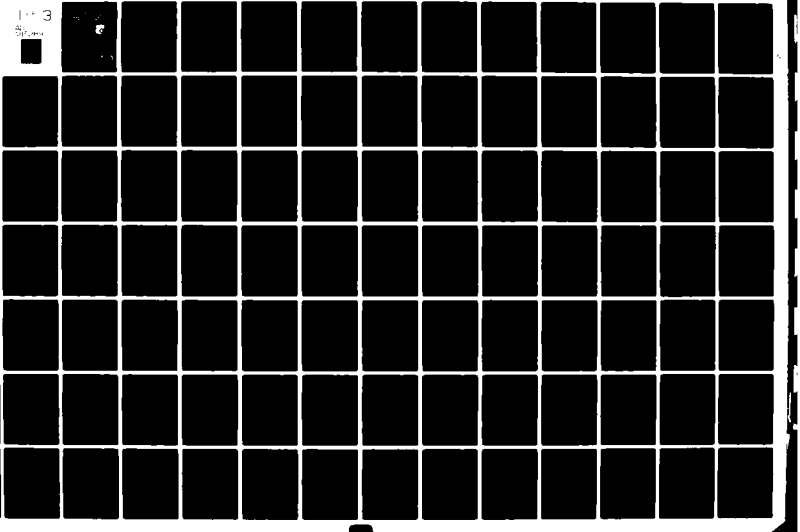
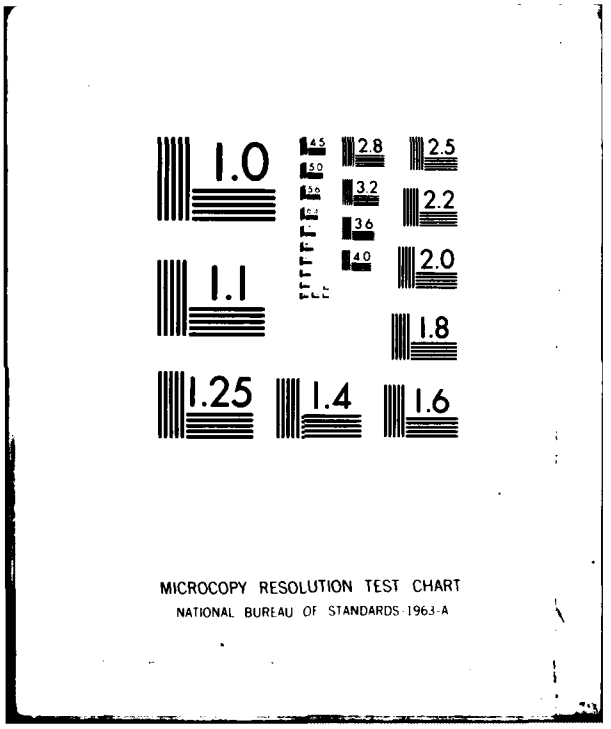
AD-A115 289 PRATT AND WHITNEY AIRCRAFT GROUP WEST PALM BEACH FL G--ETC F/G 21/5
FULL-AUTHORITY FAULT-TOLERANT ELECTRONIC ENGINE CONTROL SYSTEMS--ETC(U)
DEC 81 M E MCGLONE, W J DAVIES, T B SMITH F33615-79-C-2082
UNCLASSIFIED PWA-FR-15054 AFWAL-TR-81-2121 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AFWAL-TR-81-2121

FULL-AUTHORITY FAULT-TOLERANT ELECTRONIC ENGINE CONTROL SYSTEMS FOR VARIABLE CYCLE ENGINES

Technical Report

M. E. McGlone, W. J. Davies, R. J. Miller
Pratt & Whitney Aircraft Group
Government Products Division
P. O. Box 2691
West Palm Beach, Florida 33402

Dr. T. B. Smith, Dr. J. H. Lala
Charles Stark Draper Laboratories
555 Technology Square
Boston, Massachusetts

W. Peck
Hamilton Standard
Windsor Locks, Connecticut

December 1981

Final Report for Period August 1979 — September 1981

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

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.

Paul T. Adams Jr.
PAUL T. ADAMS, JR.
Project Engineer

Lester L. Small
LESTER L. SMALL
Technical Area Manager
Controls and Diagnostics

FOR THE COMMANDER

James M. Shipman
JAMES M. SHIPMAN, Maj, USAF
Deputy Director
Turbine Engine Division

"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.

AIR FORCE/56780/25 May 1982 — 100

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. Report Number AFWAL-TR-81-2121	2. Govt Accession No. AD-A113 289
3. Recipient's Catalog Number	
4. Title *(and Subtitle)* FULL AUTHORITY FAULT-TOLERANT ELECTRONIC ENGINE CONTROL SYSTEMS FOR VARIABLE CYCLE ENGINES TECHNICAL REPORT	5. Type of Report & Period Covered Final 1 August 1979 — 1 September 1981
	6. Performing Org. Report Number FR-15054
7. Author(s) Michael E. McGlone, Pratt & Whitney Aircraft William J. Davies, Pratt & Whitney Aircraft T. Basil Smith, Draper Labs Wm. C. Peck, Hamilton Standard	8. Contract or Grant Number(s) F33615-79-C-2082
9. Performing Organization Name and Address United Technologies Corporation Pratt & Whitney Aircraft Group Government Products Division P.O. Box 2691, West Palm Beach, FL 33402	10. Program Element, Project, Task Area & Work Unit Numbers 62203F/3066/30660388
11. Controlling Office Name and Address Aero Propulsion Laboratory (POTC) Air Force Wright-Aeronautical Laboratories (AFSC) Wright-Patterson Air Force Base, Ohio 45433	12. Report Date December 1981
	13. Number of Pages
14. Monitoring Agency Name & Address *(if different from Controlling Office)*	15. Security Class. *(of this report)* Unclassified
	15a. Declassification/Downgrading Schedule

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 Control Systems, Full-Authority Engine Control, Fault-Tolerant Engine Control, Digital Engine Control, Engine Control Reliability

20. Abstract *(Continue on reverse side if necessary and identify by block number)*

This Full Authority Fault Tolerant Electronic Engine Control program (FAFTEEC) was performed under Contract F33615-79-C-2082. The program was a 25-month study to develop design guidance for utilizing redundancy to provide control system architectures capable of very high levels of reliability. The study configured several such systems and evaluated the reliability, cost-of-ownership, weight and implementation.

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

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

20. Abstract *(Continued)*

Conclusions of this program were that FAFTEEC goals are obtainable through redundancy and that the resulting system can be obtained at a reasonable cost and weight through dual system advanced technology.

Analysis provided by the FAFTEEC allows for the following conclusions to be reached:

- FAFTEEC goals are reasonable and obtainable
- Redundant systems are required
- Single string technology is not cost and weight effective
- Coverage of dual systems is extremely important
- Coverage via software is complex, costly and will not provide 100 percent coverage
- Dual system technology must be included throughout all system components.

TABLE OF CONTENTS

CONTENTS (Continued)

CONTENTS (Continued)

LIST OF ILLUSTRATIONS

ILLUSTRATIONS (Continued)

ILLUSTRATIONS (Continued)

ILLUSTRATIONS (Continued)

CONTENTS (Continued)

LIST OF TABLES

LIST OF TABLES (Continued)

FOREWORD

This report describes work conducted for the Components Branch; Turbine Engine Division; Aero Propulsion Laboratory, Air Force Wright Aeronautical Laboratories, Wright-Patterson Air Force, Ohio under Contract No. 33615-79-C-2082, Digital Engine Contract Reliability Program.

The work reported, herein was performed during the period 1 August 1979 through 1 February 1982 under the direction of Charles E. Ryan, Jr, project engineer. The report was released by the author in February 1982.

The program was conducted by Pratt & Whitney Aircraft Group, Government Products Division, West Palm Beach, Florida, with subcontracts, let to Hamilton-Standard Division of United Technologies Corporation and the Charles Stark Design Laboratories, Boston, Mass.

SECTION 1

SUMMARY

This report details the analysis and study procedures used to conduct the FAFTEEC program. Section 3 describes the engine applications and the Baseline Control. The Baseline Control system is defined in detail by providing a description of the control mode used and the system components. A Failure Mode and Effects Analysis of the system at a functional level is provided by Section 4.

Section 5 provides a description of each of the candidate systems. Each system architecture is described and the differences between system architectures, component technologies, and system coverages is defined. Section 6 projects failure rates for the system components at the LRU level. The failure rates are established by historical data and then projected for the FAFTEEC system components at maturity.

Section 7 describes the reliability modeling of each of the candidate systems and the results of the modeling by projecting reliability values for each of the systems. Reliability drivers and coverage are described for each system. A detailed description of the Markov Reliability Model is described in Appendix A along with a step-by-step procedure for modeling the baseline system as an example.

A packaging study was completed for the electronic control box configuration and is described in Section 8.

Section 9 details the techniques used to evaluate the systems for overall system benefits and deficiencies. The system acquisition costs, weights, and mean time between faults (MTBF) are tabulated. A cost-of-ownership is described which includes life cycle cost analysis, cost attributed to lost aircraft, and reduced fleet sizes, available through improved mission reliability.

Sections 10 and 11 provide a discussion of the study results and conclusions and recommendations.

Section 12 outlines what is being done in parts of the industrial control industry. The telephone and automotive industry were originally included in the proposal. In addition, the study was expended to include airframe manufacturers to allow an overview of high reliability digital flight control systems.

Section 13 presents an indepth review of Trip Reports to Bell Laboratories, the Naval Research Laboratory, Ford Motor Company, Chrysler Corporation and General Dynamics.

SECTION 2

INTRODUCTION

The objective of this program was to identify redundancy/redundancy management provisions required in the architectures of Full-Authority Fault-Tolerant Electronic Engine Control (FAFTEEC) systems to provide very high levels of reliability. The reliability goals specified were 2.5×10^{-6} failures per hour maximum with 2.5×10^{-7} desired.

The judicious use of redundancy is an established practice in industries such as flight control, missile control, and nonflight industries like the telephone companies. The design of redundant system architectures and the reliability analysis of such systems are relativily new to the gas turbine propulsion industry. It was an intent of the FAFTEEC program to take advantage of the technology developed by these industries and apply it to evolve fault-tolerant control system architectures for gas turbine engines.

The FAFTEEC program combined the expertise of Pratt & Whitney Aircraft gas turbine propulsion control system designers, Hamilton Standard engine mounted digital electronic control designers, and Charles Stark Draper Laboratories. The Draper Laboratories have an established background in the design and reliability modeling of redundant digital electronic control architectures for flight control applications. This team configured several candidate FAFTEEC systems with varying levels of redundancy and then evaluated these systems to project system mission reliability, maintenance reliability, cost, weight, and cost-of-ownership.

SECTION 3

SYSTEM APPLICATION

ENGINE DESCRIPTION

The variable cycle engine used for the FAFTEEC system definition is the Advanced Technology Demonstrator Engine (ATDE) which is a non-mixed-flow, variable cycle, high performance augmented turbofan. The engine, shown schematically in Figure 1, has variable geometry fan inlet guide vanes, compressor stators, high and low pressure turbine stators, and modulated core and fan exhaust nozzles. A compressor bleed is also provided for compressor stability during start. Fuel is modulated to the main combustor and augmentation is provided by three augmentor segments or burning zones in the fan duct air stream. The station identification for this engine is shown schematically by Figure 2. This engine is a "paper" engine. It was used as a vehicle for the FAFTEEC studies.

UTILIZATION

The FAFTEEC control systems are structured to be employed on the engine of a high performance, single engine combat aircraft as the principal application, but will also be applicable to each engine of a two engine aircraft without requiring significant modification.

The mission time for both aircraft has been assumed to be:

1. Three (3) hr — 90 percent of airframe life
2. Ten (10) hr — 10 percent of airframe life

All of the FAFTEEC systems have been structured to include full authority digital electronic control which is engine mounted and cooled with aircraft tank fuel. The redundancy level of the electronic control computers varies with the different FAFTEEC systems being considered. The fuel delivery temperature has been assumed to be:

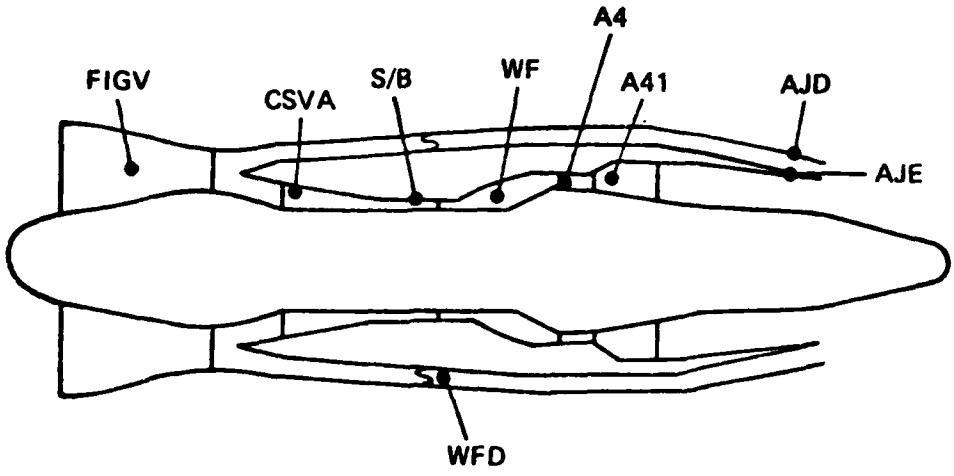
1. T = 57°F), 97 percent of Mission Time
2. T = (171°F), 3 percent of Mission Time

BASELINE CONTROL SYSTEM DEFINITION

The Baseline Control System has been configured to be a full authority digital electronic control system. It has been implemented as a single string system since it was considered that such a system would provide maximum freedom in the selection of the redundancy configuration.

The primary control of the variable cycle engine selected will be provided by the baseline system, as illustrated in Figure 3. The control modes, described later in this section, have been designed to allow closed loop no-trim operation of the engine.

The operation of the ATDE has been reviewed to identify those minimum control inputs and outputs which are required to provide a control mode which would allow nonaugmented operation of the engine within safe operating limits. This control mode has been implemented as a backup software control mode. As long as these essential digital control inputs and outputs are operational and the digital control processor is operationally safe, operation of the engine can be maintained by the digital electronic control, thus providing fail-soft operation of the electronic control.



- FIGV - Fan Inlet Guide Vane - Open Loop*
- CSVA - Compressor Stator Vane Angle - Open Loop
- WF - Gas Generator Fuel Flow - Closed Loop**
- AJE - Core Exhaust Nozzle Area - Closed Loop
- A4 - High Pressure Turbine Inlet Area - Closed Loop
- A41 - Low Pressure Turbine Inlet Area - Closed Loop
- AJD - Duct Stream Exhaust Nozzle Area - Closed Loop
- WFD - Augmentor Fuel Flow (Duct) - Open Loop
- S/B - Starting Bleed

* Open Loop - Geometry or Fuel Flow Scheduled as a Function of Engine State, i.e. FIGV = $f(N_1C_2)$

** Closed Loop - Geometry or Fuel Flow Modulated To Maintain an Engine State, i.e. W_F Varied To Maintain Scheduled P_5/P_2.

FD 178814

Figure 1. Variable Cycle Engine Control Loops

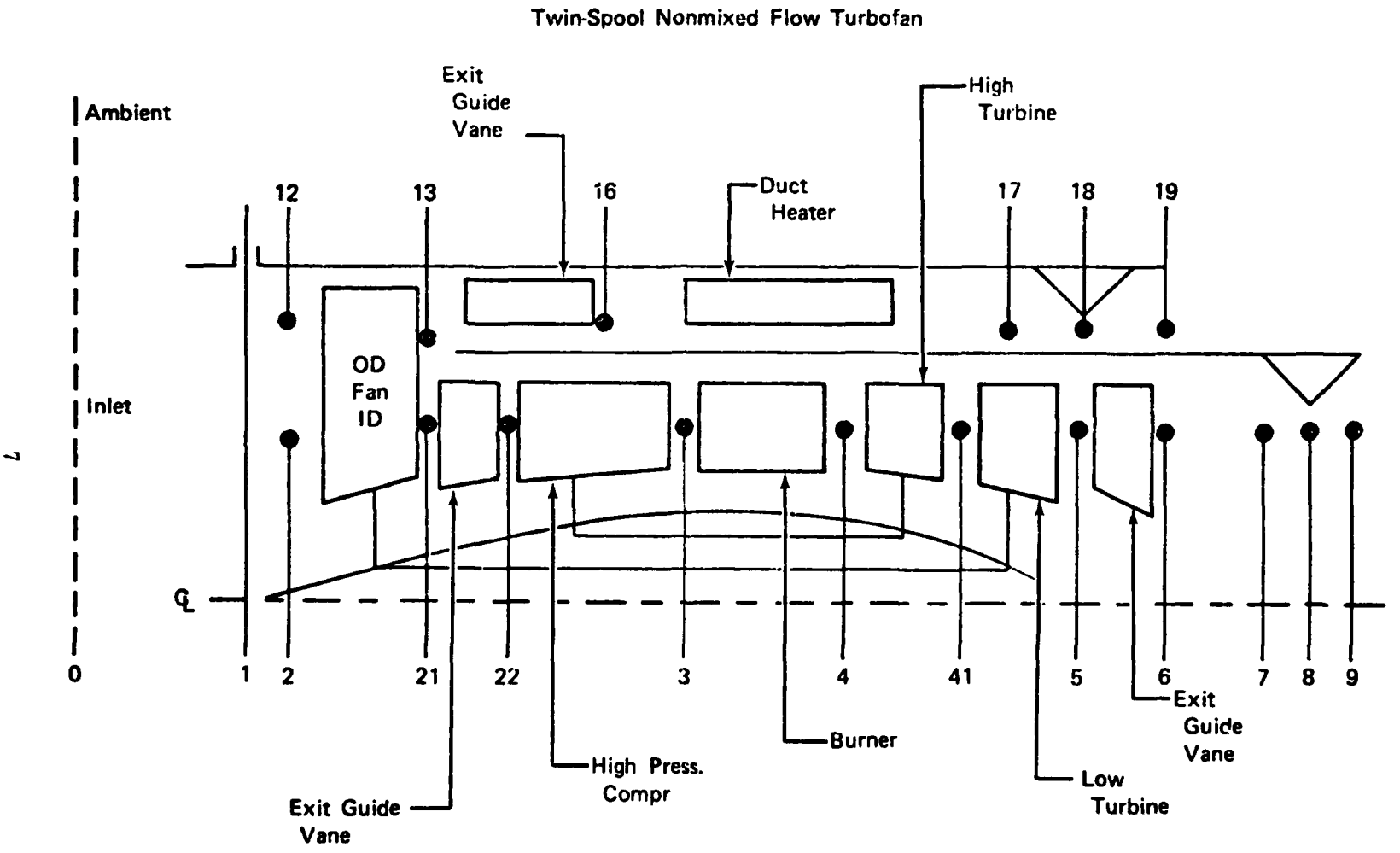


Figure 2. Station Identification

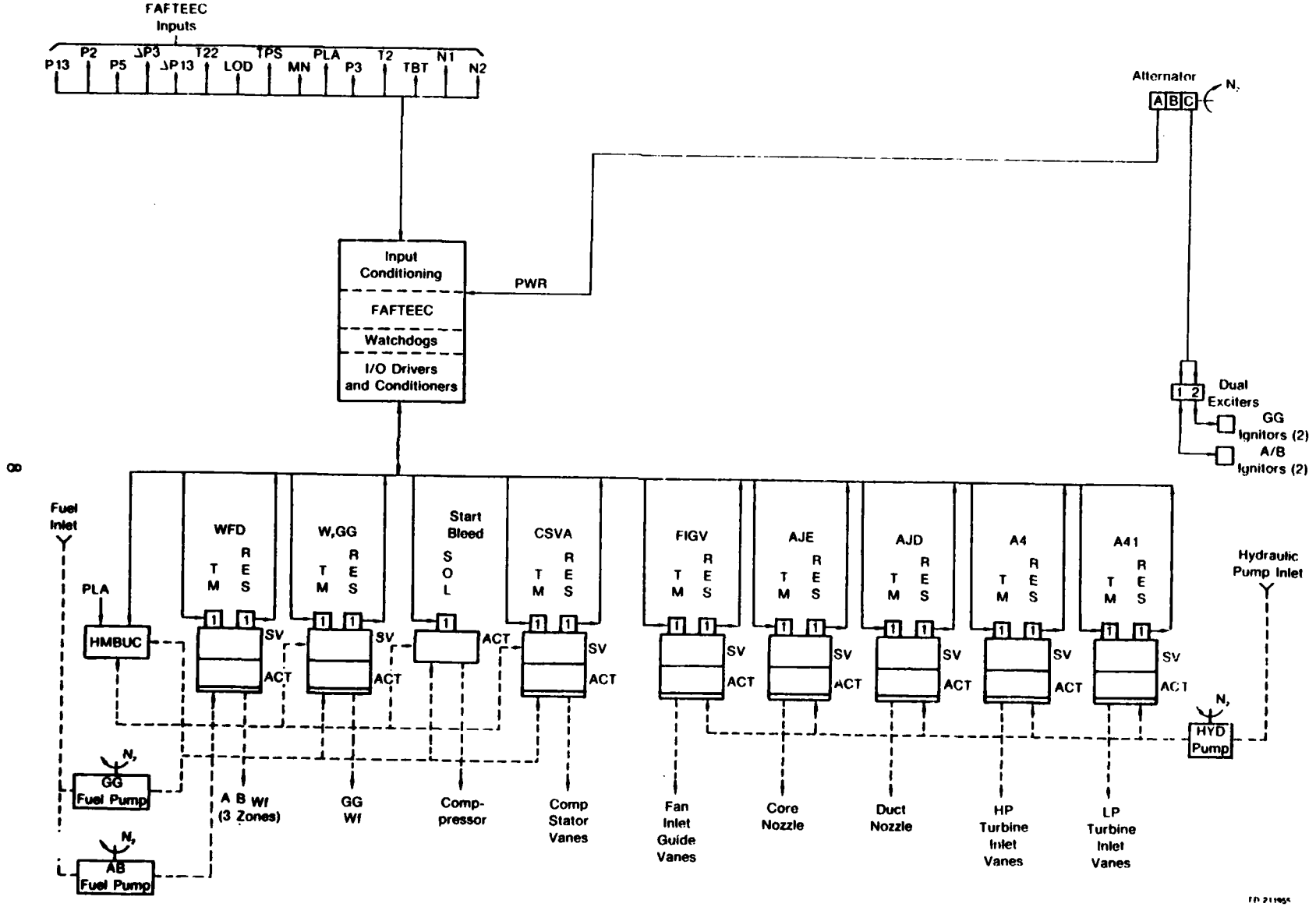


Figure 3. FAFTEEC Baseline-Single String

Should a failure of one of the critical inputs or outputs, electrical power, or processor occur, the digital electronic control would initiate transfer to the backup hydromechanical control system. This system would implement a get home control mode similar to the digital electronic backup control.

BASELINE CONTROL SYSTEM

The Baseline Control System from the FAFTEEC program is shown in Figure 3. The system as configured is single strand in both the electronic and electrohydromechanical components. All the control system computations are executed by the engine-mounted electronic control. A hydromechanical backup is incorporated in the system for added safety; it provides a get home capability in the event of an electronic control failure. The backup control may be selected either automatically by the electronic control or manually by pilot action.

The engine actuators for both fuel flow and variable geometry control are designed with single wound torque motors for the FAFTEEC Baseline Control System. The resolvers, which provide feedback information to the control, are single-wound units. Individual components are described in more detail later in this report.

This system is the basic system upon which all of the various FAFTEEC candidate systems are based. These systems, which feature various levels of redundancy, are described in Section 5 of this report.

CONTROL MODES

This section describes the various loops used in the control of the ATDE engine and is applicable not only to the baseline configuration but to all FAFTEEC systems. Each loop is described in terms of required input parameters, effect of the loop on engine operation, and how the control loop is scheduled. Control of each variable of a complex engine may be categorized as open loop or closed loop, depending upon whether the value of the variable is programmed along some schedule, or modulated until some measured engine performance criteria are met. Table 1 lists the control modes selected for each of the variables in the ATDE engine, together with the related sensed parameters. Limiting loops are also provided to prevent exceeding maximum turbine blade temperature, burner case pressure, and engine motor mechanical speed limits.

TABLE 1. SELECTED CONTROL MODES FOR THE ATDE TURBOFAN ENGINE

Engine Variable	*easured Type Loop*	*Parameters*
Fan Inlet Guide Vane Angle (FIGV)	Open Loop	N1, T2
Compressor Stator Vane Angle (CSVA)	Open Loop	N2, T22
Gas Generator Fuel Flow (WF)	Closed Loop (Integral)	P5/P2
High Pressure Turbine Inlet Area (A4)	Closed Loop (Integral)	(P3-PS3)/P3
Low Pressure Turbine Inlet Area (A41)	Closed Loop (Integral)	N2, T22
Core Stream Exhaust Nozzle Area (AJE)	Closed Loop (Integral)	N1, T2
Duct Stream Exhaust Nozzle Area (AJD)	Closed Loop (Integral)	(P13-PS13)/P13
Duct Heater Fuel Flow (WFD)	Open Loop	WAD, Corrected Airflow
Start Bleed	Open Loop	T2, T22

GAS GENERATOR FUEL FLOW (WF) CONTROL LOOP

Sensed input parameters required for the WF control loop include the following:

PLA	—	Power lever angle
P2	—	Fan inlet total pressure
T2	—	Fan inlet total temperature
P5	—	Low pressure turbine discharge total pressure
N1	—	Low rotor speed
N2	—	High rotor speed
(ΔP/P)3	—	Differential pressure, station No. 3
T22	—	High compressor inlet total temperature
P3	—	Compressor discharge total pressure
TBT	—	High pressure turbine blade temperature

Constant match variable temperature (CMVT) operation 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 the power setting (Figure 4). A correlation schedule between the WF and AJE loops provides scheduling of AJE to eliminate 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 in order to set power while AJE is constant. The high pressure turbine inlet area (A4) now maintains the desired compressor operating line and the low pressure turbine inlet area (A41) maintains the desired relationship between low and high rotor corrected speeds.

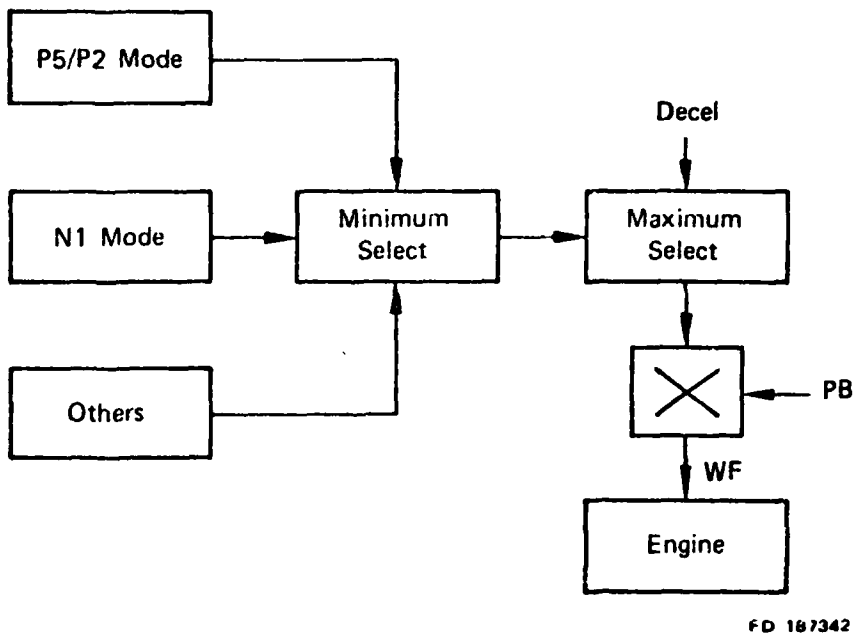


Figure 4. WF Control Logic (Sheet 1 of 3)

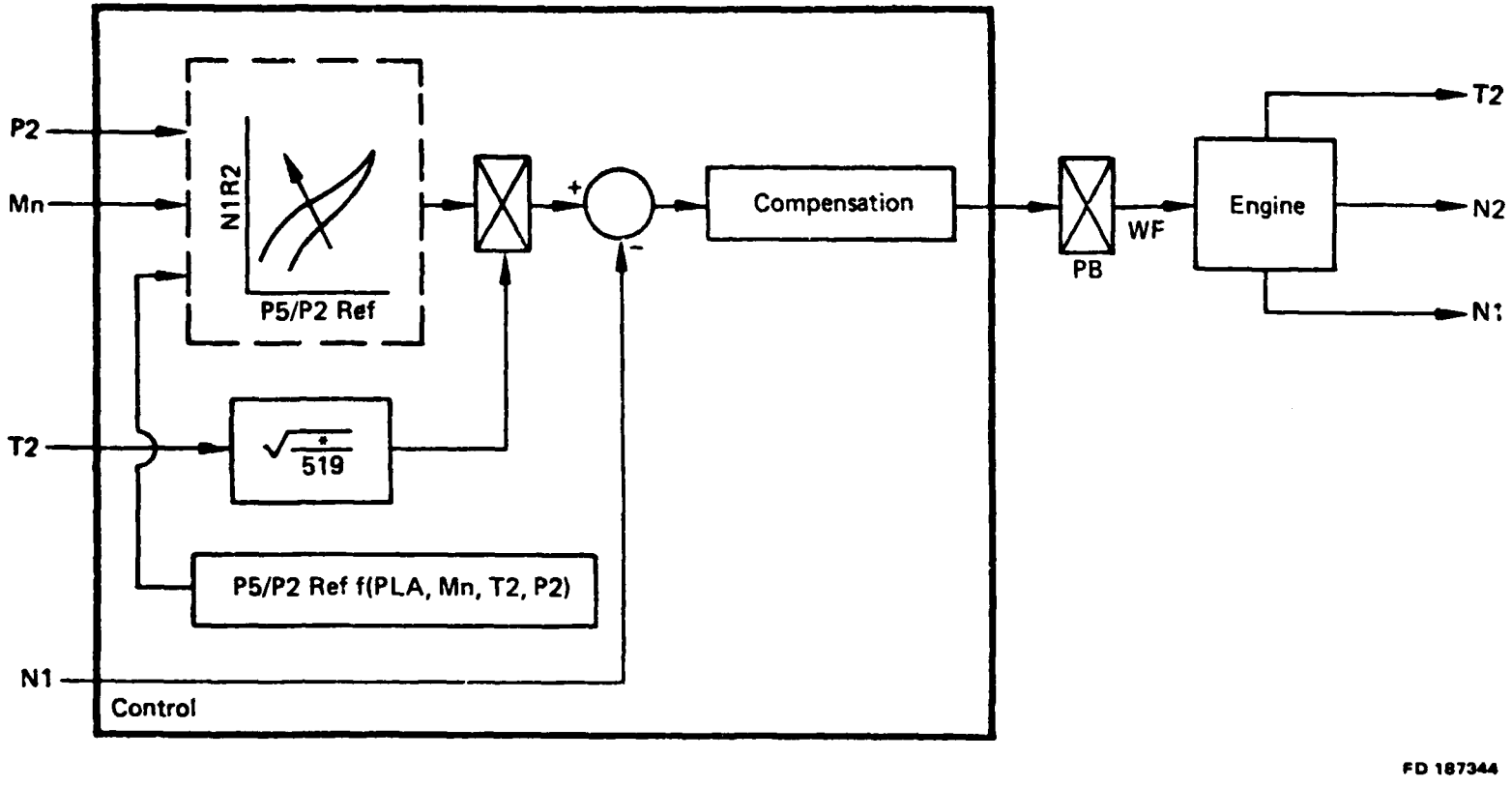


Figure 4. WF Control Logic: N1 Mode (Sheet 2 of 3)

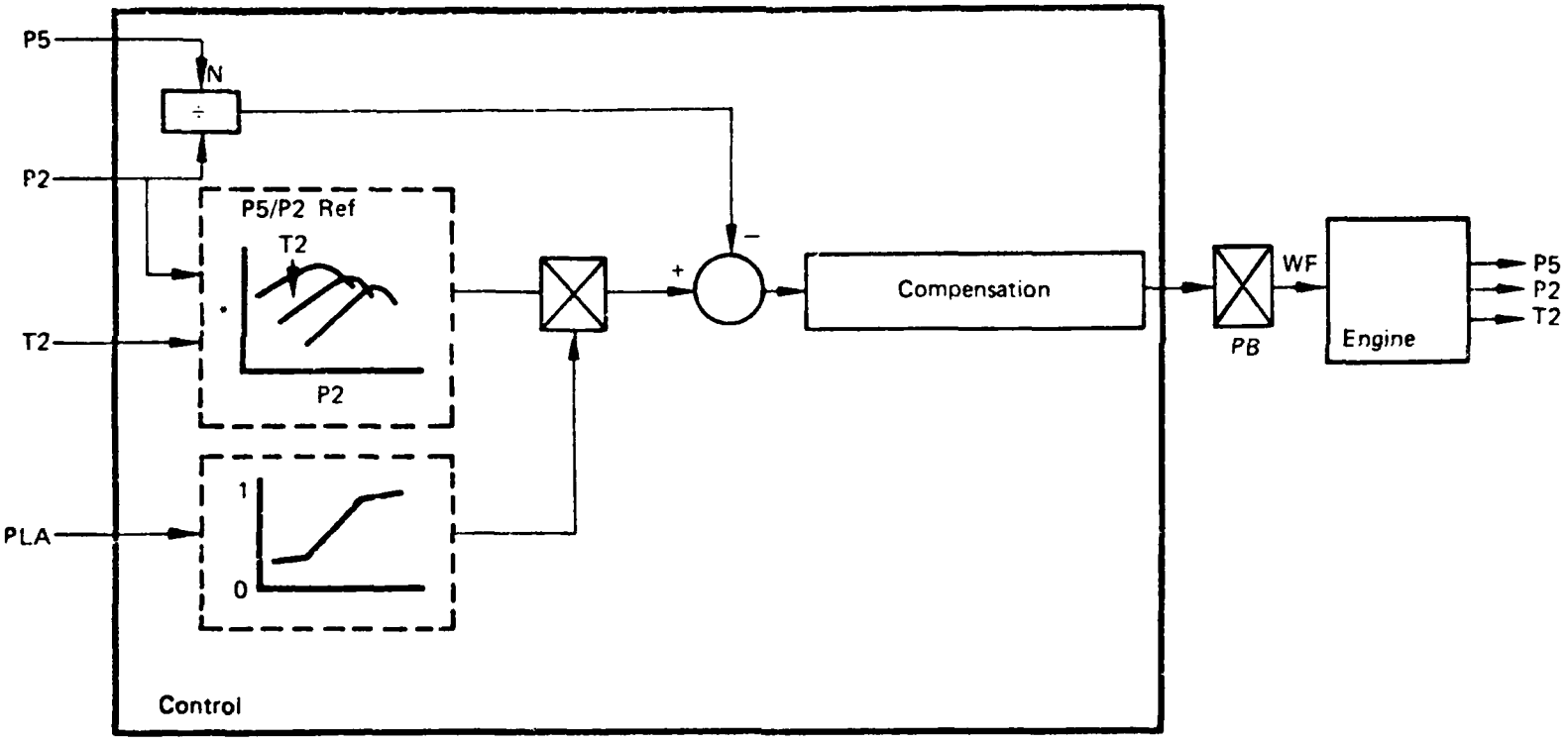


Figure 4. WF Control Logic: P5/P2 Mode (Sheet 3 of 3)

This loop transition is accomplished with the first "MINIMUM SELECT 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 (N1 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 (N1 error) for steady-state operation, and the N1 mode will be selected by the logic as the controlling mode. Conversely, above breakpoint power, the low rotor speed schedule is raised out of the way so that the pressure ratio path can be selected.

The third block going through the Minimum Select logic labeled "OTHERS" contains the starting WF/PB schedule and five limiting functions:

Accel limit
Turbine blade temperature limit
Burner pressure limit
Compressor discharge temperature limit
High rotor speed limit

Exceeding any of these limits results in control fuel flow cutback.

Protection against main burner blowout and excessive temperature rates of change during decelerations is provided by the fuel-air limiting loop acting through the maximum select block in the fuel flowpath. Main burner fuel-air ratio is calculated based upon a synthesized value of compressor airflow which is calculated from the thermodynamic characteristic for corrected airflow versus (ΔP/P)3, the sensed value of compressor discharge pressure (PS3), and a synthesized value of compressor discharge temperature (T3SYN). T3SYN is determined from a compressor characteristic as a function of corrected airflow and corrected speed. The error between the synthesized fuel-air ratio and the minimum limit on fuel-air ratio acts through the maximum select block in the fuel flow loop to control the deceleration

CSVA CONTROL LOOP

Required input parameters for the CSVA control loop:

N2
T22

In order for the compressor to achieve its high design pressure ratio, a decrease in compressor flow area from inlet to exit is required. On account of the change in flow area at off-design (low) RPM, the airflow through the front stages would be too great for the latter stages if variable vanes were not utilized. Both the angle of attack and airflow must be reduced at the front of the compressor at low RPM, and then increased at high RPM to attain a proper match throughout the entire compressor operating range.

The use of variable vanes properly achieves this airflow match while maintaining high efficiency, stall margin, and pressure ratio. Like the fan inlet guide vanes, these vanes are cambered to reduce the per stage ratio and airflow at low RPM. In order to obtain a high performance and surge margin during acceleration to high RPM, it is required that the vanes schedule from cambered toward axial, and during deceleration from axial to cambered (Figure 5). Compressor stator vane angle (CSVA) is an open loop type control schedule as a function of high compressor rotor speed (N2R) and T22.

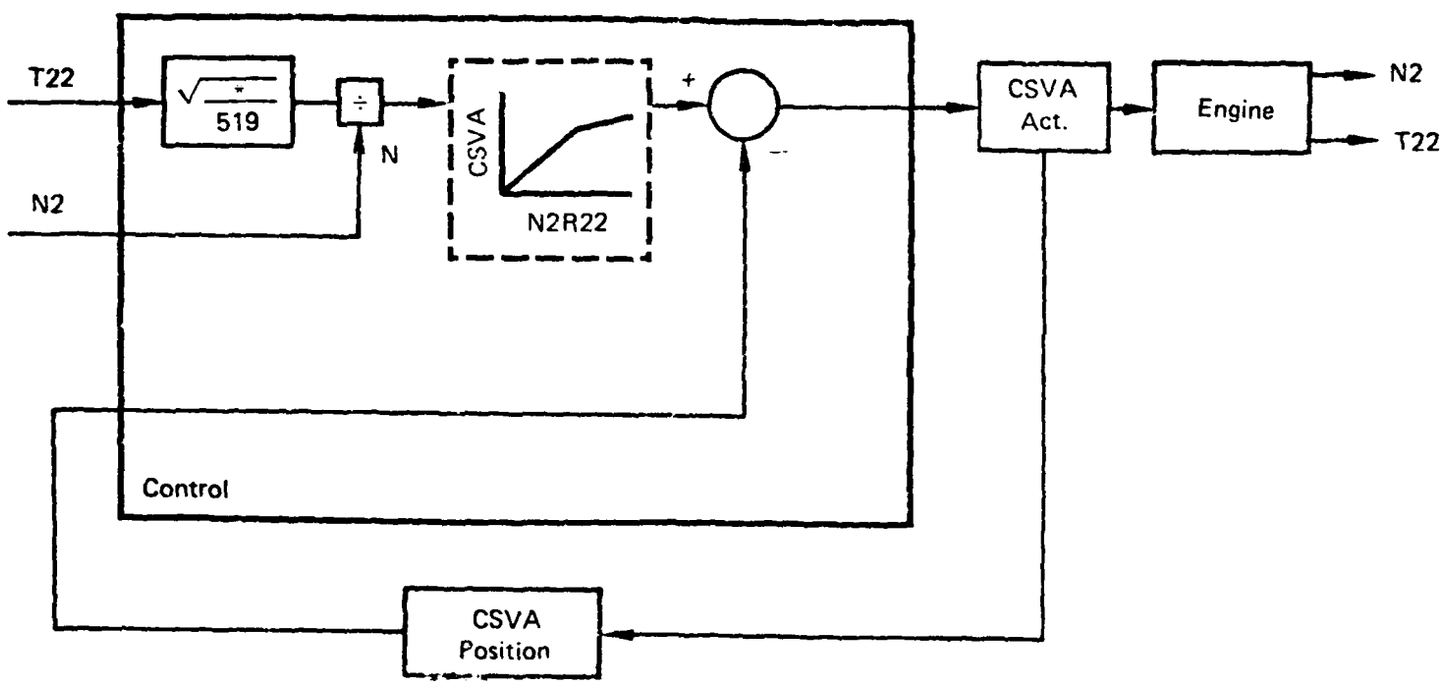


Figure 5. CSVA Control Loop

AUGMENTOR FULE CONTROL LOOP

The following are the required input parameters for the WFD control loop:

(ΔP/P)3
P13
T22
T2
PLA

The duct stream augmentor control mode schedules duct area (AJD) and duct fuel-air ratio versus PLA and trims AJD to maintain the scheduled value of fan discharge Mach number which is a function of (ΔP/P)13 (Figure 6). A value of corrected duct airflow (WAR13) is synthesized from (ΔP/P)13 and then uncorrected using sensed duct pressure (P13) and synthesized duct temperature (T13). T13 is synthesized from the steady-state characteristic as a function of compressor inlet temperature (T22). Fuel-air ratio request is derived from T2, P13, and PLA and multiplied by duct airflow (WAR13) to obtain duct augmentor fuel flow (WFD).

