplished. Figure 33 depicts the 100% screening of polyimide printed circuit board modules designed to establish the optimum rate of temperature change utilizing a fixed number of cycles and temperature ranges. These characteristics have been fixed at 20 and -40°C to +100°C, respectively, to reduce the number of variables. Additionally, these values are representative of the optimum conditions derived from the aforementioned industrial studies. The option to increase the number of cycles or the range between temperature extremes can be exercised depending upon design analysis, configuration/complexity, level of piece part screening as well as from results obtained from pre-production tests.

A preproduction batch of modules is divided into 3 equal sub-batches each of which is subjected to 20 thermal cycles differing only by the thermal gradient. (See Figure 34). Dwell time at temperature extremes should be less than 10 minutes.



E 5687

FIGURE 33 100% SCREENING OF POLYIMIDE P.C. BOARD MODEL DURING PRE-
PRODUCTION PHASE



$$\text{WHERE } T = \frac{\Delta T (^\circ\text{C})}{\theta}$$

$$\Delta T (^\circ\text{C}) = 140^\circ\text{C}$$

$$\text{FOR } \theta = 15^\circ\text{C/MIN, } T = 9.33 \text{ MIN}$$

$$\theta = 20^\circ\text{C/MIN, } T = 7 \text{ MIN}$$

$$\theta = 25^\circ\text{C/MIN, } T = 5.6 \text{ MIN}$$

E - 5775

FIGURE 34 TEMPERATURE EXTREMES AT DWELL TIME

6.4.1.1 Continued

Assuming a dwell time of 10 minutes the length of test will range from 10.4 to 12.9 hours depending upon the thermal gradient employed. The traceability of a module to its thermal gradient sub-batch should be maintained through end assembly testing enabling the determination, from next higher assembly levels, of that thermal gradient which minimizes the failure occurrence of that module type. Once determined, the thermal gradient should be utilized during production testing.

The estimated yield through this subassembly level thermal screen will exceed 90% and through the end-item level screening, approach 100%.

6.4.1.2 Alumina Ceramic Modules

The alumina ceramic printed circuit board is a composite of ceramic insulating layers, interconnect patterns and a thick film alumina (Al_2O_3) substrate. The resulting monolithic unit is a sturdy, physically stable and thermally conductive device affording maximum device density and long term high reliability.

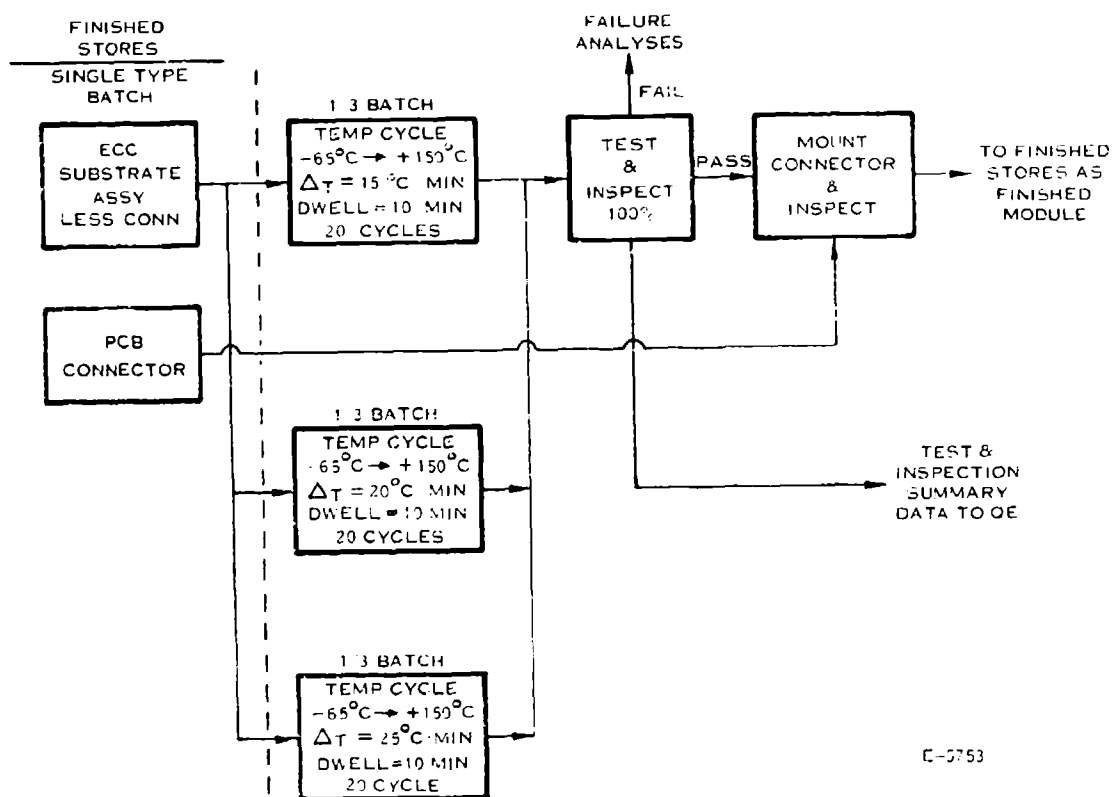
The physical properties of the alumina ceramic were taken into account when developing the 100% screening program shown in Figure 35 and related to a module comprised of leadless chip carriers (LCC) mounted on the alumina substrate board. Its high thermal stability and ease of rework characteristics, permit both the substrate and the LCC packs as a completed module assembly (less connector) to be thermal cycled concurrently.

The screening approach parallels that discussed earlier for polyimide printed circuit board modules except the temperature extremes have been increased to $-65^{\circ}C$ and $+150^{\circ}C$. The ceramic module minus the printed circuit board connector should be subjected to thermal cycling after which the connector is to be assembled, completing the ceramic module subassembly.

6.4.2 Production

That thermal cycle level of the three conducted on preproduction modules which manifests the most anomalies during module level screening but the least number of module failures of the same module at the next higher level screening level is to be selected as the production level module screen. That the screen levels selected over the family of module types may vary between types is to be anticipated.

The effectiveness of the selected screen should be monitored continuously at the next higher assembly screening level. In the event a new failure mechanism develops, identified by an increase in module failures at the next higher assembly level, the screening program for the designated module type should be examined. Options are to vary the number of thermal cycles, the



C-5753

FIGURE 35 100% PREPRODUCTION SCREENING OF MODULES INCORPORATING LCC AND CERAMIC SUBSTRATES

6.4.2 Continued

temperature range, or institute a penalty test tailored to the detection of the specific anomaly. Varying the number of cycles should be avoided, except as a last resort. The above is outlined in Figures 36 and 37.

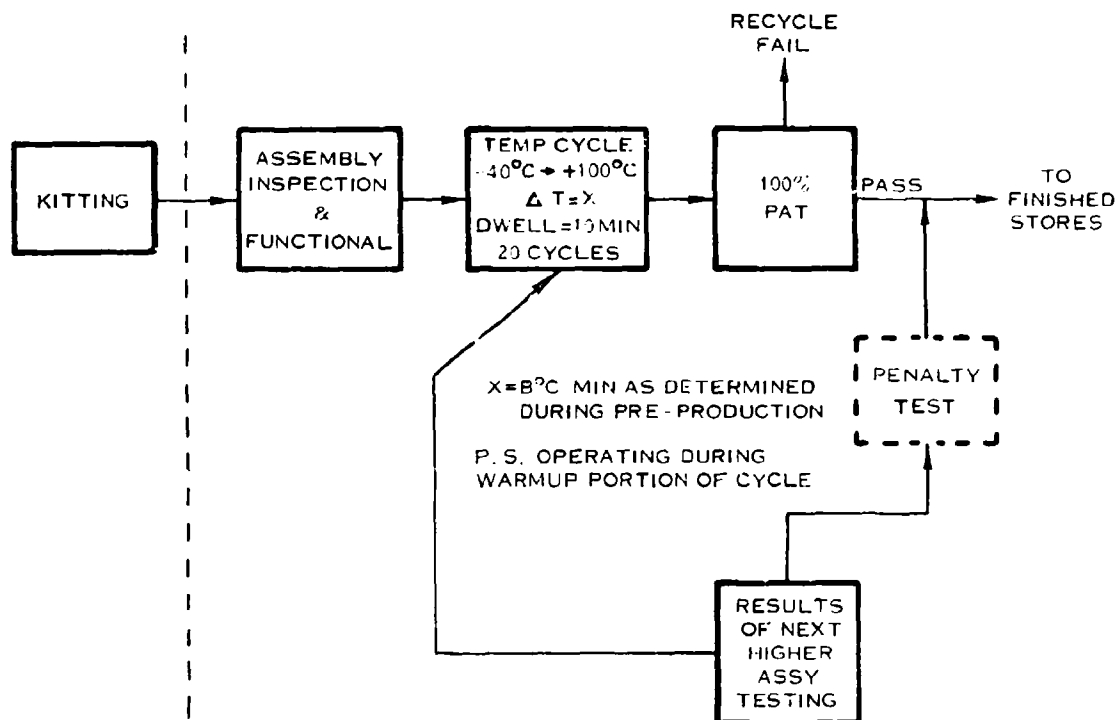
6.5 Final Assembly Level Screening

Our effort to compress the front end of the life cycle of a given equipment (wherein failures usually identified as customer returns are corrected before initial shipment) culminates at the final assembly screening level. Here, the effectiveness of module level screening is measureable, permitting, also, an assessment of the module fabrication processes to be made. What remains is the proving of the fabrication processes related to end-item level assembly and assurance testing the physical and functional interactions of the constituent modules and subassemblies.

The design of a high reliability assembly normally includes redundancy with the best form of redundancy being the physical and electrical separation of the redundant paths. Complete physical and electrical separation is usually unattainable in the pure sense due to package, control function and cost constraints. But in the practical sense, enough physical and electrical separation may exist when additional external interconnection circuitry is incorporated in the test bed to permit each path to be exercised independently. Where the equipment design or program requirements do not lend themselves to optimally separate redundant paths, obviously, the conditions of the screening test conducted must be adjusted. The screening program shown in Figure 38 has been developed with consideration given to optimum physical and electrical separation between redundant paths. When this feature is too limited or nonexistent the primary section path of the Figure would apply.

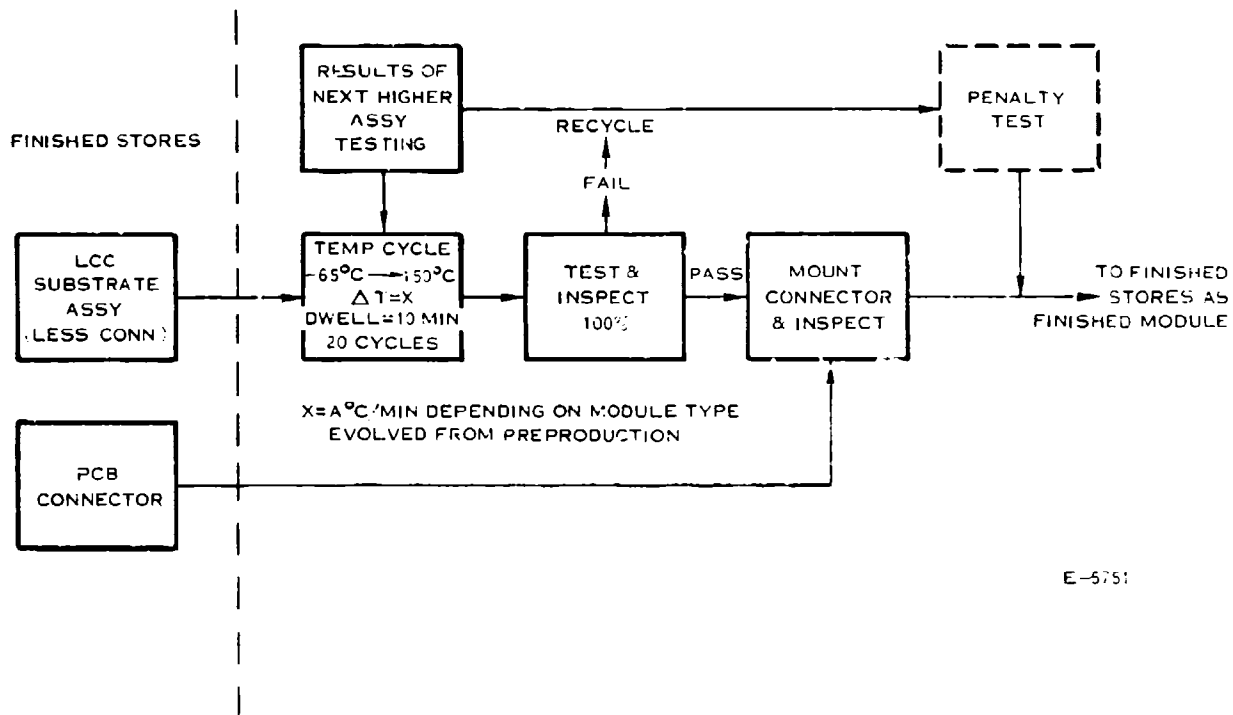
The conditions for thermal cycling an end-item assembly or equipment are dependent upon the parts mix, processes involved and the complexity of the end item. Taken from reference 53 (page II-16) is the graph entitled, "Generalized Temperature Cycling Failure Rate Curves as a Function of Equipment Complexity", shown herein as Figure 39 which represents the composite of their industry survey data normalized to show the typical relationship between complexity and number of required temperature cycles necessary to detect incipient failures. As can be seen, the more complex equipments require more cycles. From the same data the recommended number of thermal cycles for various complexity levels was derived as 1, 3, 6 and 10, respectively, for complexities of 100, 500, 2000 and 4000 electronic parts.

The credibility of having one cycle accomplish the intended result is questionable, particularly when another recommendation given was that the last cycle should be failure free. Re-examining the curve of Figure 39 in