FIGV CONTROL LOOP

Required input parameter for the FIGV control loop:

N1
N2

Variable inlet guide vanes are used to provide adequate stall margin and at the same time optimize fan performance throughout its operating range. As low rotor speed decreases from intermediate power level, the inlet guide vanes are cambered to reduce the axial velocity and flow of air through the latter stages, thus increasing the stall margin during low RPM operation (Figure 7)

Fan inlet guide vane angle (FIGV) is an open loop type control and scheduled as a function of sensed low rotor corrected speed (N1) and T2.

A4 CONTROL LOOP

Sensed input parameters for the A4 control loop:

N2
A4 POSITION
T22
P3
(ΔP/P)3

Operating above CMVT breakpoint with CSVA on schedule, the high pressure turbine inlet area (A4) controls, by way of a closed loop, the compressor discharge Mach number (i.e., compressor airflow for a constant match point) which is characterized by the difference between total and static pressures divided by total pressure of the compressor discharge (ΔP/P)3 (Figure 8). Below CMVT breakpoint, when WF controls the low rotor speed to get power, A4 then maintains the desired compressor operating line.

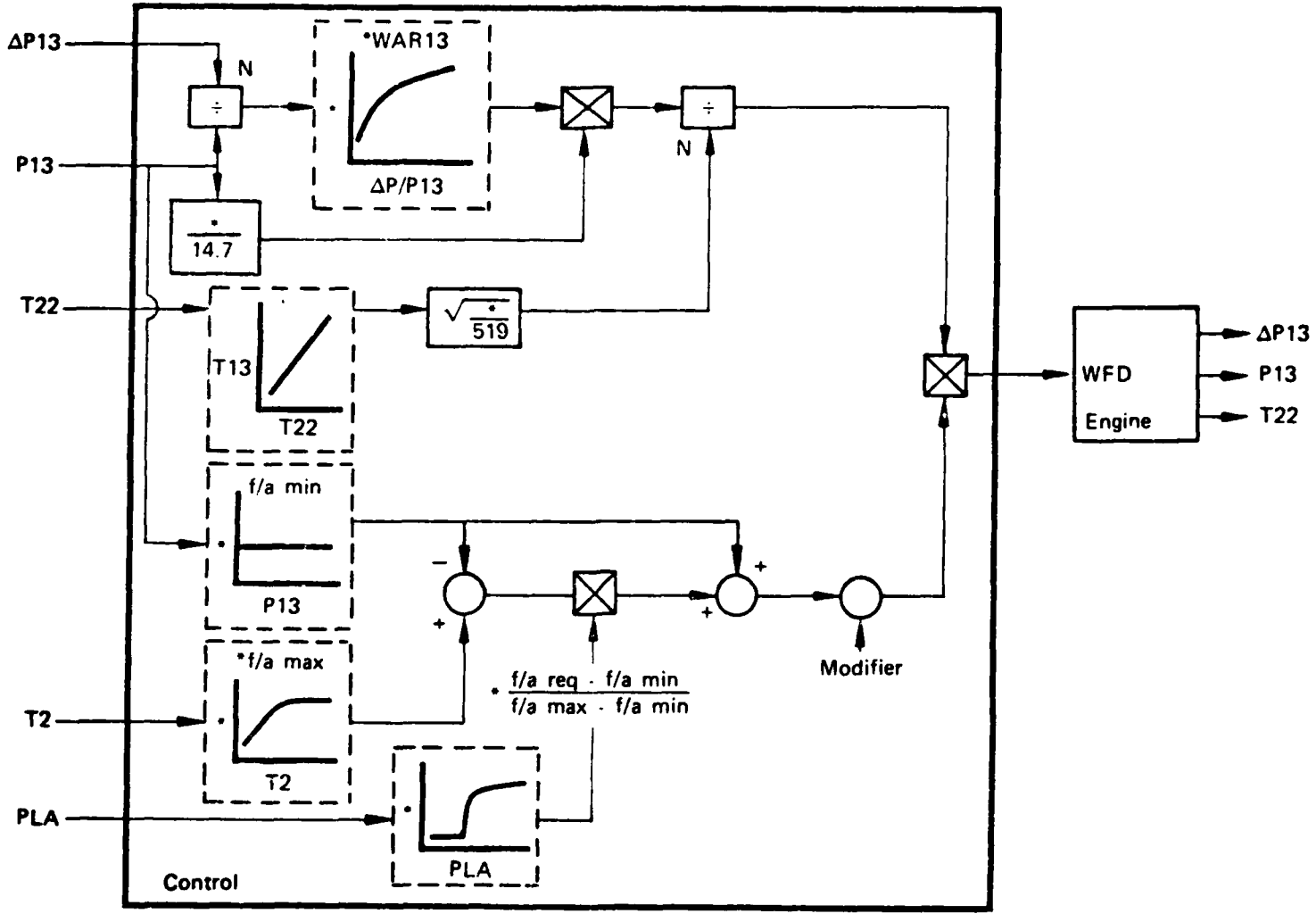


Figure 6. Augmentor Fuel Loop (Duct Only)

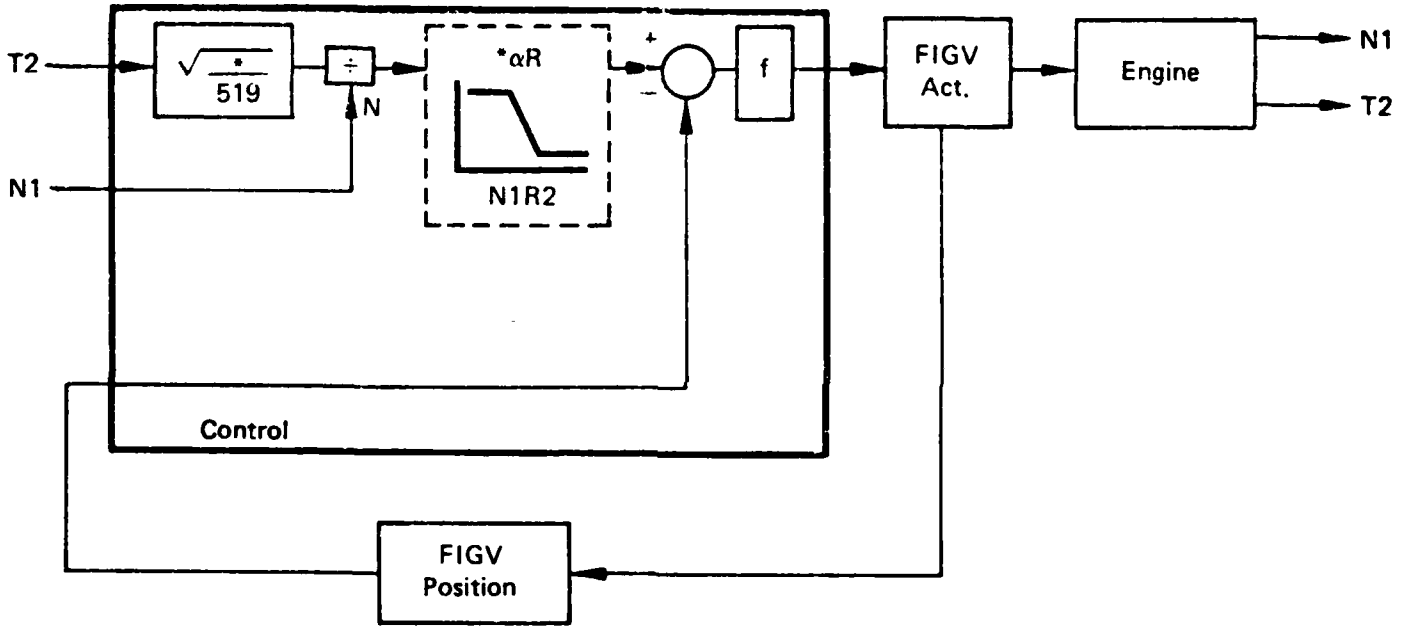


Figure 7. FIGV Control Loop

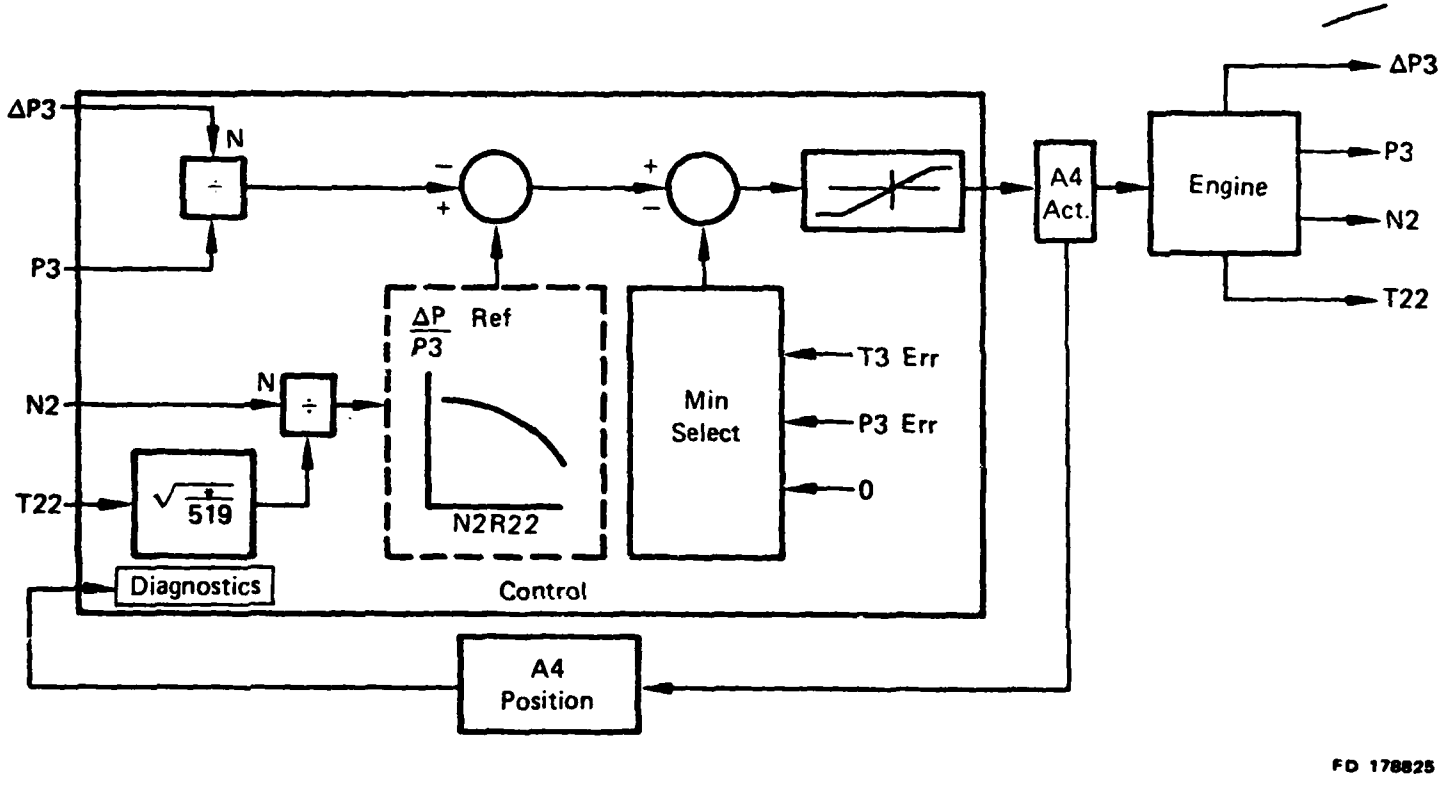


Figure 8. A4 Control Loop

A41 CONTROL LOOP

Required input parameters for the A41 control loop:

N1
N2
T22
A41 Position
T2
MN

Operating above CMVT breakpoint with CSVA on schedule, low turbine inlet area (A-41) controls compressor corrected speed to set the match of the compressor by way of a closed loop type control. During operation below CMVT match point, A41 maintains the desired relationship between low and high rotor corrected speeds (Figure 9). Low rotor speed (N1) and Mach number (MN) are used to obtain a reference high rotor speed in order to maintain the desired speed match between the two spools.

AJE CONTROL LOOP

Required input parameters for the AJE control loop:

MN
P2
T2
N1
AJE POSITION
WFReq from WF loop

With FIGV on schedule, core stream exhaust nozzle area (AJE) controls fan corrected speed by a closed loop type control. Below breakpoint of CMVT operation, AJE is held constant while WF controls low rotor speed. Above the breakpoint for CMVT operation, sensed Mach number, T2, and P5/P2 reference from the WF control loop are used to generate a reference low rotor speed which is compared with sensed low rotor speed to generate an error signal ω drive the AJE actuator (Figure 10). A correlation between WFReq and AJE is also included for transient scheduling of AJE to eliminate interaction between these two loops during rapid transients.

AJD CONTROL LOOP

Input parameters required for the AJD control loop:

N1
$(\Delta P/P)13$
P13
T2
PLA

With FIGV on schedule, the duct stream exhaust nozzle area (AJD) controls, via a closed loop, the fan discharge Mach number which is characterized by $(\Delta P/P)13$ to set the match of the fan during CMVT operation (Figure 11). During operation of the duct stream augmentor, it is important to maintain control of the fan operating point for consideration of augmentor operational limits, fan surge margin, and total engine airflow. To accomplish this, the basic duct Mach number control loop for duct exhaust nozzle area is retained from the gas generator control mode.

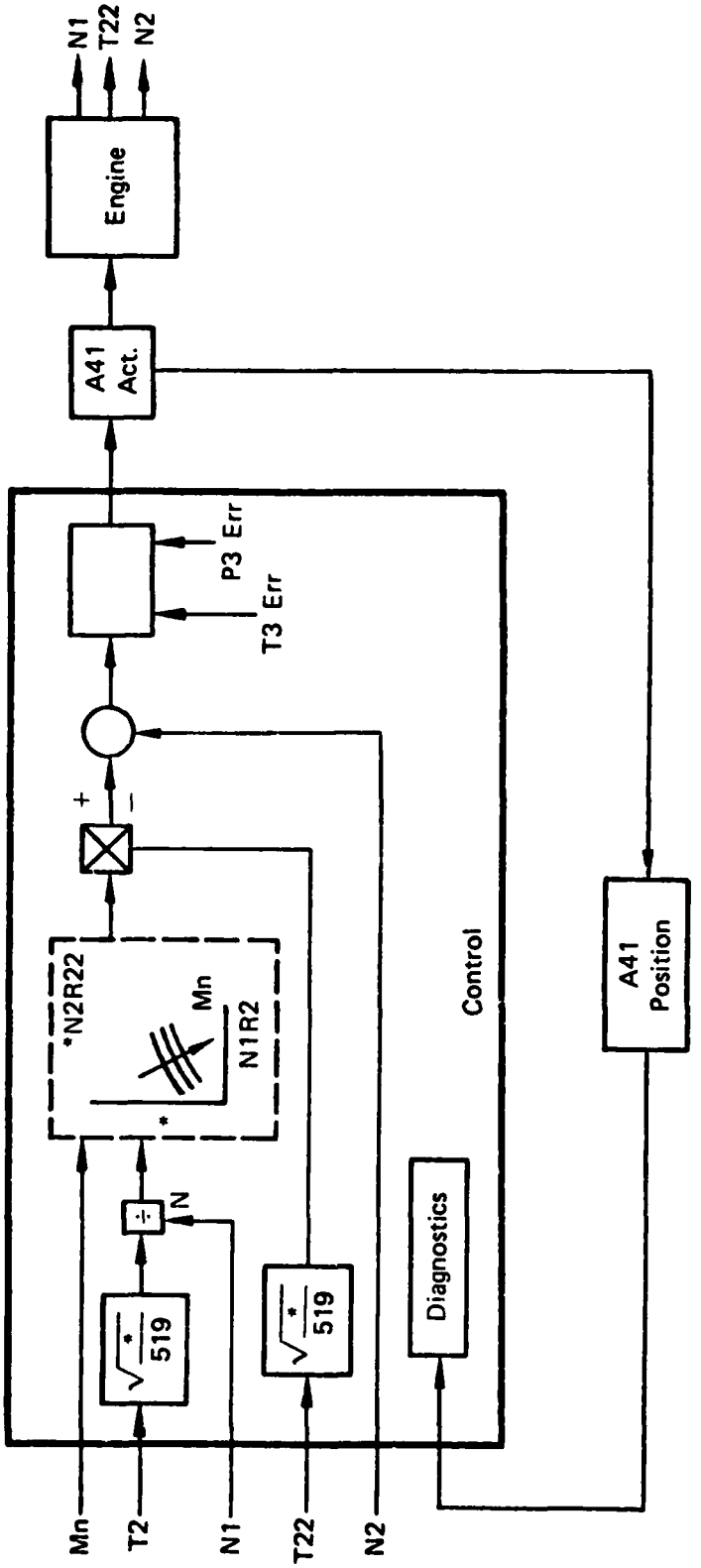


Figure 9. A41 Control Loop

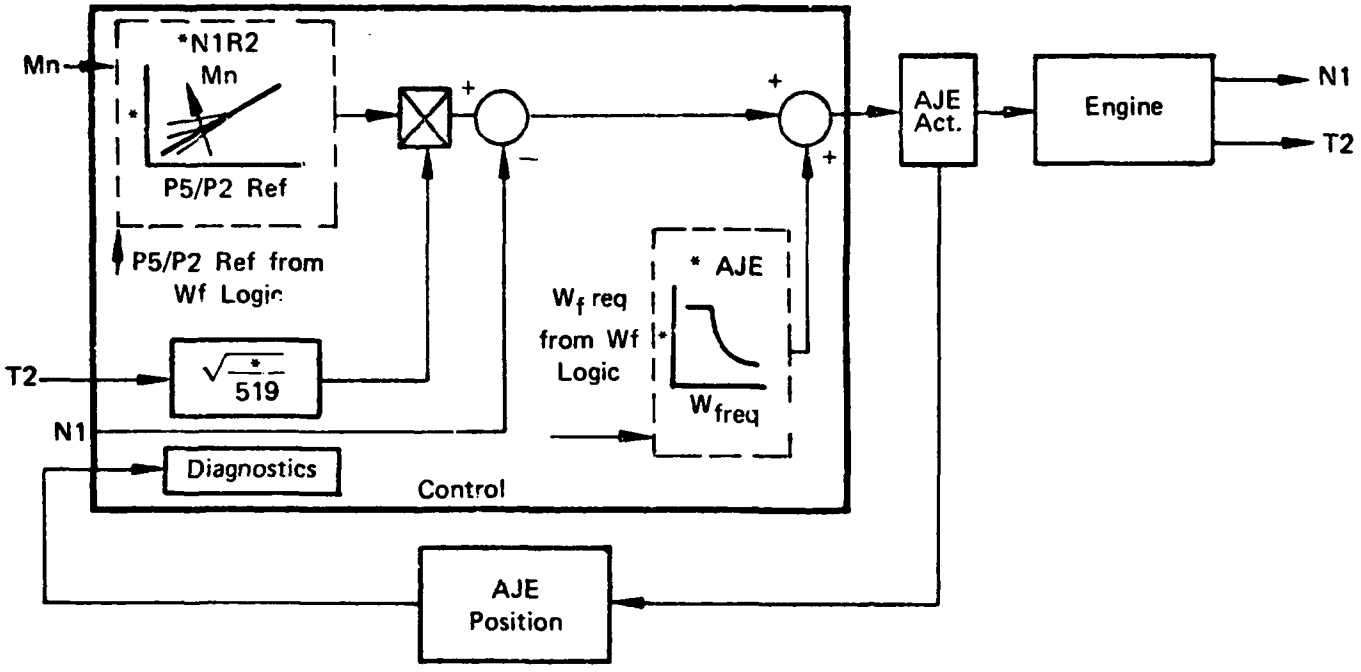


Figure 10. AJE Control Loop

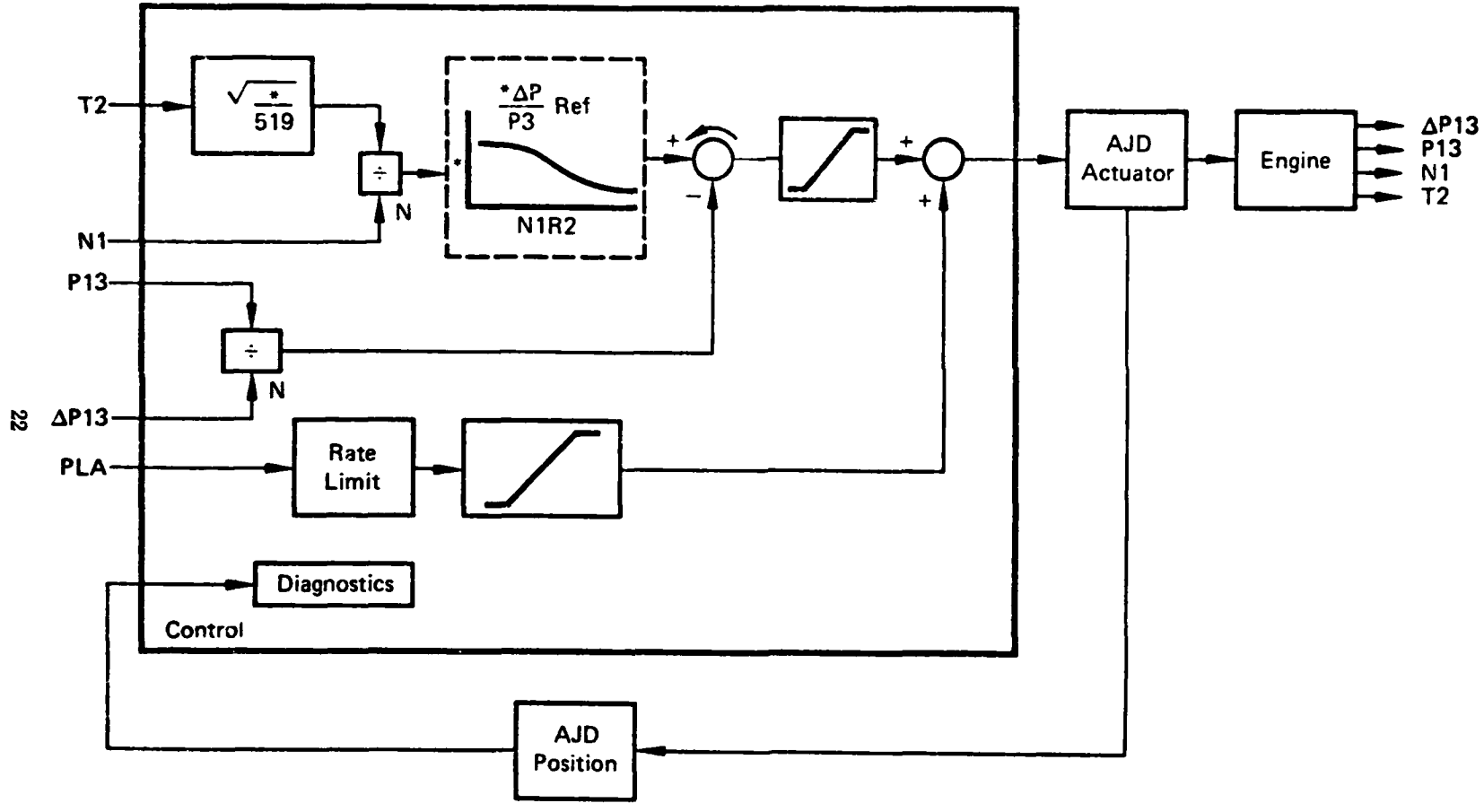


Figure 11. AJD Control Loop

START BLEED LOOP

Required input parameters for the Start Bleed loop:

N2
T22

The starting bleed is opened at starting conditions for stability accommodation and is closed at high power conditions to provide optimum compressor operation. The start bleed valve position is a function of high rotor speed (N2) and T22 (Figure 12).

HYDROMECHANICAL BACKUP CONTROL MODE

The Hydromechanical Backup Control (HMBUC) schedules gas generator fuel flow (WF), compressor stator vane angle (CSVA), and starting bleed valve position (Figure 13). WF is scheduled as a function of PLA and corrected high rotor speed (N2C2) to provide desired fuel flow ratio units (WF/P3). Accel and Decel limits to WF/P3 are scheduled as a function of N2C2 through the appropriate MIN and MAX SELECT logic. Burner pressure (P3) is then multiplied by WF/P3 to obtain the desired fuel flow. Both CSVA and starting bleed valve position are scheduled as a function of corrected high rotor speed.

DIGITAL BACKUP CONTROL (DIGBUC)

DIGBUC is a software control mode outside of the full operational control mode which implements a fail-soft philosophy for all digital failures serious enough to prevent safe operation with the normal control, with the exception of the following items:

- Loss of electrical power
- Loss of Central Processor Unit
- Loss of the following specific critical inputs and outputs:
  - T2 sensor
  - N2 sensor
  - CSVA actuator or feedback
  - P3 sensor
  - WF actuator or feedback
  - N1 sensor
  - TBT sensor.

DIGBUC will control the engine in the same manner as the hydromechanical backup control (HMBUC) but will not require a transfer to any different hardware control system components (Figure 14). The above listed exceptions require transfer to HMBUC.

FAFTEEC ELECTRONIC ENGINE CONTROL

The FAFTEEC baseline electronic engine control is designed as a single channel unit. Figure 15 is a block diagram of a system capable of handling the computation requirements necessary to control and protect the ATDE engine. Table 2 is a list of the control inputs and outputs. This list is applicable to all of the FAFTEEC systems. Various levels of redundancy are employed in the systems but the Input/Output list required for control of the ATDE engine is consistent with the baseline system.

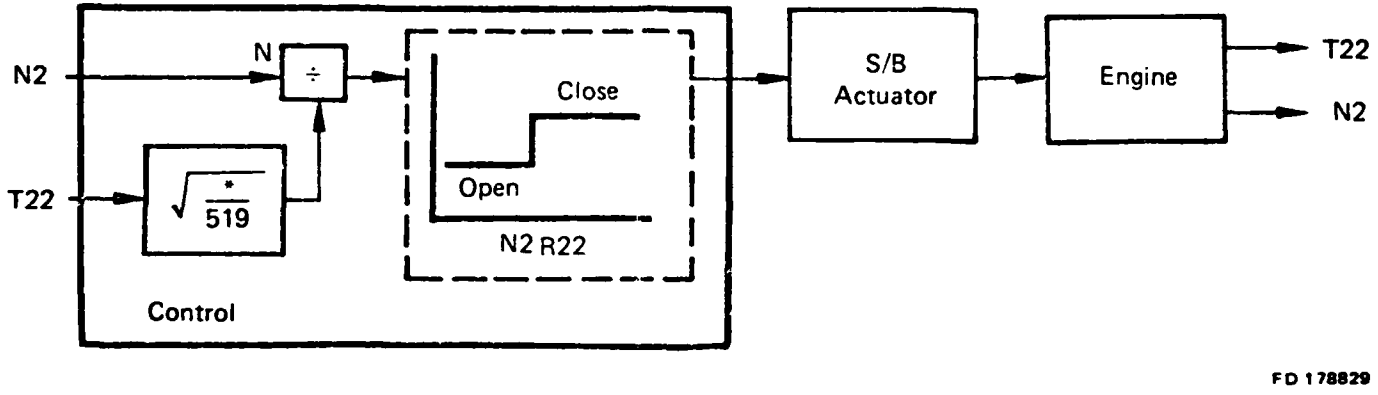


Figure 12. Start Bleed Loop

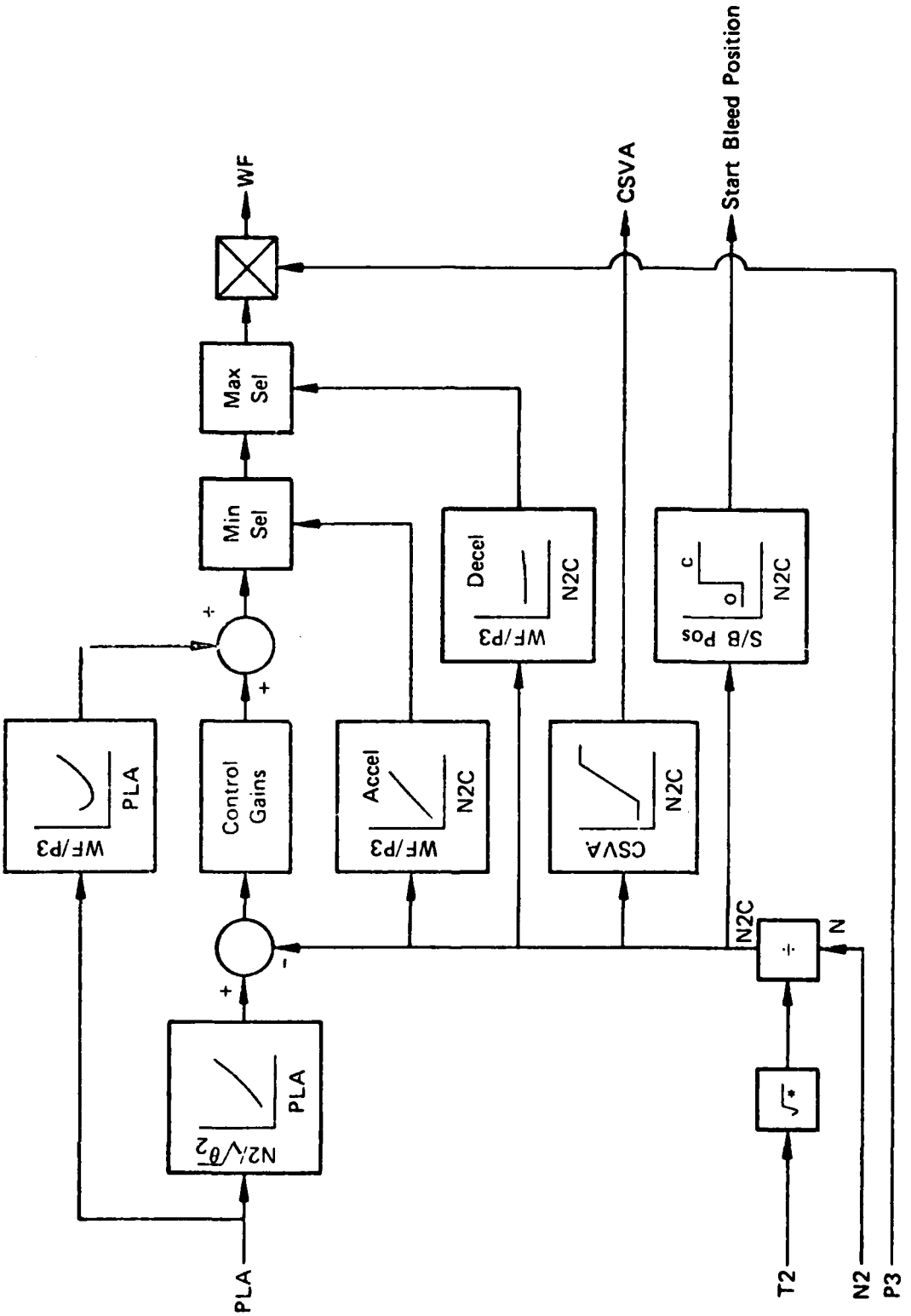


Figure 13. Backup Control Logic Diagram

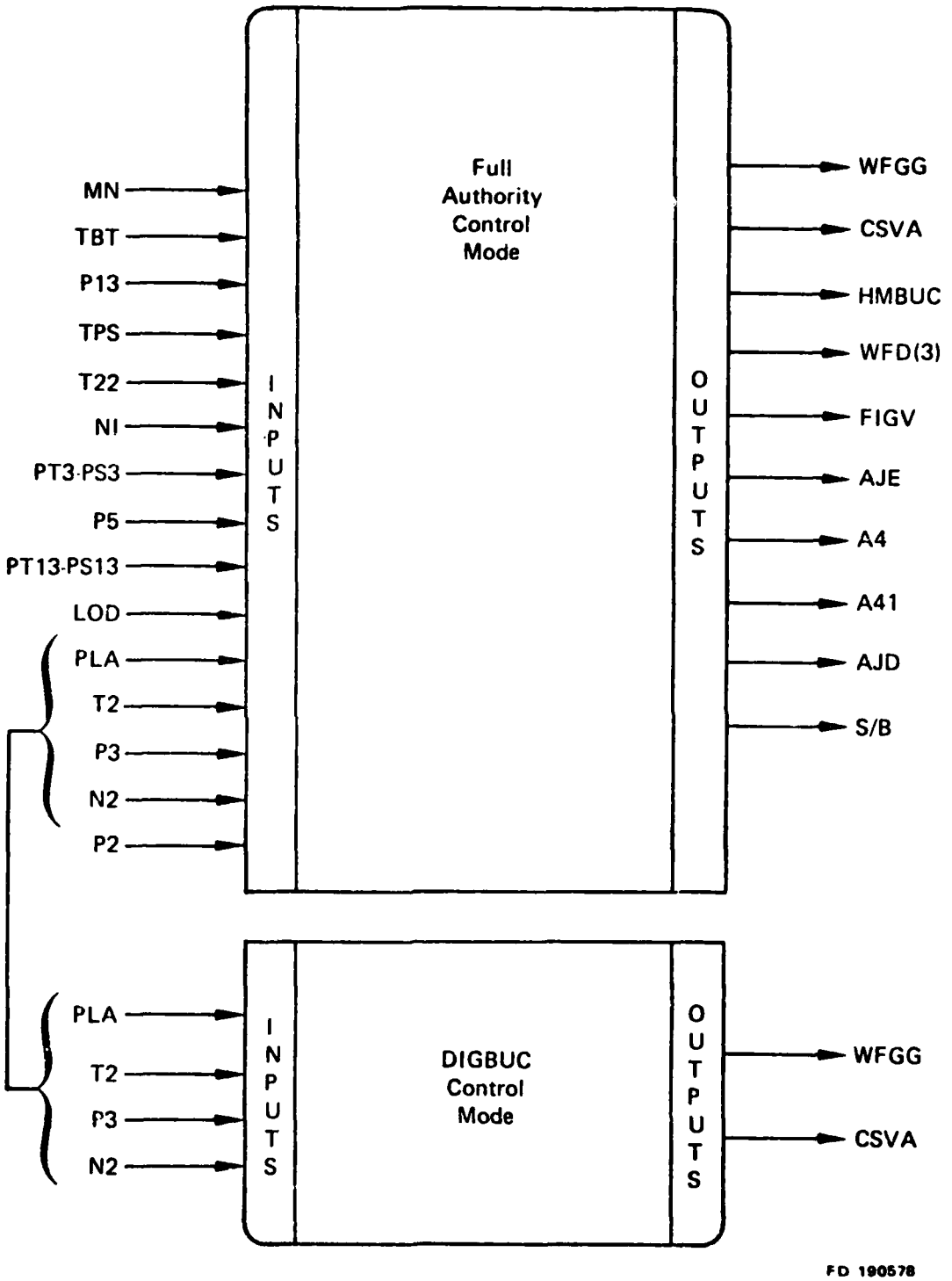


Figure 14. DIGBUC Fail-Soft Mode

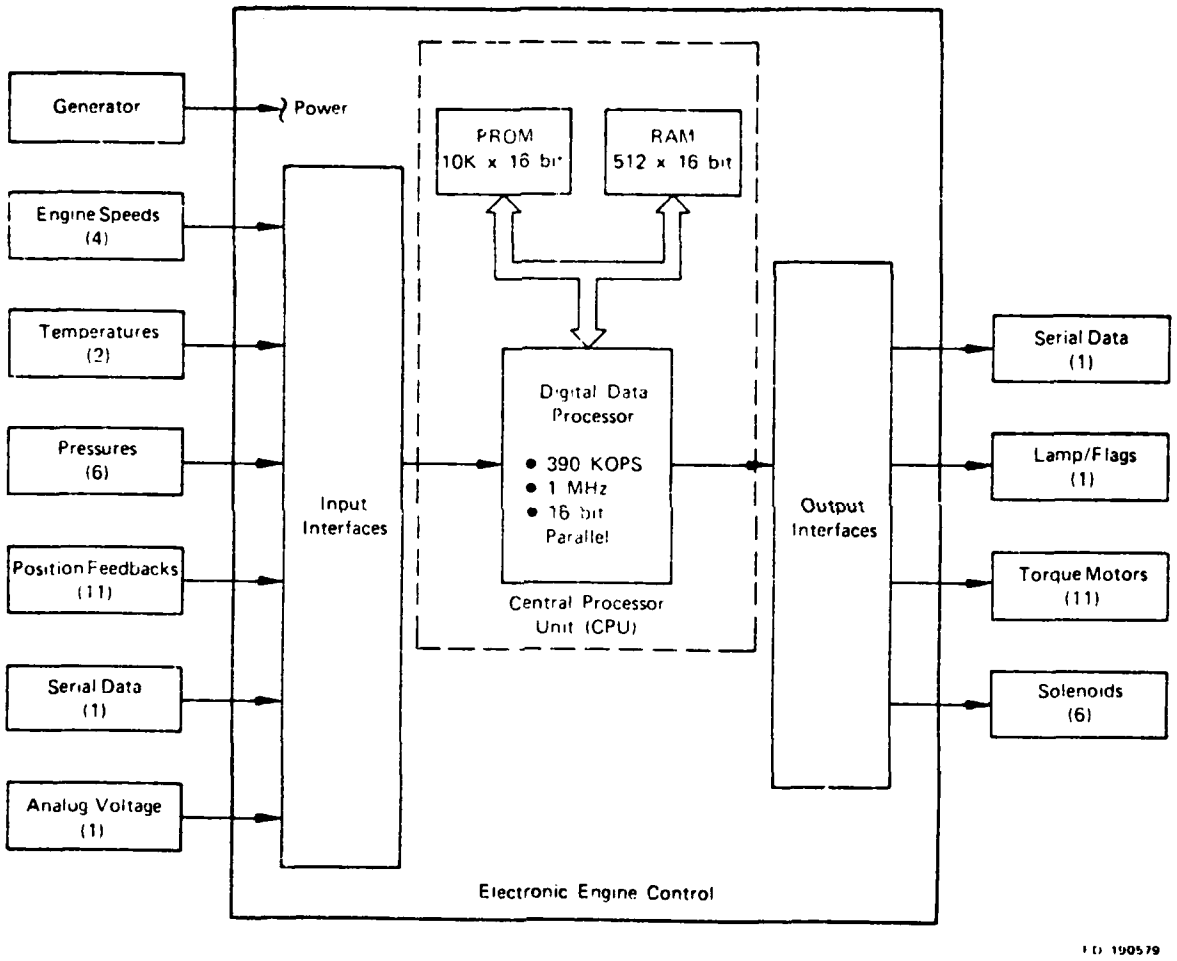


Figure 15. FAFTEEC Electronic Engine Control

TABLE 2. ELECTRONIC UNIT INPUT

Parameter	*Signal Type*
PLA	Resolver
T2	Resistance Probe
T22	Thermocouple
TBT	Analog Voltage
P2	Pneumatic
P3	Pneumatic
P3	Pneumatic
P5	Pneumatic
P13	Pneumatic
P13	Pneumatic
N1	Frequency (Mag Pickup)
N2	Frequency (Alternator)
TPS	Frequency (Mag Pickup)
FIGV	Resolver
CSVA	Resolver
WFGG	Resolver
A4	Resolver
A41	Resolver
AJE	Resolver
AJD	Resolver
WFD1	Resolver
WFD2	Resolver
WFD3	Resolver
LOD	Frequency
MN	Serial Digital
FIGV	Torque Motor Drive
CSVA	Torque Motor Drive
WFGG	Torque Motor Drive
A4	Torque Motor Drive
A41	Torque Motor Drive
AJE	Torque Motor Drive
AJD	Torque Motor Drive
WFD1	Torque Motor Drive
WFD2	Torque Motor Drive
WFD3	Torque Motor Drive
TPC	Torque Motor Drive
Start Bleed	Solenoid Drive
WFGG Shut Off Valve	Solenoid Drive
WFD1 Shut Off Vale	Solenoid Drive
WFD2 Shut Off Valve	Solenoid Drive
WFD3 Shut Off Valve	Solenoid Drive
Fault Flag	Solenoid Drive
Augmentor Ignition Solenoid	Solenoid Valve
Digital Data	Serial Digital Data

The control interfaces with the engine mounted sensors which provide pressure, temperature and speed signals. The input interface hardware accepts and conditions the resolver feedback signals, magnetic pickup speed signal, vibrating cylinder pressure transducer signals, temperature signals from the thermocouple and platinum resistance probe, turbine blade temperature pyrometer signal and discrete signals and converts them to digital data words which are transmitted to the Central Processor Unit (CPU). The CPU is part of the Computational Core (CC) which also includes the Input/Output Bus and the memory devices, which are programmed to carry out the gas generator and augmentor operating logic. Commands from the CC are converted into output signals in the output interfaces. This circuitry includes torque motor actuation signals and resolver excitation. The torque motor interface will consist of the D/A converter and an output buffer to supply current to each torque motor winding. The resolver excitation circuit will be a divider chain from the system master clock, driving a discrete component filter with multiple power op-amps as the output devices, and it will be required to be a large-amplitude, frequency-stable, low-distortion signal in order to maintain resolver accuracy.

In addition to control mode functions, the single channel concept also includes self-test and fault annunciation capabilities. Self-test is implemented in both the software and the hardware. The watchdog timer is a hardware built-in test circuit which is used to detect and either correct or flag a hung CPU condition. Its primary function is to eliminate any infinite looping that may occur as a result of an abnormal transient. This looping condition is quickly detected by the timer, as the timer must be reset by the CPU after each frame of control loop calculations. A reset pulse is given to the CPU in an attempt to restart it. All output effectors are also reset at this time and, if the CPU does not recover, the fault indicator is latched and a transfer to HMBUC is effected.

SELF-TEST

Computer system self testing is required where applicable because of the single string system architecture. The CPU must provide sufficient memory and processor time to include the required self-test routines as well as other overhead functions not directly related to engine control. The self-test routines applicable to a single channel electronic engine control are given in Table 3. FAFTEEC engine control actions in the event of an internal failure are listed in Table 13 of the FMEA section of this report.

TABLE 3. FAFTEEC BASELINE CONTROL SELF-TEST

	Tests	*In-Flight Tests*	*Pre-Flight Tests*	*Software or Hardware*
1	Input Range Limit Check	X	X	S
2	Parameter Correlation Check	X	X	S
3	Read Only Memory (ROM) Check	X	X	S
4	Computer Cycle Time Test	X	X	H
5	Output Wraparound Test	X	X	H
6	Injected Input Test		X	S
7	Canned Output Computation		X	S
8	Dynamic Loop Continuity Check	X	X	S
9	Reference Signal Check	X	X	H
10	Power Supply Test	X	X	H
11	Processor Instruction Test	X	X	S
12	Read-Write (Scratchpad) Memory Check	X	X	S
13	End of Conversion (EOC) Bit Not Detected	X	X	S
14	Hardware Parity and Code Verifier Checks	X	X	H
15	Clock Loss Detect Circuit	X	X	H
16	N1 Limiting	X	X	H
17	TBT Limiting	X	X	H

SUPPLEMENTARY ENGINE PROTECTION CIRCUITS

The FAFTEEC Baseline Control system is a single string system and therefore includes supplementary speed and temperature limiting circuitry. These circuits would be designed to provide engine protection limits separate from those provided by normal CPU calculated limits. Although they are principally intended to support the digital backup control mode (DIGBUC), they also provide an added degree of safety in all system states of operation. A preliminary block diagram of these circuits is shown in Figure 16.

For N1 protection, the frequency signal is paralleled after signal conditioning. Speed is calculated by the frequency period counter and transmitted to the I/O Bus and the FAFTEEC CPU in the normal manner. the speed limiting signal is sent to a frequency-to-DC converter. This voltage level is then compared to a fixed DC level equivalent to maximum desired speed. If the output of the comparator indicates an overspeed condition, a signal is sent to a DIGBUC-to-HMBUC switching circuit which would immediately switch to the hydromechanical backup control for engine overspeed protection.

Engine overtemperature protection is supplied in a similar manner. The turbine blade temperature (TBD) signal would be processed in the normal manner to the FAFTEEC CPU with a parallel branch to a comparator circuit. This latter circuit would compare the TBT signal to a preset voltage level equivalent to the maximum desired temperature. If this level is exceeded, the DIGBUC/HMBUC circuit would immediately switch to the hydromechanical backup control for overtemperature protection. In the final design both of the above circuits could be modified to provide biasing, rate of change sensing and sample-and-hold type circuits to help prevent erroneous trips to HMBUC.

CONTROL SYSTEM IMPLEMENTATION

BASELINE HARDWARE

The baseline FAFTEEC system is composed of hardware represented by the following set of functional diagrams. These figures represent the mechanical implementation of each control loop and associated support components such as fuel and hydraulic pumps. The diagrams also functionally show the input and output devices, electrohydraulic valves (EHV) and resolvers, respectively.

Engine sensors and electrical devices are listed in Table 4. These sensors provide pressure, temperature and speed signals to the engine control. The generator provides electrical power and the N2 speed signal to the FAFTEEC and also powers the engine ignition system.

GENERAL DESCRIPTION OF THE FAFTEEC BASELINE ENGINE ACTUATORS

The engine actuators interface with the FAFTEEC to translate the electrical commands from the computer into actual engine control actions. To accomplish this, the hydromechanical components incorporate solenoid valves to translate discrete electrical commands into discrete mechanical positions and electrohydraulic servo valves (EHV) to translate proportional signals into proportional mechanical motion. The EHV's are a two-stage valve design with a dual-wound torque motor controlled hydraulic amplifier first stage driving a three-or four-way spool valve hydraulic second stage. Single-wound resolvers are used to provide component positions to the FAFTEEC in this baseline system.

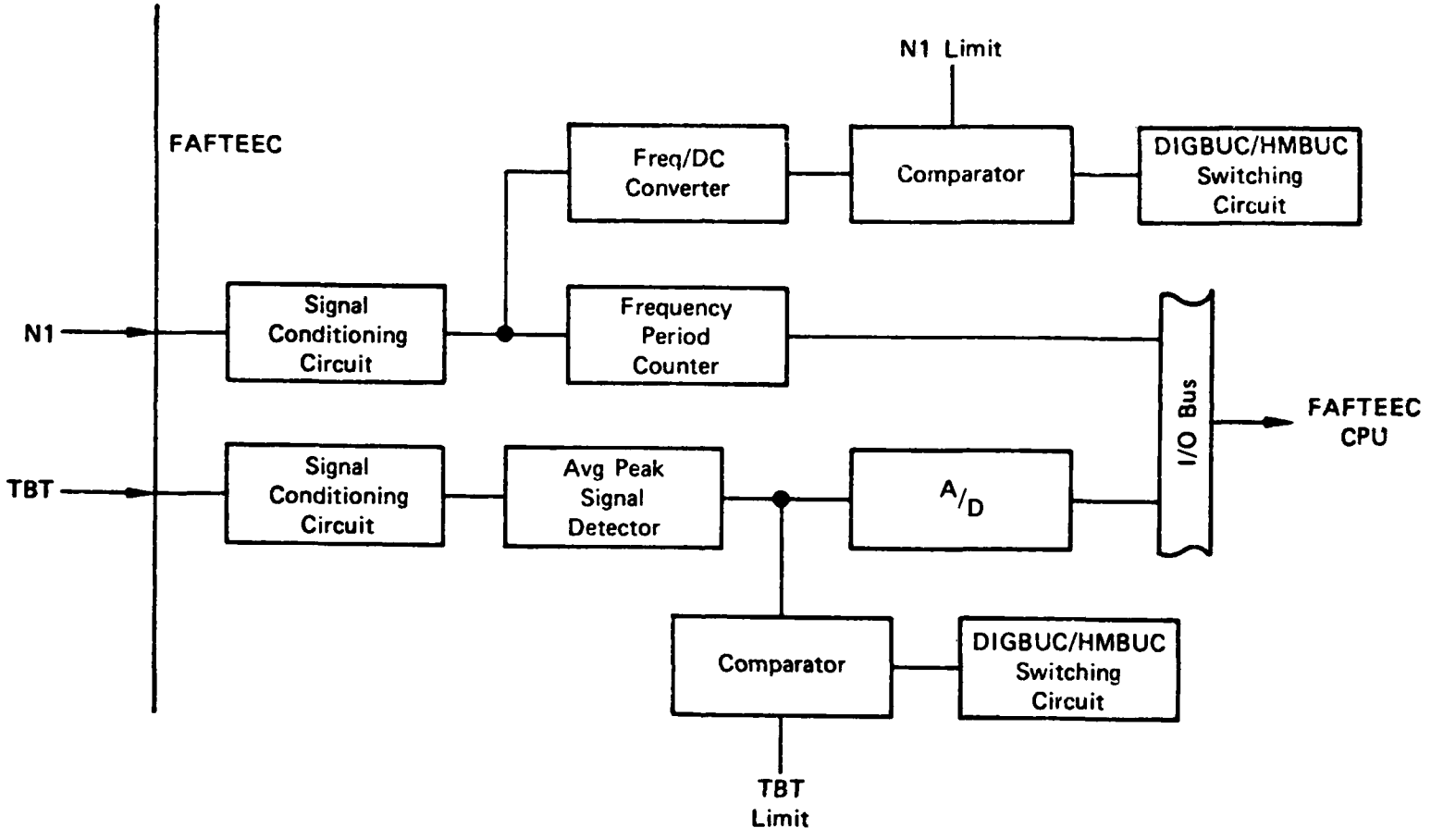


Figure 16. Speed/Temperature Limiting Circuit

TABLE 4. FAFTEEC SENSORS AND ELECTRICAL COMPONENTS

PLA	--	Power Lever Angle
P2	—	Fan Inlet Total Pressure
P3	—	Compressor Discharge Total Pressure
P5	—	Low Pressure Turbine Discharge Total Pressure
P13	—	Fan Discharge Total Pressure
ΔP3	—	P3 - PS3/P3 (PS3 - Compressor Discharge Static Pressure)
ΔP13	—	P13 - PS13/P13 (PS13 - Fan Discharge Static Pressure)
T2	—	Fan Inlet Total Temperature
T22	—	Compressor Inlet Total Temperature
TBT	—	Turbine Blade Temperature
LOD	—	Light-off Detector
N1	—	Low Rotor Speed
N2	—	High Rotor Speed
TPS	—	Turbo Pump Speed
Mn	—	Aircraft Mach Number
Alternator		
Ignition Exciters		
Gas Generator Ignitors		
Augmentor Ignitors		

GAS GENERATOR CONTROL

The gas generator control is an electrohydromechanical unit designed to control fuel flow in conjunction with the FAFTEEC computer. The gas generator control is also capable of operation with a hydromechanical backup (HMBUC) system in the event of a malfunction of the electronic control system. Figure 17 is a functional diagram of the FAFTEEC Baseline Gas Generator Control. This control is singular in the EHV, metering valve, solenoid operated shutoff valve and pressure regulator. The gas generator control servo hydraulics are supplied from the engine driven gas generator pump. In the normal mode of operation the gas generator control provides the following functions:

- Metered fuel flow to the gas generator, as scheduled by FAFTEEC
- Fuel cutoff by means of a solenoid operated cut-off valve.

Operation of the gas generator control in the HMBUC mode was described earlier in this section, under Hydromechanical Backup Control Mode.

COMPRESSOR STATOR VANE ANGLE ACTUATOR

The compressor stator vane angle actuator (CSVA) is an electrohydromechanical unit used to rotate the inlet stator vanes on the ATDE engine rear compressor. The actuator power piston is driven by fuel pressure directed by the EHV. This valve is controlled by an electrical signal from FAFTEEC to the torque motor. A single resolver linked to the power piston shaft of the actuator provides position feedback to FAFTEEC, closing the control loop (Figure 18).

Operation of the CSVA actuator in the HMBUC mode is described earlier in this section.

BACKUP CONTROL

The FAFTEEC hydromechanical backup control (HMBUC) is designed to operate the engine in a degraded but safe mode in the event of a shutdown of the electronic portion or other critical parameters in the control system. The HMBUC controls gas generator fuel flow (WF) and compressor stator vane angle (CSVA). Figure 19 is a functional description of this hardware.

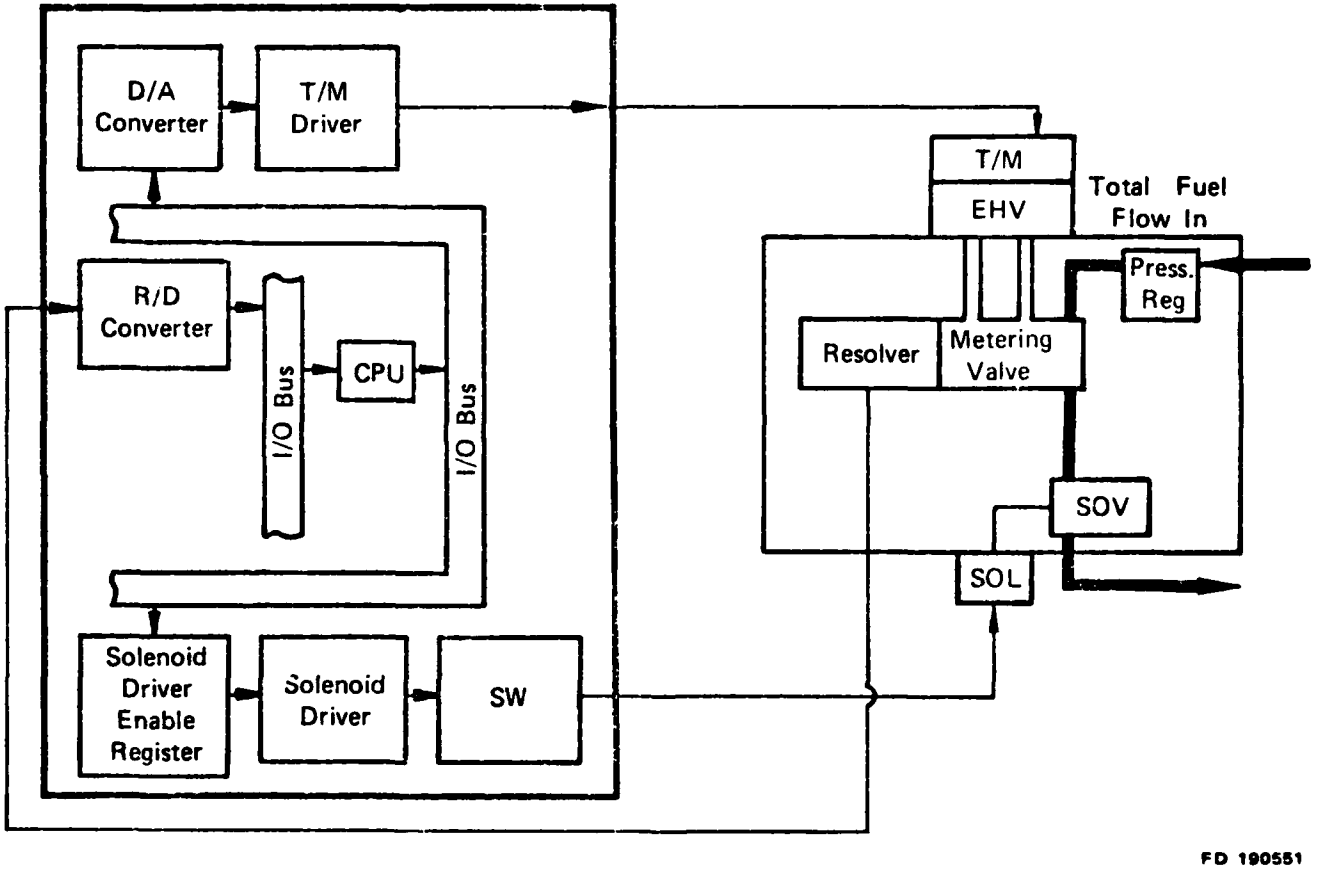


Figure 17. FAFTEEC Fuel Low Loop Implementation

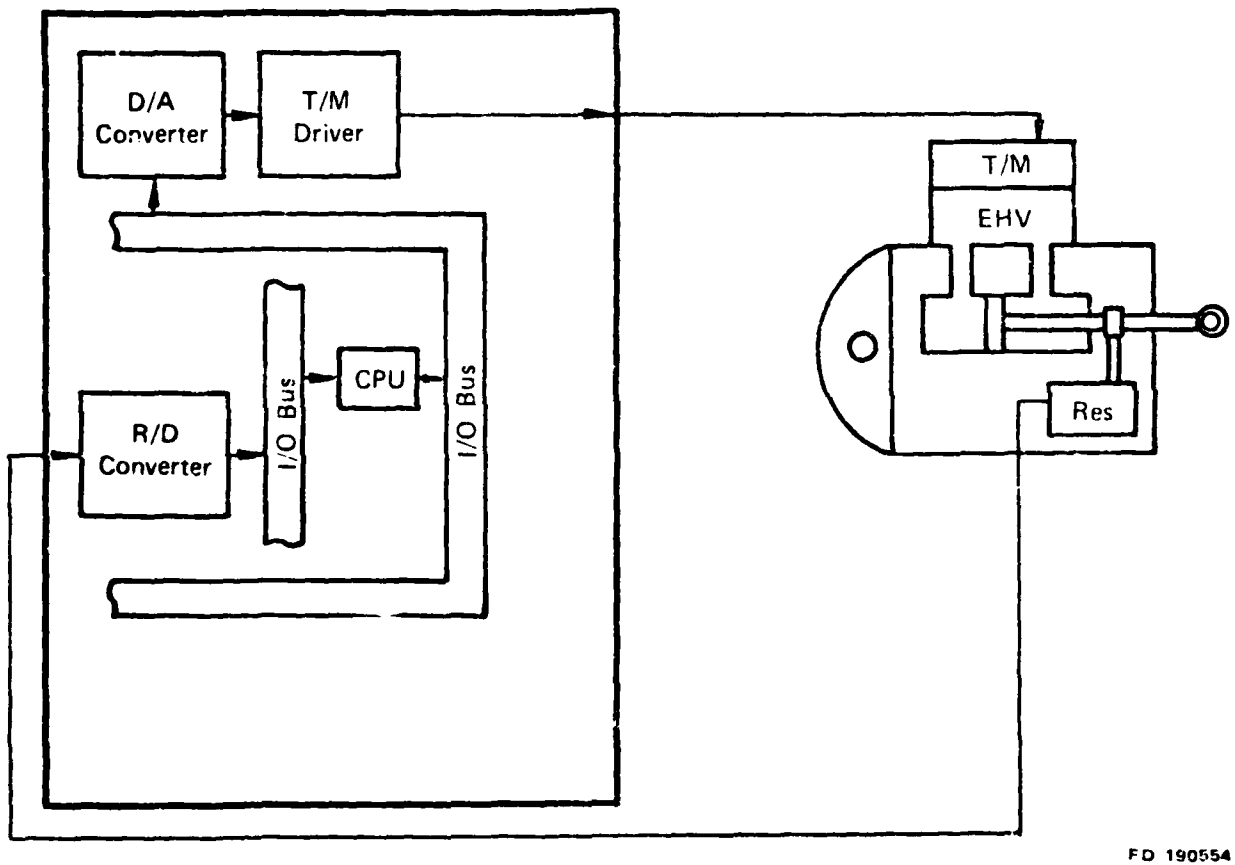


Figure 18. FAFTEEC CSVA Loop Implementation

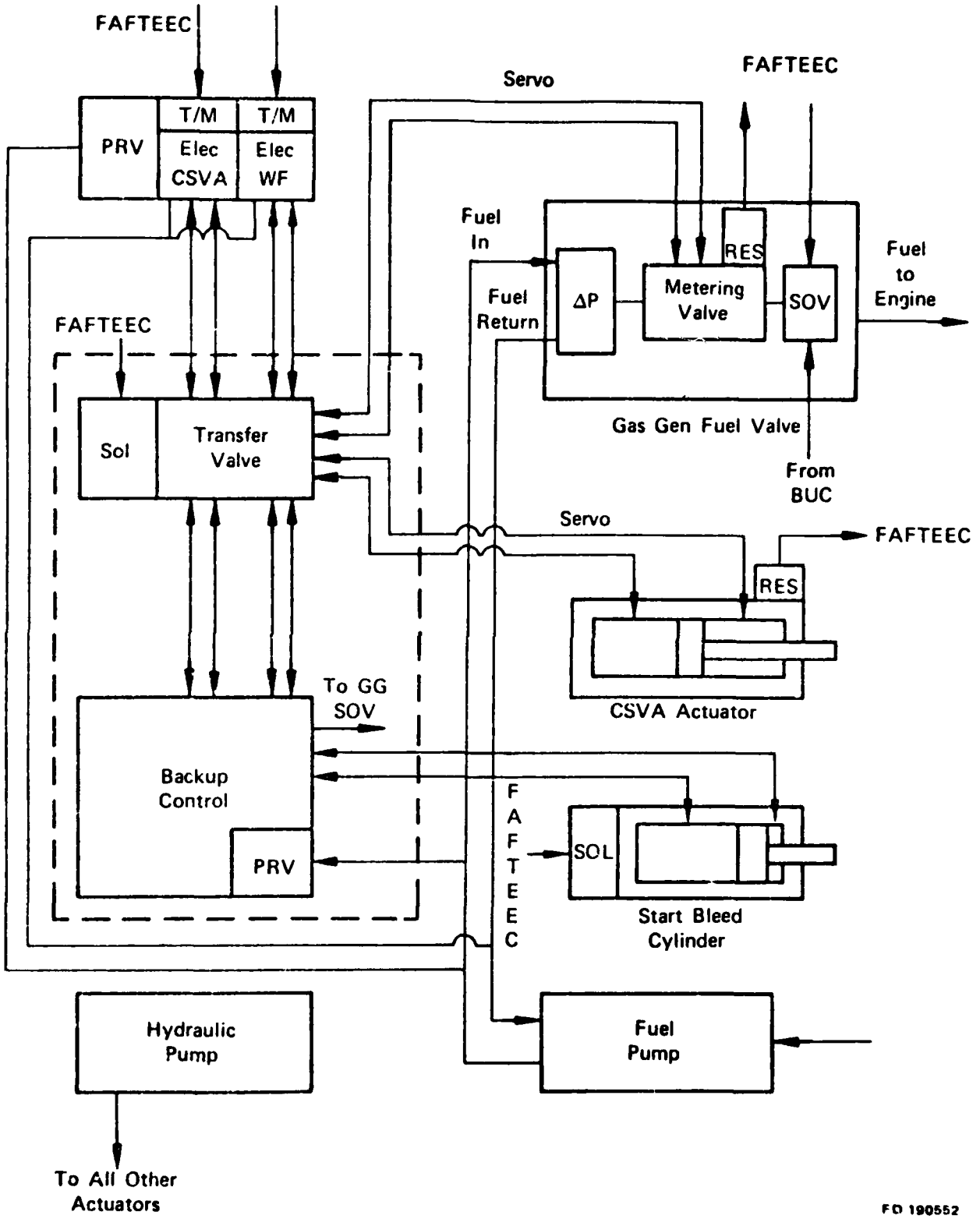


Figure 19. FAFTEEC Backup Control Implementation

The system is engaged through the solenoid operated transfer valve. The solenoid is powered, from FAFTEEC, during all operating modes except HMBUC. In the event of loss of electrical power from FAFTEEC, the solenoid is turned off and the transfer valve shifts to the backup mode. The transfer valve is a simple spring loaded spool valve. During normal operation the solenoid is energized and overcomes the spring allowing the transfer valve to direct hydraulic pressure to the appropriate electrohydraulic valves, shutting off pressure to the HMBUC. When operation in HMBUC is required, the solenoid is de-energized and the spring translates the spool valve to a position where hydraulic pressure for WF and CSVA are sent directly to the HMBUC and denied to the respective EHV's.

With the HMBUC in control, the fuel shutoff valve is held open by the mechanical linkage from the backup control and is a function of mechanical PLA input. Hydraulic pressure for positioning the fuel metering valve is directed from the EHV to the HMBUC by the transfer valve. Fuel metering valve position is controlled by HMBUC through the same lines that had been previously employed by the EHV. In a like manner control of the CSVA is directed from the EHV by the transfer valve. Control of CSVA is through the hydromechanical logic of HMBUC using the same hydraulic lines as had been used by the CSVA EHV.

AUGMENTOR CONTROL

The augmentor control provides three zones of metered fuel flow to the engine augmentor in response to electric command signals from the FAFTEEC computer (Figure 20). Each of the augmentor zones is fueled by a separate fully modulated metering valve. This valve is controlled by a torque motor controlling a single stage hydraulic servo valve which positions the metering valve. Each EHV is commanded and controlled by separate electric signals from the FAFTEEC computer. Fuel to each zone of the augmentor is shut off by an individual solenoid operated, normally closed shutoff valve. In the event of an electrical malfunction, fuel to the augmentor is shut off.

VARIABLE GEOMETRY CONTROLS

The variable geometry controls, that is, controls for the fan inlet guide vanes (FIGV), the high pressure turbine inlet area (A4), low pressure turbine inlet area (A41), core stream exhaust nozzle area (AJE) and duct stream exhaust nozzle area (AJD) will be implemented with an actuation and feedback system similar to that used for the CSVA described earlier. Each actuator will rotate the appropriate set of vanes in response to a signal from the FAFTEEC computer. The individual power pistons are driven by hydraulic pressure directed by the EHV. The feedback position of the valves is supplied by a single-wound resolver linked to the actuator power piston (Figure 21). Each of the above listed valves will be sized for the individual loads imposed by the various variable geometry functions. In the event of a reversion to HMBUC, the actuators will lose power and slew to a position so as not to preclude continued safe operation of the engine.

MAIN FUEL PUMP

The main fuel pump consists of an integral dual-element configuration with a centrifugal boost stage and a fixed-displacement vane stage. The boost stage supplies pressurized fuel to the main fuel pump vane stage and to the augmentor fuel pump when an augmentation permission signal clutches in a high flow centrifugal flow element. The gas generator bypass valve, located on the gas generator control, regulates flow output to maintain a constant pressure drop across the gas generator metering valve. The boost pump and gas generator vane pump are mounted on the same shaft and directly driven by the engine gearbox. A functional block diagram of the main fuel pump is shown in Figure 22.

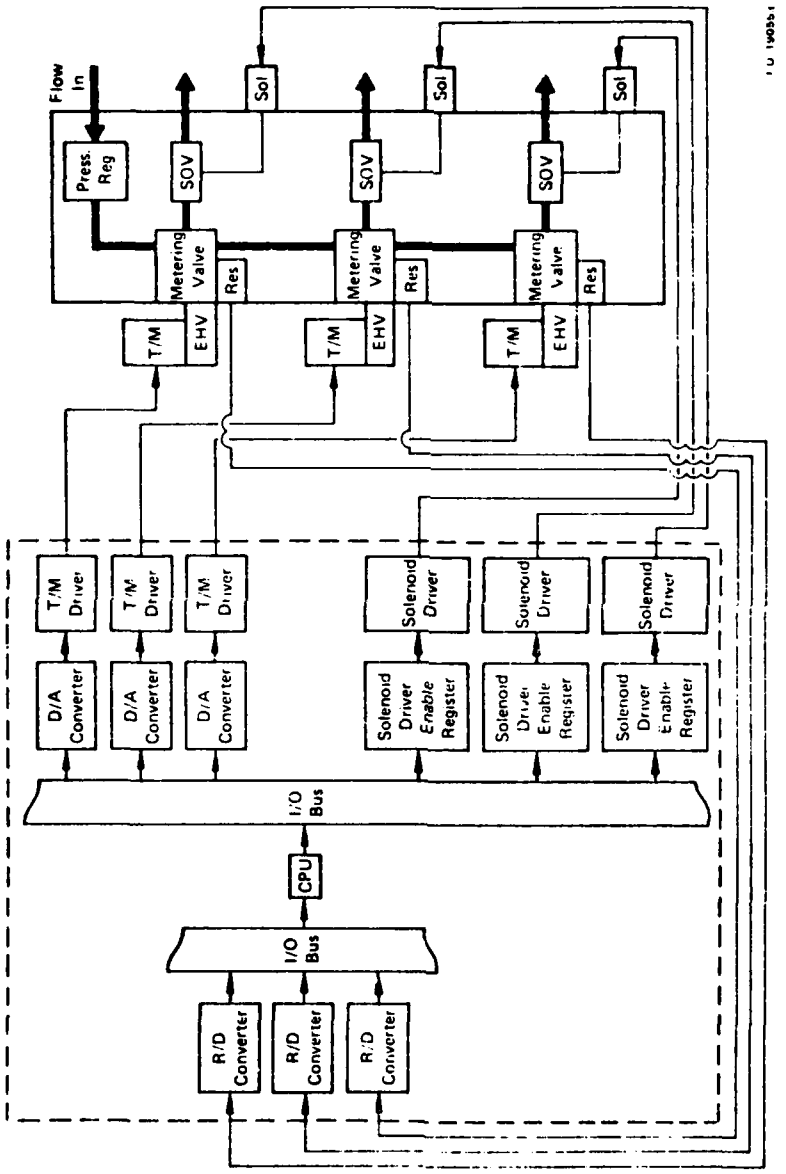


Figure 20. FAFTEEC Augmentor Loop Implementation

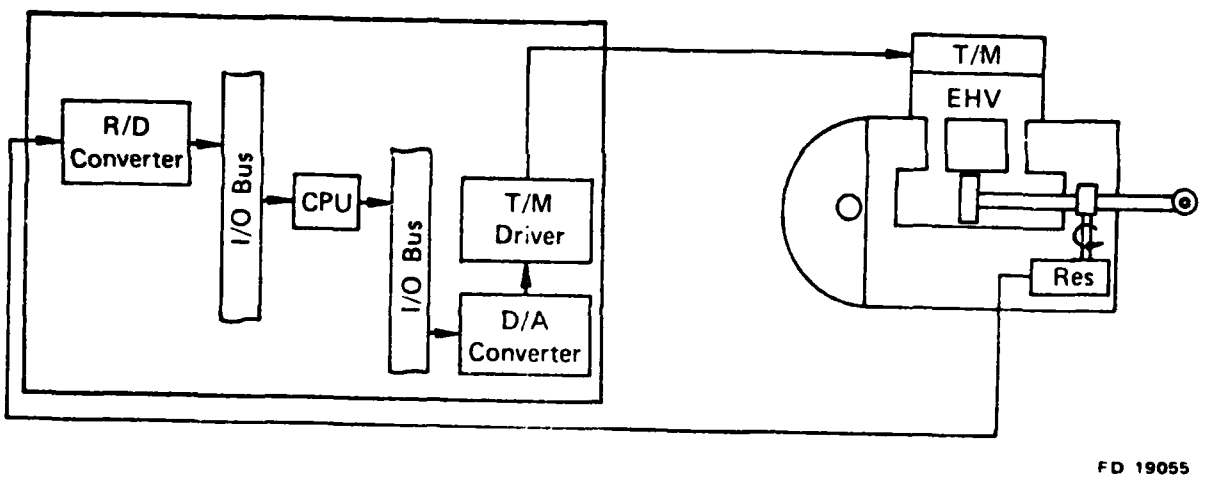


Figure 21. FIGV, A4, A41, AJE and AJD Loop Implementation

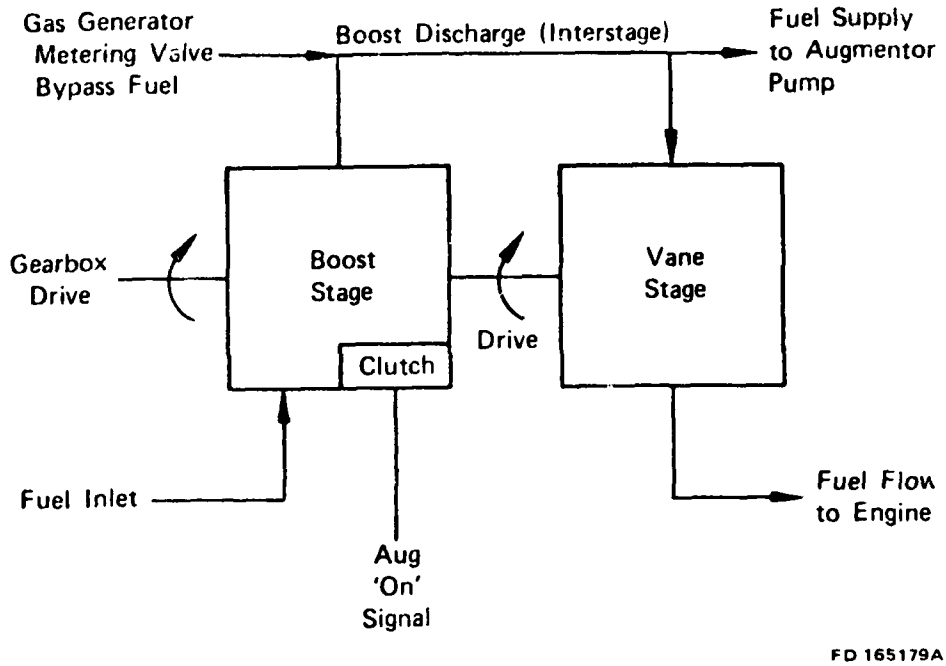


Figure 22. Main Fuel Pump Functional Block Diagram

AUGMENTOR FUEL PUMP

The augmentor fuel pump provides fuel flow to the augmentor control for quickfill and metered flow distribution. This pump is a single-stage centrifugal pump driven by an air impulse turbine. A butterfly valve, located in the air inlet line, controls pump speed by regulating turbine air supply. During nonaugmentation engine operation, the butterfly valve is closed to minimize fuel temperature rise and improve specific fuel consumption. A functional block diagram of the augmentor fuel pump is shown in Figure 23.

HYDRAULIC PUMP

The hydraulic pump is a gearbox mounted variable displacement pump. This pump provides actuation pressure for the variable geometry actuators except for CSVA. The pump contains all of the necessary relief, regulation, and pressure compensating valves as part of the pumping unit.

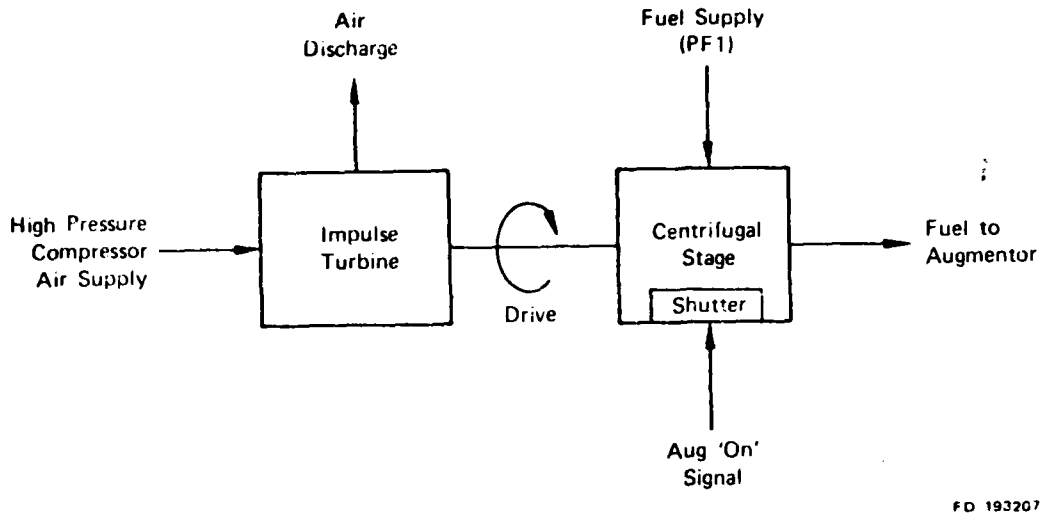


Figure 23. Augmentor Fuel Pump Functional Block Diagram

ALTERNATOR

The alternator stator and rotor are mounted on the engine gearbox bearings and shaft in order to provide a permanent magnet type, engine driven alternator. The alternator provides electrical power to the FAFTEEC and other engine electrical functions. The alternator contains the following windings:

- One nonregulated, three phase winding to furnish power and the N2 signal to FAFTEEC
- One nonregulated, single phase gas generator ignition winding
- One nonregulated, single phase augmentor ignition winding.

IGNITION SYSTEM (EXCITERS AND IGNITERS)

The ignition exciter is a hermetically-sealed unit which contains one gas generator ignition circuit and one augmentor ignition circuit. The dual ignition exciter provides a stored energy level to each spark igniter for main ignition and a lower energy level to the spark igniter for augmentor ignition. Electrical power is supplied to each exciter circuit by electrically independent windings of the engine alternator.

Spark igniters conduct the high energy potential created by the exciter and allow the energy to discharge across an air gap located at the proper position in the combustion chamber. The augmentor and gas generator igniters are functionally the same, but differ in physical dimensions to accommodate mounting differences.

SECTION 4
FAILURE MODES AND EFFECTS ANALYSIS

The FAFTEEC Failure Modes and Effects Analysis (FMEA) is based on the control system required for the ATDE engine. In those candidates which imploy redundancy it is generally necessary that two or more devices fail in order to produce equivalent loss of information or actuation authority. In these systems synthesis techniques are not employed as a substitute for failed sensors. In certain of these systems information is shared across the data link between redundant electronic controls and in the event of a sensor malfunction, cross-talked information may be used in the active engine control. Synthesis techniques are used to arbitrate as to which of two disagreeing sensors is to be selected.

This FMEA catalogs the effect on engine operation due to the loss of sensor information or engine actuation authority. It does not analyze the effect of individual sensor devices or actuator device failures as these may or may not lead to loss of valid sensor information or actuation authority depending upon the redundancy level of the control. Failure effects of individual devices are covered in the sections describing each of the candidate systems. For the baseline system loss of a single string component is equivalent to loss of sensor information or actuation authority.

For modeling purposes, all actuators are considered to have failed either full open or full closed. Intermediate states were considered in the analysis but did not provide any extremes of operation not covered in the failures mentioned above.

In the event of the total loss of electrical signal to the torque motor or loss of hydraulic power, the actuator will slew to the preset failure position, either full open or full closed. For the valve to fail to the non-fail-safe direction requires some type of mechanical linkage failure causing the system to become wedged or contamination sufficient to cause sticking.

Solenoids fail in a manner similar to the actuators. Total loss of electrical power causes the spring loaded valve to return to the predetermined failure position. Again, mechanical failure or contamination could cause a solenoid operated valve to stop at a position other than desired. This case is considered in the model to be the opposite of the desired failure direction, a worst case, and no intermediate positions are considered.

LEVELS OF SYSTEM DEGRADATION

The control systems are capable of operation in several levels of performance ranging from "OK" to "HMBUC." A complete definition of these system states is given in Table 5.

ACTUATOR FAILURE EFFECTS

This section on Actuator Failure Effects was derived from computer simulation data generated as part of the Navy Full Authority Digital Electronic Control (FADEC) program (Ref 1). The data were verified and modified as required for use as part of the FAFTEEC Baseline Control System.

In order to evaluate the hardware required to implement FAFTEEC backup control functions, a study was first performed to determine the minimum backup control logic required for a variable cycle engine including the permissible positioning of all engine variable geometries for safe engine operation in the event of a primary control channel malfunction.

TABLE 5. SYSTEM STATES

OK	No control system failures.
ALERT	Single or double failure resulting in less than 2% loss in intermediate thrust and less than 5% loss in fan or compressor surge margin.
DEGRADED PERFORMANCE (DP)	Single or double failure resulting in 90 to 98% intermediate thrust, or 5 to 10% loss in surge margin with functional augmentor and engine limit protection.
ABORT	Single or double failure resulting in nonfunctional augmentor or 70 to 90% intermediate thrust, or greater than 10% loss in surge margin and functional engine limit protection.
DIGBUC	More than two failures or any number of failures resulting in less than 70% intermediate thrust or possibility of exceeding engine limits and no failures being part of a critical loop, i.e., T2, P3, N2, CSVA, WFGG, or PLA.
HMBUC	Same as DIGBUC except one or more failures is part of a critical loop as defined above, loss of electrical power, or loss of hydraulic power.
IFS	Inflight shutdown.

Actuator control loop design for simplex systems generally results in a particular saturated (end-of-travel) position for the failure case where all command paths are lost. If necessary, the servo system is designed such that the end-of-travel position preferable for performance and/or safe operation considerations is assured by features such as a mechanical spring load. Preferred failure direction for the engine variable geometry actuators was established by simulating failure of each actuator with the ATDE computer simulation to maximum and minimum positions and observing the effects on engine operation. This study indicated that any one actuator saturated to a preferred end-of-stroke position for nonaugmented engine operation can be tolerated with the exception of the high pressure compressor stator vane actuation loop. It was observed that the preferred end-of-stroke failure direction of the actuators at sea level static was indicative of operation at any flight condition. The impact on engine performance at sea level static conditions is shown in Figures 24 through 29, which illustrate changes in net thrust (FN), thrust specific fuel consumption (TSFC), high pressure turbine inlet temperature (T4), fan surge margin (SMFAN), and high pressure compressor surge margin (SMHPC) for each end-of-stroke actuator position where particular performance variations were found to be significant with the other variable geometry control loops operating normally.

Plots of engine performance at sea level static standard day with the high pressure turbine area saturated (Figure 24) indicate that the preferred failure direction should be toward maximum area, because saturation toward minimum area results in insufficient high pressure compressor surge margin.