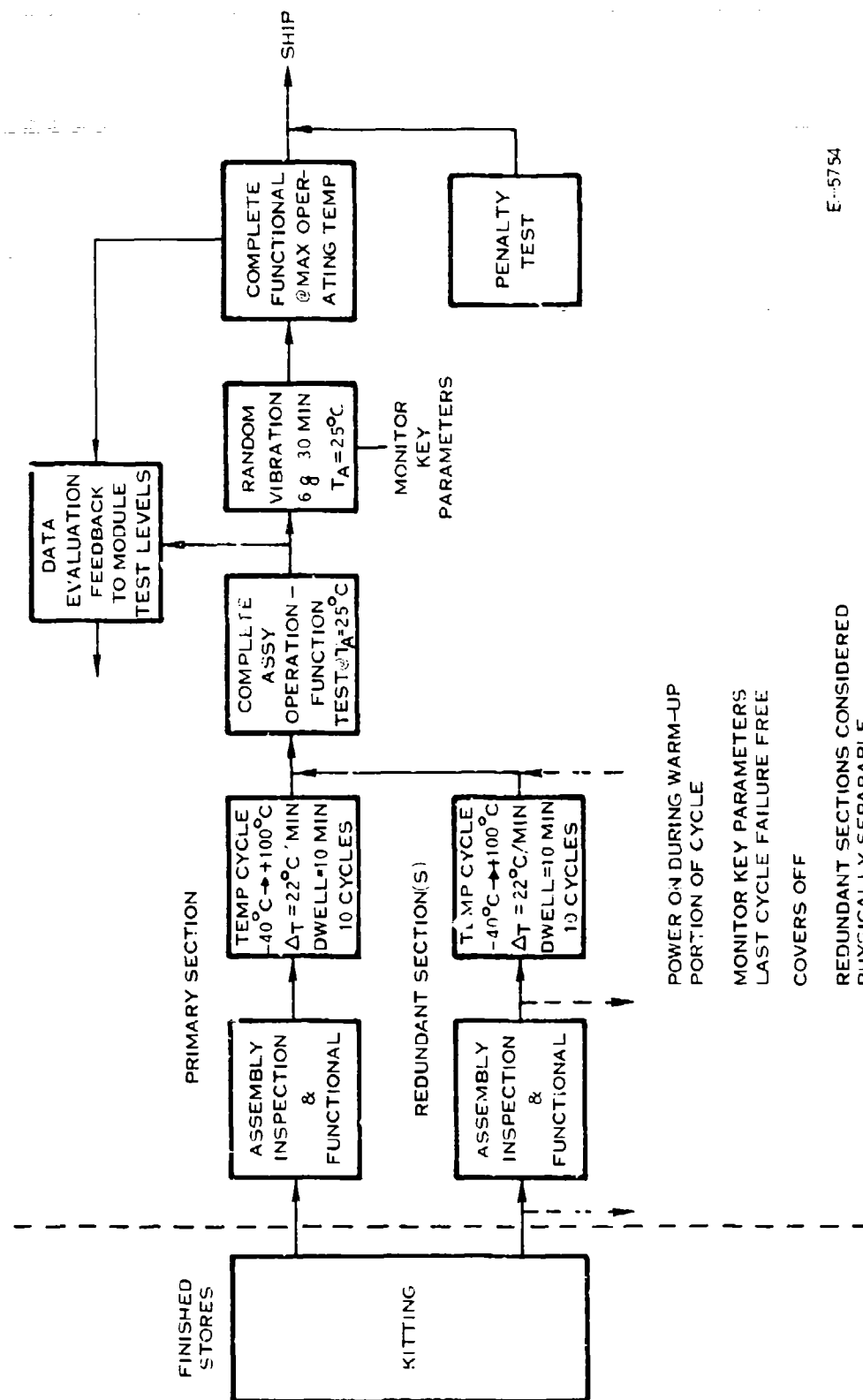
E 5752

FIGURE 36 100% SCREENING OF MODULES INCORPORATING POLYIMIDE PC BOARDS DURING PRODUCTION PHASE



E-5751

FIGURE 37 100% SCREENING OF PRODUCTION MODULES INCORPORATING LCC AND CERAMIC SUBSTRATES



E-5754

FIGURE 38 PRODUCTION ACCEPTANCE TEST OF END-ITEM EQUIPMENT

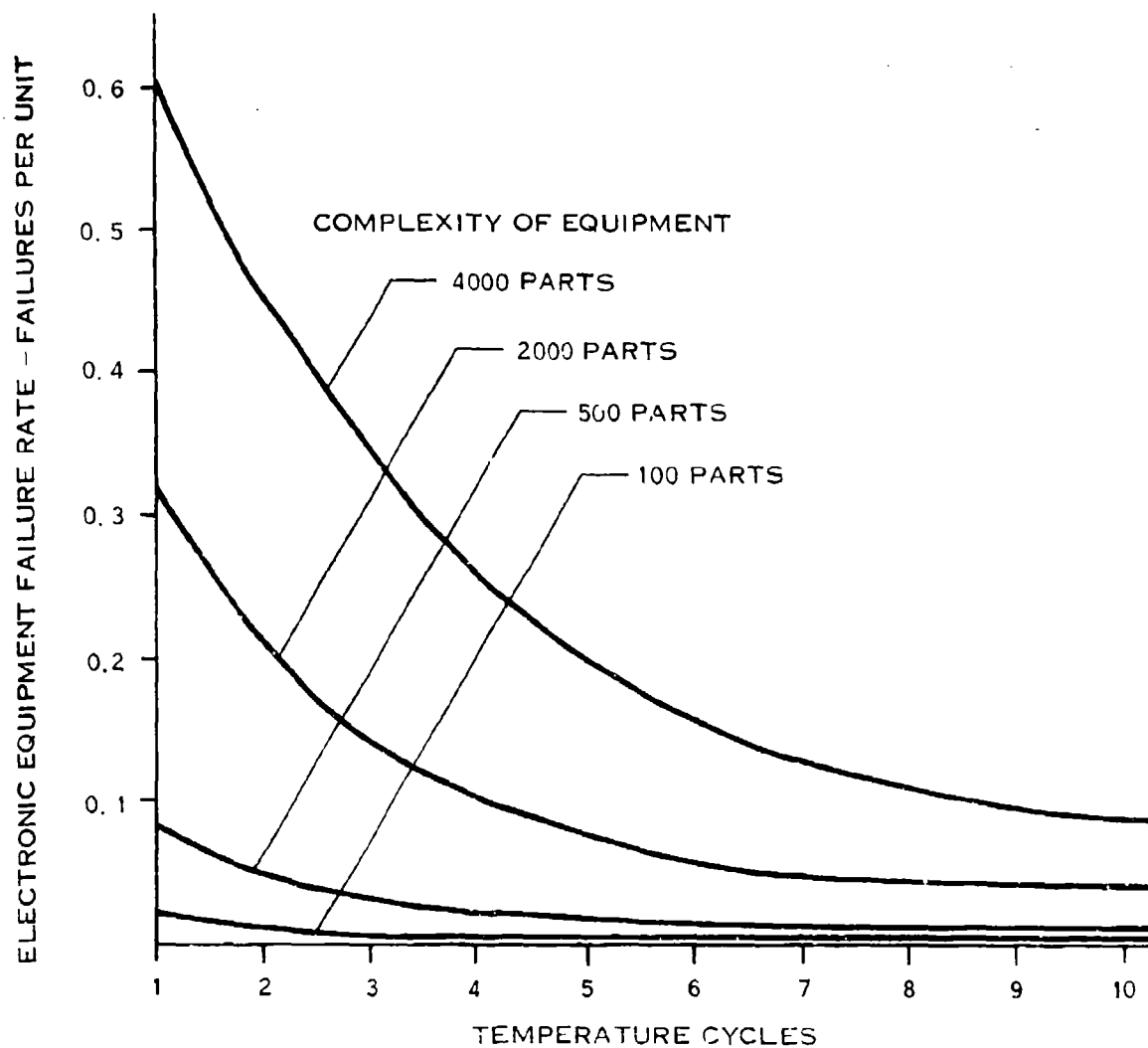


FIGURE 39 GENERALIZED TEMPERATURE CYCLING FAILURE RATE CURVES
AS A FUNCTION OF EQUIPMENT COMPLEXITY

6.5 Continued

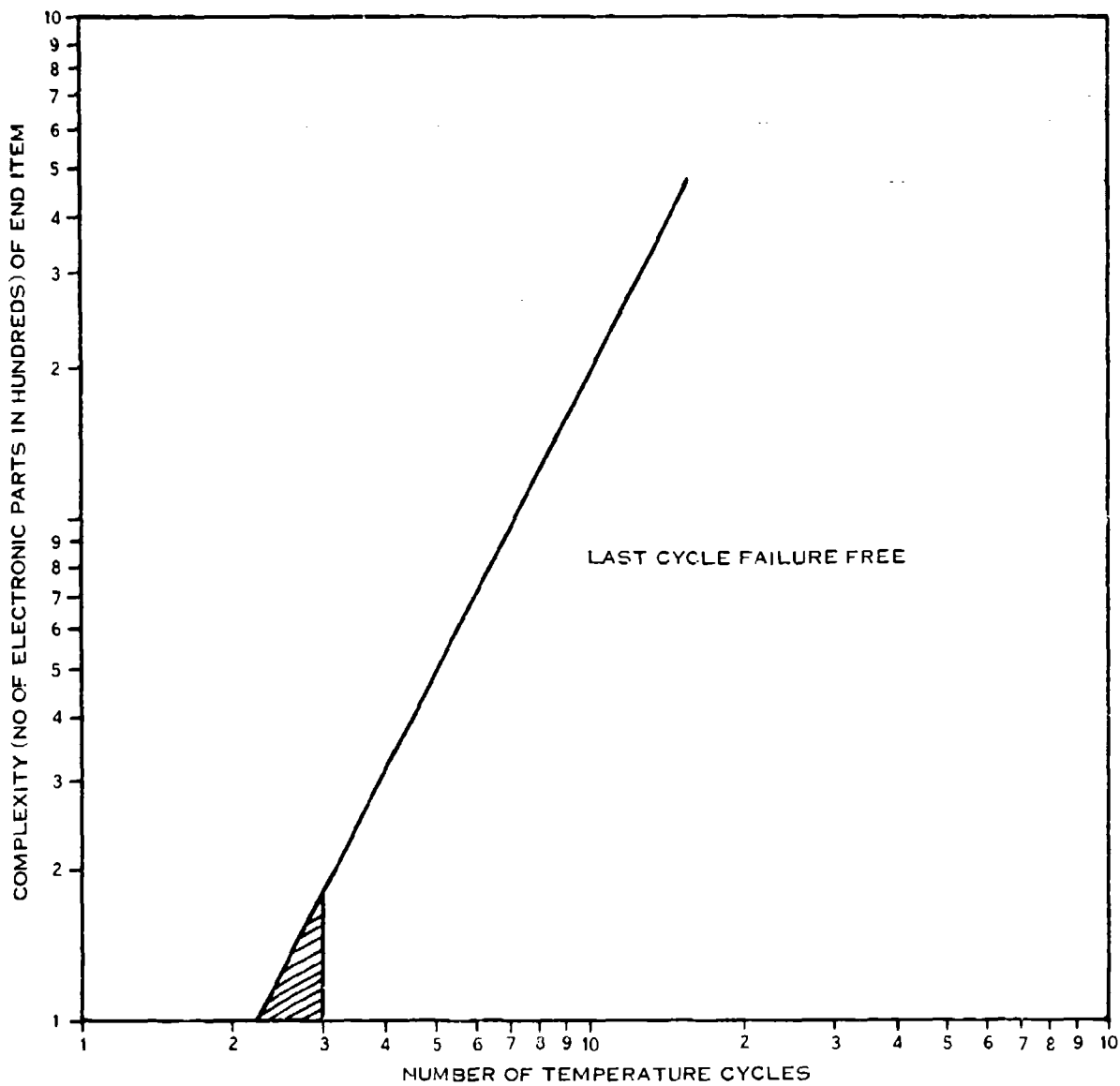
terms of net improvement of increasing the number of cycles to that number which more closely corresponds to the flat portion of the curve one can readily recognize an approximate 3 to 1 reduction in risk of a field failure for the case where complexity is 100 parts by increasing the number of cycles to 3. Improvement factors in the area of 2 to 1 for the other complexity levels are also recognizable at the cost of a few additional thermal cycles.

Following the guidelines given in reference 53, as modified above, the number of cycles may be determined as a function of the equipment complexity per the following scale expanded in Figure 40 for extrapolation purposes.

<u>Number of Electronic Parts</u>	<u>Number of Cycles</u>
100	3
500	5
2,000	10
4,000	14

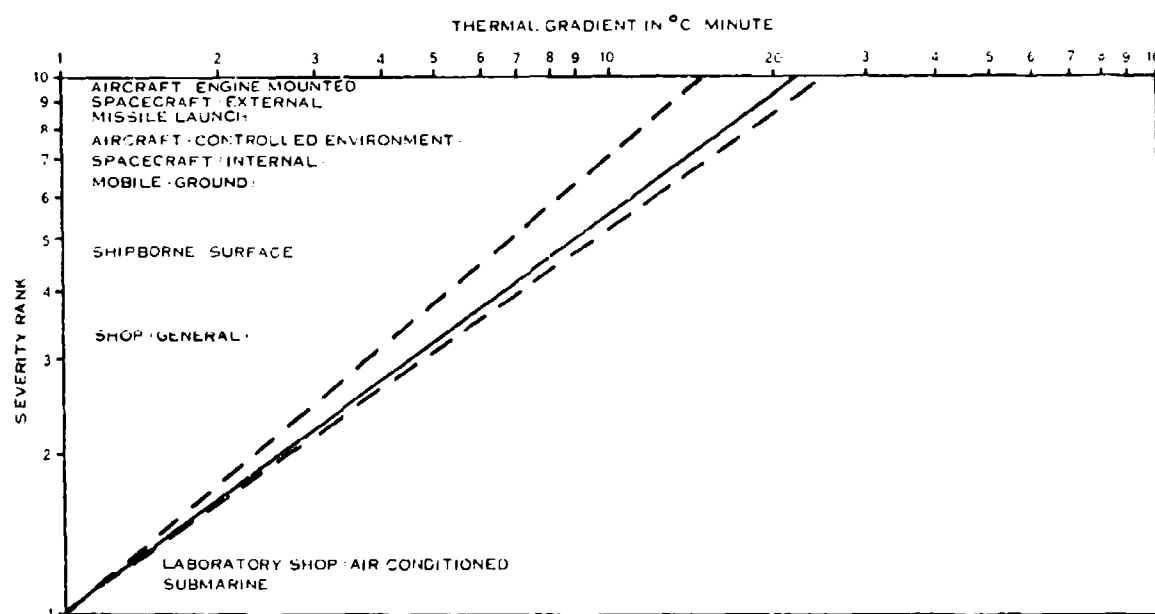
The thermal cycle screen shown in Figure 38 is based on an equipment complexity taken from the above for 2000 electronic parts corresponding to 10 thermal cycles (from Figure 40). The important aspects of the temperature range are (1) that there should be a delta of at least 160°F (71°C) between upper and lower extremes, and (2) that it should be representative of the use environment. Since in the equipment application being dealt with here, the temperature extremes normally are -40°C and +100°C, they were selected as the thermal conditions of the 100% screen. What will have the most effect in causing incipient failures to occur during the 10 cycles of thermal cycling is the temperature gradient.

The most effective thermal gradient for a given equipment will be that which best represents that found in its use environment. The normal range of thermal rates of change found should be between 1°C and 22°C; and the higher gradients are the most effective when utilized as a screen. The engine mounted environment in which hardware must provide continuous service over a number of years, normally can be considered to be one of the most severe. Design aspects built into the hardware such as externally supplied cooling and vibration isolation, tend to reduce the severity of the engine environment, however. In any case if one considers the range of use environments to be scaled from 1 to 10 with the most benign being 1, the most severe being 10, the engine mounted environment would be ranked in the vicinity of 10 (See Figure 41). The profile of the specified use environment, in other words, must be completely understood before an intelligent judgement in the selection of a thermal gradient intended as the rate of change in temperature during a thermal cycling test can be made. The enhancement of



E-5778

FIGURE 40 DETERMINATION OF NUMBER OF TEMPERATURE CYCLES AS A FUNCTION OF EQUIPMENT COMPLEXITY



E 1703

FIGURE 41 TEMPERATURE RATE OF CHANGE OF EQUIPMENT IN ITS USE ENVIRONMENT BY SEVERITY RANK

6.5 Continued

reliability at the end-item screening level is dependent upon the ability, or effectiveness, of the screening process in isolating incipient failure mechanisms that would ordinarily occur early in the life cycle of the hardware. Having determined the severity level of the use environment as being between 8 and 10, the thermal gradient to be applied during the temperature cycle screen approximates 22°C/min in the worst case.

Dwell time, the final parameter to be established, should be between 1 and 10 minutes. From the various referenced publications, the general consensus is that temperature soak periods do little to enhance reliability. Therefore, it is necessary only to establish thermal stability at either extreme and continue cycle testing. But to assure maximum effectiveness of the thermal gradient, equipment should be turned off on the down trend and be turned on when the temperature upswing commences.

Equipment should be thermal cycled with covers off where mechanically feasible. Studies have shown that covers offer some insulation from the cooling medium to the inner parts and assemblies.

While it may be cost prohibitive to perform functional testing, even on a limited scale, during the temperature cycling test, key output parameters should be monitored through some simplified means to alert test personnel of the occurrence of a fail condition. Special attention should be given to the determination of the condition of the key parameters during the last cycle, however, since this last cycle should be failure free. In the event a failure occurs during the thermal screen additional temperature cycles are to be conducted as a function of the complexity, ease, and quality of workmanship of the resulting repair action. Useful as a guide in making this determination is the following based upon excerpts of reference 53.

Percentage of Total Parts Repaired/Replaced	Number of Final Consecutive Temperature Cycles which must be survived by the Repaired/Replaced Portion of the Hardware*			
	4000 Parts (14 Cycles)	2000 Parts (10 Cycles)	500 Parts (5 Cycles)	100 Parts (3 Cycles)
0 to 0.1%	1	1	N/A	N/A
0.1% to 1%	2	1	1	N/A
1% to 5%	4	2	1	1
5% to 10%	6	4	2	1

*Additional cycles, as appropriate, should also be added when the repair cannot be easily and reliably performed.

6.5 Continued

Finally, having completed the temperature cycle test, a complete standard functional test should be performed at ambient temperature to determine the integrity of the balance of the parameters. The resulting data in conjunction with the failure data emanating from the thermal cycle test is to be evaluated in terms of module sensitivity. From this evaluation the effectiveness of the module level screening is to be measured. In the ideal case, all module related failures have been isolated during module testing and what remains are end-item, assembly peculiar failure mechanisms. Should the analysis effort prove the existence of a module-related failure mechanism, the module level screening conditions should be adjusted accordingly.

Returning to the production acceptance testing of the end item, from Figure 38 the next screen is random vibration. The extensive study and evaluation efforts referenced, conclusively show that sinusoidal vibration levels contained in MIL-STD-781B are ineffective. Experience at Hamilton Standard also echoes the conclusion reached. Support is given to random vibration for 30 minutes in each axis with equipment operating and of course monitored. The levels selected should be at least maximum specified values.

A complete functional test would follow the random vibration screen to ascertain that all parameters remain within specified limits. The temperature at which the final functional is to be conducted should be the specified maximum operating temperature, particularly during the development (pre-production) phase and should be conducted on enough hardware items to statistically prove the end item at that temperature. When the qualitative analysis supports the decision, reverting to the more simple ambient of 25°C could be done.

Penalty tests should be devised to screen any end-item peculiar failure mechanisms on an as required basis depending upon screening results and/or customer returns. Again the penalty test incorporated at the end item level should be aimed at resolving process, assembly, or test problems germane to the end assembly. Where a failure mechanism can be isolated to a lower level of assembly, the incorporation of the penalty test should be at that level where economically feasible.

6.6 Reliability Development Testing

A significant contribution to accelerating the maturity of equipments can be attained by the employment of CERT (Combined Environmental Reliability Test) testing on electronic engine controls. CERT is a form of reliability test that is oriented toward "developing" reliability rather than "demonstrating fixed" reliability. The reliability development test process is particularly

6.6 Continued

useful in the engine control area because comparable field experience is accrued at an extremely low rate, perhaps as low as 25 hours per month per aircraft. At this rate it could conceivably take years before MTBF values such as 25,000 hours can be substantiated. The cost of implementing corrective actions on user owned equipment is exorbitant, logistically difficult to administer, and reduces system availability. Thus, the overall purpose of CERT is to accumulate several thousand control operating hours in a simulated real world environment with early production units. The process objective then is to ensure theoretically and empirically that follow-on production controls will enter service with a high MTBF. This is illustrated in Figure 42.

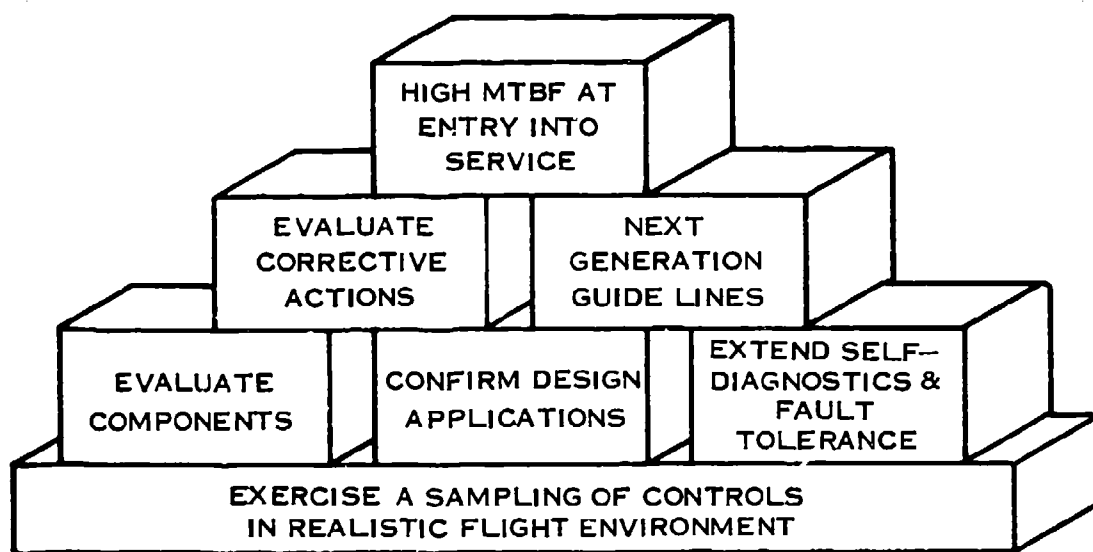
The CERT test facility provides sensor inputs and output loads for control operation. The environmental conditions which are obtained from actual flight profiles are applied in cycles and the performance of the controls monitored. Figure 43 illustrates a hypothetical reduction of real world conditions to CERT test conditions.