Examination of engine performance with a saturated low pressure turbine area actuator (Figure 25) indicates that the preferred failure direction is toward maximum area, because failing to the minimum area results in loss of thrust and fan surge margin and also significantly increases turbine inlet temperature relative to normal engine operation.

Engine performance curves with a saturated fan duct exhaust nozzle area actuator (Figure 26) indicate that the preferred direction is toward minimum fan duct nozzle area. Although this direction results in reduced fan surge margin at low power conditions, the engine performance is nearly nominal at higher power settings. Saturating the fan duct actuator to the maximum area results in abnormally high turbine inlet temperature, increased fuel consumption, and a significant thrust loss relative to normal engine operation.

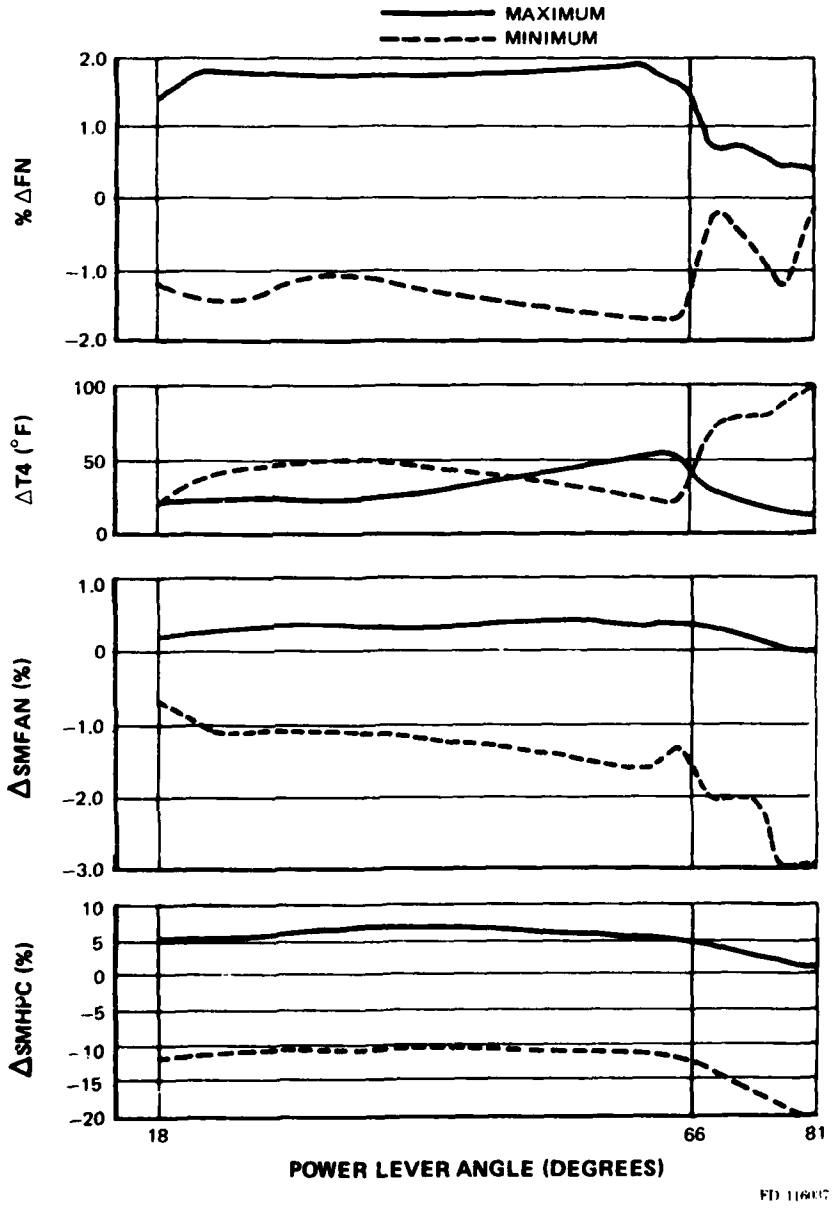


Figure 24. High-Pressure Turbine Area (A4) Failure Effects at Sea Level Static Conditions

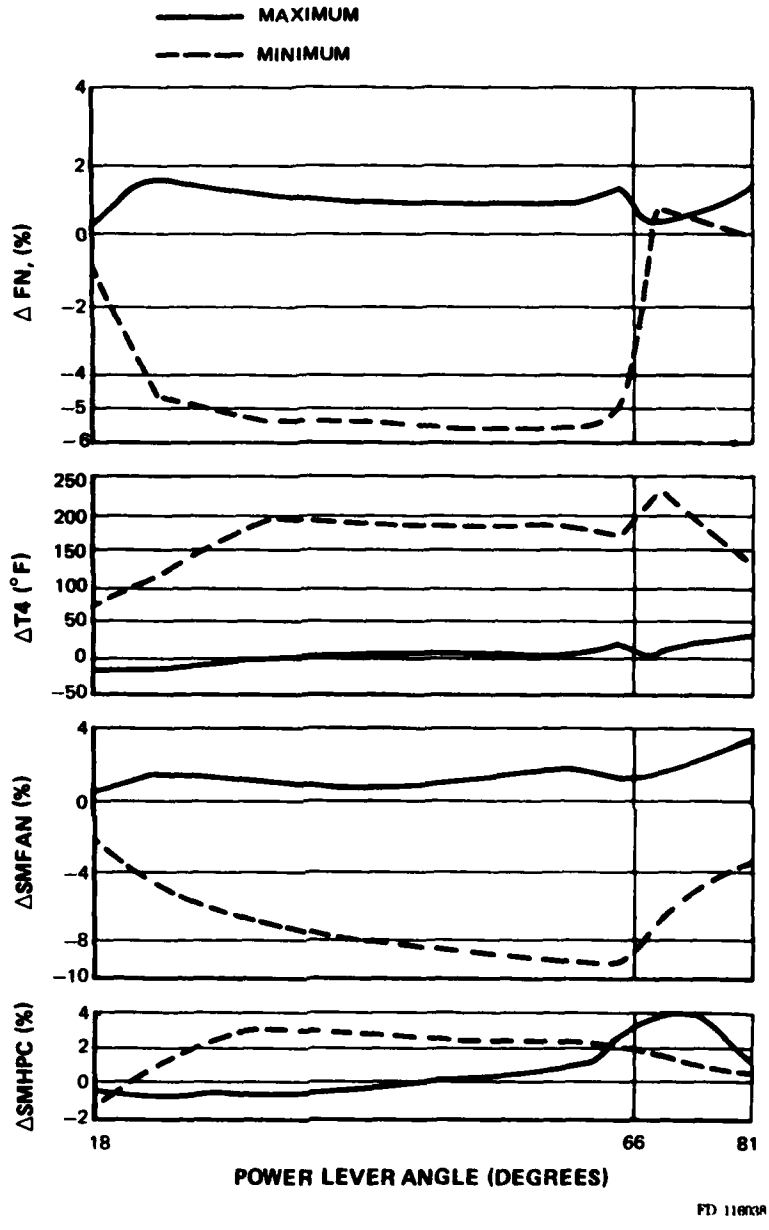


Figure 25. Low-Pressure Turbine Area (A41) Failure Effects at Sea Level Static Conditions

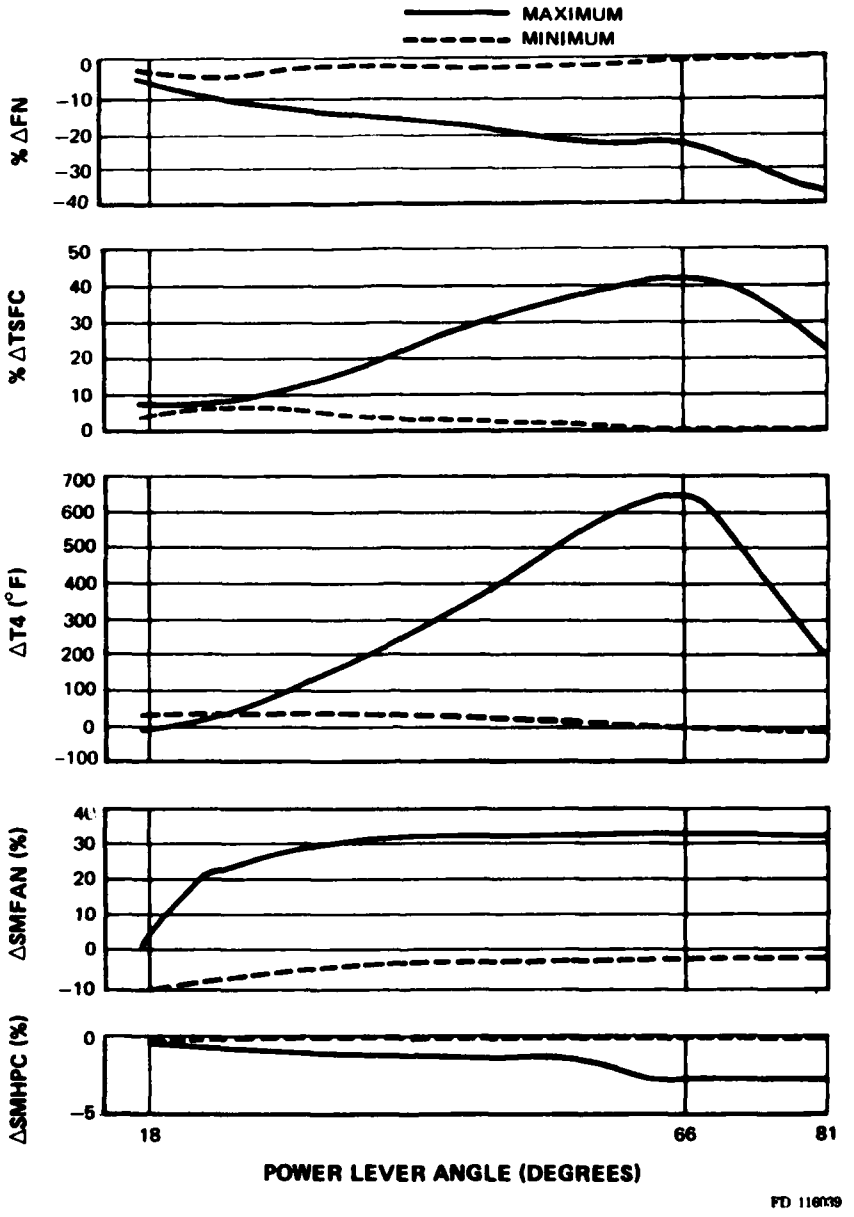


Figure 26. Fan Duct Exhaust Nozzle Area (AJD) Failure Effects at Sea Level Static Conditions

Performance results with the gas generator exhaust nozzle saturated (Figure 27) indicate that the preferred direction is toward maximum area. This would permit normal engine operation up to the CMVT breakpoint power setting while experiencing thrust loss only at higher power settings. Saturating the gas generator exhaust nozzle to the minimum area would result in an undesirable power lever/thrust relationship and higher turbine inlet temperature at lower power lever settings.

Engine performance with a saturated fan inlet guide vane actuator is illustrated in Figure 28. The curves show that the preferred failure direction is the closed position. Although the open position results in greater thrust at higher power settings, it would provide insufficient fan stability margin at reduced power settings.

Curves which show engine performance with the high pressure compressor stator vane actuator saturated (Figure 29) indicate that saturating the vanes in either direction will not provide acceptable operation over the full operating range. Saturating the vanes open results in excessive loss in compressor surge margin at low power settings, while failing them closed produces significantly increased turbine inlet temperature and excessive loss in thrust, fan surge margin, and compressor surge margin relative to normal engine operation at high power settings. With the full closed failure mode for the high pressure compressor stator position the control would protect the engine at high power against loss of surge margin or excessively high turbine temperatures by decelerating the engine more rapidly than the vanes close. This mode, the closed position, was selected because it also provides safe windmilling with the engine shut down in flight.

FAILURE MODES AND EFFECTS ANALYSIS RESULTS

For this FMEA the effects are described in terms of the six separate states: Alert, Degraded Performance, Abort, DIGBUC, HMBUC, and IFS. The System State, shown in the following tables, describes the engine condition resulting from the failures listed. The six System States are as described in Table 6. Tables 7 through 17 describe the FMEA for the FAFTEEC Control Modes.

TABLE 6. SINGLE SENSOR FAILURE

Failed Sensor	*System State*
N1	HMBUC
N2	HMBUC
P13	ABORT
ΔP13 (P13-PS13)	ABORT
P2	DIGBUC
P3	HMBUC
ΔP3 (P3-PS3)	DIGBUC
P5	DIGBUC
T2	HMBUC
T22	DIGBUC
TPS	ABORT
PLA	HMBUC
TBT	HMBUC

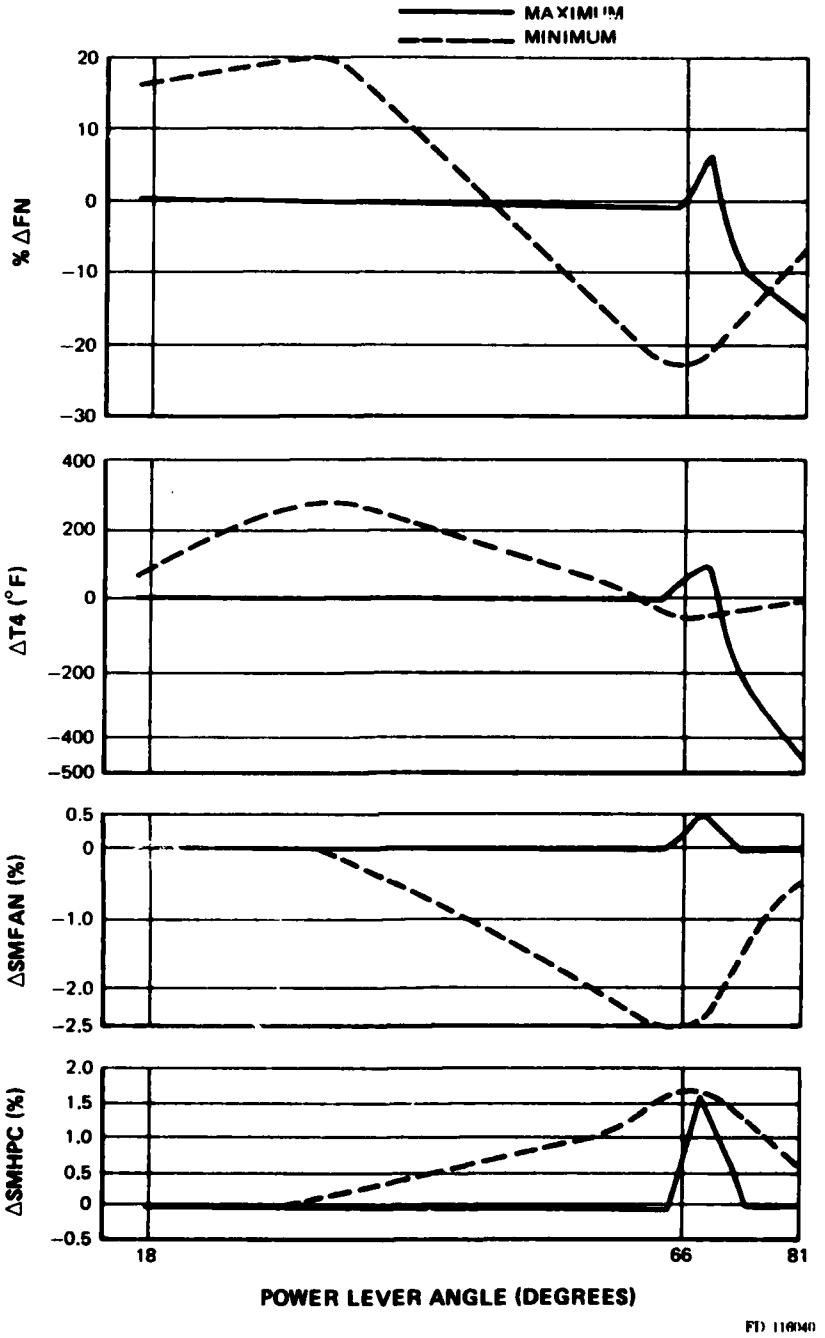


Figure 27. Gas Generator Exhaust Nozzle Area (AJE) Failure Effects at Sea Level Static Conditions

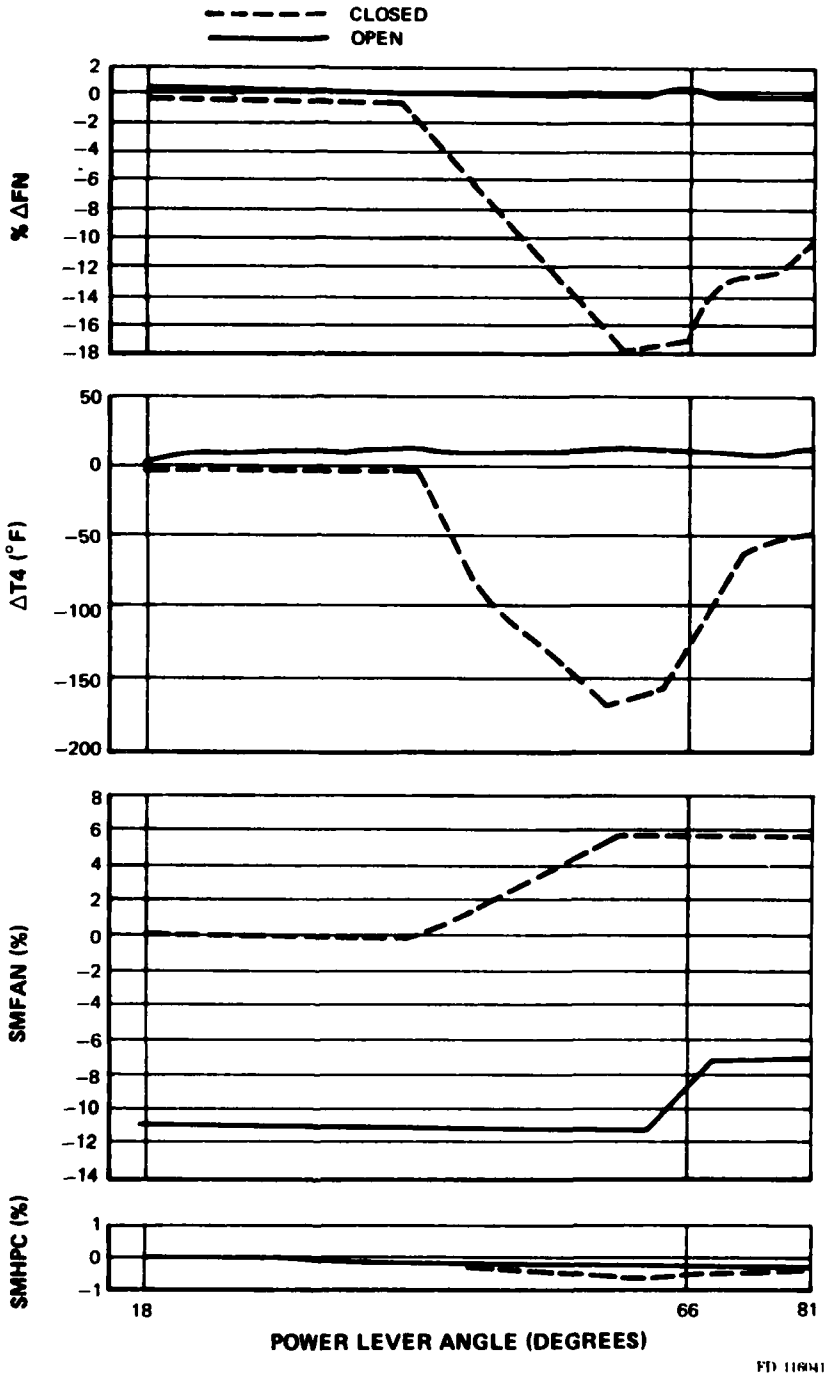


Figure 28. Fan Inlet Guide Vane Angle (FIGV) Failure Effects at Sea Level Static Conditions

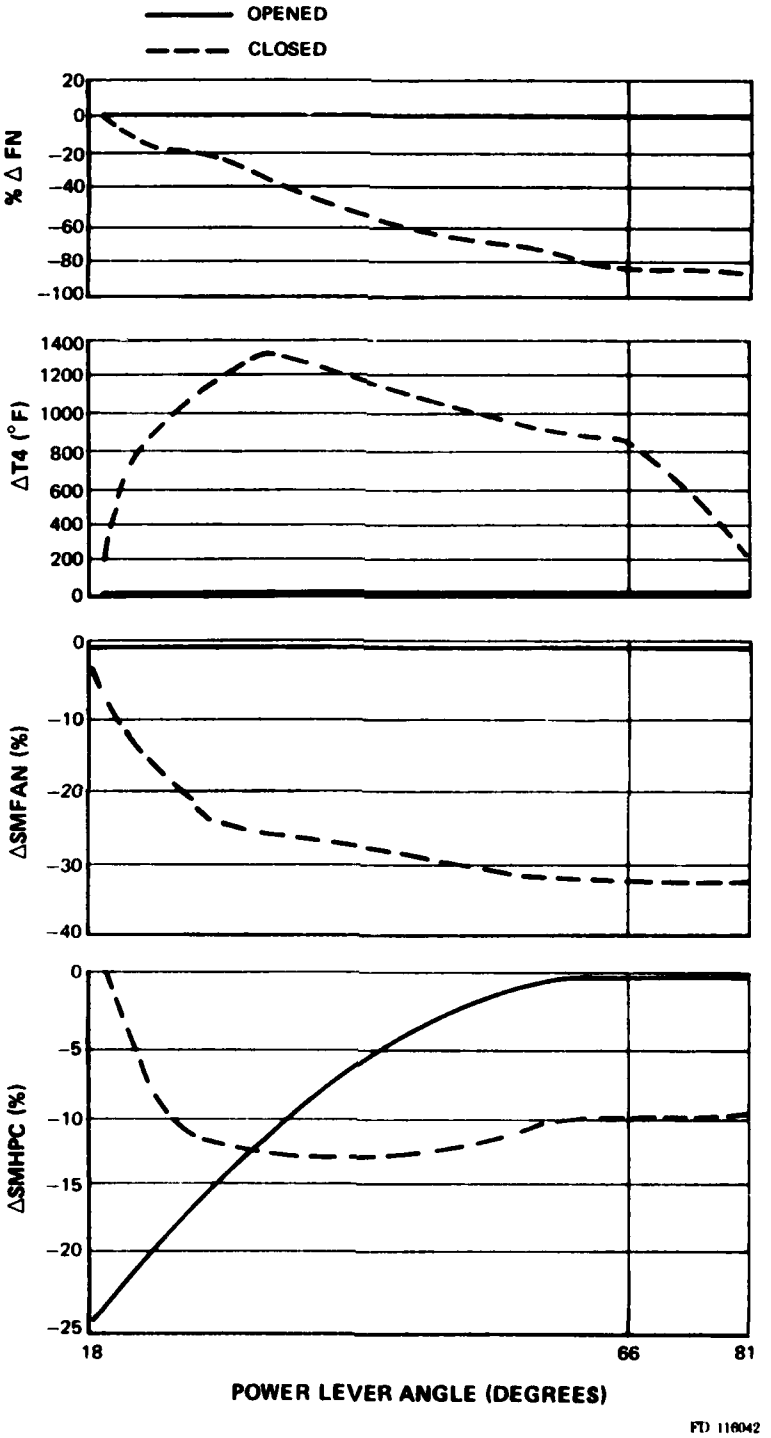


Figure 29. Compressor Stator Vane Angle (CSVA) Failure Effects at Sea Level Static Conditions

TABLE 7. DOUBLE SENSOR FAILURES

Failed Sensors		
S1	S2	System State
N1	N2	HMBUC
N1	P13	HMBUC
N1	ΔP13	HMBUC
N1	P2	HMBUC
N1	P3	HMBUC
N1	ΔP3	HMBUC
N1	P5	HMBUC
N1	T2	HMBUC
N1	T22	HMBUC
N1	TPS	HMBUC
N1	PLA	HMBUC
N2	P13	HMBUC
N2	ΔP13	HMBUC
N2	P2	HMBUC
N2	P3	HMBUC
N2	ΔP3	HMBUC
N2	P5	HMBUC
N2	T2	HMBUC
N2	T22	HMBUC
N2	TPS	HMBUC
N2	PLA	HMBUC
P13	ΔP13	ABORT
P13	P2	DIGBUC
P13	P3	HMBUC
P13	ΔP3	DIGBUC
P13	P5	DIGBUC
P13	T2	HMBUC
P13	T22	DIGBUC
P13	TPS	ABORT
P13	PLA	HMBUC
P2	P3	HMBUC
P2	ΔP3	DIGBUC
P2	P5	DIGBUC
P2	T2	HMBUC
P2	T22	DIGBUC
P2	TPS	DIGBUC
P2	PLA	HMBUC
P3	ΔP3	HMBUC
P3	P5	HMBUC
P3	T2	HMBUC
P3	T22	HMBUC
P3	TPS	HMBUC
P3	PLA	HMBUC
ΔP3	P5	DIGBUC
ΔP3	T2	HMBUC
ΔP3	T22	DIGBUC
ΔP3	TPS	DIGBUC
ΔP3	PLA	HMBUC
P5	T2	HMBUC
P5	T22	DIGBUC
P5	TPS	DIGBUC
P5	PLA	HMBUC
T2	T22	HMBUC
T2	TPS	HMBUC
T2	PLA	HMBUC
T22	TPS	DIGBUC
T22	PLA	HMBUC
TPS	PLA	HMBUC

TABLE 8. SINGLE FEEDBACK FAILURE*

Failed F/B	*System State*
A4	ALERT
A41	ALERT
FIGV	DP
CSVA	HMBUC
AJE	DP
AJD	ABORT
WFGG	HMBUC
WFD	ABORT

*Note: Assumes actuator is driven to preferred direction.

TABLE 9. DOUBLE FEEDBACK FAILURES

Failed F/B's		
F1	*F2*	*System State*
A4	A41	ABORT
A4	FIGV	ABORT
A4	CSVA	HMBUC
A4	AJE	ABORT
A4	AJD	ABORT
A4	WFGG	HMBUC
A4	WFD	ABORT
A41	FIGV	ABORT
A41	CSVA	HMBUC
A41	AJE	ABORT
A41	AJD	ABORT
A41	WFGG	HMBUC
A41	WFD	ABORT
FIGV	CSVA	HMBUC
FIGV	AJE	ABORT
FIGV	AJD	ABORT
FIGV	WFGG	HMBUC
FIGV	WFD	ABORT
CSVA	AJE	HMBUC
CSVA	AJD	HMBUC
CSVA	WFGG	HMBUC
CSVA	WFD	HMBUC
AJE	AJD	ABORT
AJE	WFGG	HMBUC
AJE	WFD	ABORT
AJD	WFGG	HMBUC
AJD	WFD	ABORT
WFGG	WFD	HMBUC

TABLE 10. SINGLE ACTUATOR FAILURE

Failed Actuator	*Open*	*Closed*
A4	ALERT*	ABORT
A41	ALERT*	DP
FIGV	ABORT	DP*
CSVA	HMBUC	HMBUC*
AJE	ABORT	DP*
AJD	DIGBUC	ABORT*
WFGG	HMBUC	HMBUC*
WFD	DIGBUC	ABORT*

Note:(*) Denotes Preferred Direction

TABLE 11. DOUBLE ACTUATOR FAILURES

Failed Actuators					
A1	*A2*	*Open/Open*	*Closed/Closed*	*Open/Closed*	*Closed/Open*
A4	A41	ABORT	ABORT	ABORT	ABORT
A4	FIGV	ABORT	ABORT	ABORT	ABORT
A4	CSVA	HMBUC	HMBUC	HMBUC	HMBUC
A4	AJE	ABORT	ABORT	ABORT	ABORT
A4	AJD	ABORT	ABORT	ABORT	ABORT
A4	WFGG	HMBUC	HMBUC	HMBUC	HMBUC
A4	WFD	DIGBUC	ABORT	ABORT	DIGBUC
A41	FIGV	ABORT	ABORT	ABORT	ABORT
A41	CSVA	HMBUC	HMBUC	HMBUC	HMBUC
A41	AJE	ABORT	ABORT	ABORT	ABORT
A41	AJD	ABORT	ABORT	ABORT	ABORT
A41	WFGG	HMBUC	HMBUC	HMBUC	HMBUC
A41	WFD	DIGBUC	ABORT	ABORT	DIGBUC
FIGV	CSVA	HMBUC	HMBUC	HMBUC	HMBUC
FIGV	AJE	ABORT	ABORT	ABORT	ABORT
FIGV	AJD	ABORT	ABORT	ABORT	ABORT
FIGV	WFGG	HMBUC	HMBUC	HMBUC	HMBUC
FIGV	WFD	DIGBUC	ABORT	ABORT	DIGBUC
CSVA	AJE	HMBUC	HMBUC	HMBUC	HMBUC
CSVA	AJD	HMBUC	HMBUC	HMBUC	HMBUC
CSVA	WFGG	HMBUC	HMBUC	HMBUC	HMBUC
CSVA	WFD	HMBUC	HMBUC	HMBUC	HMBUC
AJE	AJD	ABORT	ABORT	ABORT	ABORT
AJE	WFGG	HMBUC	HMBUC	HMBUC	HMBUC
AJE	WFD	DIGBUC	ABORT	ABORT	DIGBUC
AJD	WFGG	HMBUC	HMBUC	HMBUC	HMBUC
AJD	WFD	DIGBUC	ABORT	DIGBUC	DIGBUC
WFGG	WFD	HMBUC	HMBUC	HMBUC	HMBUC

TABLE 12. FEEDBACK/ACTUATOR FAILURE COMBINATIONS

F/B	*Actuator*	*Open*	*Closed*
A4	A4	ALERT	ABORT
A4	A41	ABORT	ABORT
A4	FIGV	ABORT	ABORT
A4	CSVA	HMBUC	HMBUC
A4	AJE	ABORT	ABORT
A4	AJD	DIGBUC	ABORT
A4	WFGG	HMBUC	HMBUC
A4	WFD	DIGBUC	ABORT
A41	A4	ABORT	ABORT
A41	A41	ALERT	DP
A41	FIGV	ABORT	ABORT
A41	CSVA	HMBUC	HMBUC
A41	AJE	ABORT	ABORT
A41	AJD	DIGBUC	ABORT
A41	WFGG	HMBUC	HMBUC
A41	WFD	DIGBUC	ABORT
FIGV	A4	ABORT	ABORT
FIGV	A41	ABORT	ABORT
FIGV	FIGV	ABORT	DP
FIGV	CSVA	HMBUC	HMBUC
FIGV	AJE	ABORT	ABORT
FIGV	AJD	DIGBUC	ABORT
FIGV	WFGG	HMBUC	HMBUC
FIGV	WFD	DIGBUC	ABORT
CSVA	A4	HMBUC	HMBUC
CSVA	A41	HMBUC	HMBUC
CSVA	FIGV	HMBUC	HMBUC
CSVA	CSVA	HMBUC	HMBUC
CSVA	AJE	HMBUC	HMBUC
CSVA	AJD	HMBUC	HMBUC
CSVA	WFGG	HMBUC	HMBUC
CSVA	WFD	HMBUC	HMBUC
AJE	A4	ABORT	ABORT
AJE	A41	ABORT	ABORT
AJE	FIGV	ABORT	ABORT
AJE	CSVA	HMBUC	HMBUC
AJE	AJE	ABORT	DP
AJE	AJD	DIGBUC	ABORT
AJE	WFGG	HMBUC	HMBUC
AJE	WFD	DIGBUC	ABORT
AJD	A4	ABORT	ABORT
AJD	A41	ABORT	ABORT
AJD	FIGV	ABORT	ABORT
AJD	CSVA	HMBUC	HMBUC
AJD	AJE	ABORT	ABORT
AJD	AJD	DIGBUC	ABORT
AJD	WFGG	HMBUC	HMBUC
AJD	WFD	DIGBUC	ABORT
WFGG	A4	HMBUC	HMBUC
WFGG	A41	HMBUC	HMBUC
WFGG	FIGV	HMBUC	HMBUC
WFGG	CSVA	HMBUC	HMBUC
WFGG	AJE	HMBUC	HMBUC
WFGG	AJD	HMBUC	HMBUC
WFGG	WFGG	HMBUC	HMBUC
WFGG	WFD	DIGBUC	HMBUC
WFD	A4	ABORT	ABORT
WFD	A41	ABORT	ABORT
WFD	FIGV	ABORT	ABORT
WFD	CSVA	HMBUC	HMBUC
WFD	AJE	ABORT	ABORT
WFD	AJD	DIGBUC	ABORT
WFD	WFGG	HMBUC	HMBUC
WFD	WFD	DIGBUC	ABORT

TABLE 13. FEEDBACK/SENSOR FAILURE COMBINATIONS

F/B	Sensor	System State
A4	N1	HMBUC
A4	N2	HMBUC
A4	P13	ABORT
A4	ΔP13	ABORT
A4	P2	DIGBUC
A4	P3	HMBUC
A4	ΔP3	DIGBUC
A4	P5	DIGBUC
A4	T2	HMBUC
A4	T22	DIGBUC
A4	TPS	ABORT
A4	PLA	HMBUC
A41	N1	HMBUC
A41	N2	HMBUC
A41	P13	ABORT
A41	ΔP13	ABORT
A41	P2	DIGBUC
A41	P3	HMBUC
A41	ΔP3	DIGBUC
A41	P5	DIGBUC
A41	T2	HMBUC
A41	T22	DIGBUC
A41	TPS	ABORT
A41	PLA	HMBUC
FIGV	N1	HMBUC
FIGV	N2	HMBUC
FIGV	P13	ABORT
FIGV	ΔP13	ABORT
FIGV	P2	DIGBUC
FIGV	P3	HMBUC
FIGV	ΔP3	DIGBUC
FIGV	P5	DIGBUC
FIGV	T2	HMBUC
FIGV	T22	DIGBUC
FIGV	TPS	ABORT
CSVA	PLA	HMBUC
CSVA	N1	HMBUC
CSVA	N2	HMBUC
CSVA	P13	HMBUC
CSVA	ΔP13	HMBUC
CSVA	P2	HMBUC
CSVA	P3	HMBUC
CSVA	ΔP3	HMBUC
CSVA	P5	HMBUC
CSVA	T2	HMBUC
CSVA	T22	HMBUC
CSVA	TPS	HMBUC
CSVA	PLA	HMBUC
AJE	N1	HMBUC
AJE	N2	HMBUC
AJE	P13	ABORT
AJE	ΔP13	ABORT
AJE	P2	DIGBUC
AJE	P3	HMBUC
AJE	ΔP3	DIGBUC
AJE	P5	DIGBUC
AJE	T2	HMBUC
AJE	T22	DIGBUC
AJE	TPS	ABORT
AJE	PLA	HMBUC

(Continued)

AJD	N1	HMBUC
AJD	N2	HMBUC
AJD	P13	ABORT
AJD	ΔP13	ABORT
AJD	P2	DIGBUC
AJD	P3	HMBUC
AJD	ΔP3	DIGBUC
AJD	P5	DIGBUC
AJD	T2	HMBUC
AJD	T22	DIGBUC
AJD	TPS	ABORT
AJD	PLA	HMBUC
WFGG	N1	HMBUC
WFGG	N2	HMBUC
WFGG	P13	HMBUC
WFGG	ΔP13	HMBUC
WFGG	P2	HMBUC
WFGG	P3	HMBUC
WFGG	ΔP13	HMBUC
WFGG	P5	HMBUC
WFGG	T2	HMBUC
WFGG	T22	HMBUC
WFGG	TPS	HMBUC
WFGG	PLA	HMBUC
WFD	N1	HMBUC
WFD	N2	HMBUC
WFD	P13	ABORT
WFD	ΔP13	ABORT
WFD	P2	DIGBUC
WFD	P3	HMBUC
WFD	ΔP3	DIGBUC
WFD	P5	DIGBUC
WFD	T2	HMBUC
WFD	T22	DIGBUC
WFD	TPS	ABORT
WFD	PLA	HMBUC

TABLE 14. SENSOR/ACTUATOR FAILURE COMBINATIONS

Sensor	*Actuator*	*Open*	*Closed*
N1	A4	HMBUC	HMBUC
N1	A41	HMBUC	HMBUC
N1	FIGV	HMBUC	HMBUC
N1	CSVA	HMBUC	HMBUC
N1	AJE	HMBUC	HMBUC
N1	AJD	HMBUC	HMBUC
N1	WFGG	HMBUC	HMBUC
N1	WFD	HMBUC	HMBUC
N2	A4	HMBUC	HMBUC
N2	A41	HMBUC	HMBUC
N2	FIGV	HMBUC	HMBUC
N2	CSVA	HMBUC	HMBUC
N2	AJE	HMBUC	HMBUC
N2	AJD	HMBUC	HMBUC
N2	WFGG	HMBUC	HMBUC
N2	WFD	HMBUC	HMBUC
P13	A4	ABORT	ABORT
P13	A41	ABORT	ABORT
P13	FIGV	ABORT	ABORT
P13	CSVA	HMBUC	HMBUC
P13	AJE	ABORT	ABORT
P13	AJD	DIGBUC	ABORT
P13	WFGG	HMBUC	HMBUC
P13	WFD	DIGBUC	ABORT
ΔP13	A4	ABORT	ABORT
ΔP13	A41	ABORT	ABORT
ΔP13	FIGV	ABORT	ABORT
ΔP13	CSVA	HMBUC	HMBUC
ΔP13	AJE	ABORT	ABORT
ΔP13	AJD	DIGBUC	ABORT
ΔP13	WFGG	HMBUC	HMBUC
ΔP13	WFD	DIGBUC	ABORT
P2	A4	DIGBUC	DIGBUC
P2	A41	DIGBUC	DIGBUC
P2	FIGV	DIGBUC	DIGBUC
P2	CSVA	HMBUC	HMBUC
P2	AJE	DIGBUC	DIGBUC
P2	AJD	DIGBUC	DIGBUC
P2	WFGG	HMBUC	HMBUC
P2	WFD	DIGBUC	DIGBUC
P3	A4	HMBUC	HMBUC
P3	A41	HMBUC	HMBUC
P3	FIGV	HMBUC	HMBUC
P3	CSVA	HMBUC	HMBUC
P3	AJE	HMBUC	HMBUC
P3	AJD	HMBUC	HMBUC
P3	WFGG	HMBUC	HMBUC
P3	WFD	HMBUC	HMBUC
ΔP3	A4	DIGBUC	DIGBUC
ΔP3	A41	DIGBUC	DIGBUC
ΔP3	FIGV	DIGBUC	DIGBUC
ΔP3	CSVA	HMBUC	HMBUC
ΔP3	AJE	DIGBUC	DIGBUC
ΔP3	AJD	DIGBUC	DIGBUC
ΔP3	WFGG	HMBUC	HMBUC
ΔP3	WFD	DIGBUC	DIGBUC
P5	A4	DIGBUC	DIGBUC
P5	A41	DIGBUC	DIGBUC
P5	FIGV	DIGBUC	DIGBUC
P5	CSVA	HMBUC	HMBUC

TABLE 15. SENSOR/ACTUATOR FAILURE COMBINATIONS

Sensor	*Actuator*	*Open*	*Closed*
P5	AJE	DIGBUC	DIGBUC
P5	AJD	DIGBUC	DIGBUC
P5	WFGG	HMBUC	HMBUC
P5	WFD	DIGBUC	DIGBUC
T2	A4	HMBUC	HMBUC
T2	A41	HMBUC	HMBUC
T2	FIGV	HMBUC	HMBUC
T2	CSVA	HMBUC	HMBUC
T2	AJE	HMBUC	HMBUC
T2	AJD	HMBUC	HMBUC
T2	WFGG	HMBUC	HMBUC
T2	WFD	HMBUC	HMBUC
T22	A4	DIGBUC	DIGBUC
T22	A41	DIGBUC	DIGBUC
T22	FIGV	DIGBUC	DIGBUC
T22	CSVA	HMBUC	HMBUC
T22	AJE	DIGBUC	DIGBUC
T22	AJD	DIGBUC	DIGBUC
T22	WFGG	HMBUC	HMBUC
T22	WFD	DIGBUC	DIGBUC
TPS	A4	ABORT	ABORT
TPS	A41	ABORT	ABORT
TPS	FIGV	ABORT	ABORT
TPS	CSVA	HMBUC	HMBUC
TPS	AJE	ABORT	ABORT
TPS	AJD	DIGBUC	ABORT
TPS	WFGG	HMBUC	HMBUC
TPS	WFD	DIGBUC	ABORT
PLA	A4	HMBUC	HMBUC
PLA	A41	HMBUC	HMBUC
PLA	FIGV	HMBUC	HMBUC
PLA	CSVA	HMBUC	HMBUC
PLA	AJE	HMBUC	HMBUC
PLA	AJD	HMBUC	HMBUC
PLA	WFGG	HMBUC	HMBUC
PLA	WFD	HMBUC	HMBUC

TABLE 16. OTHER FUEL SYSTEM COMPONENTS

Function	*Failure*	*System State*
Augmentor Fuel Flow	Failure Either Direction Close Shutoff Valves	ABORT
Gas Generator Fuel Flow	Engine Shutdown	IFS
Hydraulic Pressure	Engine Shutdown	IFS
W_F Shutoff	Will Not Start	IFS
W_{FD} Shutoff	Stuck Closed, No Augmentor	ABORT
Aug Ignition	No Augmentor (Duct Aug Will Not Autolite)	ABORT
BUC Selector	BUC Performance Will Result	HMBUC
FAFTEEC	Requires BUC Operation	HMBUC
GG Ignition	No Restart Capability	ALERT
Alternator Power	No Electrical Power	HMBUC

TABLE 17. FAFTEEC COMPUTER

Component	*Failure Effect*	*System State*
Power Supply	FAFTEEC Computer Shutdown	HMBUC
CPU	FAFTEEC Computer Fails	HMBUC 99% Active 1%
MEMORY	FAFTEEC Computer Fails	HMBUC 85% Active 15%
BUS	FAFTEEC Computer Fails	HMBUC
Watchdog Timer	FAFTEEC Computer Fails	HMBUC (If ACTIVE all subsequent CPU, MEMORY or BUS, or Clock Failures are Active.