The CERT program should be operated in a test-fix-retest with delayed design fixes at three points. This is shown in Figure 44 as points F1, F2 and F3 on the time scale. The reliability of the control is expected to show growth during the test intervals with a jump expected at the time of the delayed fixes.

The increases in reliability at the time of delayed fixes occur as a result of a closed-loop corrective action system. Each failure during the CERT test period is analyzed for cause. The cause of the failures are categorized and collected into general areas of responsibility such as components, workmanship, design, etc. A decision is made to fix immediately or delay the fix to the next milestone. Previous fixes are closely monitored from the time of incorporation for recurrence to evaluate the effectiveness of any changes made to the control.

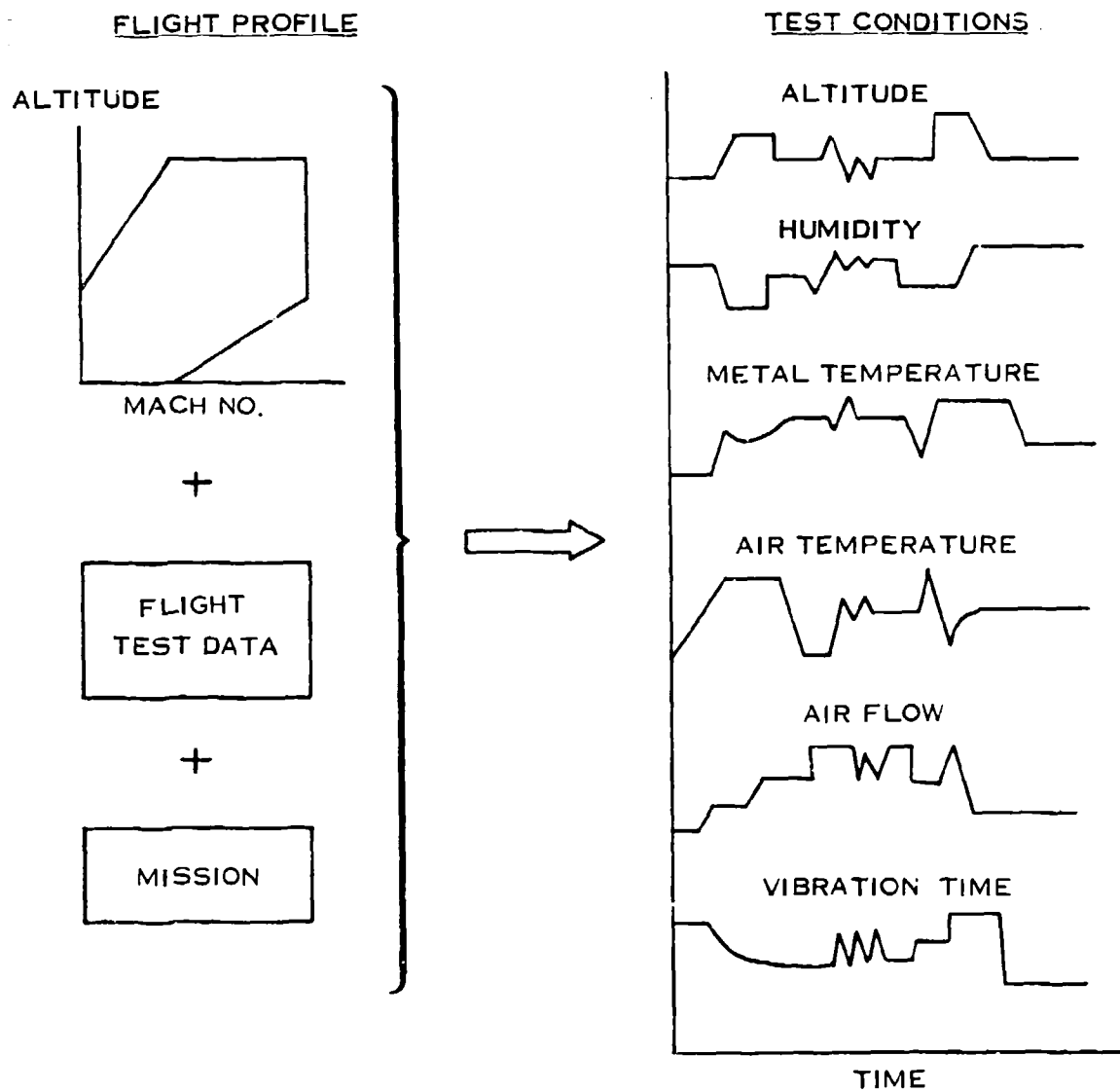
The past practice of purging all failures associated with a failure mode that has theoretically been eliminated by a fix will not be followed when assessing reliability. This practice is an unnecessary and unacceptable procedure when applied to reliability assessment. With the recent advances in reliability growth procedures and mathematical modeling, purging is unnecessary because of the newer statistical methods to analyze data with changing failure rates.

In the case for projecting reliability growth, it may be necessary to weight some of the failure modes based on a percentage of fix effectiveness when subsequent test data indicates a decrease in the failure rate for that mode.



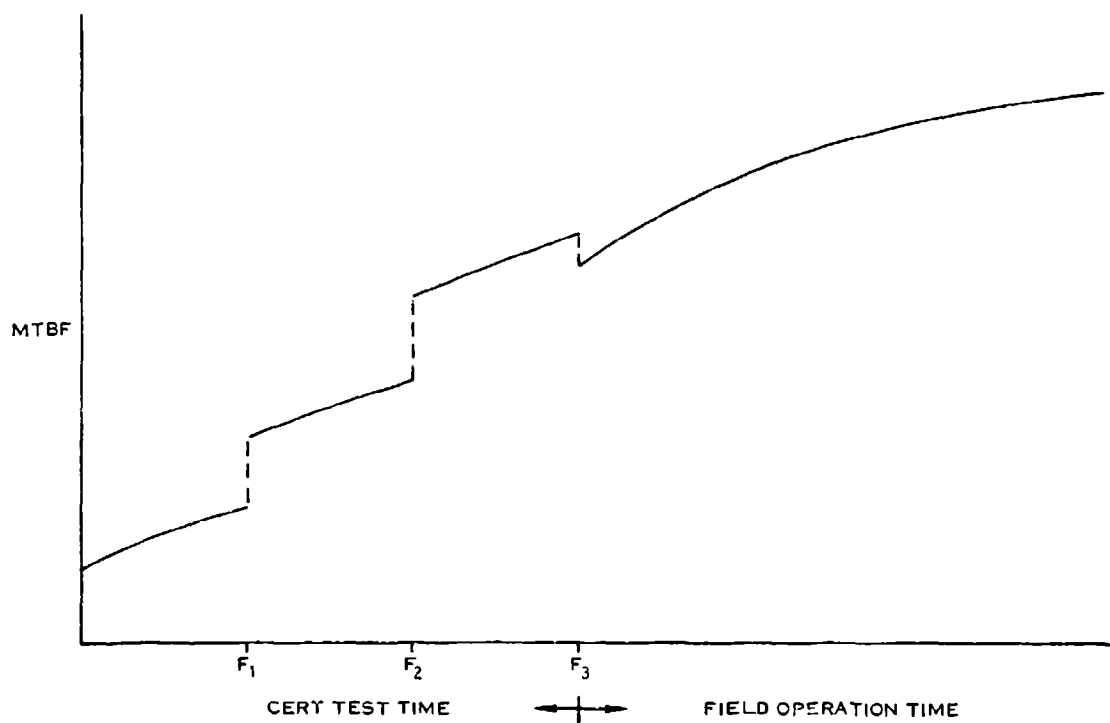
E-5703

FIGURE 42 CERT OBJECTIVES



E-6214

FIGURE 43 CERT TEST CONDITIONS



E-5709

FIGURE 44 RELIABILITY GROWTH CYCLE

6.6 Continued

At the conclusion of the CERT test phase of the program, the generalized growth curve in Figure 44 shows an initial drop in projected reliability. This drop is expected to offset the gains which could be anticipated for the last delayed fix. This lowered value of expected growth is caused by differences in actual versus simulated environments and field personnel unfamiliarity in handling and maintaining a new product. However, the reliability growth rate is expected to quickly resume the projected growth rate after a short shakedown period.

6.7 Reliability Growth Modeling

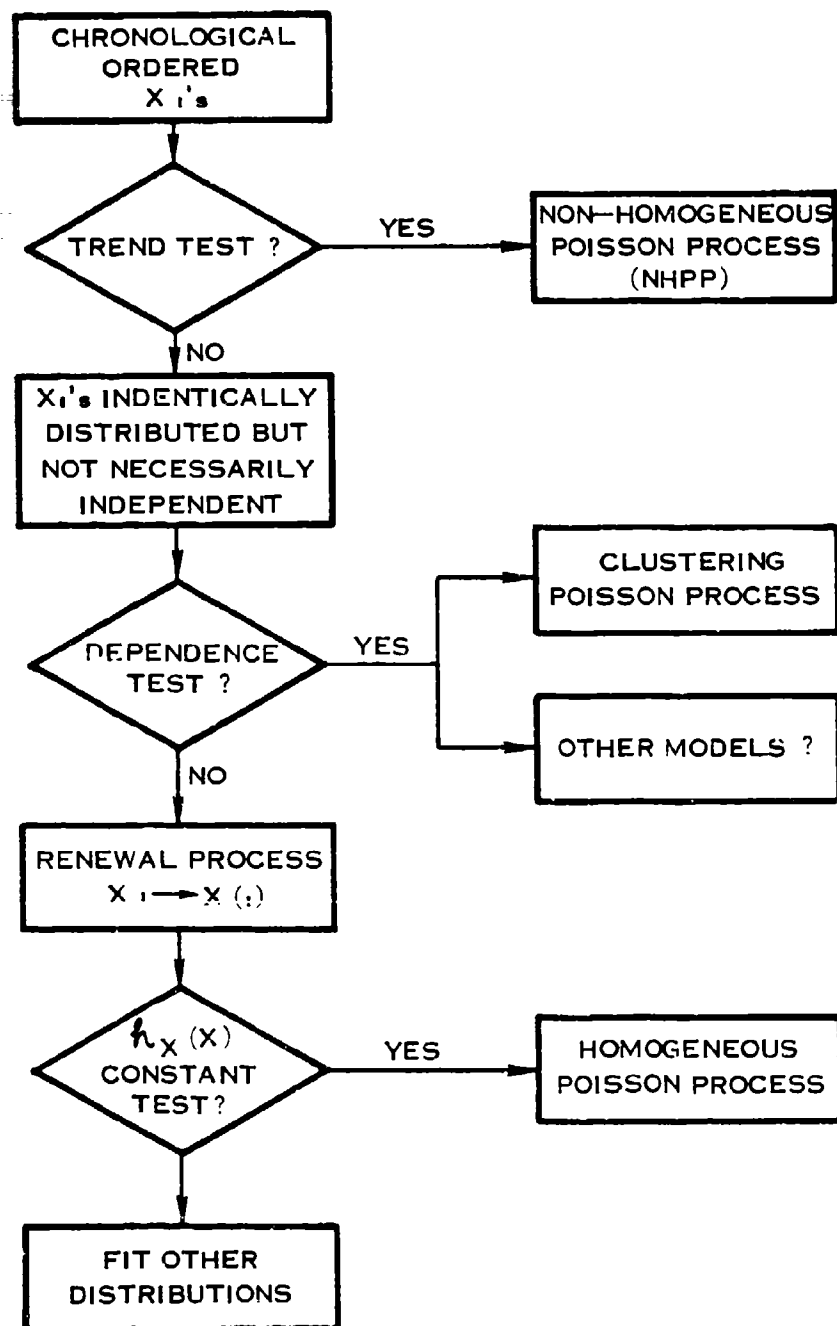
The development of designs and growth tests must be evaluated by sound mathematical techniques. The timely application and accuracy of these techniques is necessary to assure that:

- a. They will aid in the program planning so that milestones may be put into perspective with respect to the reliability goals.
- b. They will identify and quantify the impact of corrective actions.
- c. They will aid in allocation and reallocation of resources to achieve goals within the other program constraints.
- d. Optimization of the reliability growth process is achieved.

6.7.1 Generalized Statistical Analysis

A Generalized Statistical Analysis Flow Chart is shown in Figure 45 which presents a summary of the basic notions on how a reliability growth analysis should be performed. There are a great number of details required to perform a specific analysis but broadly speaking, the flow chart shows the main steps in an analysis.

The reliability growth modeling presented in the remainder of this guide will primarily be concerned with the Non-homogeneous Poisson Process (NHPP) which is also known as the Army Material Systems Analysis Activity (AMSAA) reliability growth model.



E-5700

FIGURE 45 GENERALIZED STATISTICAL ANALYSIS FLOW CHART

6.7.1.1 Trend Testing

Trend tests, i.e., tests to determine whether there is a long term tendency for successive times between failures to become smaller (or larger), are discussed next. If a trend exists the Non-homogeneous Poisson Process is the simplest stochastic process which may be an adequate representation. It is possible that a more complex model may be required, but it has been shown no such model for repairable system reliability is really necessary from a statistical viewpoint.

The simplest way to perform a trend test is to plot cumulative number of failures versus cumulative operating time as in the graph of Figure 46. If times-between-failures are tending to become smaller and smaller, a concave-up shape will result as depicted in the figure. Conversely, if the times are getting larger, the plot will be concave-down. An alternate procedure is to estimate the average rate of occurrence of failures in three or more subintervals. In Figure 47, $P(t)$ is estimated for each subinterval by dividing the number of failures in that subinterval by $t_0/3$. Wearout (growth) is indicated if the successive estimates become larger (smaller). In extreme enough cases "eyeball" analyses of such plots will be adequate to disclose reliability growth or long term wearout. In most cases, however, quantitative tests will be necessary.

Under the null hypothesis of a homogeneous Poisson Process the T_i will be independent and uniformly distributed on $(0, t_0)$. Hence, for critical values corresponding to the 5% level of significance,

$$\left(\frac{\sum_{i=1}^n T_i}{n t_0} - \frac{1}{2} \right) \left(\sqrt{12n} \right)$$

can be considered to be unit normal distributed, for n as small as 3, under the null hypothesis. This test had the following simple interpretation: under wearout (growth) the T_i will tend to occur after (before) the midpoint of the observed interval. Hence, under wearout (growth), n will

$$\sum_{i=1}^n T_i / n t_0$$

tend to be large (small). In other words, significantly large (small) values of the standardized variate

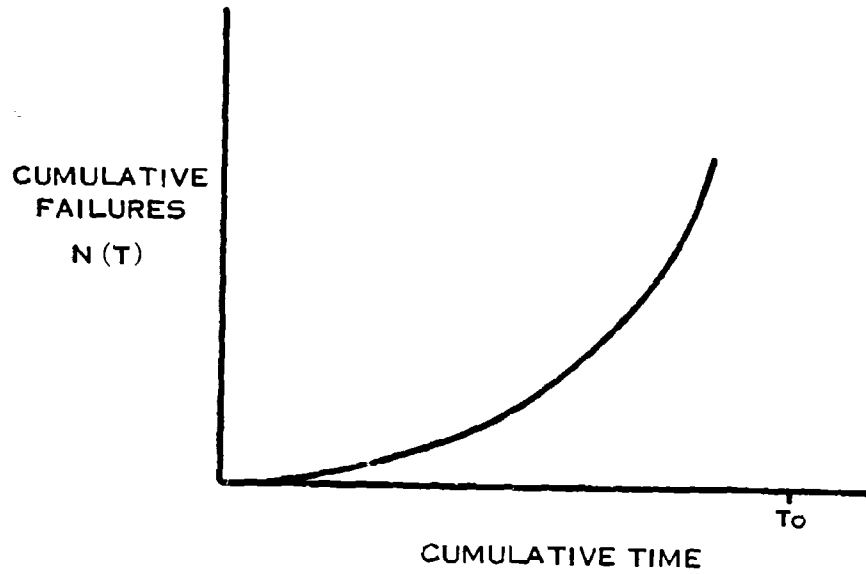


FIGURE 46 CUMULATIVE FAILURES

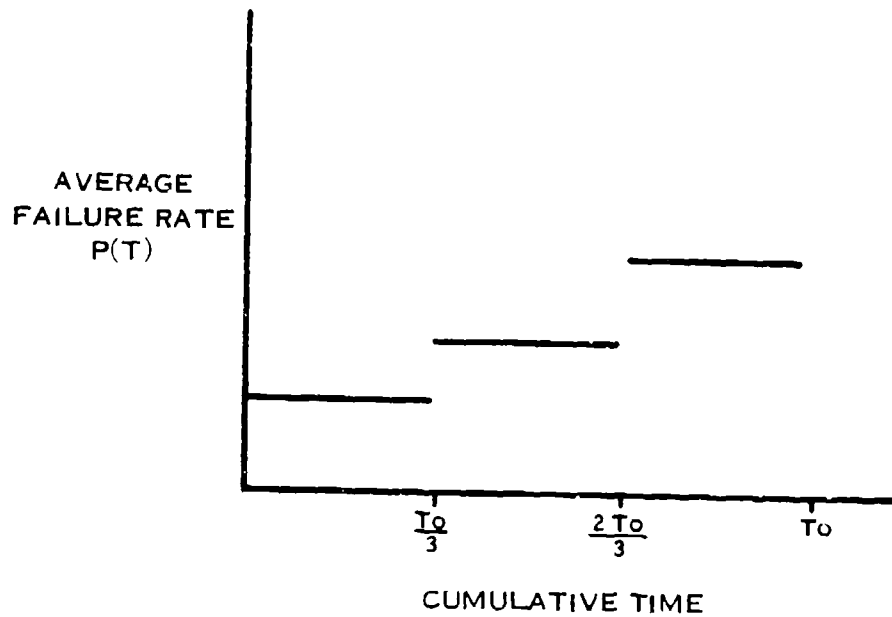


FIGURE 47 AVERAGE FAILURE RATE

6.7.1.1 Continued

$$\left(\frac{\sum_{i=1}^n T_i}{n t_0} - \frac{1}{2} \right) \left(\sqrt{12n} \right)$$

show significant evidence of wearout (growth). Since this test is so simple to implement and to interpret, it may appear to be "quick and dirty". Actually, however, it has been shown to be an optimum test against at least two plausible models by Cox (1955) and Bates (1955).