SECTION 5

FAFTEEC REDUNDANCY CONFIGURATIONS

SYSTEM 1 — BASELINE SINGLE STRING

The FAFTEEC Baseline Control System, Section 3, and the Failure Modes and Effects Analysis, Section 4, provide the basis upon which the redundant FAFTEEC control configurations are built. The candidate FAFTEEC systems are summarized in Table 18 and described below. It should be noted that all of the FAFTEEC control systems use a dual ignition system to be consistent with the design practice on military engines. For reference the Baseline, single string, FAFTEEC control system, as described in Section 3, is included as Figure 30.

SYSTEM 2 — DUAL CONTROL (GAS GENERATOR FUNCTIONS)

The dual FAFTEEC control system is selectively redundant such that no single failure causes reversion to the hydromechanical backup control. The selectively replicated sensors are listed as "FAFTEEC Dedicated Inputs" on Figure 31. The electronic controls are replicated (dual). The actuators are all driven by dual wound torque motors with dual feedback resolvers. Each half of the dual control drives one coil of each torque motor and uses one feedback resolver. The torque motor and the hydromechanical components of the servo valves and actuators are all simplex except for the gas generator metering valve, and the compressor stator vane actuator. A single failure of either of these functions would cause reversion to the backup control and thus they employ dual torque motors and dual hydromechanical components.

The gas generator fuel pumps in this system serve dual purposes; they provide gas generator fuel flow and also a source of hydraulic pressure to the fuel metering valve, the compressor stator vane actuator, and backup control. A single hydraulic pump provides servopressure to all of the other noncritical gas generator and augmentor functions.

The hydromechanical backup control implementation is identical to that of the baseline system Figure 19. As with the baseline the hydromechanical backup, control for this system will be fuel powered, in this case, by fuel pressure from the dual gas generator pumps.

The alternator is made up of separate windings, on a common shaft, each powering one half of the FAFTEEC electronic control. Separate windings on the same shaft are dedicated to the ignition system. This alternator configuration is common to all of the dual or dual duplex FAFTEEC systems.

SYSTEM 3 — FULLY DUAL CONTROL SYSTEM

The fully dual FAFTEEC control system is a totally dual system (Figure 32). All of the component parts of the system; sensors, computers, actuators and fuel pumps, hydraulic pumps, and ignition are dual.

Each half of the fully dual FAFTEEC electronic control monitors engine operating conditions through its own complete set of sensors. The electronic controls have the capability to trade sensor information over a data link coupling the units.

TABLE 18. REDUNDANCY CONFIGURATIONS

System	Sensor Sets	Computers	Actuators				Pumps			
			T/M	SV	ACT	RES	Fuel GG/Aug	Hyd	Ignition	
1. Baseline	1	1	1	1	1	1	1/1	1	2	
2. Dual Gas Generator	1/2[1]	2	2	1/2[1]	1	2	2/1	1	2	[1]1/2 Indicates single with dual in areas that cause reversion to HMBUC
3. Fully Dual	2	2	2	2	1	2	2/2	2	2	
4. Advanced Dual	2	2	2	2	2	2	2[4]	2	2	
4A. Dual Noncross Strapped	2	2[2]	2	2	2	2	2[4]	2	2	[2]Not cross-strapped
5. Dual with Triplex Computers	2	3[3]	2	2	2	2	2[4]	2	2	[3]Dual plus voter
6. Dual with Dual-Dual Computers	2	4	2	2	2	2	2[4]	2	2	[4]Gas generator and augmentor
6A. Dual with Dual-Dual Microcomputers	2	12	2	2	2	2	2[4]	2	2	
7. Enhanced Dual System	2	3 or 4	2	2	2	2	2	2	2	

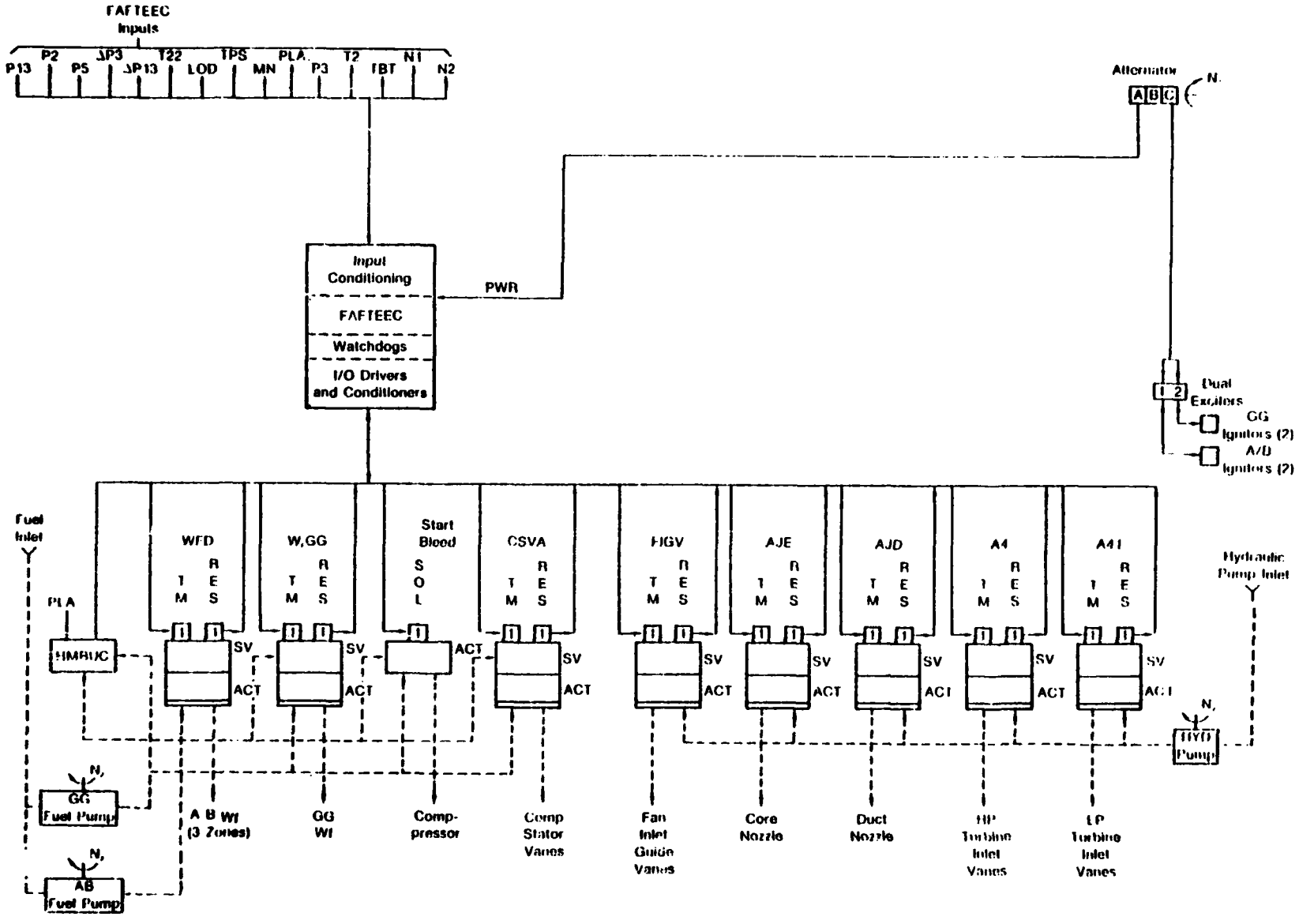


Figure 30. FAFTEEC System 1 Baseline Single String

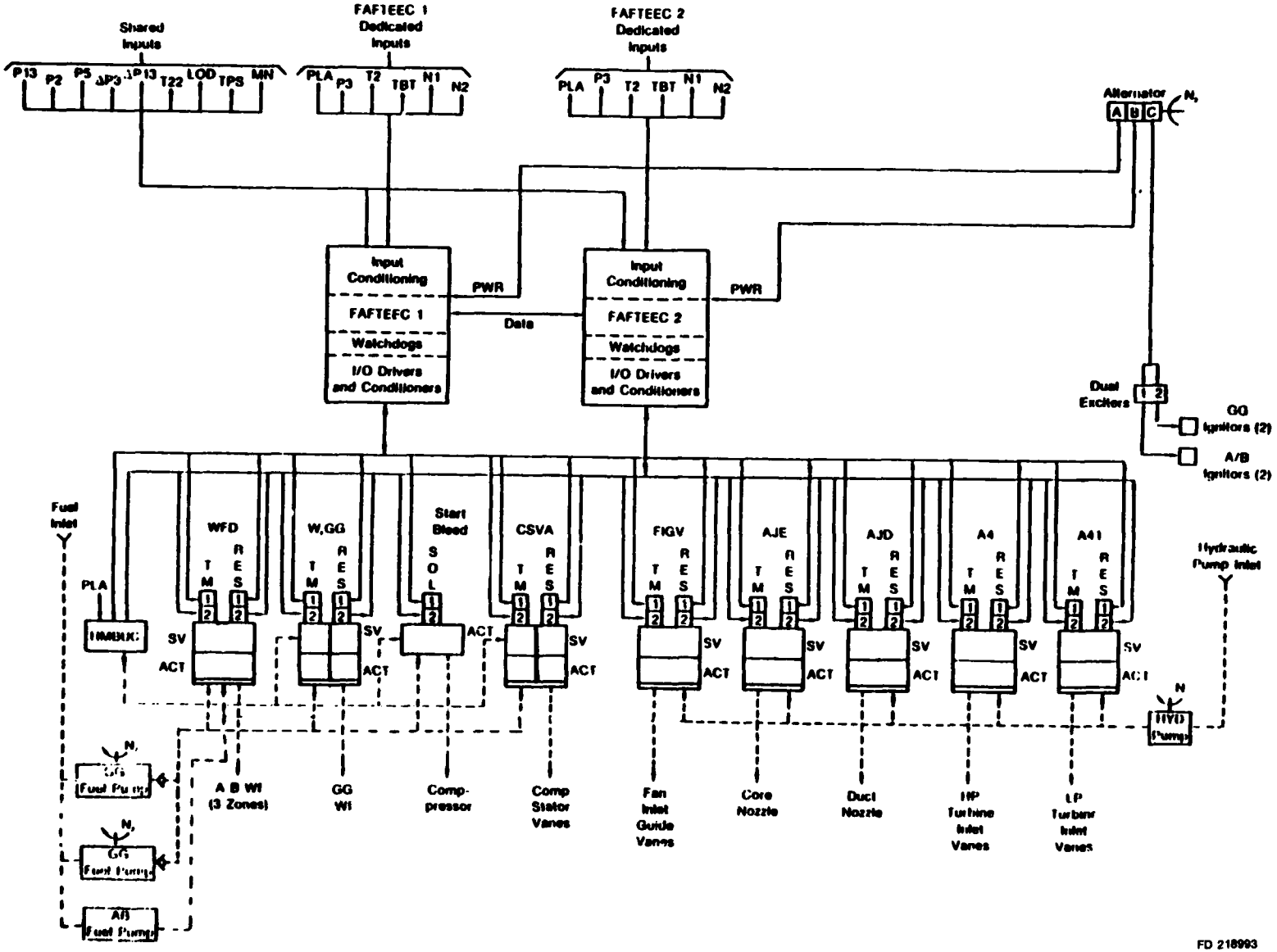


Figure 31. FAFTEEC Dual Gas Generator Functions System 2

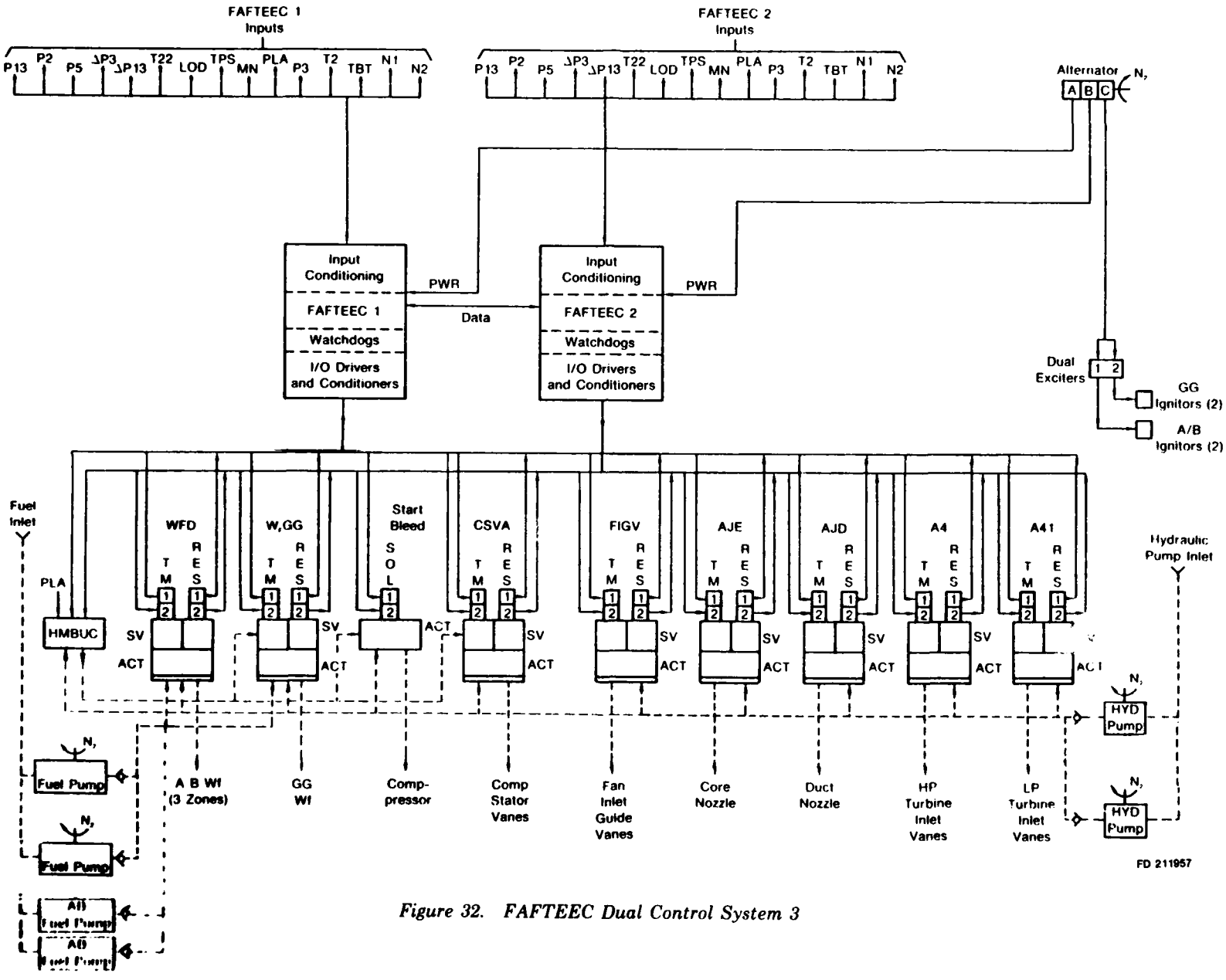


Figure 32. FAFTEEC Dual Control System 3

The actuators are dual piston actuators, positioned by dual servovalves and powered by dual wound torque motors. Each winding of the torque motors is driven by one of the FAFTEEC electronic controls. Separate feedback resolvers provide separate servo loop closure in each channel. This control system employs the same type of actuator design, dual piston, on all actuators as used in System 2 for the gas generator metering valve, and compressor stator vain actuator.

All of the pumps in this FAFTEEC system are dual and dedicated to a particular function. There are separate gas generator, augmentor and hydraulic pumping systems. The fuel pumps are based on current engine operating systems and use vane pumps for gas generator fuel flow and centrifugal pump for the augmentor. These pumps are sized such that the loss of one pump in either or both fuel supply systems does not impact engine operation. The dual hydraulic piston pumps are used to power all of the engine actuators and the hydromechanical backup control in this and all of the redundant FAFTEEC systems. In the event of a failure, either remaining pump is capable of supplying sufficient pressure for engine actuator operation.

SYSTEM 4 — ADVANCED DUAL CONTROL SYSTEM

System 4 is a dual system as described in Section 5; however, it employs advanced technology components to achieve reliability rather than doubling everything as was done in System 3. This concept was used to improve the fuel pumping system and actuators as compared to System 3. All other components in the two systems, sensors, electronic controls, hydraulic pumps, alternator and ignition remain unchanged from the previous system.

A system diagram is shown in Figure 33 which indicates the differences in the system architectures. As can be seen the total number of fuel pumps required has been reduced from four to two. This may be accomplished by using centrifugal pumping for supplying fuel flow to the engine only and using hydraulic pump pressure for all actuation and servosupply. The fuel pumps are configured in a dual fashion as shown by Figure 34 and supply fuel to both the augmentor or gas generator. Studies have shown the dual centrifugal pumps can be sized which will provide an acceptable fuel temperature rise and still provide the reserve capacity to allow operation of the main engine over the full flight envelope and operation of the augmentor over 75% of the full-flightenvelope with a single pump failure.

The engine actuators have also been changed to incorporate technology more in line with a redundant system architecture. This has been accomplished by using a tandem piston actuator approach. The tandem piston is then interfaced with the hydraulics and electronics through a direct drive type servovalve which utilizes dual coils as shown in Figure 35. These actuation and pumping systems are the basis of the remaining FAFTEEC control systems. These other systems, 4A through 7, differ from System 4 only in the electronic control portion of the systems.

SYSTEM 4A — DUAL CONTROL SYSTEM NONCROSS STRAPPED

System 4A is designed to establish the impact on the FAFTEEC systems of extensive cross-channel data link traffic between electronic controls. The system chosen for this comparison is the FAFTEEC System 4. Figures 33 and 36 show that Systems 4 and 4A are similar except for the data link between the controls. Electronic implementation of the system is described in Section 10.

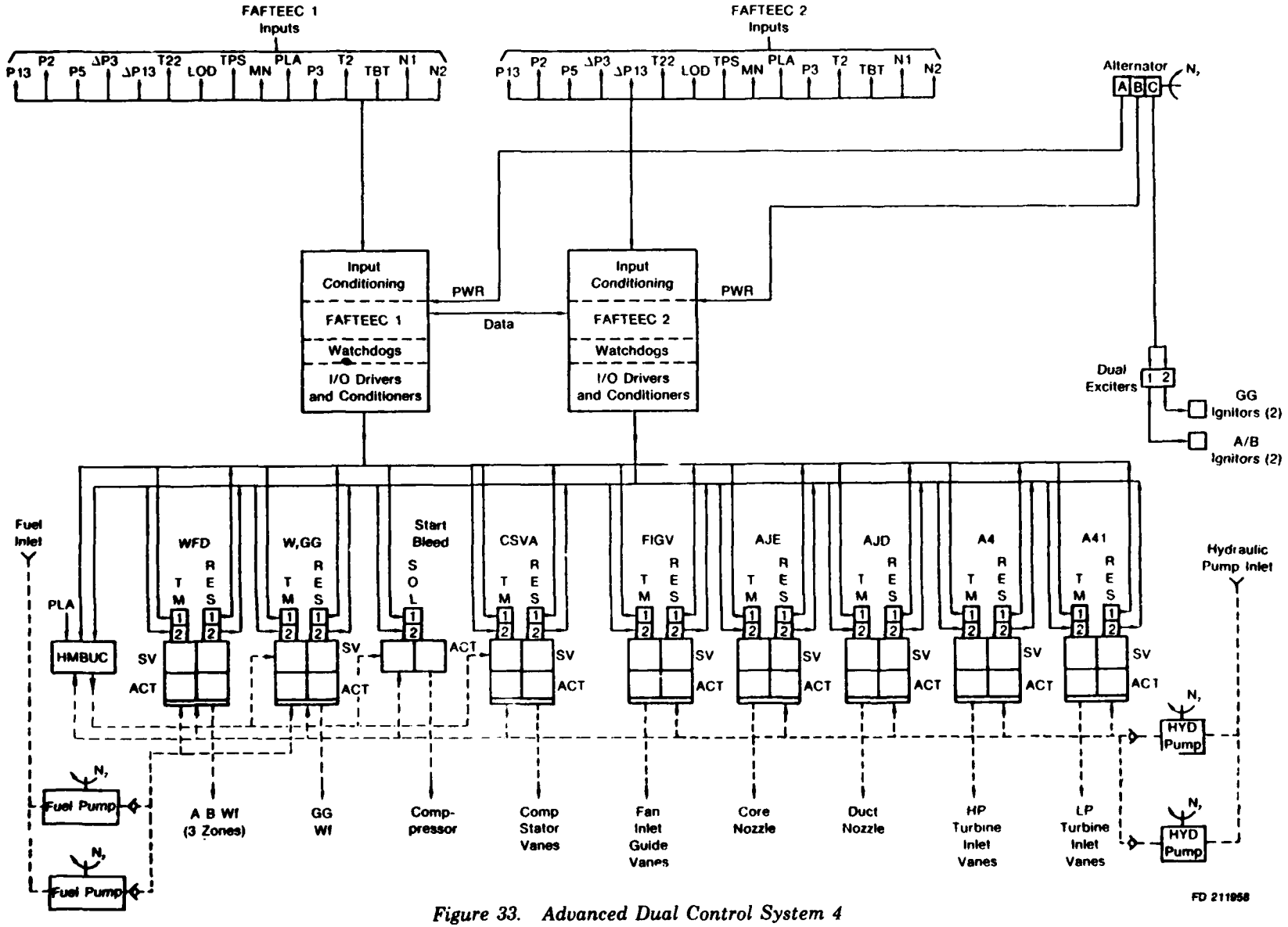


Figure 33. Advanced Dual Control System 4

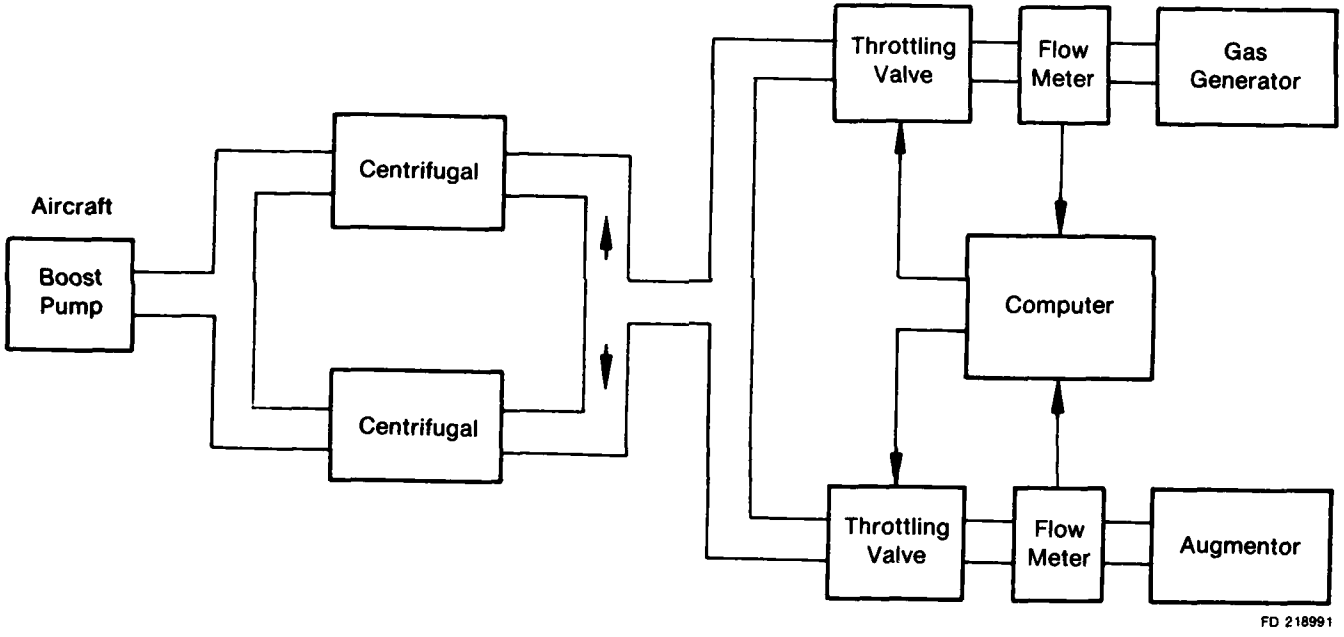


Figure 34. FAFTEEC Dual Centrifugal Pumps

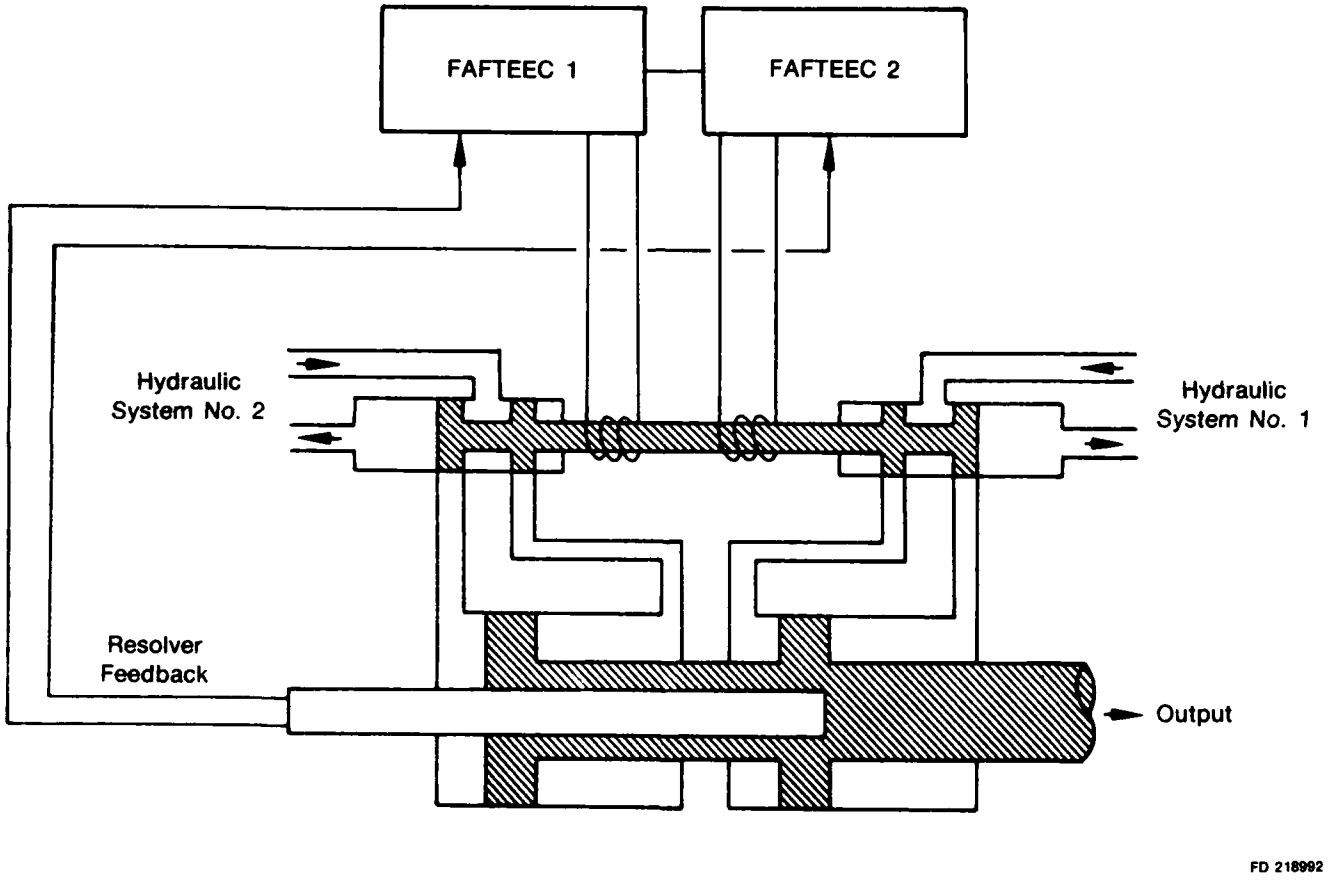


Figure 35. FAFTEEC Dual Control (Dual Actuators)

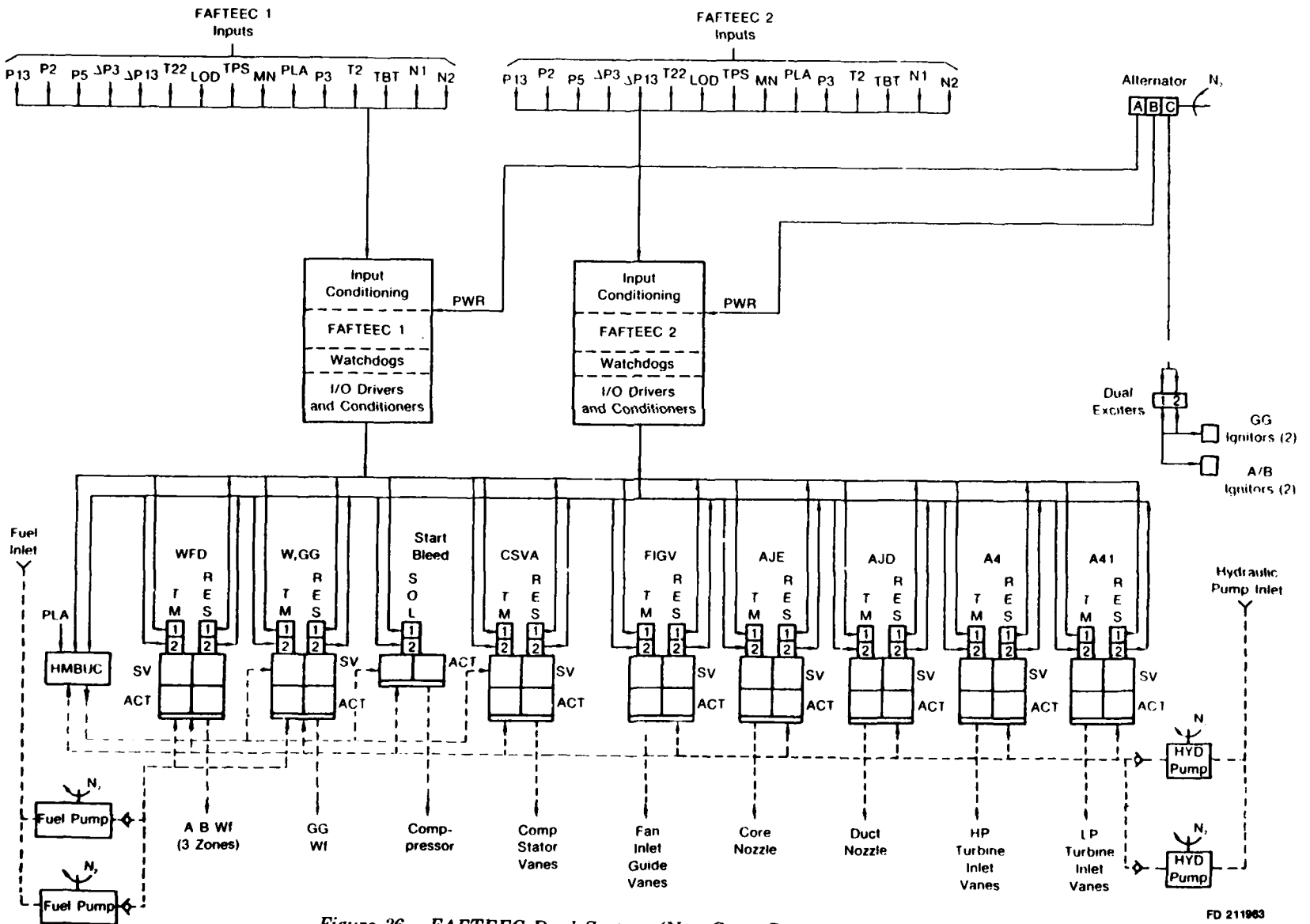


Figure 36. FAFTEEC Dual System (Non Cross-Strapped) System 4A

SYSTEM 5 — DUAL CONTROL SYSTEM WITH TRIPLEX COMPUTERS

System 5 employs the hardware shown in Figure 37, that is, the dual sensor, actuator, and pumping components of System 4, coupled with three electronic controls. The third computer in this system acts as an independent computational element and is used with voter hardware to disconnect channel 1 or 2, should they fail. The third computer was added to improve the computer coverage to 100% through a hardware voting scheme. Channel 3 does not have a sensor set or output drivers but instead checks the inputs and calculation results from both of the other. It relies upon cross-linked data to function. In the event of a disagreement the system is fail operational and the disagreeing channel is disengaged. First failure computer coverage is therefore 100%.

SYSTEM 6 — DUAL SYSTEM WITH DUAL-DUAL COMPUTERS

FAFTEEC System 6, Figure 38, uses the inputs, outputs, pumping system, alternator and ignition system described for System 4, Section 5. The electronic control implementation is with Dual-Dual computers. In this system the two major channels contain a pair computers which operate on a single set of input data. Dual output commands from each pair of processors is compared in a hardware voter in each major channel. Failure of the output commands to compare properly generates a signal which disables the entire major channel and transfers control to the other major channel. Essentially, each major channel of the computer is structured to be 100% fail-passive. First failure computer coverage is therefore 100%.

SYSTEM 6A — DUAL CONTROL SYSTEM WITH DUAL/DUAL MICROCOMPUTERS

The organization of System 6A, Figure 39, is the same as that employed in System 6 except that the single processor pairs are replaced with three single-chip microcomputer pairs per channel. Each pair handles the computations for one of the following three functions: gas generator control, engine geometry control, and exhaust nozzle control.

Such a configuration was studied because of speculation that it provides a means of employing single chip microcomputer technology, with a potential cost and packaging advantage over faster but more complex multichip mono-processor designs. A seventh processor is included in each major channel to interface with external units and provide common fault storage capability. This processor will collect data from the control CPU's for transmittal over the MIL-STD-1553B data bus.

ENHANCED DUAL SYSTEMS

All of the systems discussed to this point fail to achieve desired FAFTEEC goals due to inadequate fault coverages. Both systems 5 and 6 address the coverage issue by enhancing the dual architecture of System 4 to achieve 100 percent first fault coverage for computer faults. Selective enhancements will be required in either of these systems to raise sensor coverage to nearer 100%. To an extent, refined analytic technique employing sensor synthesis or simply better self-test hardware and software will achieve some of the required enhancements of sensor coverage. It will also probably be necessary to provide for some selective replication of sensor inputs where this proves the most cost effective means of coverage.

System 7 is an enhanced version of System 5 or 6. Reliability projection for this system were then made assuming perfect coverage of all sensor faults. It is expected that perfect coverage of sensor faults could be achieved by reasonableness checks, synthesis or sensor inputs, and selected sensor replication where synthesis if found to be difficult to achieve.

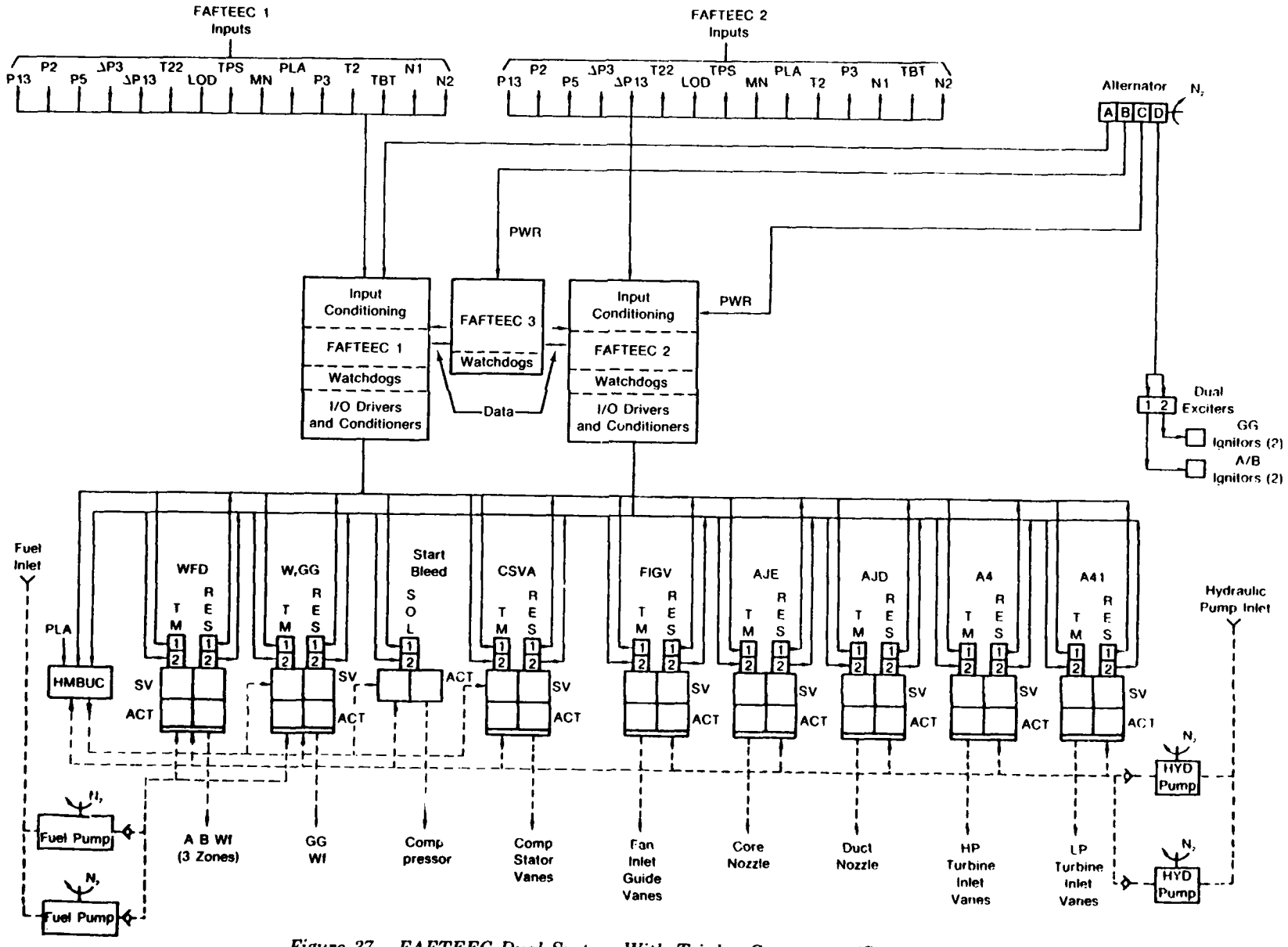


Figure 37. FAFTEEC Dual System With Triplex Computers (Systems 5)

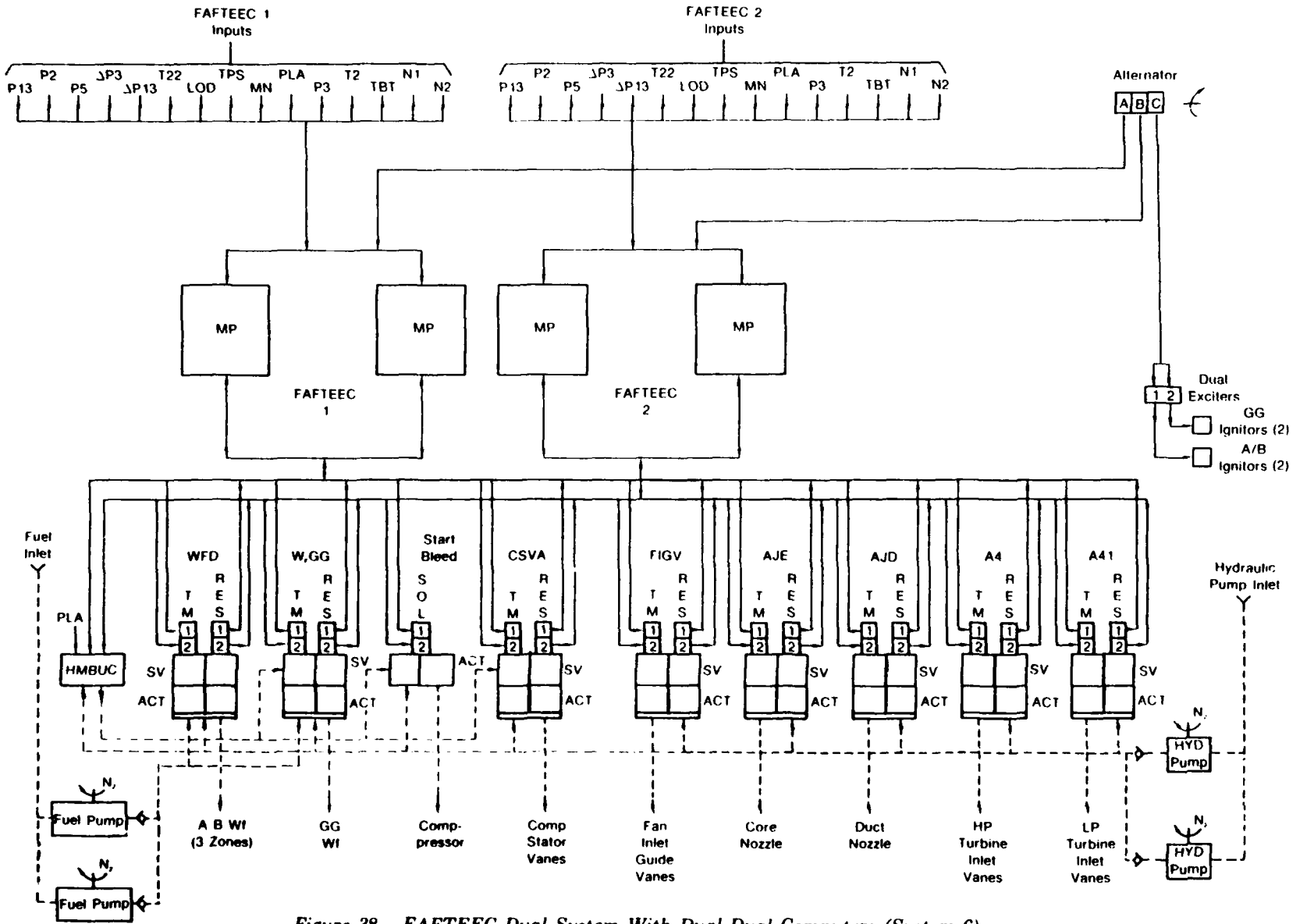


Figure 38. FAFTEEC Dual System With Dual-Dual Computers (System 6)

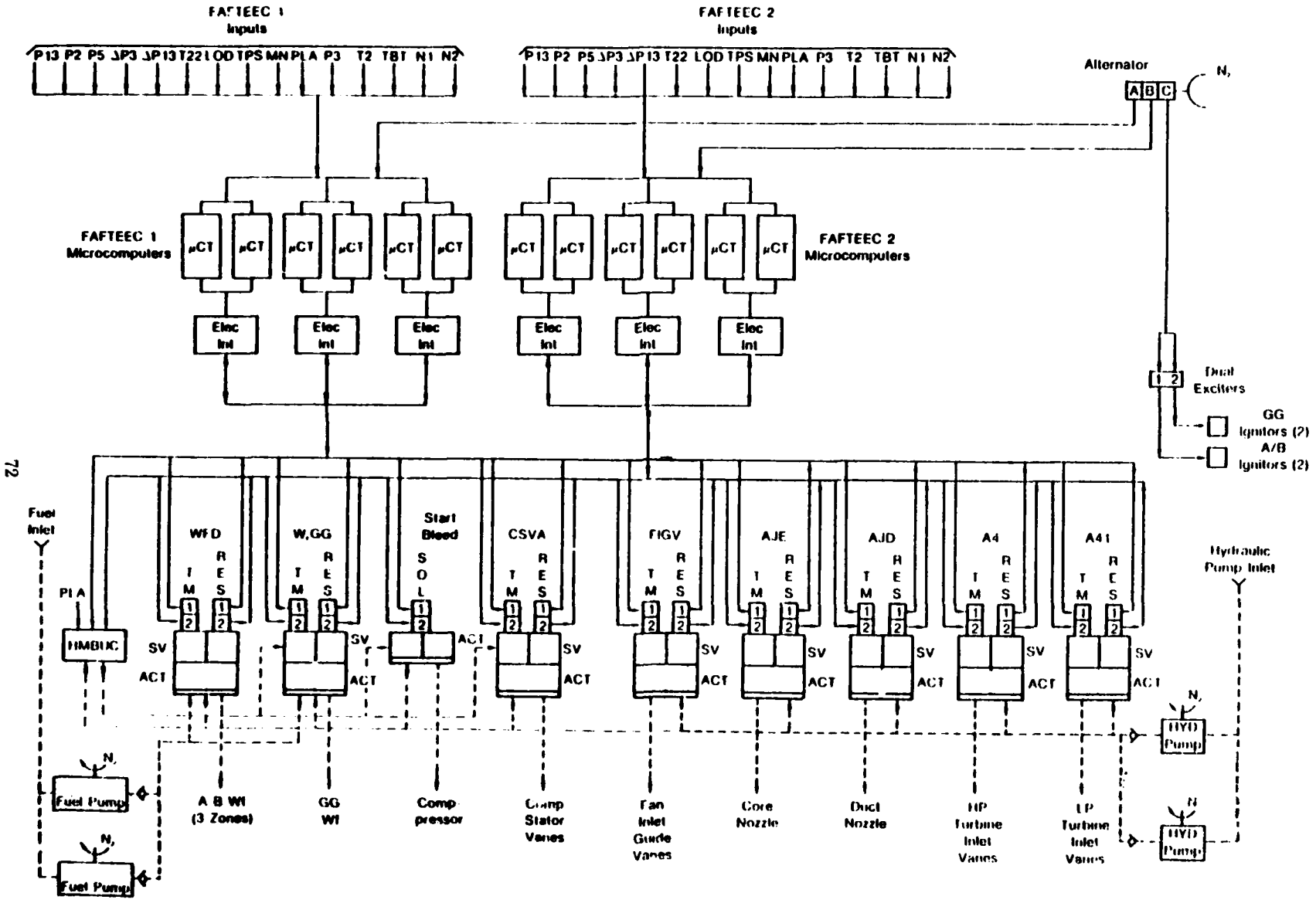


Figure 39. FAFTEEC Dual With Dual-Dual Microcomputers (System 6A)

SECTION 6

COMPONENT FAILURE RATE PREDICTIONS

FAILURE RATE PROJECTIONS

Failure rate projections were derived from Pratt & Whitney Aircraft engine field experience, when this data was available. If actual engine operating data was not available then Pratt & Whitney Aircraft supplier's field experience was used. When values for mature hardware were not available, Duane growth slope plots were used to project reliability value to 1 million hours of operation.

Two reliability projections were made for each component; one for failures which could cause mission abort or worse and one for defect related failures which are not serious enough to impact engine performance during a mission but which would require maintenance action. Reliability modeling using the first projectioin and life cycle cost calculation used the second.

FAILURE RATE PROJECTIONS FOR RELIABILITY MODELING

This material is presented to describe the process used to project failure rate data for use in the Markov Reliability Model. The major sources of information for these data are F100 engine field experience and Hamilton Standard reliability analysis of the electronic control portion of the system. (The HSD data is also based on field experience.) Other sources were used where required to determine the reliability of a particular component or subcomponent.

The F100 engine control system data component reflects field experience on overall failure rates for parts from 500,000 operating hours of life. The FAFTEEC components differ in complexity from the F100 parts and therefore are adjusted to reflect these differences. To convert these overall failure rates to values usable for FAFTEEC, two factors were applied.

The first of these was the ratio of failures causing aborts ion the field to overall field failure rates. This ratio is not available for all parts so a factor was developed for a general class of parts, e.g., 38.5 percent of actuator failures cause abort and 50 percent of cable failures cause abort Table 19 shows the analysis used to develop the value used for the compressor stator vane actuator (CSVA). This actuator is divided into an actuation and feedback section for use in the Markov model.

The adjusted failure rate (Table 19, column 4) is the product of the failure rate and the abort rate factor. It can be noted that some components have a factor of 1.0. This indicates that any failure would cause a loss of function and thus an abort situation would exist. The subcomponent failure rates may now be added to determine a component failure rate which leads to an abort. For example the CSVA actuator sum is 18.0 and the feedback 17.3 for a component at 500,000 hr.

A second adjustment was then made to project component reliability at maturity. The reliability growth slope curves from field experience were evaluated to determine the percentage of improvement to be expected at maturity. This improvement factor was then applied to the abort failure rate. For the CSVA this value is about 0.9 and the overall failure rate is reduced accordingly. These final values for the CSVA (16 for the actuator and 16 for the feedback) represent a projected mature failure rate of the component. Table 20 illustrates this second adjustment.

TABLE 19. CSVA FAILURE RATE CALCULATION

Component	*Failure Rate*	*Abort Factor*	*Failure Rate-Aborts*
Actuation			
T/M Servovalve	20.0/vendor	0.385	7.7
Actuating Valve	6.9/vendor	0.385	2.7
T/M Interface	3.29/HSD	1.0	3.3
Cables	8.5/F100	0.50	4.3
			18.0
Feedback			
Resolver	13.0/F100	0.385	5.0
R/D Conversion and Excitation	8.8/HSD	1.0	8.8
Cables	7.0/F100	0.50	3.5
			17.3

TABLE 20. CSVA FAILURE RATE CALCULATION FOR ABORT FACTOR ADJUSTMENT

Actuation	18.0
x maturity factor	0.94
Adjusted Failure Rate	16.9
Feedback	17.3
x maturity factor	0.94
Adjusted Failure Rate	16.3

Work sheets for WFGG and T2 are included as Table 21 and 22 to show sample calculations at various levels of component complexity. Table 23 depicts tabulation of all of the FAFTEEC values for use in the Markov model.

TABLE 21. WGFF FAILURE RATE CALCULATION

Component	*Failure Rate*	*Abort Factor*	*Failure Rate-Aborts*
Actuation			
T/M and Servovalve	20.0/vendor	0.419	8.4
Metering Valve	3.4/vendor	0.419	1.4
P Regulator	1.3/vendor	0.419	0.5
Solenoid	5.0/F100	0.419	2.1
Shut Off Valve	1.1/vendor	0.419	0.5
Fuel Lines	0.76/F100	0.0	0.0
T/M Interface	3.29/HSD	1.0	3.3
T/M Cables	8.5/F100	0.5	4.3
Solenoid Driver	0.9/HSD	1.0	0.9
Solenoid Cables	7.0/F100	0.5	3.5
			24.9
			x.94*
			23.4**
Feedback			
Resolver	13.0/F100	0.419	5.4
R/D Conversion and Excitation	8.8/HSD	1.0	8.8
Cables	7.0/F100	0.5	3.5
			17.7
			x.94*
			16.8**

*Growth Slope Factor
**Abort Failure Rate for Mature Component

TABLE 22. T2 FAILURE RATE CALCULATION

Component	*Failure Rate*	*Abort Factor*	*Failure Rate-Aborts*
Pt. Resistance Probe	27.0/F100	0.50	6.8
Cables and Connectors	7.0/F100	0.50	3.5
A/D Conversion	9.7/HSD	1.0	9.7
			20.0
			x.9*
			18.0**

*Growth Slope Factor
**Abort Failure Rate for Mature Component

TABLE 23. FAFTEEC COMPONENT FAILURE RATE

Component	Failure Rate 500K hr	Failure Rate Aborts 500K hr	Failure Rate Aborts With Growth 1 Meg hr	Projected Mature Failure Rate 1 Meg hr
N2	25	10	9	22
T2	44	20	18	39
P3	19	12	11	17
WFGG	51	25	23	48
WFGG F/B	29	18	17	27
PLA	29	18	17	27
CSVA	39	18	17	36
CSVA F/B	29	17	16	27
HMBUC TRANS VLV	25	11	11	23
P2	19	12	11	17
P5	19	12	11	17
P13	19	12	11	17
P3	19	12	11	17
P13	19	12	11	17
N1	51	13	12	46
T22	44	15	13	39
TBT	67	39	35	60
LOD	46	28	25	41
MN	10	6	6	9
WFD	128	62	58	121
WFD F/B	69	36	34	65
FIGV	37	17	16	35
FIGV F/B	22	10	17	21
AJE	41	19	18	35
AJE	22	10	17	21
AJD	41	19	18	35
AJD F/B	22	10	17	21
A4	37	17	16	35
A4 F/B	22	10	17	21
A41	37	17	16	35
A41 F/B	22	10	17	21
Start Bleed	20	10	10	19
GG Pump	142	31	27	122
Aug Pump	142	31	27	122
Hyd Pump	100	21	17	80
GG Ign	79	13	12	74
Aug Ign	82	16	14	69
Computer	65	41	39	62
Alternator	78	8	8	73
	1811	718	700	1633

SECTION 7

SYSTEM RELIABILITY MODELING AND RESULTS

SYSTEM RELIABILITY MODELING

This section describes the reliability modeling results for the various FAFTEEC control system architectures. The Markov modeling methodology used to obtain the results and the detailed mathematical models for each system are described in Appendix A. Three parameters are used to measure the reliability of a FAFTEEC control system. The three parameters are as follows:

Probability of transfer to HMBUC: This measures the likelihood that the electronic control system will transfer engine control to the Hydromechanical Backup Controller. This transfer may take place due to one or more failures in the primary control system components such as sensors, actuators, or the computational core such that the electronic controller is incapable of safe engine control. This probability is dependent on the mission length. Therefore, it is computed and plotted as a function of time for a wide time range.

Probability of mission abort: This measures the likelihood that the engine performance as measured by thrust would not be sufficient to complete the mission. This may happen due to one or more failures in the sensors, actuators, pumps or the computational core of the electronic controller. This parameter is also a function of mission time and is plotted for a wide range of time.

Mean time between failures: This is a measure of the overall MTBF. The MTBF, therefore, is highest for the simplex system and smallest for a system with maximum redundancy. It is not necessarily correlated with the probabilities of mission abort or transfer to backup.

The fault tolerance of each candidate FAFTEEC system as measured by the above criteria is described in the following sections. It is compared to the desired and the minimum goals set for the FAFTEEC program. The desired probability of transfer to HMBUC is 2.5×10^{-7} per hr and the desired mission abort probability is 2.5×10^{-6} per hr. The maximum goals are an order of magnitude worse than the desired goals. That is, the maximum transfer to HMBUC goal is 2.5×10^{-6} per hr and the maximum mission abort goals is 2.5×10^{-5} per hr. The general interpretation of these probability goals is that they are cumulative probabilities rather than rates. For example, the desired likelihood of not completing a 3-hr mission should not exceed 7.5×10^{-6}, or the desired likelihood of transferring to HUMBUC during a 10-hr mission should be 2.5×10^{-6} or less. The FAFTEEC mission length is expected to be 3 hr for 90 per cent of the missions and 10 hr for the remaining missions. Most reliability results in the succeeding sections are therefore quoted for these time lengths.

BASELINE SYSTEM (SYSTEM 1)

System Description

The baseline FAFTEEC architecture is a single string system. All the components are simplex without any redundancy. Various components of the baseline control system included in the reliability model are as follows.

There is a single computer which includes the central processing unit (CPU), the read-only and read/write memories (ROM and RAM), the clocking circuitry, the input-output interfaces and a watchdog timer. The inputs to the computer come from a number of sensors. The sensors are organized into two groups as follows.

HMBUC Critical Sensors: These sensors are required for the electronic controller to continue to operate safely. If a sensor from this group fails the electronic controller transfers engine control to the hydromechanical backup controller (HMBUC). These sensors are N1, N2, P3, T2, TBT and PLA.

Mission Abort Critical Sensors: These sensors are required to maintain engine thrust above the mission abort level. A failure of any sensor from this group would result in engine performance below that required to complete the mission. These sensors are P13, P13, P2, P3, P5, T22 and TPS.

The variable cycle engine actuators controlled by the digital controller are as follows:

FIGV:	Fan Inlet Guide Vane
CSVA:	Compressor Stator Vane Angle
WFGG:	Gas Generator Fuel Flow
ADE:	Core Exhaust Nozzle Area
A4:	High Pressure Turbine Inlet Area
A41:	Low Pressure Turbine Inlet Area
WFD:	Augmentor Fuel Flow
AJD:	Augmentor Exhaust Nozzle Area

The effect of an actuator failure on the engine performance depends upon the final position of the failed actuator. This may vary from a maintenance alert to transfer to HMBUC. For the reliability modeling purposes two failure positions of each actuator (open and closed) are taken into account. The actuators are biased to fail in a preferred direction so as to minimize the impact of the failure on the engine performance.

Associated with each actuator is a feedback sensor that relays the actuator position to the computer. A loss of a feedback sensor implies that the corresponding actuator is driven in the preferred failure direction into its mechanical stop. The effect of a single feedback sensor failure is, therefore, the same as if the corresponding actuator had failed in the preferred direction.

The hydromechanical parts and other miscellaneous components of the control system modeled here include a hydraulic pump, an alternator, a core or gas generator fuel pump, an augmentor fuel pump, gas generator ignitor, augmentor ignitor, BUC fuel selector valve and a light-off-detector (LOD). The hydraulic pump powers all the actuators except WFGG and CSVA which are powered by the fuel pump.

Baseline (System 1) Results

The baseline control system is segmented into seven subsystems for the modeling purposes. Each subsystem is mathematically represented by a Markov model. This partitioning has been done to minimize the total number of states as well as to keep the overall modeling process tractable. The set of components to be included in each model has been chosen so that there is a minimum of interaction between these sets. The complete reliability model for the baseline system is detailed in Appendix A.

Figures 40 and 41 show the probability of mission abort or worse and the probability of transfer to HMBUC or worse, respectively, as a function of time for the baseline control system. The probability of transfer to HMBUC or worse implies that the probability of certain events which are worse than transfer to HMBUC in terms of engine performance are also included. Examples of such events are inflight engine shutdown (e.g., ignitor failure followed by engine flame-out) and engine damage (due to active computer failure). Similarly, probability of mission abort or worse includes the probability of events worse than mission abort such as transfer to HMBUC, IFS, etc. The program goals for probability of transfer to HMBUC and mission abort are also shown in figures 40 and 41.

It is seen from these figures that the reliability of the baseline control system misses the desired goal by approximately three orders of magnitude at the nominal mission time of 3 hr. For example, the likelihood of transfer to HMBUC is 8.2×10^{-4} compared to the desired goal of 7.5×10^{-7} at 3 hr. Similarly, the likelihood of aborting a mission is 1.5×10^{-3} compared to the desired goal of 7.5×10^{-6} at 3 hr.

Since all components in the baseline control system are simplex they all directly contribute to one or more of the system failure modes. Additionally, there is no single component or failure mode which is the dominant contributor toward HMBUC or mission abort. A failure of any HMBUC critical sensor or actuator (WFGG and CSVA), the core fuel pump or the computer would result in a transfer to HMBUC. The relative contribution of each of these components to the likelihood of this transfer is proportional to their respective failure rates. Similarly, a failure of any mission abort critical sensor or actuator (A4, A41, AJE, AJD, FIGV and WFD), hydraulic pump or the augmentor fuel pump would result in mission abort.

The modeling results indicate that there are virtually no components except the final stages of the actuators which are adequately reliable in simplex or single string application. Therefore, redundancy will be required to some degree in all elements of the system. A sensitivity analysis of the baseline system was performed to determine if there were any one factor contributing to the poor reliability performance (compared to the desired reliability goals). Figures 42 to 45 show the baseline system reliability if a single component or a group of components are assumed to have increased reliability. As can be seen, increasing the reliability of only one aspect of the system is inadequate to reach the overall FAFTEEC goal. For example, even if the computer is assumed to have infinite reliability, a baseline failure probability (transfer to HMBUC) of 10^{-3} at 3 hr is all that is obtained. Figure 46 is an indication of the degree to which the reliability of all components would need to be improved in order to meet system design goals with the baseline structure. This would require uniform improvements in component life times by a factor of between 1000 and 10,000. Such an approach is impractical. The only alternative is to use redundancy judiciously in the amount necessary for each component. The following sections describe various approaches to controlling the FAFTEEC control system redundantly and their impact on the reliability.

DUAL REDUNDANT SYSTEMS

Several control system architectures were analyzed that fall into the general dual redundant category. The number and type of components that are redundant in each system is different. In addition, there are architectural differences in the area of the computational core between various dual systems. The following subsections briefly describe the architecture of each dual system and their reliability results.

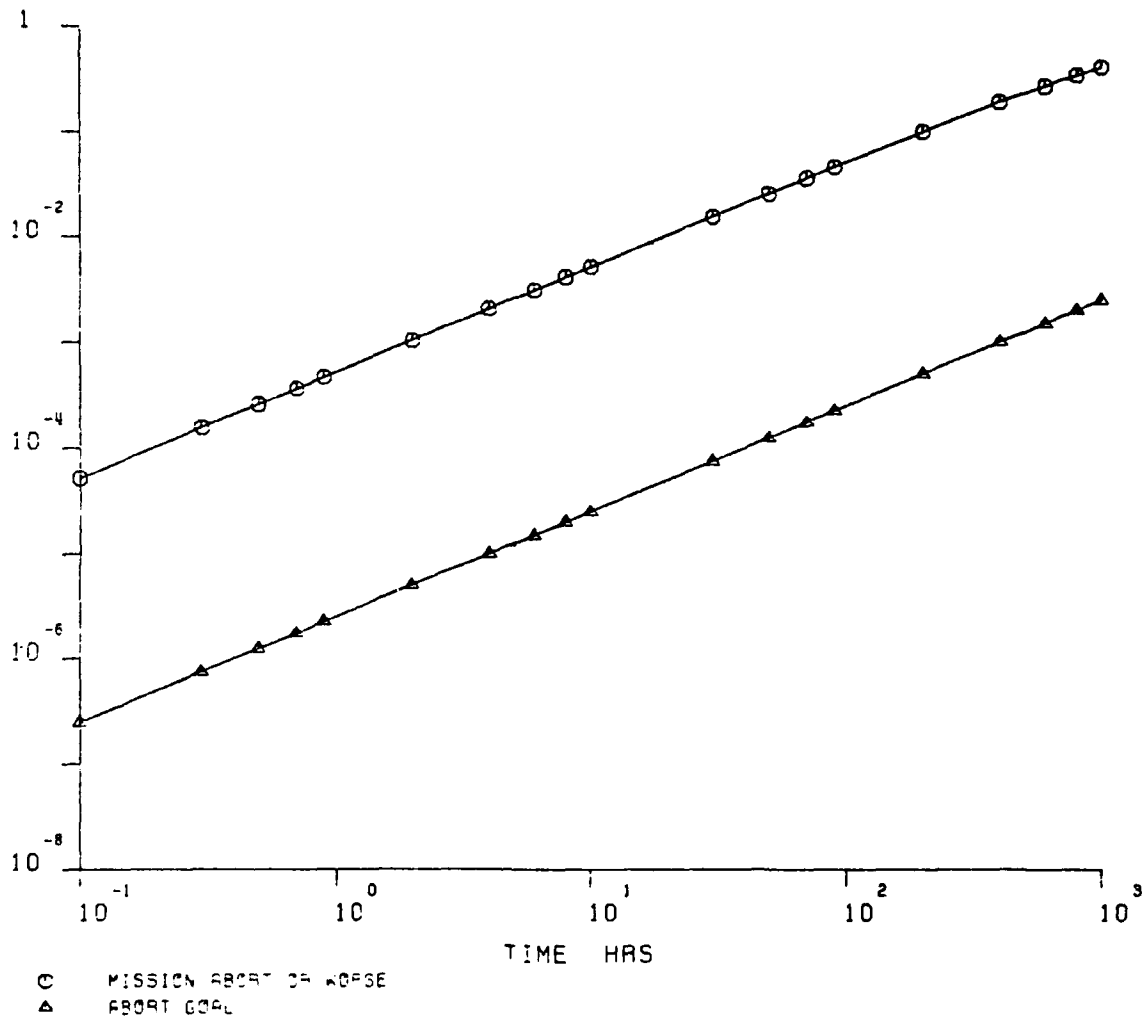


Figure 40. FAFTEEC Baseline Reliability Evaluation: Simplex System (Mission Abort)

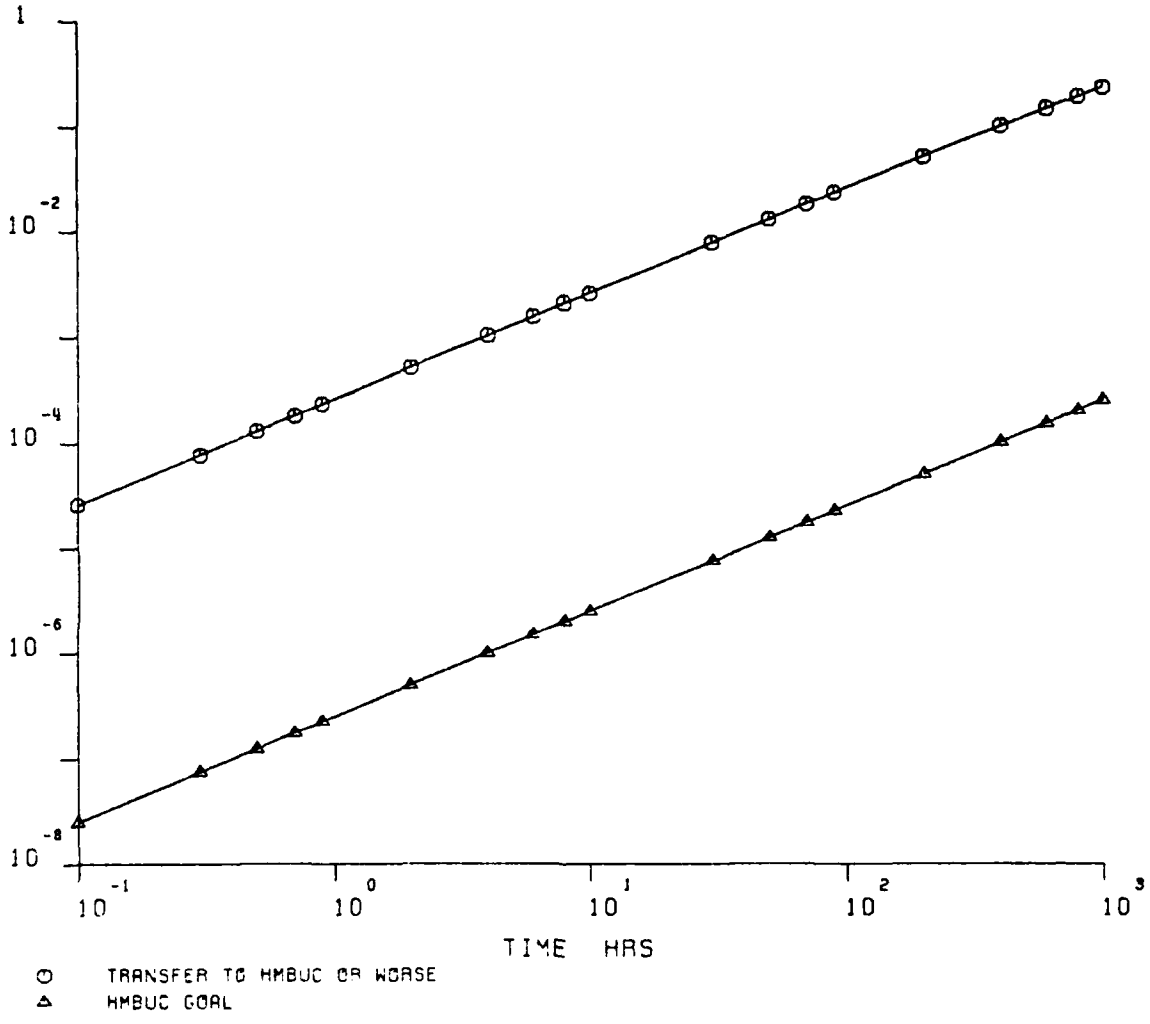


Figure 41. FAFTEEC Baseline Reliability Evaluation: Simplex System (Transfer to HMBUC)

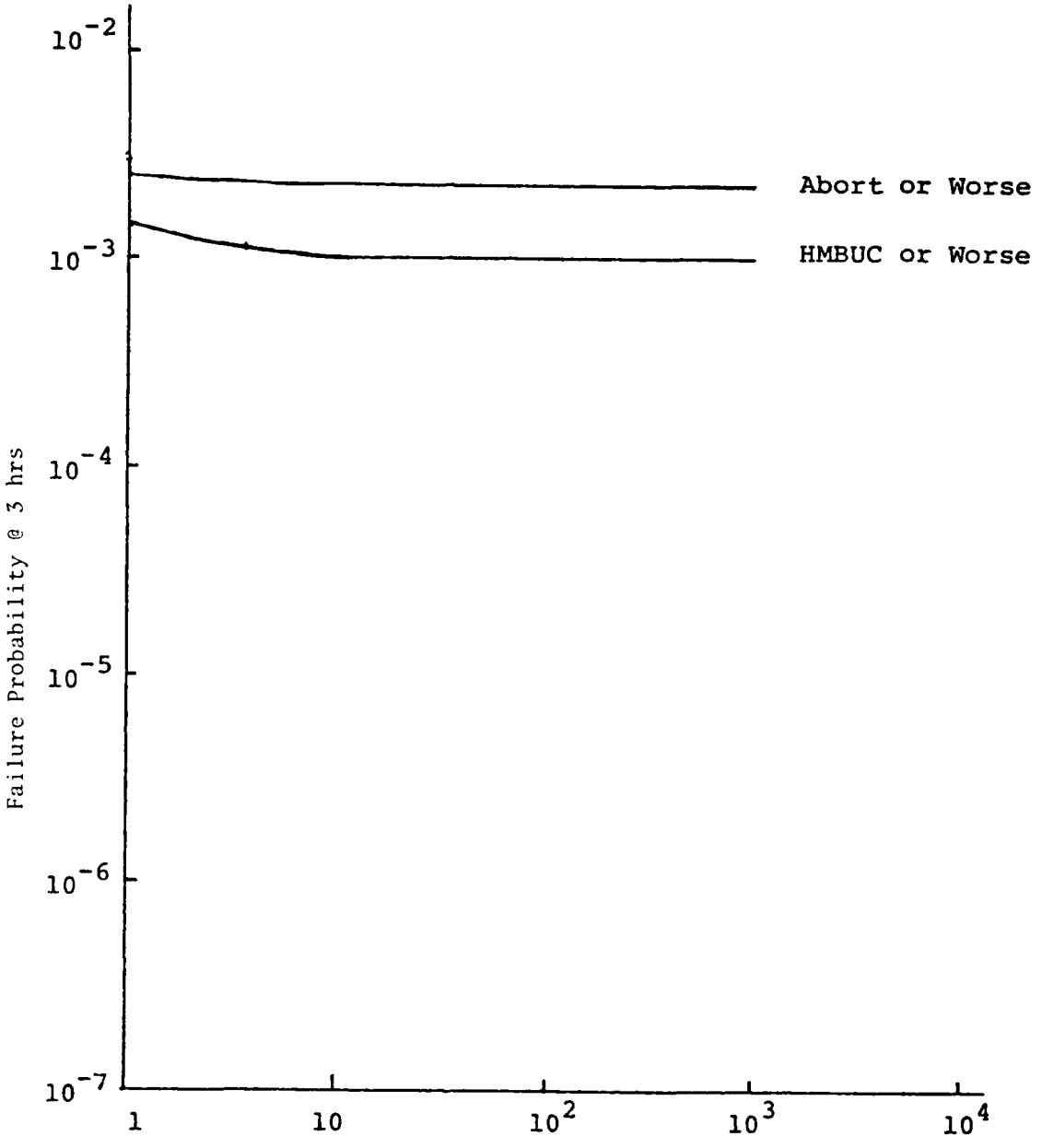


Figure 42. FAFTEEC Reliability Improvement Due to Improvement in Computer Reliability

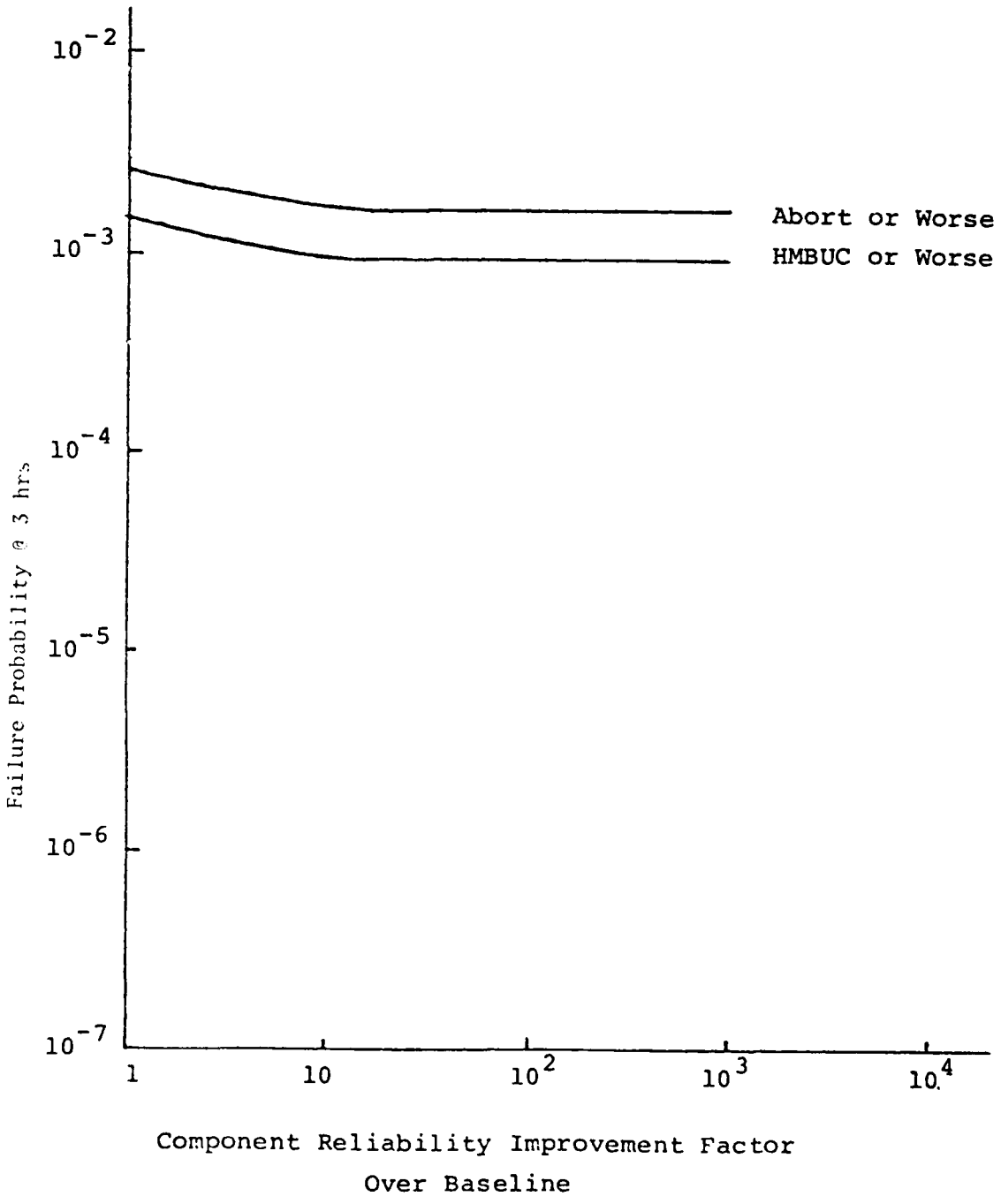
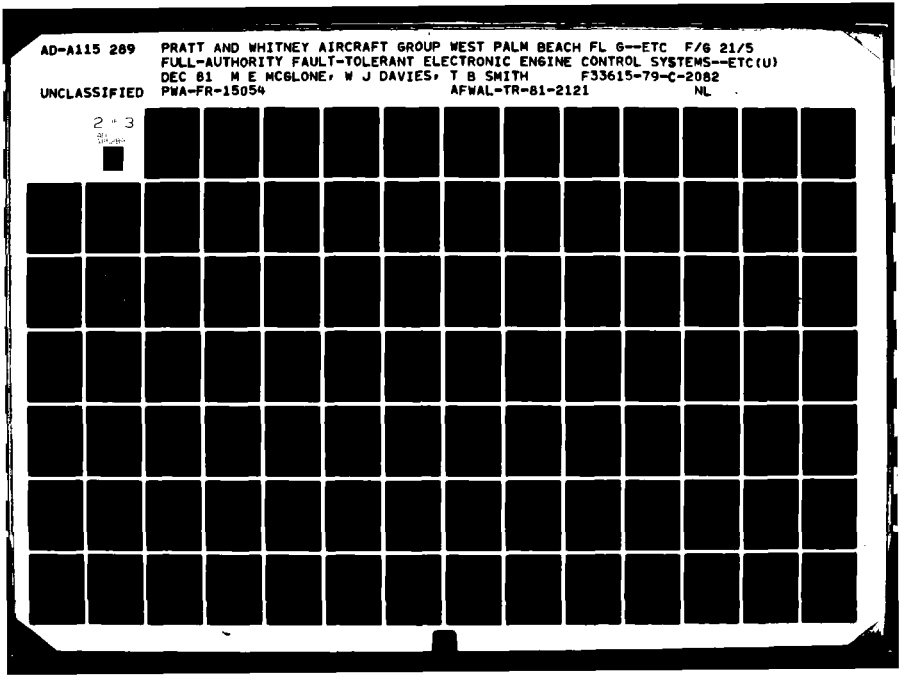
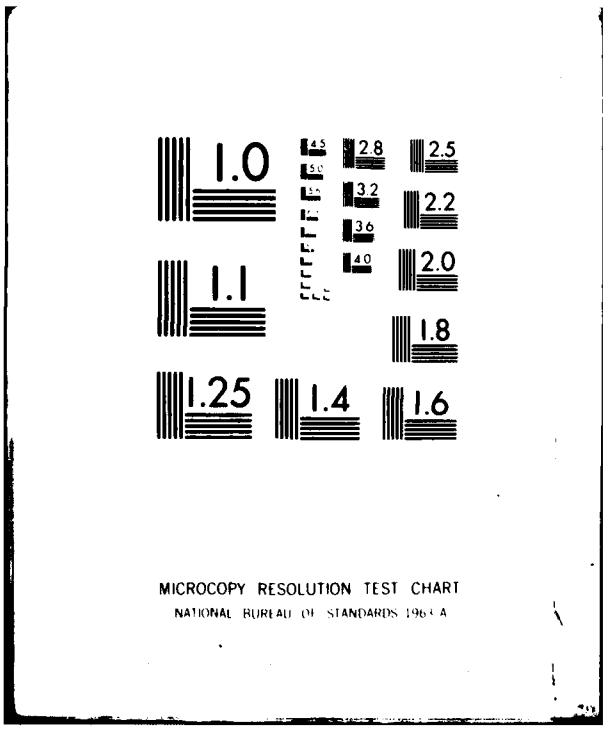


Figure 43. FAFTEEC Reliability Improvement Due to Improvement in Sensor Reliability

AD-A115 289 PRATT AND WHITNEY AIRCRAFT GROUP WEST PALM BEACH FL G--ETC F/G 21/5
FULL-AUTHORITY FAULT-TOLERANT ELECTRONIC ENGINE CONTROL SYSTEMS--ETC(U)
DEC 81 M E MCGLONE, W J DAVIES, T B SMITH F33615-79-C-2082
UNCLASSIFIED PWA-FR-15054 AFWAL-TR-81-2121 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