Laplace's test is not consistent against alternatives where the rate of occurrence of failure is non-monotone in such a way that $E(\sum T_i/n t_0) = 1/2$. In this case, a test developed by Hollander and Proschan (1974) is superior.

6.7.1.2 AMSAA Reliability Growth Model

6.7.1.2.1 Basis of the Model. The US Army Material Systems Analysis Activity (AMSAA) employs a stochastic process to model reliability growth. This model adequately represents the improvement in reliability during development for a wide variety of systems. It is applicable to systems for which usage is measured on a continuous scale; for example, time in hours or distance in miles. For the sake of simplicity usage is referred to as time in the sequel. Duane (7) first observed that, for each of several systems, the number of failures accumulated at total operating time t could be approximated by λt^β , in which λ and β were positive parameters which varied from one system to another. The exponent must be less than one for representation of reliability growth. Historical data indicate that intensive reliability improvement programs are characterized by this parameter being in the range from .5 to .7.

6.7.1.2.2 Stochastic Formulation. Crow (56) formulated a statistical model to describe the pattern of reliability growth. This model provides that the average number of failures accumulated by time t is expressed as λt^β , but the actual number of failures observed to that time is a random variable described by the Weibull process. Other references on this process include

Kemphorne and Folks (57), Englehardt and Bain (58), Bassin (59), Crow (60), (61), Finklestein (62), and Lee and Lee (63). This development supplies methods for calculating statistically valid estimates of the mean time between failures which the system would exhibit if no further improvements are incorporated. This constitutes a means for monitoring reliability growth during the development process.

6.7.1.2.3 Cumulative Number of Failures. The total number of failures, $N(t)$, accumulated on all test items in cumulative test time t is a random variable with the Poisson distribution. The probability that exactly n failures occur between the initiation of testing and total test time t is

$$P \{ N(t) = n \} = \frac{m(t)^n e^{-m(t)}}{n!}$$

in which $m(t)$ is the mean value function; that is, the expected number of failures expressed as a function of test time. To describe the reliability growth process this function is of the form

$$m(t) = \lambda t^\beta$$

in which λ and β are positive parameters.

6.7.1.2.4 Number of Failures in an Interval. The number of failures occurring in the interval from test time a until test time b is a random variable having the Poisson distribution with mean

$$m(b) - m(a) = \lambda (b^\beta - a^\beta).$$

The number of failures occurring in any interval is statistically independent of the number of failures in any interval which does not overlap the first interval. Only one failure can occur at any instant. The time history of the cumulative number of failures is said to be a non-homogeneous Poisson process or more precisely a Weibull process.

6.7.1.2.5 Intensity Function. The rate of change of the mean value function is called the intensity function of the process. For the reliability growth process the intensity function is

$$\rho(t) = \lambda \beta t^{\beta-1}$$

The probability of the occurrence of a failure between time t and time $t+h$ is approximately $\rho(t)h$ if the increment h is sufficiently small. The intensity function is sometimes called the failure rate; however, this concept is different from that of the failure rate or hazard rate of a life distribution.

Caution should be exercised so that the two ideas are not confused. The parameter λ is called a scale parameter because it depends upon the unit of measurement chosen for t . The parameter β is of prime importance because it characterizes the shape of the graph of the intensity function. If β is equal to one, the intensity function is constant. In that case the reliability of the system is not changing since the times between successive failures are independent, identically distributed random variables with an exponential distribution with mean λ^{-1} . If β is not equal to one the times between successive failures are not identically distributed and do not have exponential distributions. For a development process during which the system

6.7.1.2.5 Continued

improves the shape parameter β is less than one, and typically not less than .5. In this case the expected number of failures in an interval of fixed length decreases as its starting point increases. In a poorly managed reliability program improper design changes can result in degradation of system reliability. This situation is characterized by values of the shape parameter β greater than one. This indicates that the number of failures expected in a fixed increment of time is increasing with time.

6.7.1.2.6 Mean Time Between Failures. Parameters such as mean time between failures are used conventionally to represent the reliability performance of repairable systems. The use of these parameters to completely characterize reliability reflects the assumption that the times between failures are identically distributed. In particular, it is commonly assumed that these times come from the same exponential distribution. This corresponds to the special case of the reliability growth process in which the shape parameter is one. This special case is called a homogeneous Poisson process. It is proper to use the reliability growth model to predict a value of the mean time between failures for such a system. While it is in development the occurrence of failures follows the reliability growth process with a decreasing intensity function if the system is improving due to design changes. When production commences the design is fixed and therefore no further reliability improvement is assumed. The constant value of the intensity function for the production model should be approximately equal to the value of the intensity function at the end of development testing. Thus, the anticipated mean time between failures for the production model is equal to the reciprocal of the intensity function if the system is improving due to design changes. When production commences the design is fixed and therefore no further reliability improvement is assumed. The constant value of the intensity function for the production model should be approximately equal to the value of the intensity function at the end of development testing. Thus, the anticipated mean time between failures for the production model is equal to the reciprocal of the intensity function at the end of the development phase.

6.7.1.3 Reliability Growth Assessment

6.7.1.3.1 Graphical Estimation. Plots derived from the failure data provide a graphic description of test results. They furnish the analyst a means to examine the nature of the data. Graphical methods can also be used to obtain rough estimates of the reliability parameters of interest in the reliability growth process. Two types of graphs are described below. The first tells the analyst if growth is obviously demonstrated by the data. The second method goes further since it provides rough estimates of the two parameters in the expression for the intensity function.

6.7.1.3.2 Average Failure Frequency Plots. Construction of a plot of the average failure frequencies observed during testing yields a crude approximation of the intensity function. To construct such a plot divide the elapsed test time into at least three nonoverlapping intervals. These nonoverlapping intervals can be of unequal length. Next calculate the

6.7.1.3.2 Continued

frequency of occurrence of failures within each interval by dividing the number of failures in the interval by its length. Plot the failure frequency as a horizontal line at the appropriate ordinate. The line should extend over the abscissas corresponding to time within the interval. Any significant increasing or decreasing trend in the intensity function should be apparent from this plot.

6.7.1.3.3 Cumulative Failure Plots. A graph of the observed cumulative number of failures plotted against cumulative test time on full logarithmic paper furnishes crude estimates of the parameters which describe the intensity function. Taking logarithms in the expression for the mean value function yields the result

$$\ln m(t) = \ln \lambda + \beta \ln t$$

Therefore, the expression for the mean value function is represented by a straight line on full logarithmic paper. A line drawn to fit the data points representing the cumulative number of failures at the time of each failure occurrence is a suitable approximation of the true line. The ordinate of the point on the line corresponding to t equal to one is an estimate of λ . The actual slope of the line as measured with a ruler yields an estimate of the shape parameter β . Alternate methods include the plotting of the cumulative numbers of failures divided by cumulative test time or the reciprocal of that quantity. If either of those methods is used, the method for estimating the parameters is slightly more complicated.

6.7.1.3.4 Statistical Estimation. Modeling reliability growth as a non-homogeneous Poisson process permits the assessment of the demonstrated reliability performance by statistical procedures. The method of maximum likelihood provides estimates of the scale parameter λ and the shape parameter β . These estimates are used in estimation of the intensity function. The reciprocal of the current value of the intensity function is the mean time between failures that the system would exhibit in the absence of further improvements. Procedures for point estimation and interval estimation of mean time between failures are described below. The data employed in the estimation consist of failure times from testing terminated at a given time or from testing terminated at the occurrence of a specified number of failures. The procedures vary slightly for these two types of tests. A goodness of fit test to determine whether the model is appropriate to describe the data is also described below. If the exact times of failure occurrence are unknown, it may still be possible to utilize the reliability growth model. This is the case when inspections are conducted to uncover hidden failures. Procedures to use in that instance are described by grouped data.

6.7.1.3.5 Time Terminated Testing. The procedures described in this section are to be used to analyze data from tests which are terminated at a pre-determined time or tests which are in progress with data available through some time. The required data consists of the cumulative test time on all systems at the occurrence of each failure as well as the accumulated test time. To calculate the cumulative test time of a failure occurrence it is necessary to sum the test time on every system at that instant. The data then consists of the N failure times $X_1, X_2, \dots, X_N$ which occur prior to the accumulated test time T.

6.7.1.3.6 Point Estimation. The method of maximum likelihood provides point estimates of the parameters of the reliability growth process. The estimate of the shape parameter is

$$\hat{\beta} = \frac{N}{N \ln T - \sum_{i=1}^N \ln X_i}$$

Subsequently, the scale parameter λ is estimated by $\hat{\lambda} = N/T^{\hat{\beta}}$. It follows that for any time t the intensity function is estimated by $\hat{\rho}(t) = \hat{\lambda} \hat{\beta} t^{\hat{\beta}-1}$. In particular, this holds for T, the accumulated test time. The reciprocal of $\hat{\rho}(T)$ provides an estimate of the mean time between failures which could be anticipated if the system configuration remains as it is at time T. If the reliability program is expected to continue without any shift in emphasis or environment, then the intensity function may be projected into the future to predict the benefit of continued attempts to improve reliability. Although the estimators use all failure occurrences, the model is effectively self-purging. The estimator $\hat{\rho}(T)$ can be written as $\hat{\beta}(N/T)$. Note that N/T would be the estimate of the intensity function for a homogeneous Poisson process. Hence, the fraction $(1 - \hat{\beta})$ of the failures are effectively eliminated.

6.7.1.3.7 Interval Estimation. Interval estimates provide a measure of the uncertainty regarding the demonstration of reliability by testing. For the reliability growth process the parameter of primary interest is the mean time between failures that the system would exhibit after the initiation of production. The probability distribution of the point estimate of the intensity function at the end of the test is the basis for the interval estimate of the true value of the intensity function at that time. The values in Table 15 facilitate computation of confidence interval estimates for the mean time between failures. The table provides two-sided interval estimates on the ratio of the true MTBF to the estimated MTBF for several values of the confidence coefficient. If the number of failures is N and γ

TABLE 15 CONFIDENCE INTERVALS FOR MTBF FROM TIME TERMINATED TEST

N \ Y	.80		.90		.95		.98	
	L	U	L	U	L	U	L	U
2	.261	13.66	.200	38.66	.159	78.66	.124	198.7
3	.333	6.326	.263	9.736	.217	14.55	.174	24.10
4	.385	4.243	.312	5.947	.262	3.093	.215	11.81
5	.426	3.586	.352	4.517	.300	5.862	.250	8.043
6	.459	2.915	.385	3.764	.331	4.738	.280	6.254
7	.487	2.616	.412	3.298	.358	4.061	.305	5.216
8	.511	2.407	.436	2.981	.382	3.609	.328	4.539
9	.531	2.254	.457	2.750	.403	3.285	.349	4.064
10	.549	2.136	.476	2.575	.421	3.042	.367	3.712
11	.565	2.041	.492	2.436	.438	2.852	.384	3.441
12	.579	1.965	.507	2.324	.453	2.699	.399	3.226
13	.592	1.901	.521	2.232	.467	2.574	.413	3.050
14	.604	1.846	.533	2.153	.480	2.469	.426	2.904
15	.614	1.800	.545	2.087	.492	2.379	.438	2.781
16	.624	1.759	.556	2.029	.503	2.302	.449	2.675
17	.633	1.723	.565	1.978	.513	2.235	.460	2.584
18	.642	1.692	.575	1.933	.523	2.176	.470	2.505
19	.650	1.663	.583	1.893	.532	2.123	.479	2.432
20	.657	1.638	.591	1.858	.540	2.076	.488	2.369
21	.664	1.615	.599	1.825	.548	2.034	.496	2.313
22	.670	1.594	.606	1.796	.556	1.996	.504	2.261
23	.676	1.574	.613	1.769	.563	1.961	.511	2.215
24	.682	1.557	.619	1.745	.570	1.929	.518	2.173
25	.687	1.540	.625	1.722	.576	1.900	.525	2.134
26	.692	1.525	.631	1.701	.582	1.873	.531	2.098
27	.697	1.511	.636	1.682	.588	1.848	.537	2.068
28	.702	1.498	.641	1.664	.594	1.825	.543	2.035
29	.706	1.486	.646	1.647	.599	1.803	.549	2.006
30	.711	1.475	.651	1.631	.604	1.783	.554	1.980
35	.729	1.427	.672	1.565	.627	1.699	.579	1.870
40	.745	1.390	.690	1.515	.646	1.635	.599	1.788
45	.758	1.361	.705	1.476	.662	1.585	.617	1.723
50	.769	1.337	.718	1.443	.676	1.544	.632	1.671
60	.787	1.300	.739	1.393	.700	1.481	.657	1.591
70	.801	1.272	.756	1.356	.718	1.435	.678	1.533
80	.813	1.251	.769	1.328	.734	1.399	.695	1.488
100	.831	1.219	.791	1.286	.758	1.347	.722	1.423

For $N > 100$,

$$L = (1 + Z_{.5 + \frac{Y}{2}} \sqrt{2N})^{-2} \quad U = (1 - Z_{.5 + \frac{Y}{2}} \sqrt{2N})^{-2}$$

in which $Z_{.5 + \frac{Y}{2}}$ is the $(.5 + \frac{Y}{2})$ -th percentile of the standard normal distribution.

6.7.1.3.7 Continued

is the selected confidence coefficient, then the appropriate tabular values are L_N , U_N , and γ . The interval estimate of MTBF is

$$\frac{L_N, \gamma}{\hat{\rho}(T)} \leq \text{MTBF} \leq \frac{U_N, \gamma}{\hat{\rho}(T)}$$

Because the number of failures has a discrete probability distribution, these interval estimates are conservative; that is, the actual confidence coefficient is slightly larger than the stated confidence coefficient.

6.7.1.3.8 Goodness of Fit. The null hypothesis that a nonhomogeneous Poisson process with an intensity function of the form $\gamma \beta t^{\beta-1}$ properly describes the reliability growth of a particular system is tested by the use of a Cramer-von Mises statistic. An unbiased estimate of the shape parameter is used to calculate that statistic. This estimate of β is

$$\bar{\beta} = \frac{N-1}{N} \hat{\beta}$$

for a time terminated test with N failure occurrences. The estimate $\bar{\beta}$ is described as the point estimate. The goodness of fit statistic is

$$C_N^2 = \frac{1}{12N} + \sum_{i=1}^N \left[\left(\frac{x_i}{T} \right)^{\bar{\beta}} - \frac{2i-1}{2N} \right]^2$$

in which the failure times must be ordered so that $0 < x_1 < x_2 < \dots < x_N$. The null hypothesis is rejected if the statistic C_N^2 exceeds the critical value for the level of significance selected by the analyst. Critical values of C_N^2 for the .20, .15, .10, .05, and .01 levels of significance (α) have been computed and are in Table 16. The table is indexed by a parameter labeled M. For time terminated testing M is equal to N, the number of failures. If the test rejects the reliability growth model, an examination of the data may reveal the reason for the lack of fit. Possible causes of rejection include the occurrence of more than one failure at the same time or the occurrence of a discontinuity in the intensity function. In the first case, an appropriate procedure may be to group the data. In the latter case the data should be treated as a discontinuity.

TABLE 16 CRITICAL VALUES FOR CRAMER-VON MISES GOODNESS OF FIT TEST

$\alpha \backslash M$	.20	.15	.10	.05	.01
2	.138	.149	.162	.175	.186
3	.121	.135	.154	.184	.23
4	.121	.134	.155	.191	.28
5	.121	.137	.160	.199	.30
6	.123	.139	.162	.204	.31
7	.124	.140	.165	.208	.32
8	.124	.141	.165	.210	.32
9	.125	.142	.167	.212	.32
10	.125	.142	.167	.212	.32
11	.126	.143	.169	.214	.32
12	.126	.144	.169	.214	.32
13	.126	.144	.169	.214	.32
14	.126	.144	.169	.214	.33
15	.126	.144	.169	.215	.33
16	.127	.145	.171	.216	.33
17	.127	.145	.171	.217	.33
18	.127	.146	.171	.217	.33
19	.127	.146	.171	.217	.33
20	.128	.146	.172	.217	.33
30	.128	.146	.172	.218	.33
60	.128	.147	.173	.220	.33
100	.129	.147	.173	.220	.34

For $M > 100$ use values for $M = 100$.

6.7.1.3.9 Failure Terminated Testing. The procedures described in this section are applicable to tests which are terminated upon the accumulation of a specified number of failures. The procedures are only slightly different from those used for time terminated testing. The data consist of N failure times $X_1, X_2, \dots, X_N$ expressed in terms of cumulative test time and arranged in nondecreasing order.

6.7.1.3.10 Point Estimation. The method of maximum likelihood furnishes point estimates of the shape parameter β and the scale parameter λ . The estimate of β is

$$\hat{\beta} = \frac{N}{(N-1) \ln X_N - \sum_{i=1}^{N-1} \ln X_i}$$

Note that this is equivalent to the estimate for time terminated testing with the test time equal to the time of occurrence of the last failure. The scale parameter λ is estimated by

$$\hat{\lambda} = \frac{N}{T} \hat{\beta}$$

as before. The intensity function and mean time between failures are estimated as before. For small sample sizes use of unbiased estimator $\bar{\beta}$ is advisable.

6.7.1.3.11 Interval Estimation. An interval estimate of the mean time between failures that the system would exhibit in the absence of further change is also available for the case of failure terminated testing. Table 17 provides factors for the construction of two-sided interval estimates of the MTBF for several values of the confidence coefficient γ . The smaller number corresponding to the number of failures and desired confidence coefficient is divided by the point estimate of the intensity function at the end of the test to yield the lower limit of the interval. Division of the larger value by the intensity function estimate provides the upper limit.

6.7.1.3.12 Goodness of Fit. The hypothesis that the AMSAA model is appropriate can be tested using a Cramer-von Mises statistic. It is important to note the difference in the calculations from those for time terminated testing. An unbiased estimate of the shape parameter given by

$$\bar{\beta} = \frac{N-2}{N} \hat{\beta}$$

TABLE 17 CONFIDENCE INTERVALS FOR MTBF FROM FAILURE TERMINATED TEST

N	Y	.80		.90		.95		.98	
		L	U	L	U	L	U	L	U
2		.3063	33.76	.5352	72.67	.4099	151.5	.2944	389.9
3		.6340	3.937	.5137	14.24	.4054	21.96	.3119	37.60
4		.5601	5.323	.5174	7.651	.4225	10.63	.3368	15.96
5		.6568	4.000	.5290	5.424	.4415	7.147	.3603	9.995
6		.6600	3.321	.5421	4.339	.4595	5.521	.3815	7.388
7		.6656	2.910	.5548	3.702	.4760	4.595	.4003	5.963
8		.6720	2.634	.5668	3.284	.4910	4.002	.4173	5.074
9		.6787	2.436	.5780	2.989	.5046	3.589	.4327	4.469
10		.6852	2.287	.5883	2.770	.5171	3.286	.4467	4.032
11		.6915	2.170	.5979	2.600	.5285	3.054	.4595	3.702
12		.6975	2.076	.6067	2.464	.5391	2.870	.4712	3.443
13		.7033	1.999	.6150	2.353	.5488	2.721	.4821	3.235
14		.7087	1.933	.6227	2.260	.5579	2.597	.4923	3.064
15		.7139	1.877	.6299	2.182	.5664	2.493	.5017	2.921
16		.7188	1.829	.6367	2.114	.5743	2.404	.5106	2.800
17		.7234	1.788	.6431	2.056	.5818	2.327	.5189	2.695
18		.7278	1.751	.6491	2.004	.5888	2.259	.5267	2.604
19		.7320	1.718	.6547	1.959	.5954	2.200	.5341	2.524
20		.7360	1.688	.6601	1.913	.6016	2.147	.5411	2.453
21		.7398	1.662	.6652	1.881	.6076	2.099	.5473	2.390
22		.7434	1.638	.6701	1.848	.6132	2.056	.5541	2.333
23		.7469	1.616	.6747	1.818	.6186	2.017	.5601	2.281
24		.7502	1.596	.6791	1.790	.6237	1.982	.5659	2.235
25		.7534	1.578	.6833	1.765	.6286	1.949	.5714	2.192
26		.7565	1.561	.6873	1.742	.6333	1.919	.5766	2.153
27		.7594	1.545	.6912	1.720	.6379	1.892	.5817	2.117
28		.7622	1.530	.6949	1.700	.6421	1.866	.5865	2.083
29		.7649	1.516	.6985	1.682	.6462	1.842	.5912	2.052
30		.7676	1.504	.7019	1.664	.6502	1.820	.5957	2.023
35		.7794	1.450	.7173	1.592	.6681	1.729	.6159	1.905
40		.7894	1.410	.7303	1.538	.6832	1.660	.6329	1.816
45		.7981	1.378	.7415	1.495	.6962	1.606	.6476	1.747
50		.8057	1.352	.7513	1.460	.7076	1.562	.6605	1.692
60		.8184	1.312	.7678	1.407	.7267	1.496	.6823	1.607
70		.8288	1.282	.7811	1.367	.7423	1.447	.7000	1.546
80		.8375	1.259	.7922	1.337	.7553	1.409	.7148	1.499
100		.8514	1.225	.8100	1.293	.7759	1.355	.7334	1.431

For $N > 100$,

$$L = \left[1 - \sqrt{\frac{2}{N}} \left(z_{.5 + \frac{Y}{2}} \right) \right]^{-1} \quad U = \left[1 - \sqrt{\frac{2}{N}} \left(z_{.5 - \frac{Y}{2}} \right) \right]^{-1}$$

in which $z_{.5 + \frac{Y}{2}}$ is the $(.5 + \frac{Y}{2})$ -th percentile of the standard normal distribution.

6.7.1.3.12 Continued

is used in calculation of the goodness of fit statistic. The parameter for indexing that statistic is M which is one less than N , the number of failures. The Cramer-von Mises statistic is then:

$$C_M^2 = \frac{1}{12M} + \sum_{i=1}^M \left[\left(\frac{x_i}{x_N} \right)^{\bar{\beta}} - \frac{2i-1}{2M} \right]^2$$

Table 16 provides critical values for use in the test. The model is deemed inappropriate if the statistic C_M^2 exceeds the critical value for some specified level of significance α .

6.7.1.3.13 Grouped Data. It may happen that an event included within the scope of the definition of the term "failure" does not preclude the operation of the equipment. It is possible that such events are not uncovered until a thorough inspection is conducted. In this case the exact time of the failure is unknown; however, one can presume that it happened in the interval since the last inspection. The total number of failures in the interval between inspections is therefore the sum of the number of failures detected at the time of occurrence and the number of failures found in the inspection. Such totals for each interval can be used to estimate reliability growth in accordance with the AMSAA model if there are at least three intervals.

6.7.1.3.14 Point Estimation From Grouped Data. The data consist of the total number of failures in each of K intervals of test time. The first interval starts at test time zero. The intervals do not have to be of equal length. Denote the number of failures in the interval from t_{i-1} to t_i by n_i . By convention t_0 is equal to zero. The maximum likelihood estimate of the shape parameter β is the value which satisfies

$$\sum_{i=1}^K n_i \left[\frac{t_i^{\hat{\beta}} \ln t_i - t_{i-1}^{\hat{\beta}} \ln t_{i-1}}{t_i^{\hat{\beta}} - t_{i-1}^{\hat{\beta}}} - \ln t_K \right] = 0,$$

in which $t_0 \ln t_0$ is defined as zero. This nonlinear equation can be easily solved by any of several iterative procedures. The scale parameter estimate is

6.7.1.3.14 Continued

$$\hat{\lambda} = \frac{\sum_{i=1}^K n_i}{\hat{\beta} t_K}$$

which corresponds to the result for testing when all failure times are known with the exception that the estimate of β is calculated differently. Point estimates of the intensity function and the mean time between failures are calculated as explained for point estimates.

6.7.1.3.15 Goodness of Fit. A chi-squared goodness of fit test can be used to test the hypothesis that the AMSAA reliability growth model adequately represents a set of grouped data. The expected number of failures in the interval from t_{i-1} to t_i is approximated by

$$e_i = \hat{\lambda} (\hat{\beta} t_i - \hat{\beta} t_{i-1})$$

Adjacent intervals may have to be combined so that the expected number of failures in any combined interval is at least five. Let the number of intervals after this combination be K and let the number of failures in the i -th interval be N_i . Furthermore, let e_i' be the expected number of failures in the i -th new interval. Then the statistic

$$\chi^2 = \sum_{i=1}^K \frac{(N_i' - e_i')^2}{e_i'}$$

is approximately distributed as an χ^2 random variable with $K-2$ degrees of freedom. The critical values for this statistic can be found in tables of the chi-squared distribution.

6.7.1.3.16 Discontinuities in the Intensity Function. The simultaneous introduction of several design changes, a change in emphasis in the reliability program, or some other factor may cause an abrupt change in the intensity function. Such a jump should be detected by a departure from linearity in the full logarithmic plot of cumulative failures, a large change in the level of the average failure frequency, or rejection of the model by a goodness of fit test.

6.7.1.3.17 Location of Discontinuity. The cumulative test time at which a discontinuity has occurred can be determined by inspection from graphs of cumulative failures or average failure frequency. The methods presented above can then be used to estimate the intensity function by use of different parameters for the period before the jump and for the period after the jump. That is, if the discontinuity occurs at time T_J , then the intensity function is estimated by

$$\begin{aligned}\hat{p}(t) &= \hat{\lambda}_1 \hat{\beta}_1 t^{\hat{\beta}_1 - 1} & 0 < t \leq T_J \\ &= \lambda_2 \beta_2 (t - T_J)^{\beta_2 - 1} & t > T_J\end{aligned}$$

in which λ_1 and β_1 are estimated only from failures on or before T_J and λ_2 and β_2 are estimated from those failures occurring after T_J . Only the second of these equations is needed to estimate the currently achieved value of the intensity function.

6.7.2 Early Reliability Growth Evaluation

The modeling of early reliability growth by using differential equations is a very useful technique for determining and reflecting known underlying failure mechanisms which are contributing to reliability growth.

The IBM differential equation growth model advanced by Rosner (64) is highly useful in that it is one of the few models addressing burn-in and screening effects. The model takes into account the nonlinearity of early growth and incorporates very plausible assumptions.

The IBM model assumes, explicitly, that: 1) there are random (constant intensity function) failures occurring at rate λ , and 2) there are a fixed but unknown, number of nonrandom design, manufacturing and workmanship defects present in the system at the beginning of testing. Let $N(t)$ be the number of nonrandom type defects remaining at time $t \geq 0$. This model makes the intuitively plausible assumption that the rate of change of $N(t)$ with

6.7.2 Continued

respect to time is proportional to the number of nonrandom defects remaining at t . That is,

$$dN(t)/dt = -K_2N(t)$$

and hence

$$N(t) = e^{-K_2 t + c}$$

Now if we denote the unknown number of nonrandom failures present at $t=0$ by K_1 then

$$N(t) = K_1 e^{-K_2 t} \quad t > 0, K_1, K_2 > 0$$

Defining $V(t)$ to be the expected cumulative number of failures up to time t then

$$V(t) = \lambda t + K_1 (1 - e^{-K_2 t})$$

Thus, the expected cumulative number of failures by time t is the expected number of random failures by time t plus the expected number of nonrandom failures removed by time t . It should be noted that $V(0) = 0$ as expected. Moreover, as $t \rightarrow \infty$, $V(t) \rightarrow \lambda t + K_1 \rightarrow \lambda t \rightarrow \infty$, as expected.

Because of the nonlinearity of the model, the estimation of λ , K_1 and K_2 must be evaluated by iterative methods. One method of solution is a nonlinear estimation computer program based on a methodology developed by G.E.P. Box.

There are some extremely nice features of this model. In addition to being "plausible", the most interesting feature is the ability of the model to predict the time when the system/equipment is " q " fraction debugged (i.e., q fraction of the original K_1 nonrandom failures have been removed, $0 < q < 1$). The number of nonrandom defects removed by time t is clearly

$$N(0) - N(t) = K_1 - K_1 e^{-K_2 t}$$

6.7.2 Continued

and hence the fraction (of K initial nonrandom defects) removed by time t is

$$q = \frac{K_1 - K_1 e^{-\hat{K}_2 t}}{K_1} = 1 - e^{-\hat{K}_2 t}$$

Thus having estimated K_2 , say $\hat{K}_2$, we can find the time at which $q = 0.95$ of the nonrandom defects have been removed by solving for $t_{0.95}$. That is,

$$t_{.95} = \frac{-\ln 0.05}{\hat{K}_2}$$

In general, for arbitrary q , $0 < q < 1$ the time which the system/equipment is q fraction debugged is

$$t_q = \frac{-\ln (1-q)}{\hat{K}_2}$$

This equation is a powerful tool because it can be used to help determine the length of development testing, or, the debugging period.

Another important feature of the model is that the number of nonrandom failures remaining at time t can be estimated and of course is $K_1 e^{-\hat{K}_2 t}$. The estimate of λ , say $\hat{\lambda}$; gives the estimate of the long-run achievable MTBF.

The differential equation model can be used to develop reliability growth information on:

- Number of failures to be expected during any period of test or operating time.
- State and effectiveness of the CERT test phase in removing early failures.
- State and effectiveness of the production screening test phase in removing early failures.
- An estimated reliability for the control equipment during field operation.

APPENDIX A

VARIABLE CYCLE ENGINE (VCE) CHARACTERISTICS AND CONTROL MODES

(MUCH OF THE MATERIAL DEFINING VCE CHARACTERISTICS AND CONTROL MODES IN THIS APPENDIX WAS DERIVED FROM "CONTROL MODE STUDIES FOR ADVANCED VARIABLE GEOMETRY TURBINE ENGINES" BY E. BEATTIE, AFAPL-TR-75-7, NOV. 1974 (65)).

A-1 Characteristics

A.1.1 Engine Cycle Definition

Variable cycle engines such as the configuration shown in Figure A-1, incorporate variable fan stator vanes, variable compressor stator vanes, variable high- and low-pressure turbine vane areas, and variable primary and fan duct exhaust nozzle areas in a two stream exhaust configuration. This degree of variable geometry provides the propulsion system designer with improved flexibility for controlling engine operating pressures, thrust - turbine temperature - airflow relationships, engine by-pass ratio, and transient response. Probably the single most important source of performance benefit for this engine configuration over a fixed-area turbine configuration is the capability to operate at constant inlet airflow over not only the augmented power range, but also over a significant portion of the nonaugmented high power range.

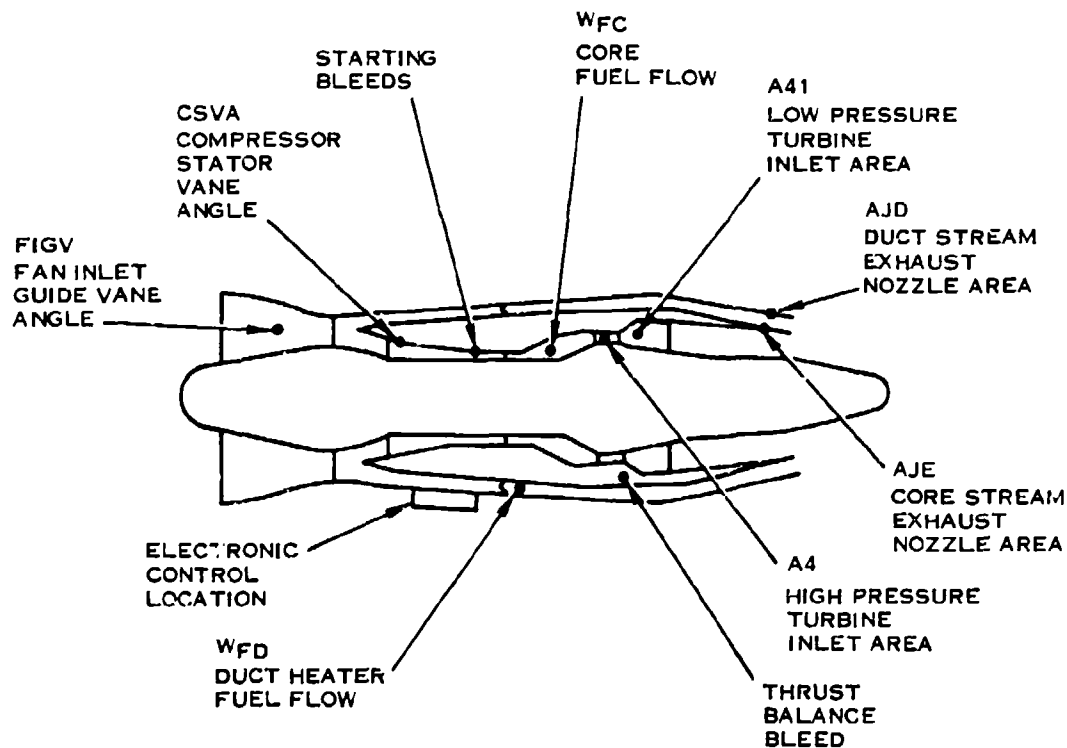
Maintaining constant airflow over a range of power settings is accomplished through a mode of operation referred to as constant match varying temperature (CMVT) operation. This mode of operation requires a constant match of rotor speeds, pressure ratios, and corrected airflow of the fan and compressor as turbine stator inlet temperature is varied. This is accomplished by changing fuel flow to set the power level, while modulating the turbine and exhaust nozzle areas to maintain constant values of high and low turbine work and constant gas flow through the compressor and fan duct. Power can be reduced in this manner from the intermediate level (highest nonaugmented power level), while maintaining a constant match of the fan and compressor until the low turbine exit flow parameter reaches its maximum allowable value, determined from consideration of pressure loss and flow separation of the exit guide vane. This power level is referred to as the breakpoint of CMVT. Below breakpoint power, constant airflow cannot be maintained, but fan and compressor operating lines and engine bypass ratio can be controlled.

Operation in the CMVT mode requires a two-stream, or nonmixed flow, exhaust nozzle configuration to avoid static pressure balancing of the two exhaust streams which would cause the fan to operate off the desired match point, and hence at lower efficiency.

A.1.1 Continued

The control flexibility provided by the variable geometry results in performance benefits which include the following:

- 1) From a cycle point of view, the variable-area turbine engine operating with the CMVT mode has a higher compression ratio for a given turbine temperature, and therefore, a cycle advantage which yields lower fuel consumption at all powers below intermediate.



E-5655

FIGURE A-1 VARIABLE CYCLE ENGINE

A.1.1 Continued

- 2) The capability to reduce thrust at constant airflow leads to a reduction in inlet and exhaust nozzle drag at part-power conditions, and therefore improvements in installed thrust specific fuel consumption.
- 3) For operation at high supersonic conditions, accurate control of engine airflow resulting from the variable geometry plus the capability for constant airflow operation and better inlet/engine matching can result in a smaller inlet size, thus reducing weight and drag while maintaining aircraft thrust requirements and propulsion system stability.
- 4) The variable areas can accommodate adjustments for cycle variation due to altitude, bleed air or horsepower extraction.
- 5) In the area of aircraft-control integration, the variable-area turbine engine offers considerable advantages over a fixed turbine engine in its ability to accommodate changes in inlet distortion level resulting from evasive maneuvers, weapons firing or special modes of operation such as V/STOL. Thus, turbine and nozzle areas can be modulated to shift fan and compressor match points thereby providing stability accommodation.
- 6) For transient operation, turbine and nozzle area modulation provides accurate control of fan and compressor operating lines resulting in improved stability during engine transients. During CMVT operation there is no requirement to change rotor speeds to change thrust which results in thrust response capabilities that are not possible with a fixed turbine engine.