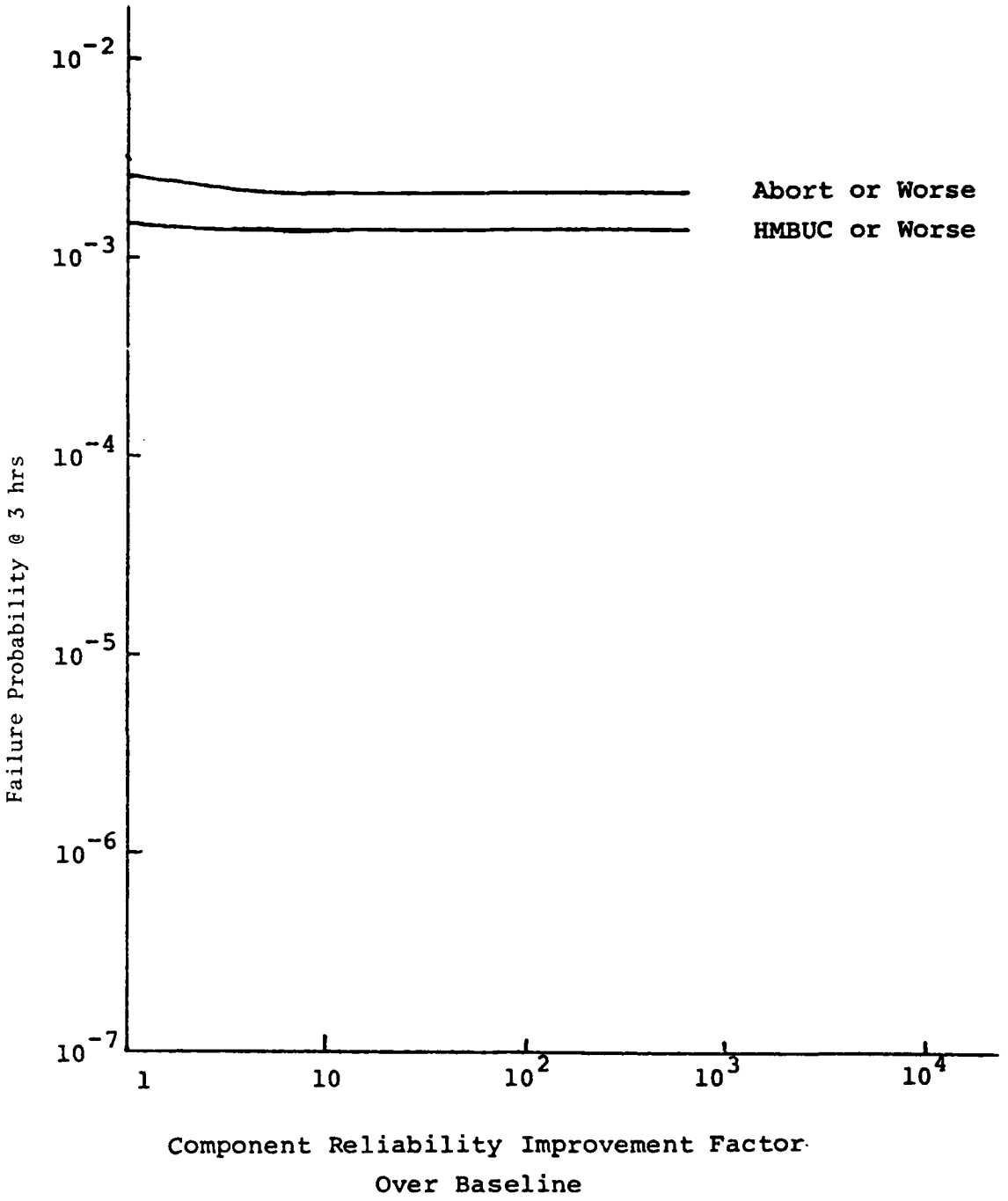


Figure 44. FAFTEEC Reliability Improvement Due to Improvement in Actuator Reliability

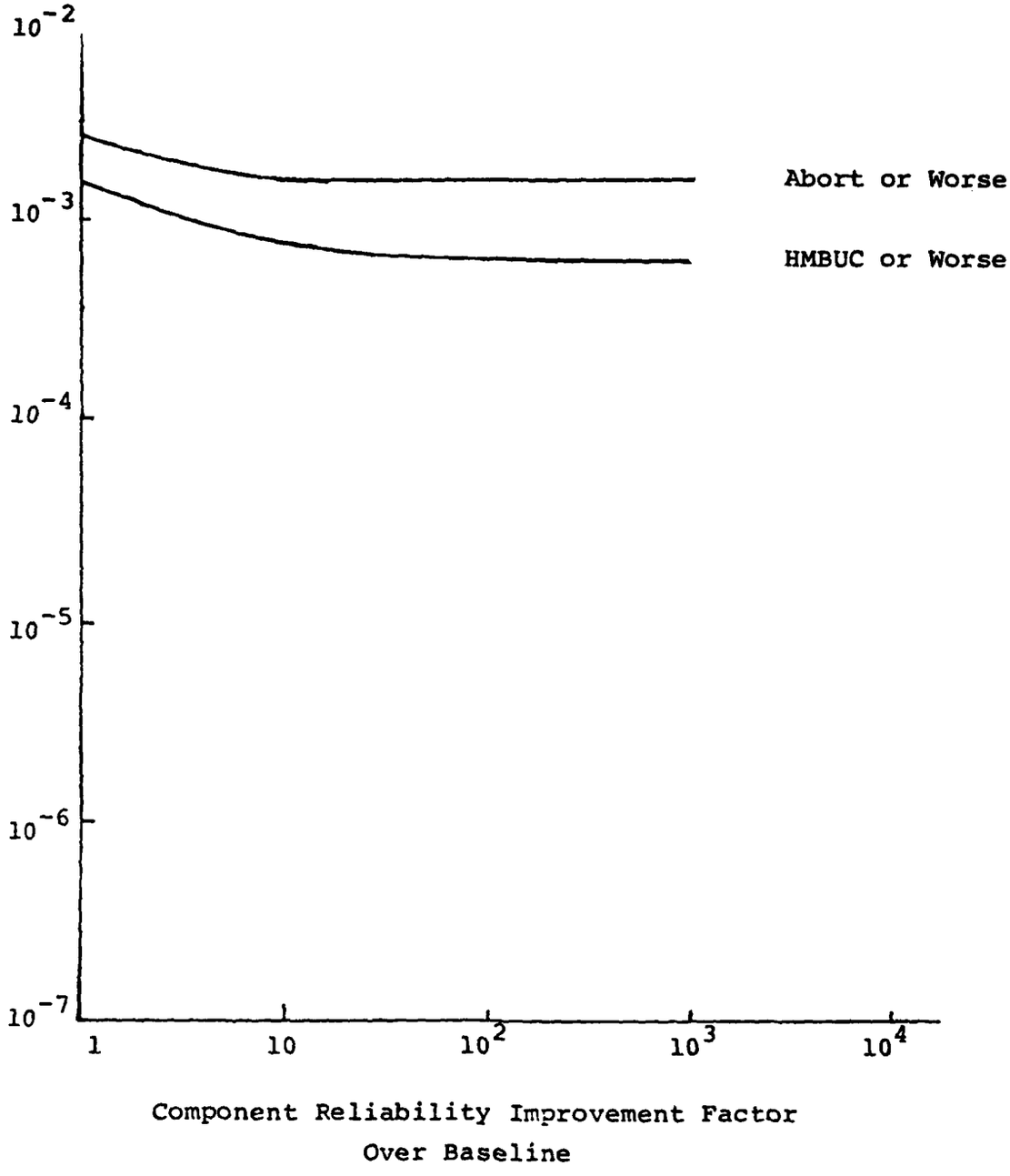


Figure 45. FAFTEEC Reliability Improvement Due to Improvement in Miscellaneous Components

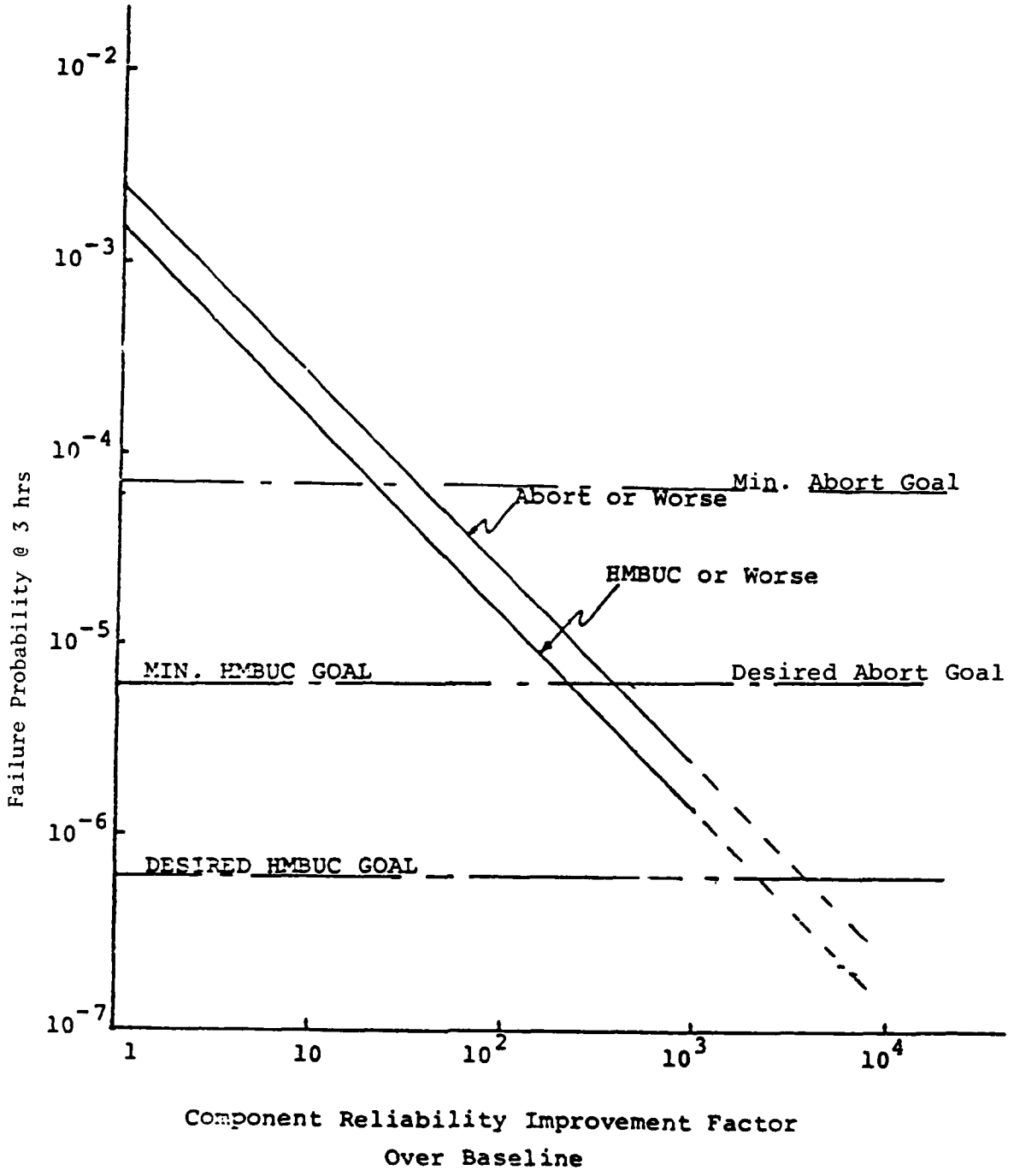


Figure 46. FAFTEEC Reliability Improvements Due to Improvement in All Components

System 2

This system is designed with the object of reducing the likelihood of transferring to the backup controller. Therefore, all HMBUC critical sensors (N1, N2, PLA, P3, T2 and TBT) have been made completely dual. The sensor redundancy extends all the way from probes to signal conditioners. The HMBUC critical actuators (CSVA and WFGG) are also dual. This includes the servovalve for each actuator. The computer and alternator to power it are duplicated. Each of the two computers has access to one set of sensors and drives one set of actuators. The two computers, however, can communicate with each other on a high bandwidth channel and exchange the sensor values and actuator commands. A good sensor in one channel can therefore substitute for the corresponding failed sensor in the other channel.

The core fuel pump (CFP) is also duplicated. The non-HMBUC critical sensors are shared by the two computational channels. That is, there is a common probe and signal conditioner for each channel. The simplex actuators have a single torque motor with dual windings and a single servovalve. The hydraulic pump is simplex.

System 2 Results

A number of assumptions were made in deriving the reliability figures for this system. The assumptions are as follows.

The coverage for all the dual redundant actuators, pumps, servovalves and output electronic interfaces is assumed to be 100 percent. That is, the electronic control system can continue to perform satisfactorily with no deterioration in engine performance if any one of the dual redundant components fails. The coverage for computer failures is assumed to be 0.95 while the coverage for sensors is assumed to be 0.99. That is, five percent of first computer failures result in transfer to HMBUC while the one percent of first sensor failures result in mission abort or transfer to HMBUC depending upon the criticality of the sensor.

Figures 47 and 48 show the probability of mission abort or worse and transfer to HMBUC or worse for System 2. The probability of transfer to HMBUC for a 3-hr mission is found to be 2.1×10^{-5} which is better than the baseline figure by a factor of 40 but still short of the desired FAFTEEC goal by a factor of about 30. It will be recalled here that System 2 was specifically configured to improve the transfer to HMBUC reliability performance. Even though all the relevant components have been made dual redundant the reliability gain has been insufficient to meet the desired goals. The reason for this can be seen in the predominant modes of failure for System 2. As seen in Table 24 there are two predominant failure modes that result in transfer to HMBUC. These are the uncovered computer and sensor failures. In an uncovered computer failure one of the two computer fails such that the failure is either not detected or it is not attributed to the correct channel. The same is true of uncovered HMBUC critical sensors. In other words, even though all HMBUC critical components have been duplicated there still are some single failures that can result in transfer to HMBUC or worse. And in fact since these single failures are the predominant system failure modes the probability of transfer to HMBUC or worse is directly proportional to mission length (up to about 100 hr) as evidenced by the results in figure 48.

The mission abort or worse likelihood for System 2 is better than an all simplex system by a factor of about six. For a 3-hr mission this probability is 2.7×10^{-4}. It will be recalled here that all the mission abort critical sensors and actuators are still simplex in System 2. The small improvement in mission abort performance is due solely to the reduced likelihood of transferring to HMBUC which is included in the mission abort likelihood. The mission abort probability is also a linear function of time (see figure 47) due to a predominance of simplex failure modes.

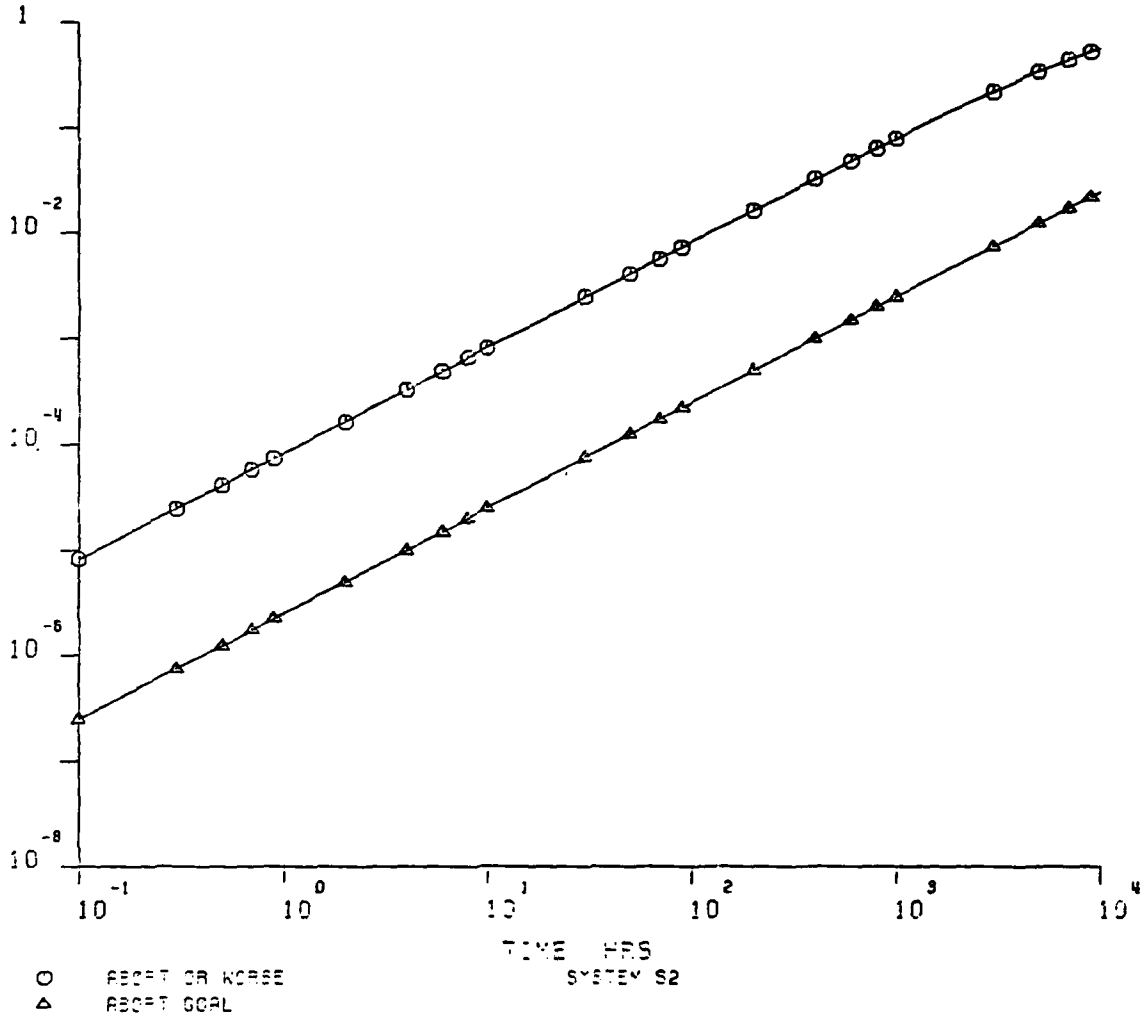


Figure 47. Abort or Worse Model System 2

TABLE 24. PREDOMINANT FAILURE MODE FMEA

System	*Mission Abort Failure Mode*	*Transfer to HMBUC Failure Modes*
System 1	Sensor, actuator, hydraulic pump, augmentor pump	Sensor, actuator, core fuel pump, computer
System 2	Simplex sensor, actuator parts, hydraulic pump	Uncovered sensor, computer failures
System 3	Simplex actuator pistons, uncovered sensor failures	Simplex actuator pistons, uncovered sensor, computer failures
System 4	Uncovered sensor failures	Uncovered sensor, computer failures
System 4A	Uncovered sensor, actuator failures	Uncovered sensor, actuator, computer failures
System 4B	Uncovered sensor failure	
System 5	Uncovered sensor failure	Uncovered sensor failure
System 5A	Simplex sensor, actuator parts, Hyd. Pump	Uncovered sensor failure
System 6	Uncovered sensor, actuator failures	Uncovered sensor, actuator failures
System 6A	Uncovered sensor, actuator failures	Uncovered sensor, actuator failures

Mission Abort: Relevant sensor and actuators are as follows:

Sensors: P2, P13, P5, ΔP3, ΔP13, T22, TPS
Actuators: A4, A41, AJE, AJD, FIG V, WFD

Transfer to HMBUC: Relevant sensor and actuators are as follows:

Sensors: N1, N2, PLA, P3, T2, TBT
Actuators: WFGG, CSVA

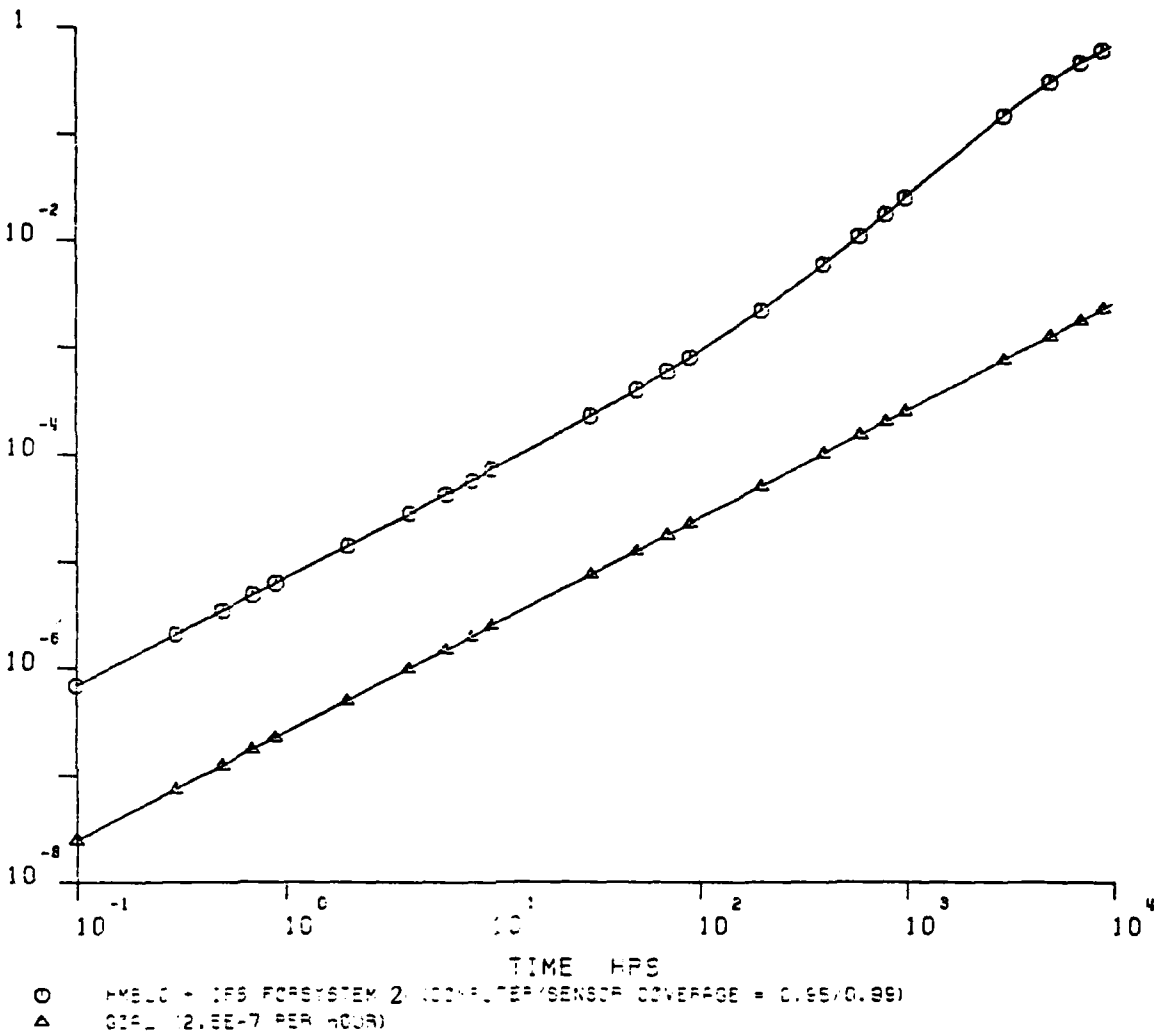


Figure 48. HMBUC and IFS System 2 (Comp/Sensor Coverage = 0.95/0.99)

System 3 Description

System 3 has been configured to improve the transfer to HMBUC as well as mission abort reliability performance over the baseline system. In addition to the redundancy employed in System 2, all the mission abort critical sensors (P2, P13, P5, ΔP3, ΔP13, T22 and TPS) as well as actuators (A4, A41, AJE, AJD, FIGV and WFD) have been made dual redundant in System 3. The hydraulic pump has also been made duplex. System 3, therefore, is a completely dual system.

System 3 Results

The coverage for computer, sensor and actuator failures for these systems is assumed to be same as that for System 2. That is, sensor failure coverage is 0.99, computer failure coverage is 0.95 and for all other components it is 1.0.

The mission abort and transfer to HMBUC probabilities for System 3 are plotted in Figures 49 and 50, respectively.

The transfer to HMBUC likelihood for System 3 is identical to that for System 2 since there is no change in HMBUC critical component configuration. In other words, transfer to HMBUC probability for the completely dual system is still about 30 times worse than the desired goal.

The main difference between systems 2 and 3 is the improvement in mission abort performance. The likelihood of not completing a 3 hr mission with a completely dual FAFTEEC is 2.6×10^{-5} (Table 24). This misses the desired goal by a factor of three. However, it is an improvement of a factor of 60 over the simplex baseline and an order of magnitude better than the partially duplex System 2. It also exceeds the minimum FAFTEEC mission abort goal which is $7.5 \times 10^{-}5$ for a 3-hr mission. The predominant failure mode is an uncovered sensor failure, that is, a failure of a mission abort critical sensor that is not detected or not identified correctly. The mission abort probability is linearly dependent upon time up to about 100 hr (see Figure 49) reflecting the predominance of the single point failure mode.

System 4 and 4A Description

System 4 is identical to System 3 in redundancy in that they are completely dual redundant, however they are different in the system architecture as was pointed out in the system description. System four uses advanced technology components structured for a dual system such as the dual centrifugal pumps and direct drive tandem actuators. These changes do not significantly affect mission abort reliability but significantly improve cost, weight, and maintenance reliability.

Systems 4 and 4A are identical in redundancy in that they are also completely dual redundant systems. However, there are some differences in the area of computational core. There is a high bandwidth communication channel between the two computers. This channel is used to exchange sensor values and actuator commands between the two computation channels. A failed sensor in one channel can be replaced by the corresponding sensor from the other channel in System 4. In System 4A the computational core architecture is such that sensor values are not routinely exchanged between the two channels. A sensor failure in one channel has the consequence of disabling that whole channel. The same is true of an actuator failure. The differences in systems 4 and 4A are related to coverage assumptions as described in the next section.

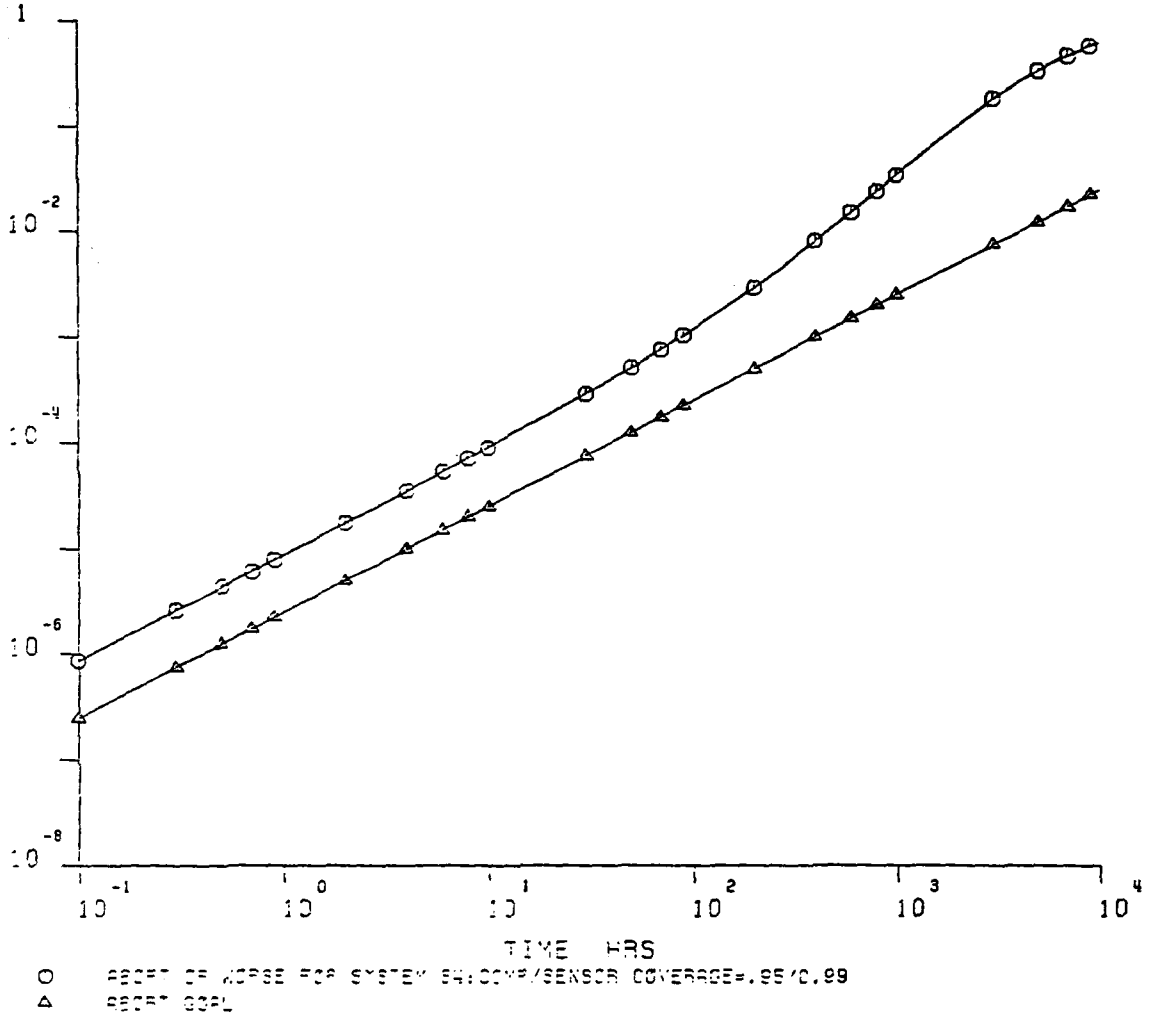


Figure 49. Abort Model for System 3 (Comp/Sensor Coverage = 0.95/0.99)

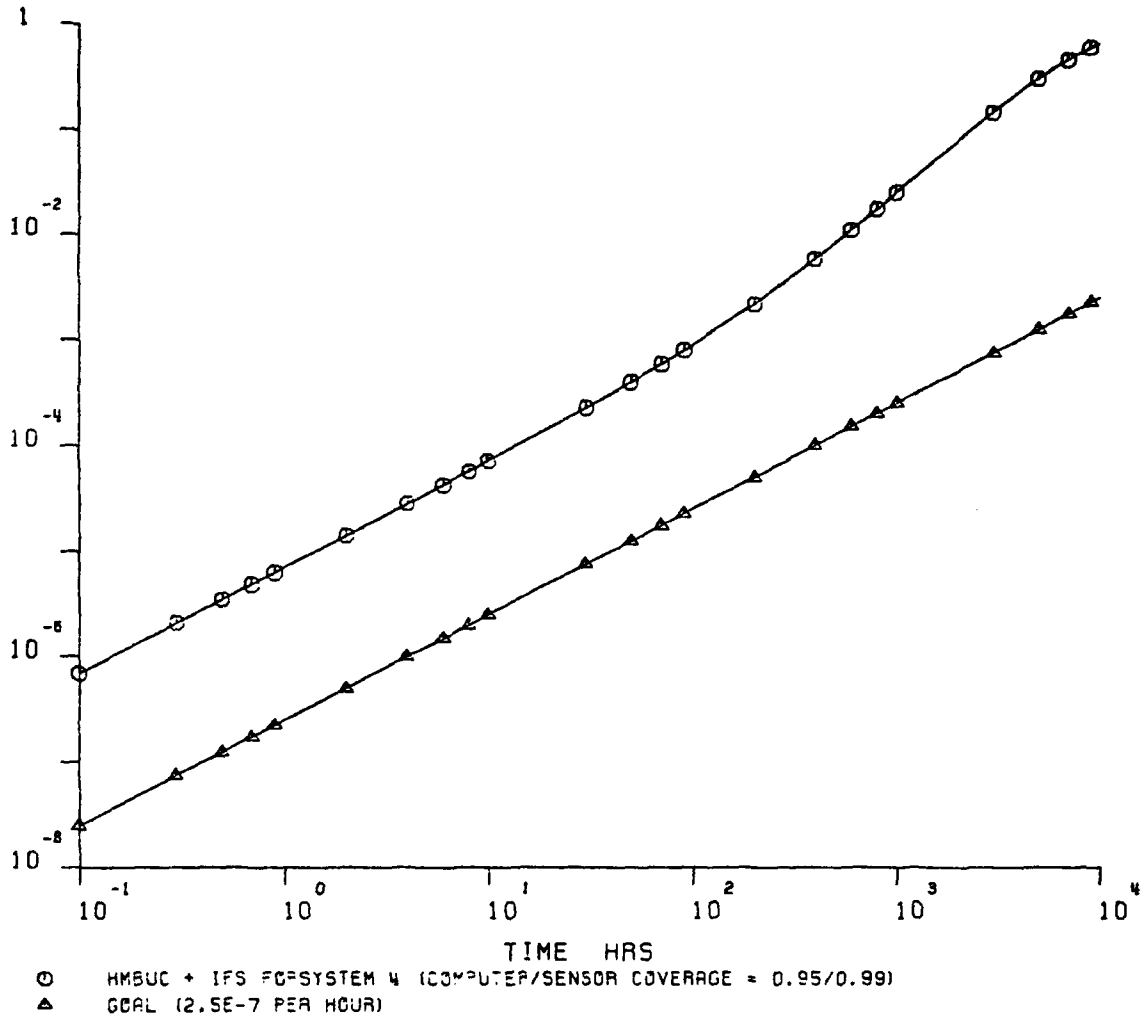


Figure 50. HMBUC and IFS for System 3 (Comp/Sensor Coverage = 0.95/0.99)

System 4 and 4A Results

The sensor coverage for these systems is assumed to be 0.99 which is same as for all other dual systems. The computer coverage, however, is assumed to be 0.90 for System 4A here rather than 0.95 as in Systm 4A, since there is no exchange of information between the two computational channels that can facilitate disagreement detection between the two computers. The actuator coverage for System 4A is assumed to be 0.99 rather than 1.0. The reason once again is the lack of information exchange between the two channels. This is a more realistic assumption for a noncross strapped duplex computer. However, results were also evaluated assuming perfect actuator coverage. These results are tabulated under System 4A.

Figure 51 to 54 show the results for System 4 and 4A. Compared to a cross strapped system the reliability performance is worse but not by a large margin. For example, for a 3-hr mission the transfer to HMBUC likelihood for the noncross strapped system (nonperfect actuator coverage) is 3.9×10^{-5} compared to 2.1×10^{-5} for a cross-strapped system. Assuming a 100 percent actuator coverage improves this slightly to 3.6×10^{-5}. Similarly, a 3-hr mission has a likelihood of being aborted of 5.8×10^{-5} for a noncross strapped system compared to 2.6×10^{-5} for a cross strapped system. Assuming perfect actuator coverage improves this likelihood to 4.2×10^{-5}.

Dual System Summary

Two major dual redundant configurations have been modeled: one is a partially duplex version to improve the transfer to HMBUC performance (System 2) and the second is a fully duplex version to enhance the mission abort performance as well (System 4). The partially duplex system has redundancy in only those items that are HMBUC critical. Duplicating these components improves the likelihood of transfer to HMBUC by a factor of 40 over baseline to 2.1×10^{-7} at 3 hr. However, it still fails to meet the desired FAFTEEC goal of 7.5×10^{-7} at 3 hr by a factor of 30. The predominant failure mode is uncovered failure of a sensor or a computer.

The likelihood of aborting a 3 hr mission with a fully dual redundant FAFTEEC is 2.6×10^{-5} which fails to meet the desired FAFTEEC goal of 7.5×10^{-5} at 3 hr. The predominant failure mode is uncovered sensor failures.

Minor variations of the fully duplex system have also been modeled with the following results. If the computers are noncross strapped the reliability decreases by a factor of about 1.5 to 2 depending upon the actuator coverage.

DUAL SYSTEM WITH TRIPLEX COMPUTATION (SYSTEM 5)

It is seen from the results of the previous section that a completely dual redundant FAFTEEC system fails to meet the desired reliability goals by a wide margin. The predominant failure modes of such a system are the uncovered computer and sensor failures. To increase coverage for the first computer failure beyond what can be reasonably achieved with a dual computer it is necessary to add a third computer. With a triplex synchronous computational core any single failure can be masked by a 2-out-of-3 majority voter. In addition, comparison of the majority voter output to the three inputs can reveal the identity of the faulty computer. In effect, the coverage for the first computer failure can be made virtually 100%.