A.1.2 Duct Stream Augmentation

The duct stream augmentor typically is operational between intermediate and maximum power, and it is not operative during part-power engine operation. The range of operation is constrained from the minimum value of fuel-air ratio required to maintain stable combustion, up to one of three possible maximum limits. These are either a maximum mechanical limit on exhaust nozzle area, a maximum exhaust nozzle temperature for structural considerations, or a maximum fuel-air ratio to avoid stoichiometric conditions. In addition, a maximum limit on the duct augmentor inlet Mach number is imposed at minimum light-off fuel-air ratio to assure consistent light-off capability.

It is the purpose of the duct augmentor and nozzle control mode to not only maintain these operational limits, but also to provide smooth augmentor lights, fast continuous modulation, minimum disturbance to total engine airflow, minimum reduction in engine stability margin, good steady-state control accuracy, and safe gas generator operation in the event of blowout. Thrust response of the duct augmentor must meet the time specifications of MIL-E-5007C. It is also desirable to obtain all of these objectives with a control mode of minimum complexity.

A.1.3 Engine Ratings

Four unique rating points can be identified for the variable cycle engine configuration shown in Figure A-1. These are intermediate, breakpoint, idle, and maximum. Intermediate power is defined as the maximum power available without augmentation and without exceeding any engine operational limits. The intermediate rating schedules were established considering desired compressor and fan match points, maximum high-pressure turbine stator inlet temperature limit, and an inlet corrected airflow schedule typical for a fighter/bomber type aircraft application.

As noted previously, power can be reduced from intermediate while holding a constant match of the fan and compressor down to breakpoint power, which is the point at which the low-pressure turbine exit flow parameter reaches its maximum allowable value.

The idle rating point was varied as a function of aircraft Mach number for this study engine. At zero Mach number the idle point is set to be 6 percent of intermediate power. Idle was set a 10 percent of intermediate power for Mach numbers ranging between 0.3 and 1.0. For Mach numbers greater than 1.5, idle power was set equal to breakpoint power in order to prevent a decrease of airflow and subsequent inlet matching problems when decreasing power from intermediate to idle. Interpolation between the power settings of Mach numbers of 0.0 and 0.3, and Mach numbers 1.0 and 1.5 provides the idle ratings for these ranges of Mach numbers.

The idle and intermediate rating points define two power settings which must be accurately scheduled by the engine control system as a function of the pilot power lever angle (PLA). However, this is not sufficient information to determine the complete shape of the control schedules. To provide ease of operation of the engine, it was found to be desirable to provide the breakpoint power setting at the same value of PLA for all flight conditions. Thus, the pilot is provided with a PLA setting above which he knows constant airflow can be maintained, and above which he can expect the engine response to be different. Finally, a requirement for an essentially linear relationship of thrust-versus-PLA between idle and breakpoint, and between breakpoint and intermediate was imposed.

The above constraints are sufficient for defining control schedules for a fixed-area turbine engine. For a variable-area turbine engine, however, these constraints can be met with a wide variety of turbine area settings between idle and breakpoint, and between breakpoint and intermediate power. Between breakpoint and intermediate power, the requirement for constant match of the fan and compressor establishes the constraints on turbine area settings. Below breakpoint power, the establishment of the desired fan and compressor operating lines and the relationship between corrected rotor speeds provide the necessary constraints. These relationships might vary depending on the aircraft mission, and for this study the operating lines were established to minimize the variation of the turbine area settings between breakpoint and idle power.

A.1.3 Continued

With the addition of augmentation, the maximum rating point is obtained at either the maximum exhaust gas temperature, maximum exhaust nozzle area or maximum fuel-air ratio. A requirement for linearity of the thrust-versus-PLA relationship is imposed between minimum augmentation and maximum power.

A discussion of the control schedules derived to meet the above rating requirements is presented following a description of the structure of the control mode.

A.1.4 Operational Limits

The operational limits of a variable cycle engine can be delineated into three categories: aerodynamic, thermodynamic, and mechanical or structural. Typical aerodynamic limits are choking of a nozzle, airflow separation along a compressor or turbine airfoil, maximum airflow, minimum augmentor inlet Mach number required for light-off, and compressor surge. The range of CMVT operation is limited by aerodynamic limits of the low turbine exit guide vane. For the low power end of the CMVT range the low-pressure turbine exit flow parameter is limited to a maximum value determined from consideration of pressure loss and flow separation of the exit guide vane. For the high power end, a minimum limit of low-pressure turbine exit flow parameter can be correlated with blade stress limits and loss in turbine performance, resulting from efficiency and flow separation effects.

Thermodynamic limits include minimum burner fuel-air ratio required to maintain burning, and maximum fuel-air ratio to avoid exceeding stoichiometric operation.

Mechanical and structural limitations include maximum rotor speeds, maximum burner case pressure, creep limits, maximum value of and rates of change of high-pressure turbine stator inlet temperature, maximum augmentor temperatures, and the entire set of control variable rate and amplitude limits.

All operational limits identified in these categories must be considered in the design of the control system. Some will affect control schedule requirements, others will affect control logic, and some will require individual control loops to guarantee avoidance of the limit. The impact of these limits on the control for this engine configuration will become more apparent in the discussions to follow.

A-2 VCF Control Modes

A.2.1 Basic Control Mode

It should be apparent that the performance gains previously noted for a variable cycle engine are not obtained without an appreciable increase in control mode complexity, relative to a fixed-area turbine engine, due to

A.2.1 Continued

the additional control variables. A simplified version of the control mode block diagram is presented in Figure A-2 for the purpose of describing basic control mode operation for the nonaugmented variable geometry turbine engine. This is basically a closed-loop, or integral controller, which implies that each control variable is determined as a function of an error between a scheduled and sensed value of an engine parameter.

In contrast, an open-loop scheduling controller simply schedules control variables as a function of engine parameters and ambient conditions. Closed-loop control is chosen over open-loop because the latter approach would require complex biasing to obtain satisfactory thrust, airflow, and compressor stability margin setting throughout the flight envelope. Also, the open-loop approach requires frequent ground trimming to account for engine production tolerance and deterioration effects which result in variation in the relationship between gas path flow area and actuator position. Finally, unrealistic precision of the turbine actuator systems would be required with open-loop control. For example, the total range of variation in a variable cycle engine high-pressure turbine vane angle for the range of steady-state modulation at constant matchpoint could be as little as 1.5 degrees. It is obvious that small errors in position setting relative to other engine geometry setting, would result in large engine performance variations.

Dynamic elements of the mode consist of the blocks labeled "compensation" and "integrator", in addition to sensors and actuators. The compensation blocks consist of variable gains and variable dynamic lead terms which are tuned to provide stable operation throughout the flight envelope. A multiplication by burner pressure (P_3) in the gas generator fuel flow (WFE) loop provides variable gain, in addition to the compensation block. The function of the integrator blocks is to modulate the various control variables such that the engine match is trimmed to null-out the control error terms in steady-state operation, thereby providing closed-loop control. Nulling the error terms means that the sensed parameters are equal to their respective requested values such that the desired steady-state engine ratings and performance are precisely maintained.

Referring to the simplified logic block diagram, fan inlet guide vane angle (FIGV) and compressor stator vane angle (CSVA), are open-loop scheduled as a function of low and high rotor corrected speeds, respectively. With CSVA on schedule, high pressure turbine inlet area (A_4) controls compressor discharge Mach number, which is characterized by the difference between total and static pressures divided by total pressure of the compressor discharge ($\Delta P/P_3$), and low turbine inlet area (A_{41}) controls compressor corrected speed ($X_{NH}/\sqrt{\theta_{22}}$) to set the match of the compressor. Similarly, the FIGV on schedule, core stream exhaust nozzle area (A_{JE}) controls fan corrected speed ($X_{NL}/\sqrt{\theta_2}$) and duct stream exhaust nozzle area (A_{JD}) controls fan discharge Mach number, which is characterized by ($\Delta P/P_1$), to set the match of the fan during constant match variable temperature (CMVT) operation. The CMVT mode of operation

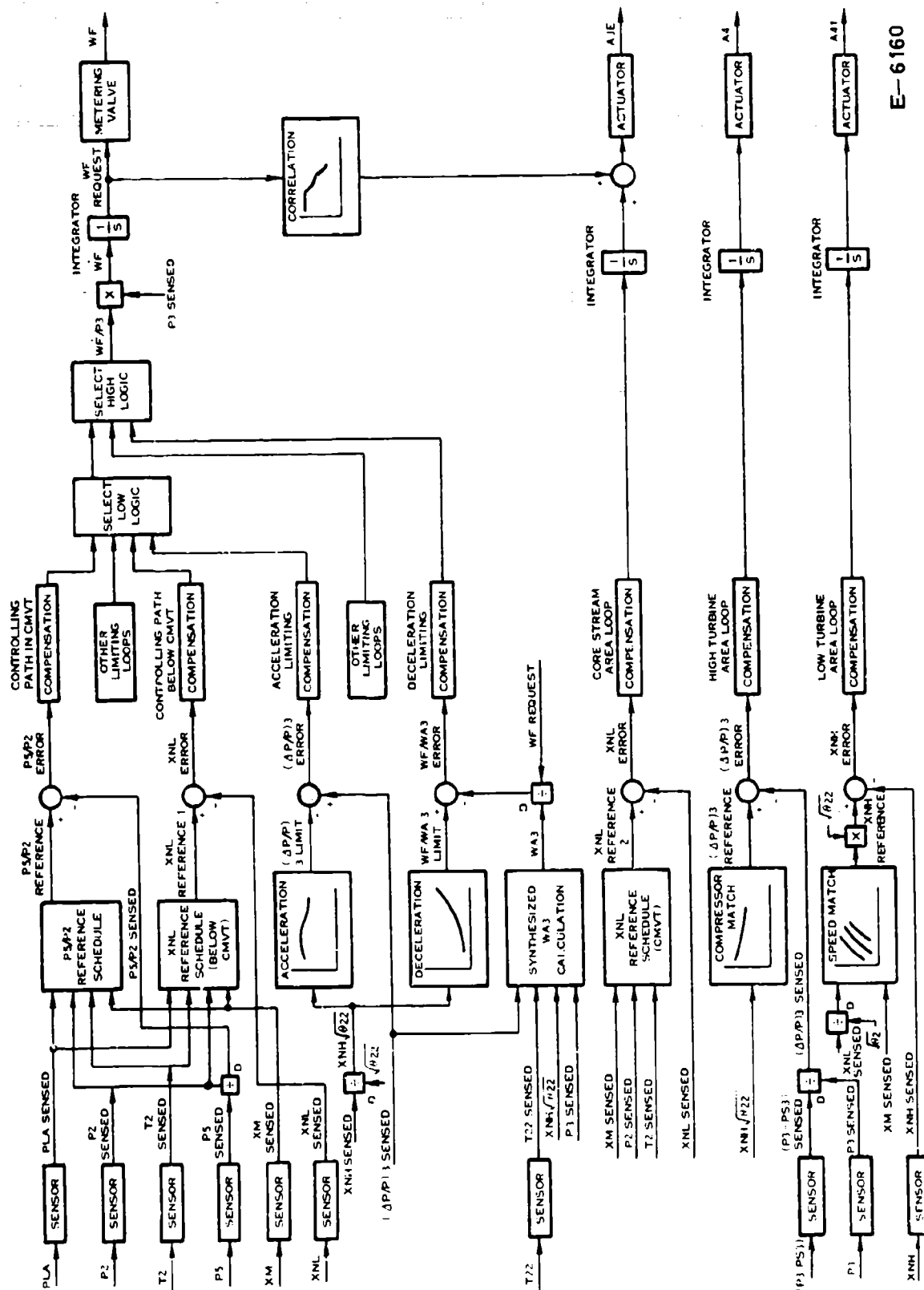


FIGURE A-2 SIMPLIFIED BLOCK DIAGRAM OF CONTROL MODE

E-6160

A.2.1 Continued

maintains a constant airflow over a range of engine power settings. Gas generator fuel flow (WF) then controls engine pressure ratio (P5/P2 or EPR) to set power. A correlation schedule between the WFE and AJE loops provides rough scheduling of AJE to eliminate detrimental interaction between these two loops during rapid transients. Below breakpoint of CMVT operation, a loop transition is made so that WF controls low rotor speed to set power and AJE is held constant. A4 now maintains the desired compressor operating line and A41 maintains the desired relationship between low and high rotor corrected speeds.

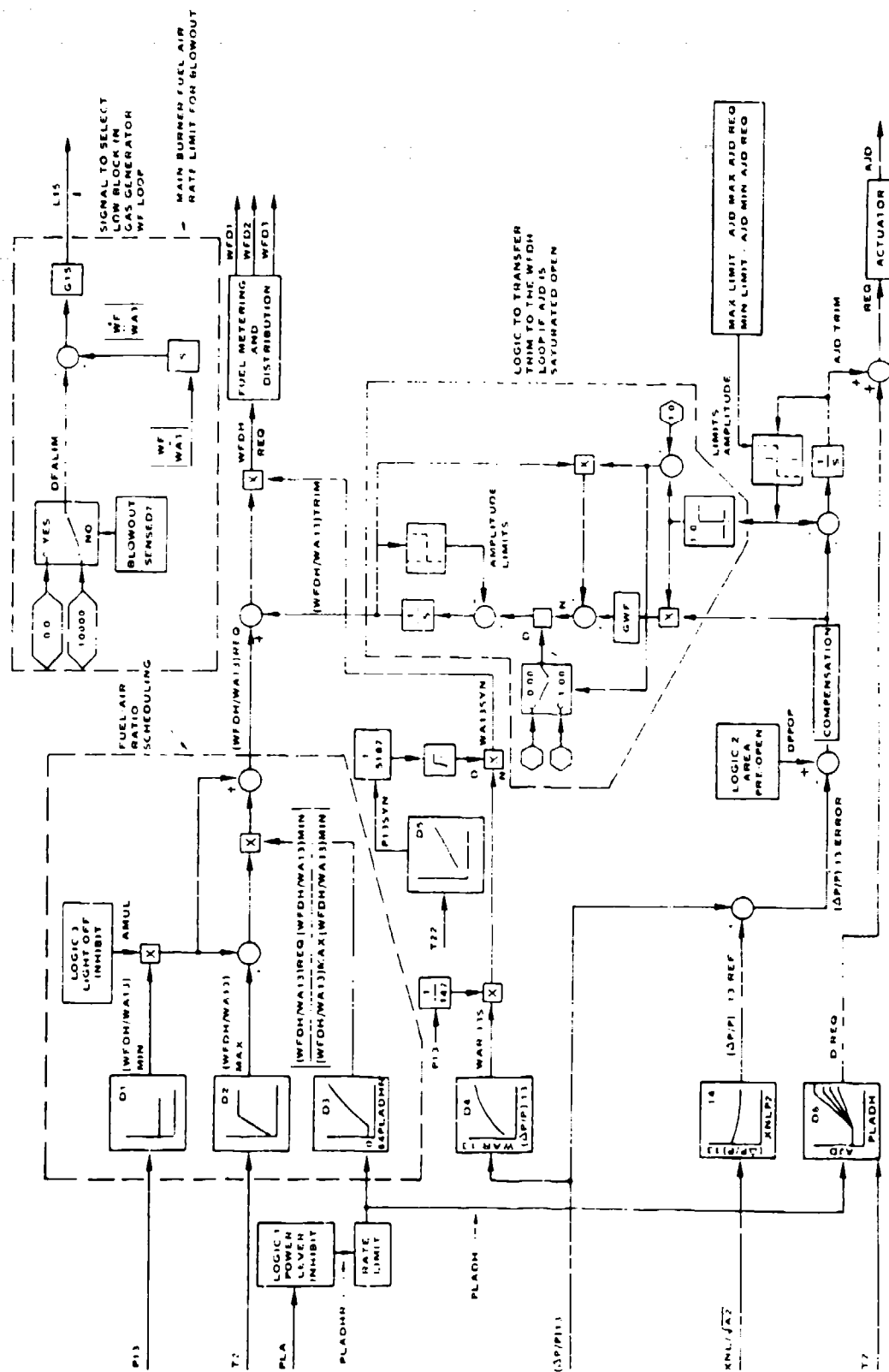
This loop transition is accomplished with the first "Select Low Logic" block in the WF control loop. Below breakpoint power, engine pressure ratio reference (P5/P2 Reference) is scheduled to remain at the breakpoint value while low rotor speed reference (XNL Reference) is scheduled to decrease as a function of power lever angle (PLA) to correspond to part-power operation. Thus, in the range below breakpoint power the compensated engine pressure ratio error (P5/P2 Error) will always be a large positive number relative to the compensated low rotor speed error (XNL Error) for steady-state operation, and the XNL error path will be selected by the logic as the controlling error. Conversely, above breakpoint power, the low rotor speed schedule is raised up out of the way so that the engine pressure ratio path will be selected.

In addition to the variable geometry and fuel flow loops, the VCE gas generator control also includes logic for starting bleed and thrust balance speed for safe engine control. The starting bleed is opened at starting conditions for stability accommodation and is closed at high power conditions to provide optimum compressor operation. The thrust balance bleed is used to change engine internal compartment pressure and maintain rotor thrust bearing load within allowable limits from startup to maximum power. Control logic for the augmentor turbopump is included in the gas generator control mode to ensure adequate hydraulic pressure for the engine actuation systems and duct augmentation fuel flow during operation of the duct heater.

A.2.2 Augmentation Control Mode

The block diagram of the augmentation control mode is presented in Figure A-3. A description of the sequence of events which occurs during a power excursion from intermediate to maximum follows.

As PLA is advanced above the intermediate power setting of 81 degrees, inhibit logic (LOGIC1) prevents the PLA signal to the duct augmentor control logic (PLADH) from increasing above 84 degrees until the engine is up to speed and the light-off detector (LOD) confirms light-off has occurred. Prior to the light-off, the duct nozzle is pre-opened (LOGIC2) by increasing the scheduled value of ($\Delta P/P$)13, thereby increasing fan surge margin to compensate for the duct pressure fluctuation, or "lighting spike", which occurs during light off.



E-9175

FIGURE A-3 VARIABLE CYCLE ENGINE CONTROL MODE— DUCT STREAM AUGMENTOR CONTROL BLOCK DIAGRAM

A.2.2 Continued

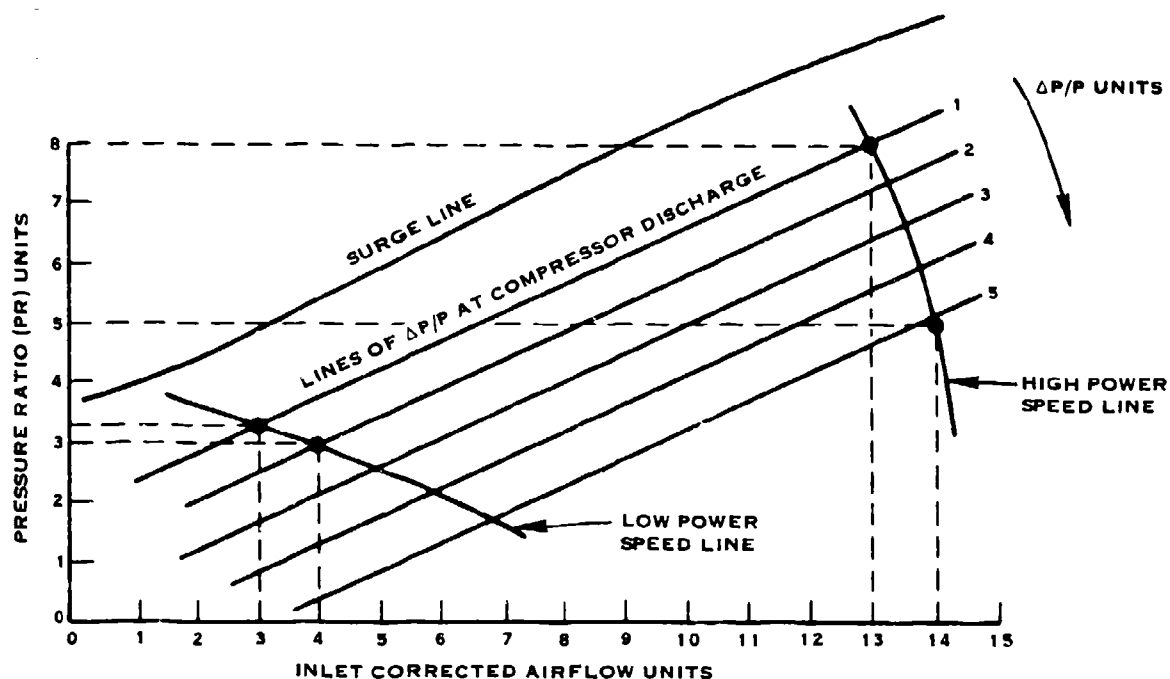
The quick-fill logic proceeds to slew the first segment metering valve to maximum travel and commands maximum pump capacity to maximize metering valve response characteristics and to fill the manifold as quickly as possible. The control monitors metering valve position feedback and uses the information along with stored dynamic characteristics for the system to predict the point in time where the metering valve must reduce flow in order to arrive at the scheduled light-off fuel flow without underfilling or overfilling the manifold. After establishing light-off, PLADH is released and ramps up to the requested PLA value. A similar sequence of events occurs on the subsequent segments which are timed approximately to ensure obtaining maximum thrust within 2 sec (MIL-E-5007D requirement) after initiation of an intermediate-to-maximum PLA step.

During the transient, rough correlation between AJD and WFDH/WA13 is provided by the steady-state schedules versus PLADH. As noted above, the AJD trim integrator acts to maintain accurate control of $(\Delta P/P)13$. If the duct exhaust nozzle area should saturate wide open, either during transient or steady-state operation, before the $(\Delta P/P)13$ error is reduced to zero, then a further increase in WFDH/WA13 would cause an oversuppression of the fan. This is due to the decrease of effective areas as exhaust temperature is increased with a constant flow area. To preclude transient fan surge or steady-state off-design operation of the fan, the integral trim action is transferred, by the logic shown in Figure A-3, to the fuel-air path to decrease fuel-air as necessary in the event the area saturates open.

A.2.3 Selection of Engine Parameters for Control

The engine parameters used in this control mode were selected to best facilitate meeting steady-state and transient performance requirements. In the CMVT range of operation, rotor speeds and compressor match points are constant, therefore a parameter other than rotor speed is required for setting power. The logical choices for a power setting parameter are turbine stator inlet temperature (T4) and engine pressure ratio (P5/P2). Considerations of sensor accuracy capabilities and correlation with thrust settings both show P5/P2 to be the superior thrust setting parameter. Also, the capability of the P5/P2 approach to maintain thrust level during horsepower and bleed extraction is considerably greater than the T4 approach.

Sensing of both rotor speeds is obviously necessary to meet the requirement of controlling rotor speeds to a constant value during CMVT. With rotor speeds controlled and CSVA and FIGV on schedule the match of the fan and compressor can be controlled with either pressure ratio or airflow (characterized by $\Delta P/P$). $\Delta P/P$ has been found to be superior to pressure ratio since at low powers the fan and compressor speed lines are shallower than at high power. The result is a control sensitivity problem when using pressure ratio, which makes it difficult to maintain the requirement of accurate airflow control. This is schematically shown in Figure A-4. Also, an important feature of the control mode is to provide accurate control of fan and compressor stability margin. $\Delta P/P$ is again the better parameter since a larger percent error in $\Delta P/P$ can be tolerated than with pressure ratio for a given percent error in surge margin, as shown in Figure A-5.

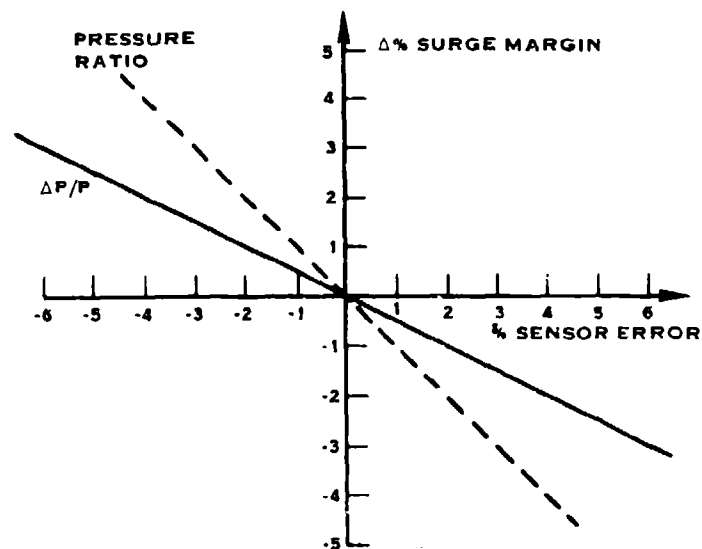


$$\frac{\Delta \text{ PR UNITS FOR 1 AIRFLOW UNIT AT HIGH POWER}}{\Delta \text{ PR UNITS FOR 1 AIRFLOW UNIT AT LOW POWER}} = \frac{3}{1/3} = 9$$

$$\frac{\Delta (\Delta P/P) \text{ UNITS FOR 1 AIRFLOW UNIT AT HIGH POWER}}{\Delta (\Delta P/P) \text{ UNITS FOR 1 AIRFLOW UNIT AT LOW POWER}} = \frac{4}{1} = 4$$

FOR $\Delta P/P$ AND PRESSURE SENSORS PROVIDING SAME AIRFLOW ACCURACY AT HIGH POWER, THE $\Delta P/P$ APPROACH WILL BE TWICE AS ACCURATE AS PRESSURE RATIO FOR AIRFLOW CONTROL AT LOW POWER.

FIGURE A-4 REPRESENTATIVE COMPRESSOR MAP



$\Delta P/P$ MEASUREMENT ONLY REQUIRES ONE HALF AS MUCH ACCURACY AS PRESSURE RATIO MEASUREMENT FOR THE SAME SURGE MARGIN ACCURACY.

FIGURE A-5 REPRESENTATIVE VARIATION OF COMPRESSOR SURGE MARGIN AS A FUNCTION OF PRESSURE RATIO AND $\Delta P/P$ ERROR.

A.2.4 Back-Up Control Modes

The minimum back-up control modes for continuing VCE operation following the occurrence of a fault in the primary control are described below.

Failure in a Single Variable Geometry Control Loop:

An acceptable back-up control mode for a failure which affects the operation of only one variable geometry control loop is to displace the variable geometry control actuator to either its maximum or minimum (open or closed) position. For most control loops, this action permits the engine to continue operating at reduced performance levels while still satisfying the criteria for acceptable back-up control called out in Section 2.1.3.2. The preferred position for each variable geometry loop in the event of its failure is given in Table A-1.

Failure in Two or More Variable Geometry Loops:

Due to the broad range of geometry variations required for normal VCE operation, the displacement of more than one actuator to its external position results in unsatisfactory engine performance. Therefore, when a fault in the primary control causes two or more variable geometry loops to malfunction, positioning of the actuators between their minimum and maximum extremes is required for acceptable back-up control.

A minimum performance back-up control mode capable of providing safe steady-state engine operation is given in Figure A-6. This control mode permits only unaugmented steady-state or slow-transient engine operation. As indicated in Figure A-6, variable geometry outputs A4, A41, AJE, and AJD are fixed at desirable positions within their operating range; however, CSVA and FIGV are positioned as a function of corrected high pressure compressor rotor speed, XNH122. Modulation of these geometries is necessary for providing acceptable back-up control performance. In addition, it is necessary to provide all of the variable geometry loops in the back-up control with trim adjustments to obtain acceptable back-up control performance.

The requirement for trim adjustments in the minimum back-up control mode is contrary to the FTF maintenance objectives mentioned previously. To eliminate trim adjustments requires implementation of the back-up control with the type of closed-loop control modes used in the gas generator control logic given in Figure A-2. The back-up control can be simplified to the extent of excluding augmentor control functions (WFD), and the CMVT control loop (P_5/P_2).

TABLE A-1

PREFERRED POSITIONS FOR SINGLE VARIABLE GEOMETRY LOOP FAILURE

<u>VARIABLE GEOMETRY</u>	<u>SYMBOL</u>	<u>FAILURE POSITION</u>
HIGH-PRESSURE TURBINE AREA	A4	MAXIMUM AREA
LOW-PRESSURE TURBINE AREA	A41	MAXIMUM AREA
FAN DUCT EXHAUST NOZZLE AREA	AJD	MINIMUM AREA
GAS GENERATOR EXHAUST NOZZLE AREA	AJE	MAXIMUM AREA
FAN INLET GUIDE VANE ANGLE	FIGV	CLOSED
COMPRESSOR STATOR VANE ANGLE	CSVA	NONE (ENGINE MUST BE SHUT DOWN)

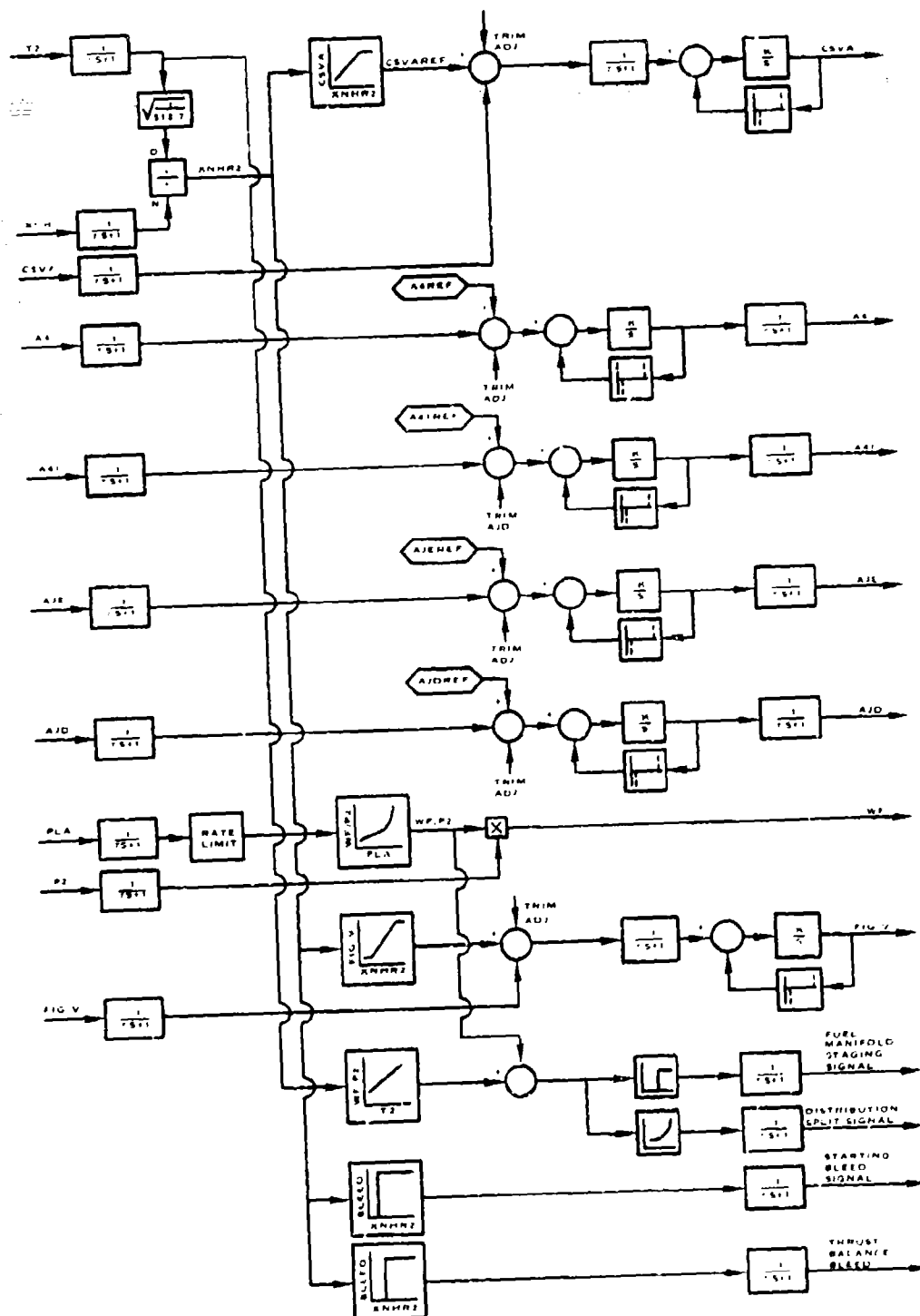


FIGURE A-6 PRELIMINARY MINIMUM BACK-UP CONTROL MODE DIAGRAM

APPENDIX B

REDUNDANCY OPERATING PLANS FOR VARIOUS CHANNEL CONFIGURATIONS

Appendix B summarizes various redundancy operating plans for system configurations of two, three, or four channels. Selection of a redundancy operating plan precedes the formulation of an exact flight safety failure likelihood equation. Careful choice of a plan is necessary to meet reliability requirements.

TWO-CHANNEL CONFIGURATION

Stand-By

The system consists of two channels, one of which is on-line and one that is off-line in the stand-by mode. When the on-line channel fails, detection and switching is accomplished by BIT. The system can tolerate only one failure.

Parallel

The system consists of two channels, both of which are on-line, but only one controls the output drivers. The other channel is inhibited. When the primary channel fails, detection and switching is accomplished by BIT. The system can tolerate only one failure.

THREE-CHANNEL CONFIGURATION

Stand-By

The system consists of three channels, one of which is on-line and the other two are off-line in the stand-by mode. When the on-line channel fails, detection and switching to a stand-by channel is accomplished by BIT. This failure/detection/switching cycle can continue until the last channel is placed on-line. The system can tolerate two failures.

Triple Modular Redundancy (TMR)

The system consists of three channels arranged in a voter configuration. The first failure is detected by cross-channel monitoring techniques and the system selects one of the two remaining good channels and places it on-line. The other remaining good channel is discarded. The system can tolerate one failure.

TMR/Simplex/Simplex

The system consists of three channels arranged in a voter configuration. The first failure is detected by cross-channel monitoring techniques and the system selects one of the two remaining good channels and places it on-line. The other remaining good channel is placed in stand-by. If the on-line channel should fail, detection and switching to the stand-by channel is accomplished by BIT. The system can tolerate two failures.

FOUR-CHANNEL CONFIGURATION

Stand-By

The system consists of four channels, one of which is on-line and the other three are off-line in the stand-by mode. When the on-line channel fails, detection and switching to a stand-by channel is accomplished by BIT. This failure/detection/switching cycle can continue until the last channel is placed on-line. The system can tolerate three failures.

TMR/Replacement

The system consists of four channels, three of which are arranged in a voter configuration and one-channel is placed in the stand-by mode. The first failure is detected by cross-channel monitoring techniques and the system switches the stand-by channel into the voter configuration. The second failure is also detected by cross-channel monitoring techniques and the system selects one of the two remaining good channels and places it on-line. The other remaining good channel is discarded. The system can tolerate two failures.

TMR/Replacement/Simplex/Simplex

The system consists of four channels, three of which are arranged in a voter configuration and one-channel is placed in the stand-by mode. The first failure is detected by cross-channel monitoring techniques and the system switches the stand-by channel into the voter configuration. The second failure is also detected by cross-channel monitoring techniques and the system selects one of the two remaining good channels and places it on-line. The other remaining good channel is placed in stand-by. If the on-line channel should fail, detection and switching to the stand-by channel is accomplished by BIT. The system can tolerate three failures.

APPENDIX C

PARAMETRIC AND FUNCTIONAL DEVICE TESTING

This appendix is included to define the specific electrical tests, conditions and end point limits used in the performance of the sample accelerated Stress Testing program. Table C-1 is a list of the parametric tests, conditions and limits and Table C-2 is the truth table used for functional testing. The tests listed in these tables are identical to the tests used by the manufacturer in order to establish correlation between the test systems.

TABLE C-1 PARAMETRIC TEST CONDITIONS

TEST SYMBOL	TEST NUMBER	CONDITIONS	MEASURE PIN	MIN	MAX	UNITS
I_{SSL}	1	$V_{DD} = 15.0 \text{ V}$ ALL INPUTS = 0 V	V_{DD}	0	20	μA
I_{SSH}	2	$V_{DD} = 15.0 \text{ V}$ ALL INPUTS = 15.0 V	V_{DD}	0	20	μA
I_{IL}	3	$V_{DD} = 15.0 \text{ V}$ ALL INPUTS = 0.0 V	$\overline{\text{CLR}}$	-0.1	0	μA
	4		CLK			
	5		D1			
	6		D2			
	7		D3			
	8		D4			
	9		PE			
	10		$\overline{\text{LD}}$			
	11		TE			
	12		$\overline{\text{CLR}}$			
	13		CLK			
	14		D1			
	15		D2			
	16		D3			
	17		D4			
$V_{OH0} = V_{DD} - V_{OH}$	18	$V_{DD} = 15.0 \text{ V}$	Q4	-50	0.001	mV
	19		Q3			
	20		Q2			
	21		Q1			
	22		C0			
	23		Q4			
	24		Q3			
	25		Q2			
	26		Q1			
	27		C0			

TABLE C-1 PARAMETRIC TEST CONDITIONS (Continued)

TEST SYMBOL	TEST NUMBER	CONDITIONS	MEASURE PIN	MIN	MAX	UNITS
I_{OH} ↓	28	$V_{DD} = 15.0 \text{ V}$ $V_{OUT} = 13.5 \text{ V}$	Q4	-99	-3.4	mA
	29	↓	Q3	↓	↓	↓
	30	↓	Q2	↓	↓	↓
	31	↓	Q1	↓	↓	↓
	32	↓	C0	↓	↓	↓
I_{OL} ↓	33	$V_{DD} = 15.0 \text{ V}$ $V_{OUT} = 1.5 \text{ V}$	Q4	3.4	99	mA
	34	↓	Q3	↓	↓	↓
	35	↓	Q2	↓	↓	↓
	36	↓	Q1	↓	↓	↓
	37	↓	C0	↓	↓	↓
I_{SSL}	38	$V_{DD} = 10 \text{ V}$ ALL INPUTS = 0 V	V_{DD}	0	10	μA
I_{SSH}	39	V_{DD} , ALL INPUTS = 10 V	V_{DD}	0	10	μA
I_{OH} ↓	40	$V_{DD} = 10.0 \text{ V}$ $V_O = 9.5 \text{ V}$	Q4	-99	-1.3	mA
	41	↓	Q3	↓	↓	↓
	42	↓	Q2	↓	↓	↓
	43	↓	Q1	↓	↓	↓
	44	↓	C0	↓	↓	↓
I_{OL} ↓	45	$V_{DD} = 10.0 \text{ V}$ $V_O = 0.5 \text{ V}$	Q4	1.3	99	mA
	46	↓	Q3	↓	↓	↓
	47	↓	Q2	↓	↓	↓
	48	↓	Q1	↓	↓	↓
	49	↓	C0	↓	↓	↓
I_{SSL}	50	$V_{DD} = 5 \text{ V}$ ALL INPUTS = 0 V	V_{DD}	0	5	μA
I_{SSH}	51	V_{DD} , ALL INPUTS = 5 V	V_{DD}	↓	↓	↓

TABLE C-1 PARAMETRIC TEST CONDITIONS (Continued)

TEST SYMBOL	TEST NUMBER	CONDITIONS	MEASURE PIN	MIN	MAX	UNITS
I_{OH} ↓	52	$V_{DD} = 5.0 \text{ V}$ $V_O = 2.5 \text{ V}$	Q4	-99	-2.4	mA
	53	↓	Q3	↓	↓	↓
	54	↓	Q2	↓	↓	↓
	55	↓	Q1	↓	↓	↓
I_{OL} ↓	56	↓	C0	↓	↓	↓
	57	$V_{DD} = 5.0 \text{ V}$ $V_O = 0.4 \text{ V}$	Q4	0.51	99	mA
	58	↓	Q3	↓	↓	↓
	59	↓	Q2	↓	↓	↓
INSAT ↓	60	↓	Q1	↓	↓	↓
	61	↓	C0	↓	↓	↓
	62	$V_{DD} = 5.0 \text{ V}$ $V_{OUT} = 5.0 \text{ V}$	Q4	1.7	99	mA
	63	↓	Q3	↓	↓	↓
↓	64	↓	Q2	↓	↓	↓
	65	↓	Q1	↓	↓	↓
	66	↓	C0	↓	↓	↓
	67	$V_{DD} = 5.0 \text{ V}$ $V_{OUT} = 0.0 \text{ V}$	Q4	-99	-1.7	mA
IPSAT ↓	68	↓	Q3	↓	↓	↓
	69	↓	Q2	↓	↓	↓
	70	↓	Q1	↓	↓	↓
	71	↓	C0	↓	↓	↓

TABLE C-2 FUNCTIONAL TEST TRUTH TABLE

PIN STEP	CLEAR 1	CLOCK 2	P1 3	P2 4	P3 5	P4 6	PE 7	VSS 8	LOAD 9	TE 10	Q _A 11	Q ₃ 12	Q ₂ 13	Q ₁ 14	CO 15	V _{DD} 16
1	0	1/	1	1	1	0	0	0	1	0	0	0	0	0	0	1
2	1		1	1	0	0	0	0	0	0	0	0	0	1	0	1
3	1		0	0	0	0	1	0	1	1	1	0	0	0	0	1
4	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
5	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
6	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
7	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
8	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
9	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
10	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
11	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
12	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
13	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
14	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
15	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
16	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
17	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
18	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
19	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
20	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
21	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
22	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
23	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
24	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
25	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
26	1		0	0	0	0	1	0	1	1	1	0	0	1	0	1
27	0		1	1	1	1	1	0	1	1	1	1	1	1	0	1

1/ ONE FULL CLOCK CYCLE DURING EACH STEP.

APPENDIX D

CONSTRUCTION EVALUATION FOR SAMPLE ACCELERATED LIFE TESTS

An analysis was made of the physical characteristics of a 16-pin cerdip to determine if there existed any physical construction features that might preclude high temperature accelerated life tests at the temperatures specified (150°C, 175°C, and 200°C). In this analysis one of the devices was delidded and a microscopic inspection was made with attention given primarily to determining the materials used in constructing the device. Table D-1 contains a summary of the results of this analysis. No device features were found that would limit high temperature operation at elevated temperatures below 250°C.

TABLE D-1 PHYSICAL CHARACTERIZATION SUMMARY

PACKAGE TYPE:	16 LEAD DUAL-IN LINE CERDIP
PACKAGE MATERIAL:	TOP: BLACK CERAMIC BOTTOM: BLACK CERAMIC LID SEAL & LEAD INSULATOR: GREY GLASS FRIT
GLASSIVATION:	SiO ₂
DIE SCRIBE METHOD:	MECHANICAL SCRIBE
DIE SIZE:	85 MIL x 57 MIL
DIE ATTACHMENT:	GOLD-SILICON EUTECTIC
WIRE MATERIAL:	ALUMINUM; 1 MIL DIAMETER
WIRE BONDING METHOD:	LEAD FRAME: ULTRASONIC BOND DIE BOND PAD: ULTRASONIC BOND
INTRACONNECT MATERIAL:	ALUMINUM
LEAD MATERIALS:	EXTERNAL: KOVAR TYPE WITH TIN PLATING LEAD FRAME: KOVAR TYPE WITH ALUMINUM PLATING

REFERENCES

1. W.A. Wulf, "Reliable Hardware/Software Architecture." IEEE Trans. on Software Engineering, June 1975.
2. W.C. Bouricius, W.C. Carter, and P.R. Schneider, "Reliability Modeling Techniques for Self-Repairing Computer Systems." Proc. of the 24th National Conference of ACM, 1969.
3. I. Bazovsky, Reliability Theory and Practice. Prentice-Hall Inc., NJ, 1961.
4. J. Von Neumann, "Probabilistic Logics and The Synthesis of Reliable Organisms From Unreliable Components." Automata Studies, Annals of Mathematics, No. 34, pp 43-98, Princeton, 1956.
5. C.E. Shannon, and E.F. Moore, "Reliable Circuits Using Less Reliable Relays." J. Franklin Inst., Vol. 262, pp 191-208 and 281-297, Sept/Oct 1956.
6. J.G. Tyron, "Quadded Logic." Redundancy Techniques for Computing Systems, Spartan Books, 1962.
7. J.T. Duane, "Learning Curve Approach to Reliability Monitoring", IEEE Aerospace, 2: pp 563-566, 1964.
8. D. Amey, "Looking Ahead at High Density Packaging." Electro. '78, Electronics Show and Convection, sponsored by IEEE and ERA, May 23-25, 1978.
9. Dr. S. Khadpe, Motorola, Inc. "Design and Cost Considerations for Ceramic Chip Carrier Packaging of Active Devices." ISHM, 1977.
10. J. Lyman, "Packaging Technology Responds to the Demand for Higher Densities." Electronics, September 28, 1978.
11. J. Prokop and D.W. Williams, Chip Carriers as a Means for High-Density Packaging. Texas Instruments, Inc., Dallas, ISHM, 1977.
12. Anon., General Electric Co., "Chip Carrier Thrives on Ceramic Substrates, Lifts Off Epoxy-Glass Boards." Electronics, June 8, 1978.

13. F.R. Pinner, Martin Marietta Corp., "Leadless Device Reflow Soldering is Reliable and Lowers Assembly Costs." Assembly Engineering, Oct. 1977.
14. Anon., "Progress in Mating Leadless Chip Carriers to P.C. Boards." Electronic Packaging and Production, December, 1978.
15. J.E. Tennimore, Martin Marietta Corp., "Using Leadless Components Technology on Printed Wiring Boards." Electronic Packaging and Production, December 1978.
16. Anon., "Manufacturing Technology for Hermetic Chip Carrier Packaging." Package Design Presentation, RCA.
17. M.L. Burch and B.M. Hargis, "Ceramic Chip Carrier - The New Standard in Packaging." 3M Company.
18. J.W. Balde and D.I. Amey, "New Chip Carrier Concepts will Impact LSI - Based Designs." EDN, September 20, 1978.
19. R.J. Clark, General Electric Co., "Microelectronics Packaging Trends: An IEPS Review." Electronic Packaging and Production, January 1979.
20. W. Lattin, T. Mathiasen (Intel Corp.), and S. Grovender (3 M Company), "64 - Pin QUIP Keeps Microprocessor Chips Cool and Accessible." Electronics, January 4, 1979.
21. R.B. Gordan, RCA Advanced Technology Laboratories, NJ, "Airborne Packaging Using Compound Hybrids With LSI." Electronic Packaging and Production, November 1978.
22. H.W. Markstein, "Chip Carrier Update." Electronic Packaging and Production, April 1979.
23. Captain R.E. Settle, Jr., Air Force Avionics Laboratory, "A New Family of Microelectronic Packages for Avionics." Solid-State Technology. June 1978.
24. Dr. J.S. Sallo, Fortin Laminating Corp., "Selecting Laminates for Multilayer and Two-Sided Rigid PCB's." Circuits Manufacturing.
25. Anon., Sanders Associates, Inc., "Polyimide Multilayers." Insulation/Circuits, October 1974.

26. R. Castonguay, MICA Corp., "Resin Systems for High-Performance Laminates." Electronic Packaging and Production, July 1979.
27. Anon., "Guidelines for Designing Multilayer Ceramic Substrates." Electronic Products Division, 3M Company.
28. R.L. Morey and P.J. Pijoan, "Thick Film Multilayer Boards: Specialized Problem Areas." C.S. Draper Laboratory, Inc., ISHM, 1978.
29. S.J. Stein, L. Spadafora, and C. Huang, Electro-Science Laboratories, Inc., "New Developments in Thick Film Conductors." Solid State Technology, January 1979.
30. Anon., "Alumina Substrates." Comco, Inc., Sun Valley, California, Bulletin No. C072C-3.
31. Anon., "Your Answer for Electronic Ceramics." Coors Porcelain Company, Golden, Colorado, Bulletin No. 955.
32. C. Malkiel, "Users Evaluate Porcelain Steel Substrates." Circuits Manufacturing.
33. R.B. Schabacker, "Porcelain Enamel Substrates for Thick Film Hybrids and P.C. Boards." The Erie Ceramic Arts Company, Presented at NEPCON/WEST, March 2, 1978.
34. D.P. Wicker and W.B. Hatfield, "Porcelain Steel Technology: A Bonafide Alternative?" The Singer Company, Corporate R&D Laboratory, ISHM, 1978.
35. Anon., "Porcelainized-Steel Substrates - Still a Ways To Go." Electronic Packaging and Production, December 1978.
36. L. Teschler, "New Circuit Boards Beat Heat and Vibration." Machine Design, January 25, 1979.
37. R.H. Van Horn, "The Design of Separable Connectors." IEEE Transactions, Vol. PHP-11, No. 3, September 1975.
38. R.H. Van Horn, "Connecting Devices for Electronic Systems - Some General Design Considerations." IEEE Transactions, Vol. PHP-11, No. 3, September 1975.

39. N. Spatz, Amp. Inc., "Selecting Electrical Connectors." Machine Design, January 26, 1978.
40. Donald F. Cottrell and Thomas E. Kirejczyk, Crimp Connection Reliability. Martin Marietta Corp., (RADC-TR-78-15), January 1978.
41. G.F. Guth, Martin Marietta Corp., Quantification of Printed Circuit Board (PCB) Connector Reliability. (RADC-TR-77-433), Final Technical Report, January 1978.
42. T.G. Grau, Bell Telephone Laboratories, Inc., "A Field Study of the Electrical Performance of Separable Connectors." IEEE Electronics Component Conference, 1978.
43. D.S. Steinberg, Singer Kearfott Div., "Avoiding Vibration in Odd-Shaped Printed Circuit Boards." Machine Design, May 20, 1976.
44. J.F. Ruzicka, "Vibration Control." Barry Wright Corp., Watertown, Mass., Electro-Technology, Science and Engineering Series, August, 1963.
45. A.B. Plant, Lucas Aerospace Limited, "The Use of Hybrid Construction Technology for High Reliability in a Harsh Environment." ISHM, 1976.
46. J.A. Ciccio and R.E. Thun, "Ultra-High Density VLSI Modules." Raytheon Company, Bedford, Mass.
47. Anon., "Long-Life Assurance Study for Manned Spacedraft Long-Life Hardware." Summary of Long-Life Assurance Guidelines, Vol. I, Martin Marietta Corporation, September 1972.
48. D. Edgerton, Jr. and I. Quart, "Hughes Aircraft Company Stress Screening Studies." Proceedings-Institute of Environmental Sciences, 1979.
49. J.W. Bathke, General Dynamics/Pomona, "Standardizing Environmental Testing in a Multi-Program Orientation." Proceedings-Institute of Environmental Sciences, 1979.
50. J.D. Brarum, "Selection and Evaluation of Environmental Screening Tests for Trident I (C4) Electronics Black Boxes." Lockheed Missiles and Space Company.

51. D.S. Peck and C.H. Zierdt, Jr., "The Reliability of Semiconductor Devices in The Bell System." Proceedings of the IEEE, Vol. 62, No. 2, pp 185-211, February 1974.
52. D.S. Peck, "New Concerns About Integrated Circuit Reliability." Bell Telephone Laboratories, Proceedings Annual Reliability Physics Symposium (IEEE), pp 1 - 6, 1978.
53. Anon., "Long-Life Assurance Study for Manned Spacecraft Long-Life Hardware." Special Long-Life Assurance Studies, Vol. 4, Martin Marietta Corporation, September 1972.
54. J. Cardinal, "Establish Manufacturing Processes for Polyimide/Glass Printed Circuit Boards." Hamilton Standard Division, Windsor Locks, Conn., March 23, 1978.
55. Anon., "Digital Evaluation and Generic Failure Analysis Data." RADC document No. MDR-10, ITF Research Institute, January 1979.
56. L.H. Crow, "Reliability Analysis for Complex Repairable Systems." AMSAA, TR-138, 1974.
57. O. Kempthorne and L. Folk, Probability Statistics and Data Analysis. Iowa State University Press, 1971.
58. M. Engle and L.J. Bain, "Prediction Intervals for Weibull Process." Technometrics, 20: pp 167-169, 1978.
59. W.M. Bassin, "Increasing Hazard Functions and Overhaul Policy." Annual Reliability Symposium, pp 173-178, 1969.
60. L.H. Crow, "On Tracking Reliability Growth." Reliability and Maintainability Symposium, pp 438-443, 1975.
61. L.H. Crow, "Confidence Interval Procedures for Reliability Growth Analysis." AMSAA, TR-197, AD-A044788, 1977.
62. J.M. Finkelstein, "Confidence Bounds on the Parameters of The Weibull Process." Technometrics, 18: pp 115-117, 1976.
63. L. Lee and S.K. Lee, "Some Results on Inference for the Weibull Process." Technometrics, 20: pp 41-45, 1978.
64. M. Posner, "Systems Analysis-Nonlinear Estimating Techniques." Reliability and Quality Control Symposium, pp 203-207, 1961.
65. E. Beattie, "Control Mode Studies for Advanced Variable-Geometry Turbine Engines" AFAPL-TR-75-7 November 1974.

66. D.J. Lando, J.P. Mitchell, and T.L. Welcher, "Conductive Anodic Filaments in Reinforced Polymeric Dielectric: Formation and Prevention." IEEE Proceedings Physics Symposium, 1979.
67. J.N. Lahti, R.H. Delaney, and J.N. Hines, "Characteristic Wear Out Process in Epoxy-Glass Printed Circuits For High Density Electronic Packaging." IEEE Proceedings Physics Symposium, 1979.