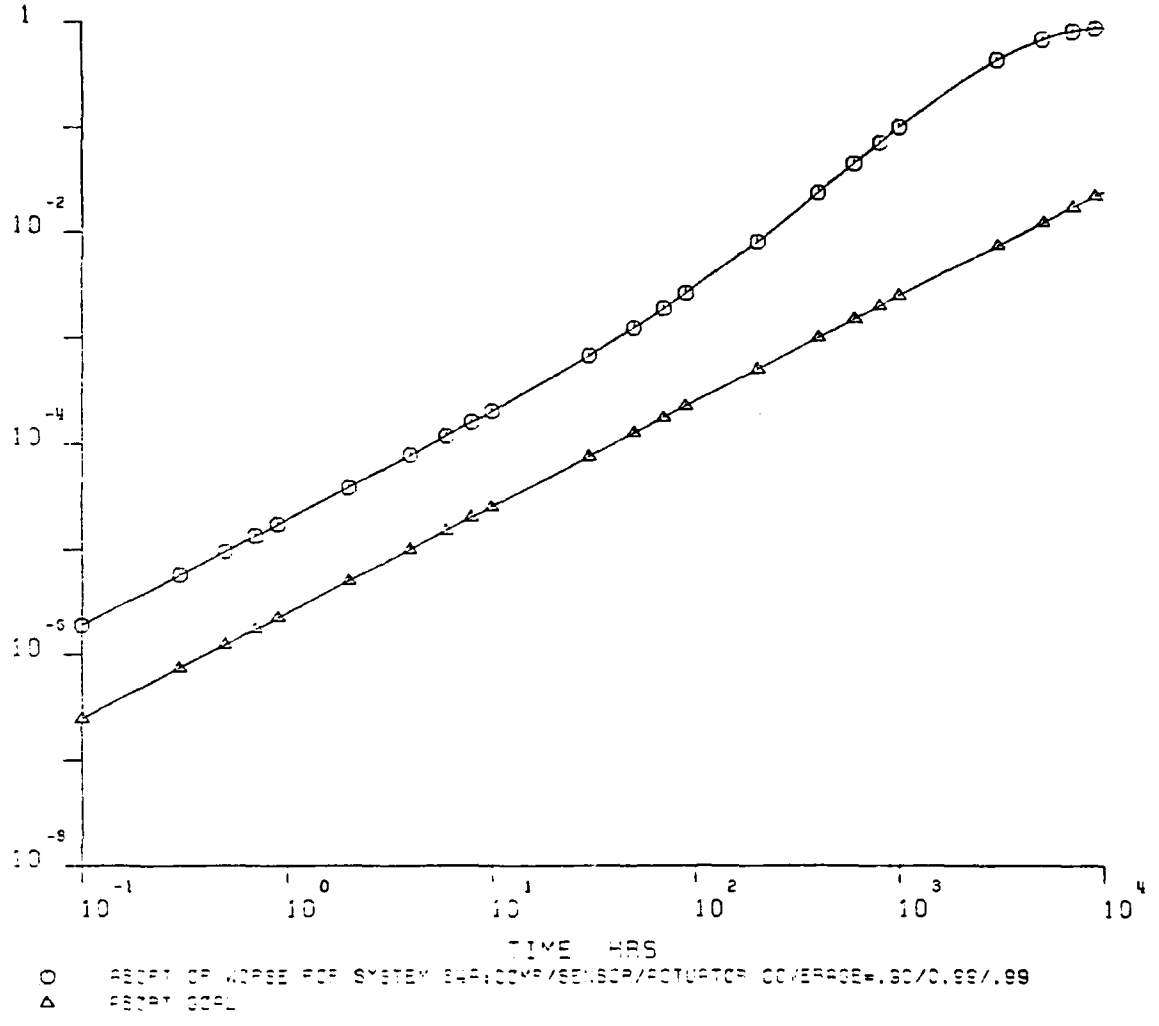


Figure 51. Abort Model for System 4 (Comp/S and A Coverage = 0.90/0.99)

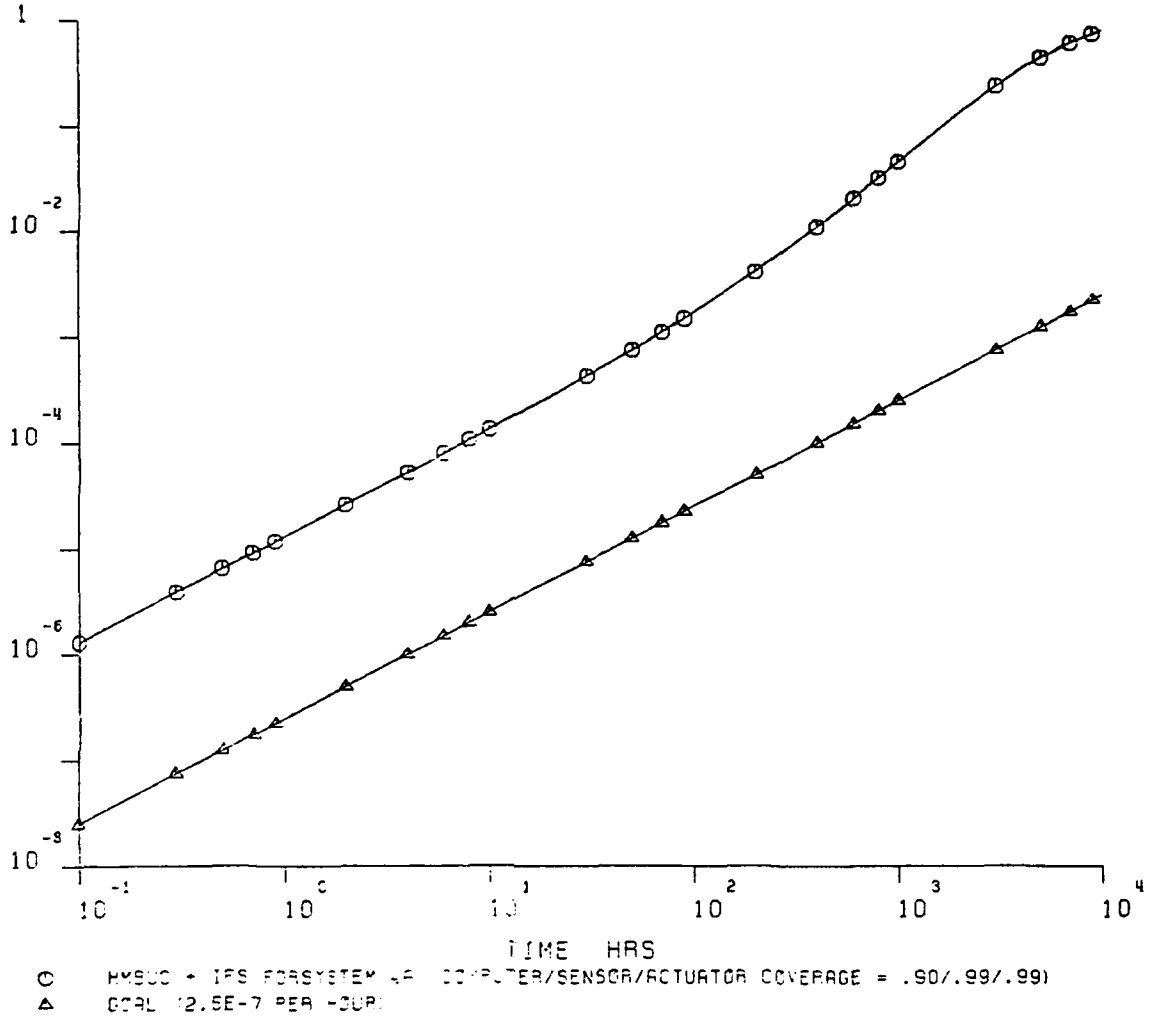


Figure 52. HMBUC and IFS for System 4 (Comp/S and A Coverage = 0.90/0.99)

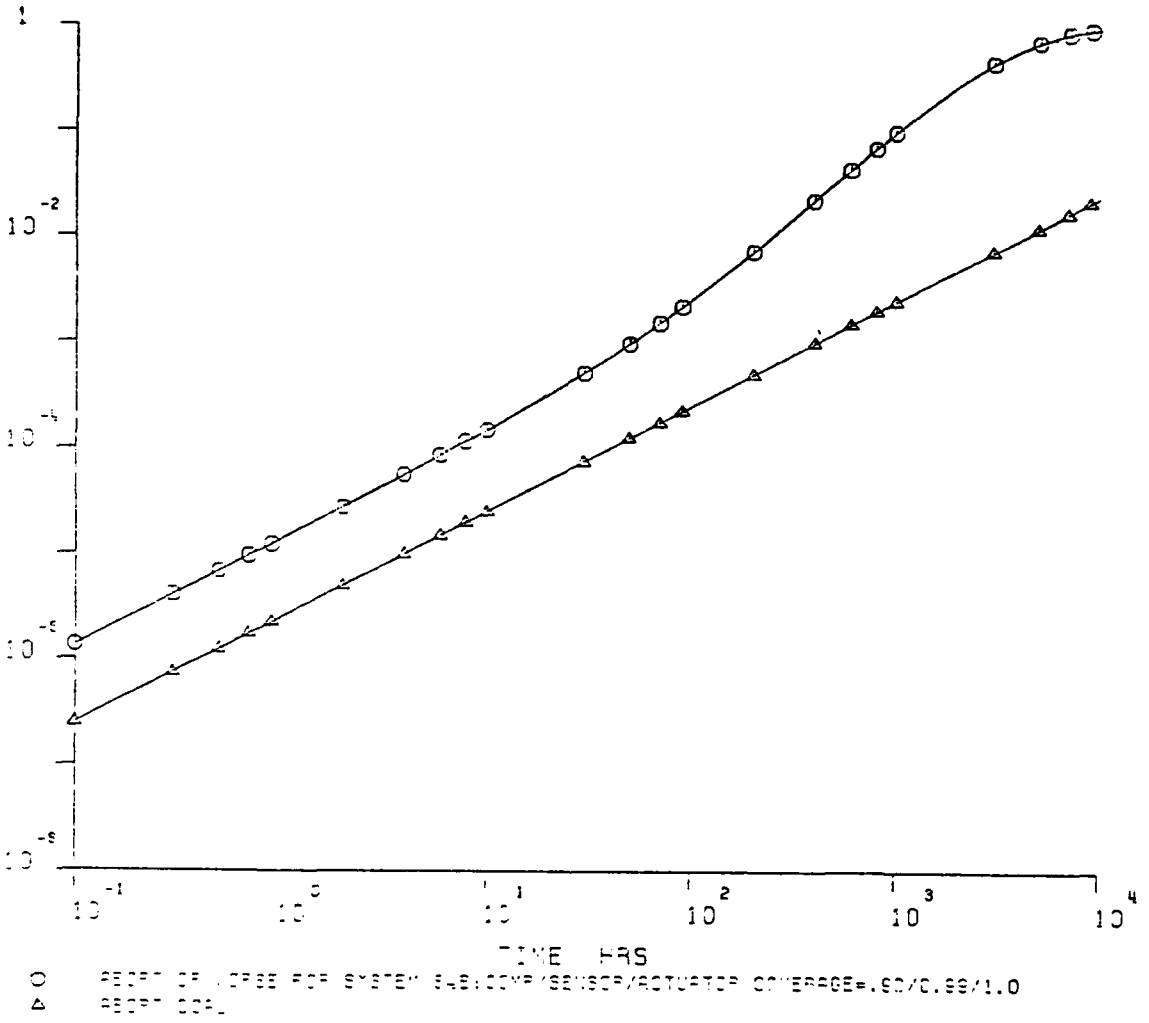


Figure 53. Abort Model for System 4A (Coverage = 0.90/0.99)

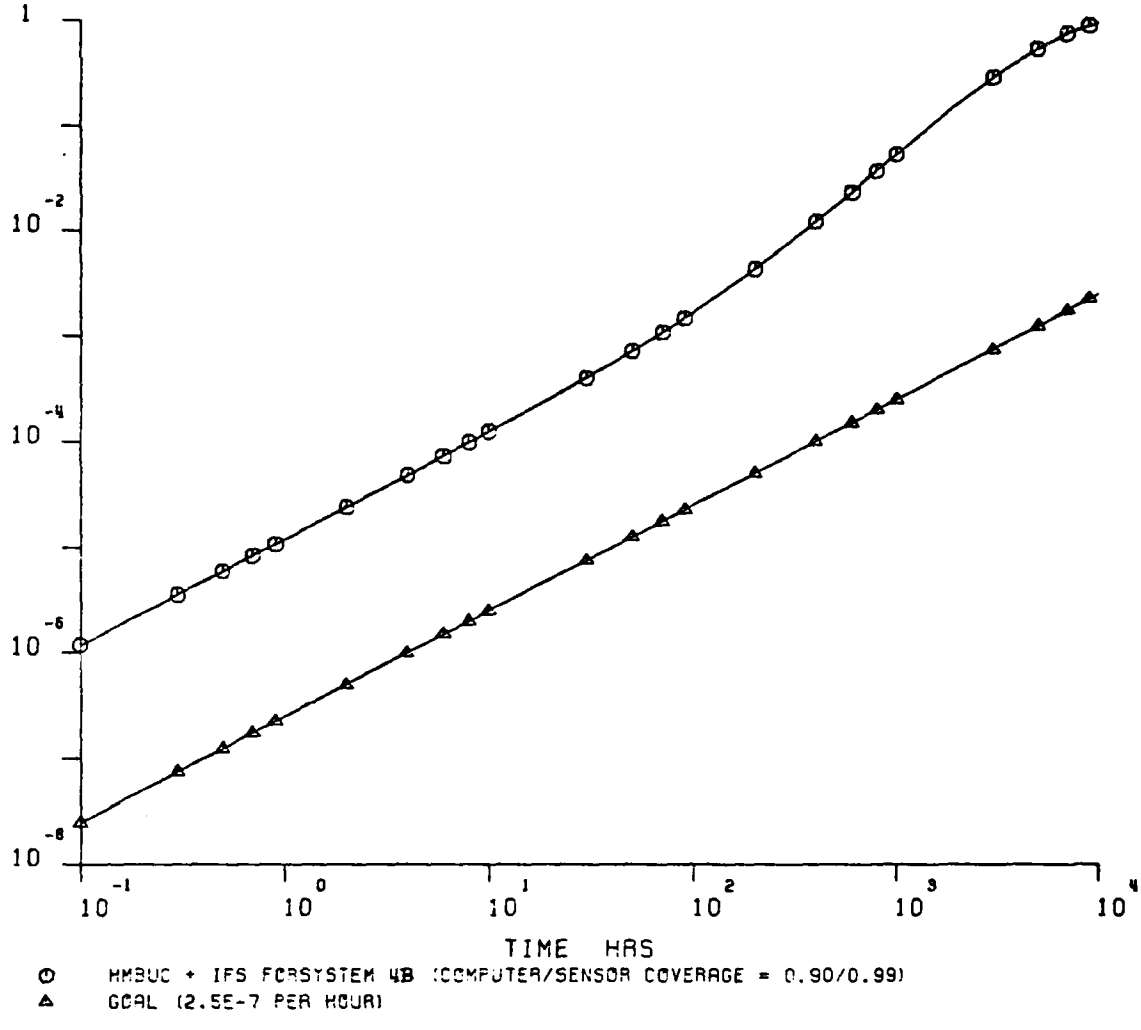


Figure 54. HMBUC and IFS for System 4A (Comp/Sensor Coverage = 0.90/0.99)

System 5 is basically a dual system (same as System 4) but the computation core has been triplicated. The third computer is powered by its own alternator. This sytem was evaluated assuming perfect coverage for the first computer failure. Other coverage factors are assumed to be same as that for System 4. That is, sensor coverage is assumed to be 0.99 and the actuator coverage is assumed to be 1.0. The reliability results for System 5 are shown in Figures 55 and 56. The probability of transfer to HMBUC is still a linear function of time in the range of mission time that is of interest. Thereafter it increases sharply indicating a different failure mode. Up to about 50 hr the predominant failure mode is uncovered sensor failures. Since the sensor coverage is assumed to be 0.99, 1% of the total sensor failure rate (HMBUC critical sensors only) contributes directly to the transfer to HMBUC probability. The computer failures are no longer a factor in the transfer to HMBUC likelihood for one to ten hour missions. The overall impact of these two factors is that the likelihood of transferring to HMBUC has improved to 6.2×10^{-6} for a 3 hr mission (compared to 2.1×10^{-5} for a completely dual system) but it is still short of the desired FAFTEEC goal by a factor of about 3. System 5, however, is the first system configuration so far that meets the minimum FAFTEEC goal for transfer to HMBUC of 7.5×10^{-6} for a 3-hr mission. Since the system reliability is a linear function of time in the time range of interest, the minimum goal is exceeded by the same margin for 1 hr as well as for 10-hr missions.

The mission abort performance of the partially triplex system has similar characteristics as the transfer to HMBUC performance. As seen in Figure 55, the likelihood of aborting a mission is linearly dependent on the length of the mission for the time range of interest. The likelihood of aborting a 3 hr mission is 1.1×10^{-5} compared to 2.6×10^{-5} for the completely dual system and 7.5×10^{-6} which is the desired FAFTEEC goal. The System 5 performance does exceed the minimum goal of 7.5×10^{-5} by a comfortable margin. The predominant reason for aborting a mission is uncovered sensor failures.

In summary, the partially triplex system fails to meet the desired mission abort as well as transfer to HMBUC goals but does exceed the corresponding minimum goals. Since the predominant failure mode is the uncovered failure of a sensor, it is logical to improve the sensor coverage in order to improve the system reliability performance.

DUAL SYSTEM WITH DUAL/DUAL COMPUTATION

System 6 is a completely dual redundant system. It has the same configuration as System 4 except in the area of computational core. System 6 has been configured with two major computation channels each of which has two paired computers. The two paired computers in a major channel work with the same sensor inputs and are synchronized. The sensor coverage is assumed to be .99 and the actuator coverage 1. The coverage for the first computer failure is assumed to be 1.0. The reliability results under the assumptions are essentially the same as System 5.

DUAL SYSTEM WITH DUAL/DUAL MULTIMICROPROCESSORS

System 6A is a completely dual redundant system. It has the same configuration as System 4 except in the area of the computational core. System 6A has been configured such that there are separate microprocessors for each part of the variable cycle engine. There are two channels for each of these functions. Each channel has two synchronized microprocessors. The variable geometry control is divided into three functions as follows.

1. CSVA and WFGG
2. AJE, AJD and WFD
3. FIGV, A4 and A4.1.

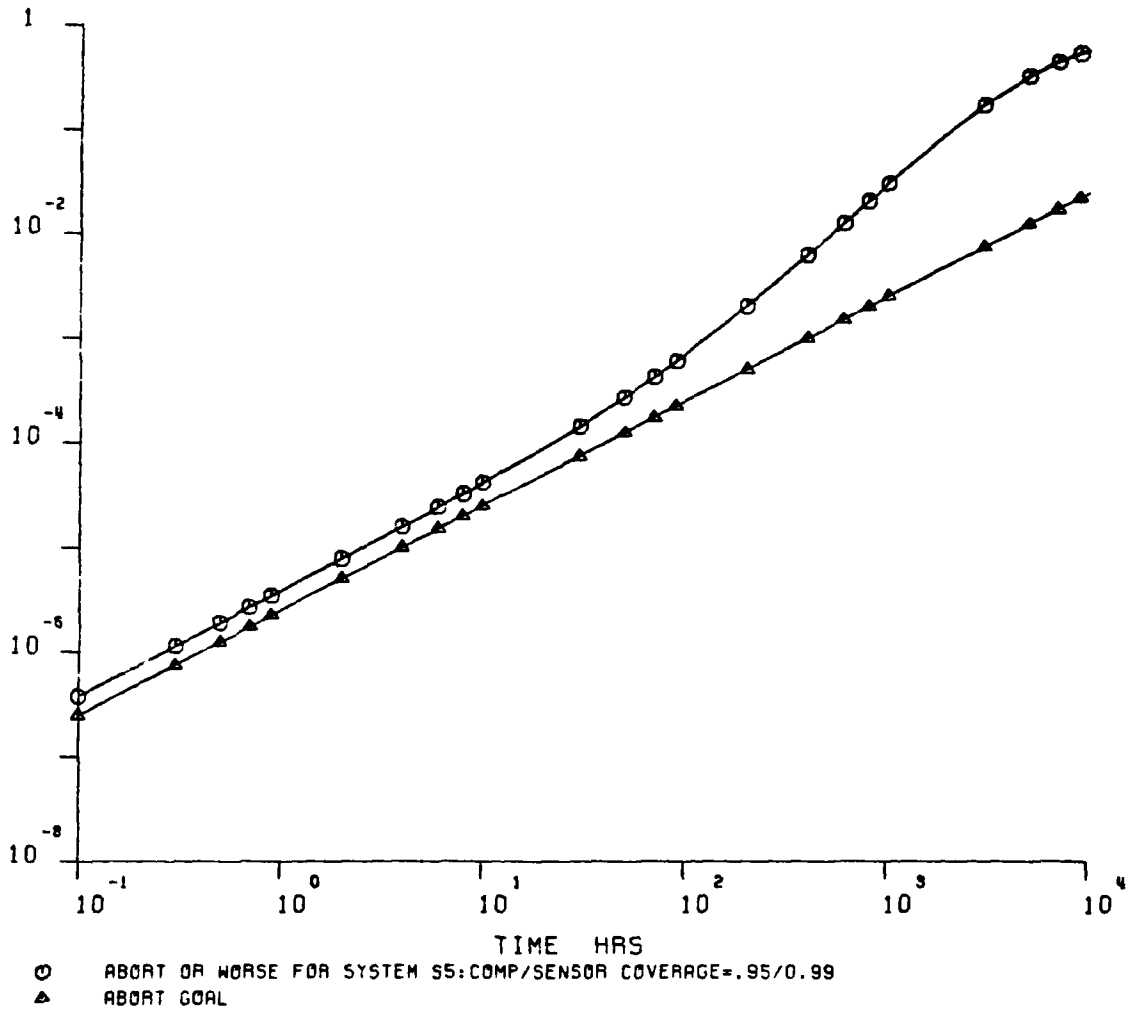


Figure 55. Abort Model for System 5 (Comp/Sensor Coverage = 1/0/0.99)

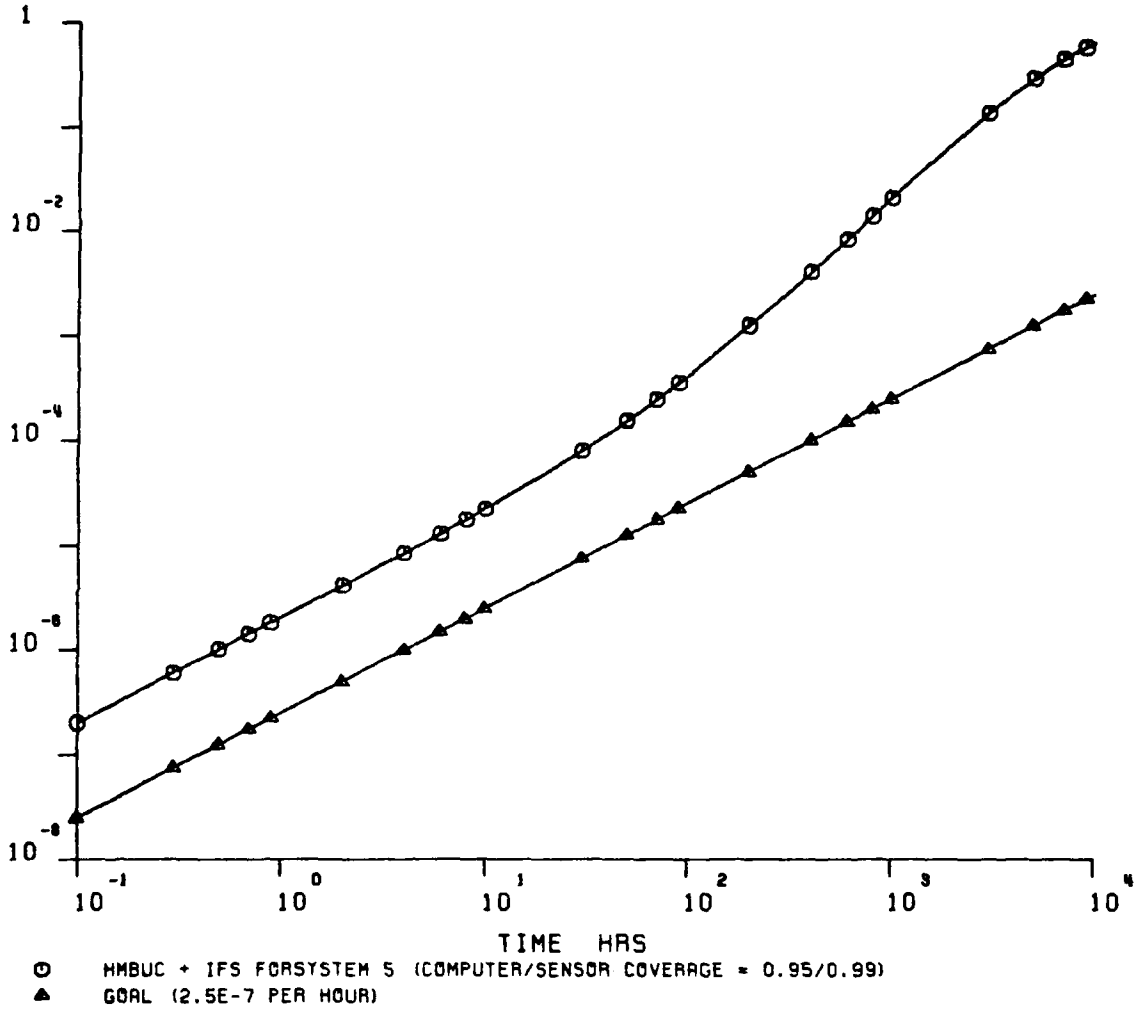


Figure 56. HMBUC and IFS for System 5 (Comp/Sensor Coverage = 1/0/0.99)

The reliability results of System 6A are the same as those for Systems 5 and 6 as shown in figure 54. These systems all exhibit the same reliability results since they are the same except for the computer redundancy architecture. In all cases the added computer redundancy improves the coverage of the computer to 100%.

System 7 is an enhanced dual system. It differs from System 5, 6, and 6A in that not only is the computer coverage enhanced to 100% but so is the sensor coverage. The results of the improved coverage provides a system which will meet the FAFTEEC reliability goals. The probability mission abort of System 7 for a 3 hr mission 0.7×10^{-6} compared to a goal of 7.5×10^{-6}. The probability of transfer to the back-up control for a 3 hr mission is 1.2×10^{-7} compared to a desired goal of 7.5×10^{-7}.

SECTION 8

ELECTRONIC CONTROL PACKAGING

BACKGROUND

Reliability modeling of a variety of FAFTEEC system configurations has resulted in the identification of nine candidate systems for packaging study. Five different electronic control packaging configurations will satisfy the nine systems requirements and are described in the next section.

All controls have been packaged with one channel per box using leadless chip carrier technology as described in Reference 1. The first four electronic controls use an advanced 3 chip processor implemented in gate-array technology. The fifth configuration utilizes a single chip microprocessor with the characteristics of a next generation, T.I. 9940.

ELECTRONIC ENGINE CONTROL CONFIGURATIONS

Each of the five configurations uses multi-level vectored interrupts in order to handle the various input converters and to provide the input data in a timely way.

Communication to external devices is provided by two methods in each channel. A UART is provided for diagnostic test purposes only. The normal communications will be via a MIL-STD-1553B data bus. This interface is configured as a single remote terminal in each channel. Bus Controller or Bus Monitor operations are not provided by the EEC.

The EAROM has been sized in order to store three types of data; specifically, total operating time, fault history, and calibration constants for the pressure sensors. The replacement of a pressure sensor will also require that these constants be changed by the repair facility. The test UART will serve as the interface to the CPU for this change.

Baseline Control

A single channel gathers all sensor signals through one set of input conversion hardware to a single high speed gate array processor which commands a single set of effectors through a single set of output drivers, Figure 57.

Dual Controls

Two separate channels gather sensor signals through separate dedictated input conversion circuits to separate high speed gate array processors, each of which commands separate windings on the variously redundant effectors, Figure 58. They are interconnected by a high speed data link.

Dual Controls With Voting Computer

Two separate channels gather sensor signals through separate dedicated input conversion circuits to separate high speed gate array processors which command separate windings on variously redundant actuators. A voting processor receives sensor data from each of the two main channels by data link, Figure 59. Calculated commands are passed between all processors by data link. Hardware voting generates disable signals to remove a faulty main channel from control.

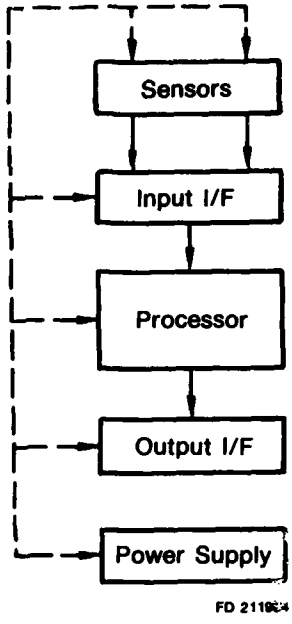


Figure 57. FAFTEEC Computers Simplex Configuration (System 1)

Dual-Dual Controls With Centralized Processing

Two separate channels gather sensor signals through separate dedicated input conversion circuits to pairs of high-speed gate array processors in each channel, Figure 60. Output commands from each pair of processors are compared in a hardware voter in each channel. Failure of output commands to compare properly generates a signal which disables the entire channel and control transfer to the other channel. Commands which agree will enable the output interface circuits to drive the separate windings on the redundant actuators. Cross-link communication between the two separate channels provides a means of fault detection for the sensors and signal conditioning circuits.

Dual/Dual Controls Using Multiple Micro-Computers

Basic channel organization is the same used with the single processor acrhitecture. The gate-array processor pairs are replaced with three single chip microcomputer pairs per channel, Figure 61. Each pair handles the computations for one of the following three functions: Gas generator control, engine geometry control, and exhaust nozzle control. The sensors and sensor interfaces are organized in the same manner as the previous dual/duplex system. A Direct Memory Access (DMA) Control in each channel uses the addressing sequence stored in PROM to select the multiplex switch positions and control the operation of the various converters. The eleven input converters produce digital data words which are deposited in the correct DMA RAM locations by the DMA Controller. Interrupts are required from the DMA Controller to each CPU in order to coordinate the engine control algorithms with the input data. A seventh processor is included in each channel to interface with external units and provide common fault storage capability. Use of this seventh CPU per channel eliminates the need for an EAROM and 1553B data bus. External command data will be distributed by this seventh processor.

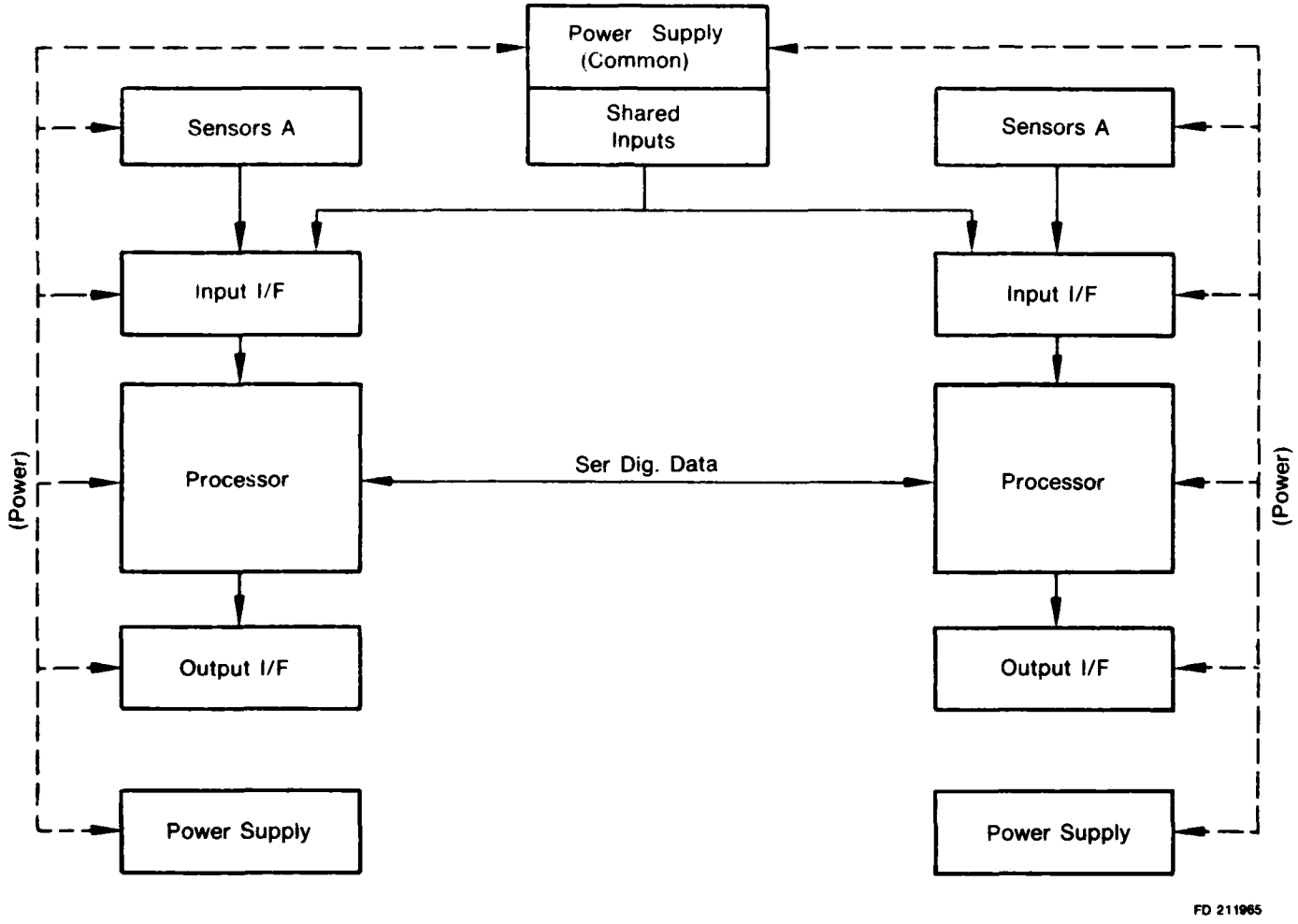


Figure 58. Dual Configuration (Systems 2, 3, 4 and 4A)

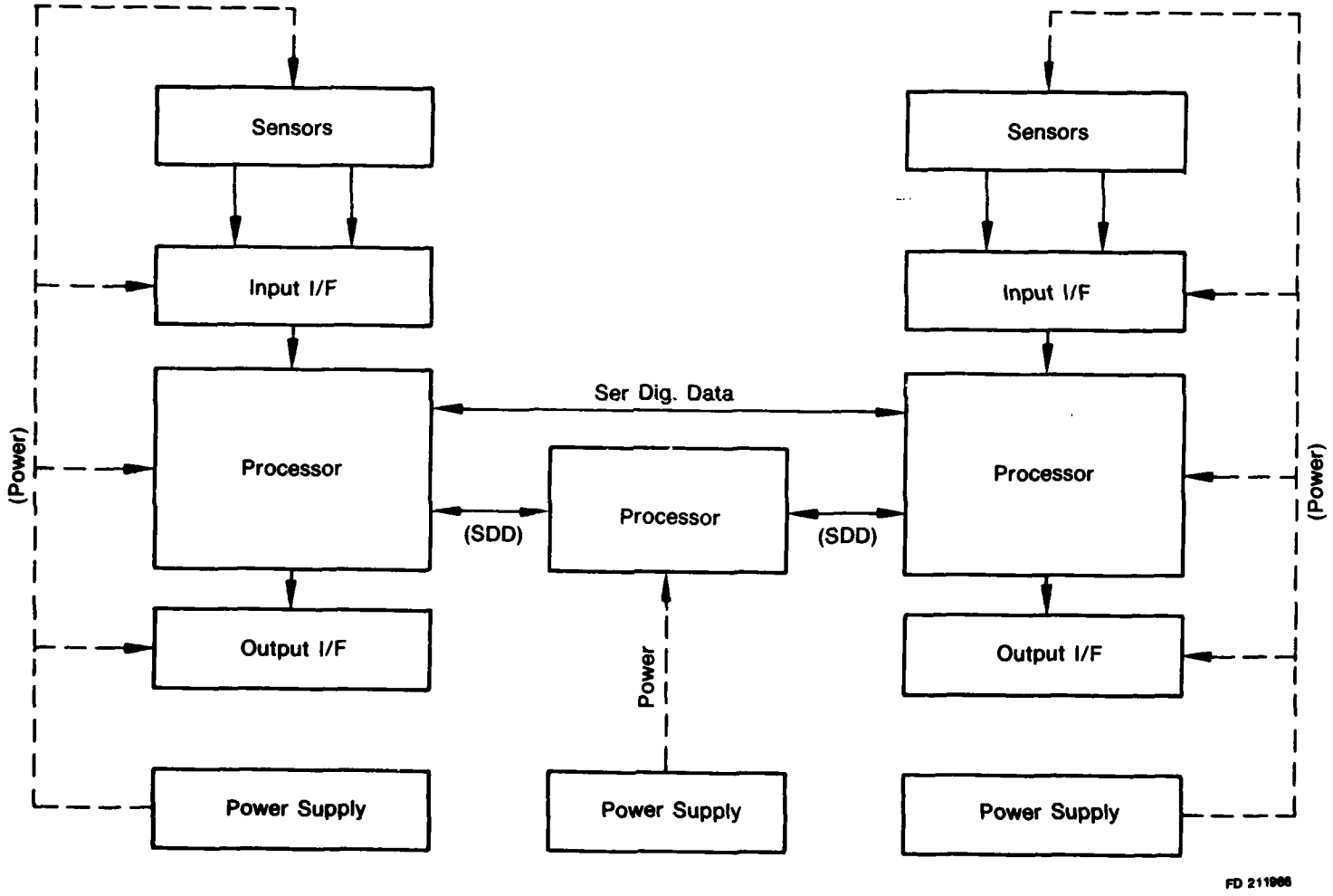


Figure 59. Dual Plus Voter Configuration (System 5)

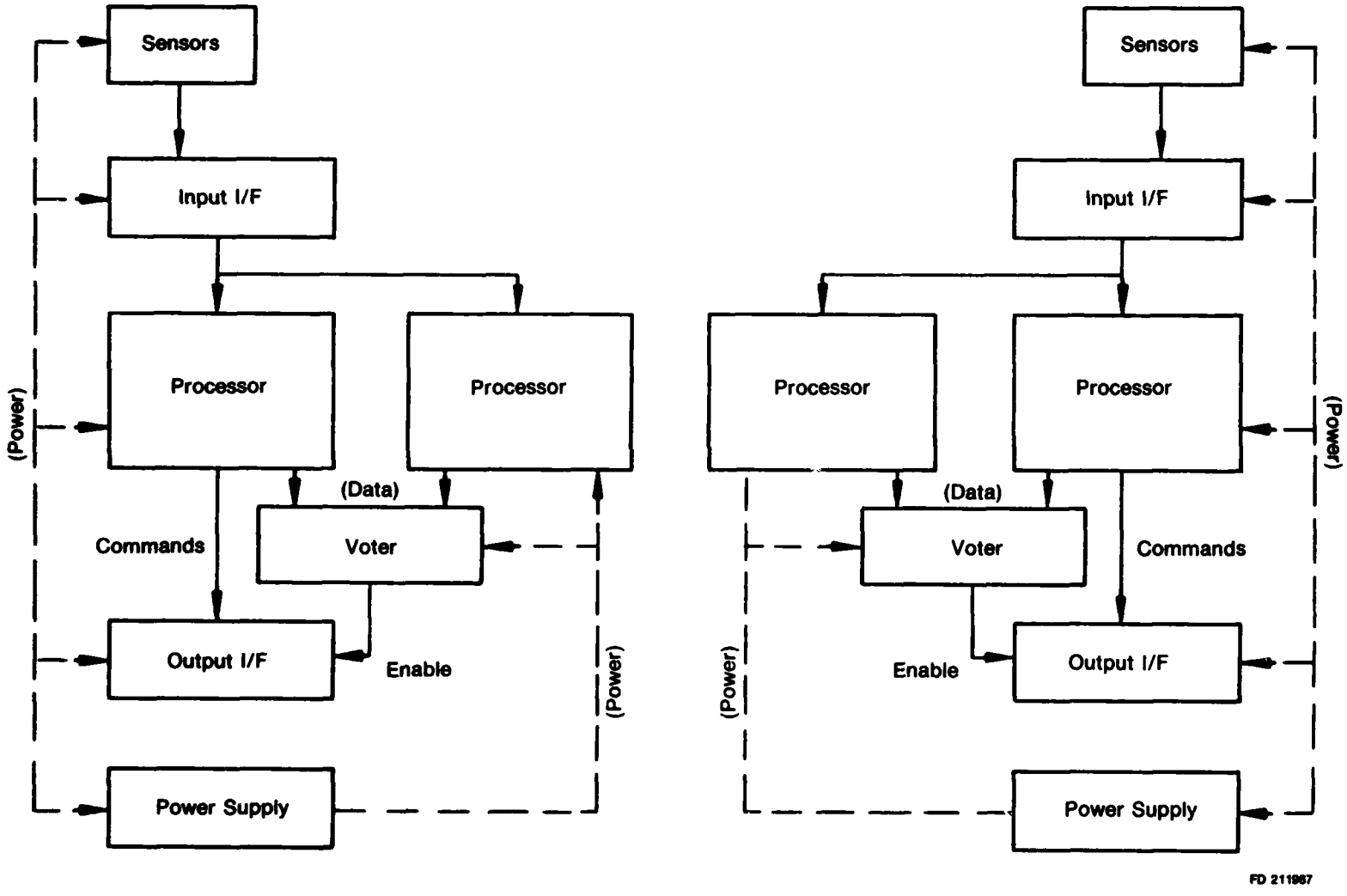


Figure 60. Dual Duplex Configuration (System 6)

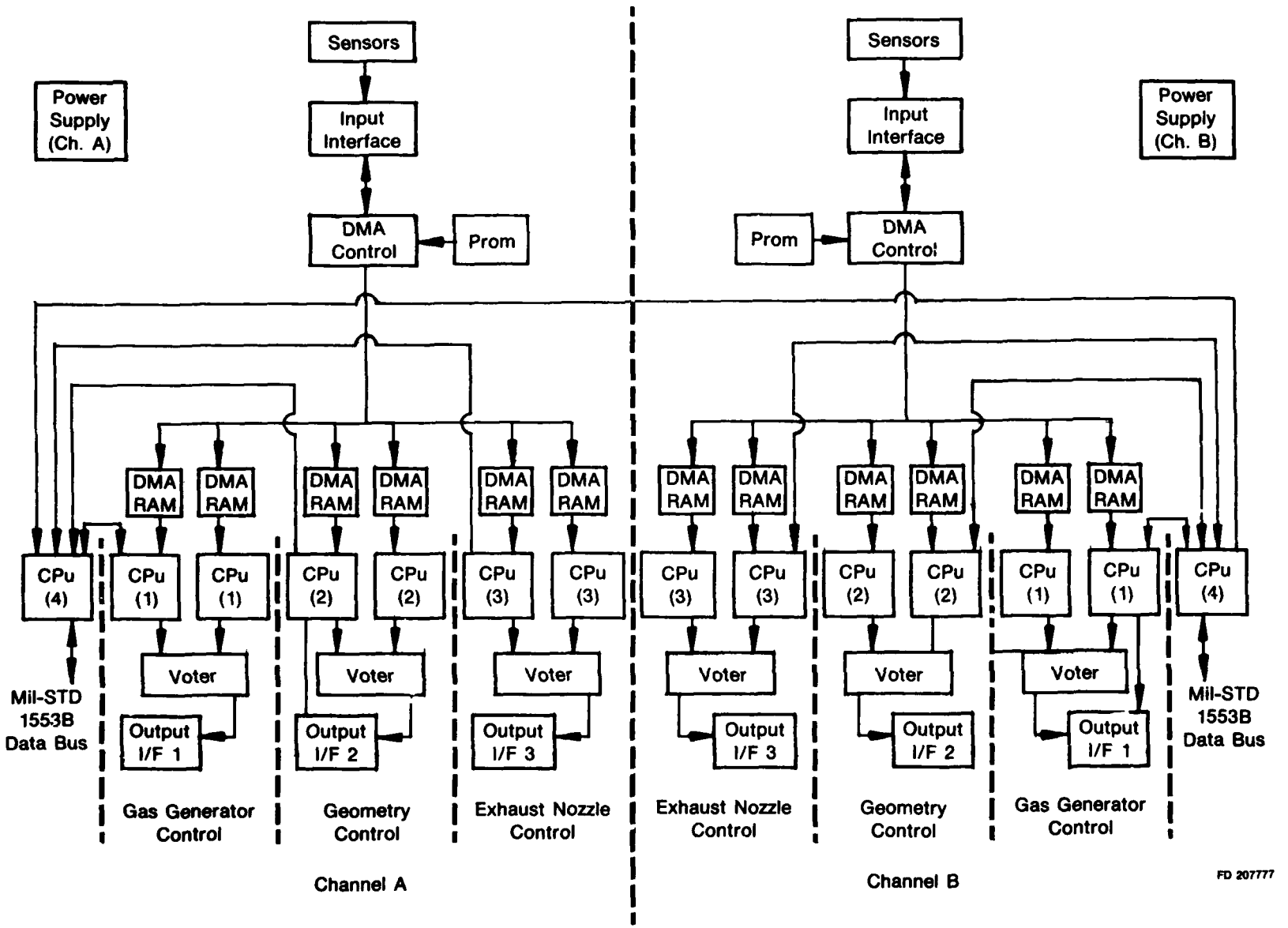


Figure 61. Dual/Duplex Configuration Using Distributed Processing (System 6A)

PACKAGING

A preliminary electrical design has been completed for each EEC configuration. Electrical modules and parts lists have been prepared and packaging for these parts is described in the following sections. Included with this packaging summary are the results of software comparisons conducted for each of the five electronic configurations.

Configuration and Installation

External features of the control are designed for handling and installation using published human engineering guides and engine fuel control design experience. Figure 62 shows the external configuration of a typical control. FAFTEEC package characteristics are summarized in Table 25. A weight breakdown for each system is shown in Table 26.

The control is mounted with four straight in bolts minimizing mounting tolerances. Connectors are oriented horizontally to the ground, when installed, to prevent contaminants from collecting in the backshell of the engine harness connector plugs.

The pressure transducers are mounted on the side of the control with the pressure ports facing downward to prevent moisture ingestion. The control is equipped with electrical I/O connectors polarized to ensure proper mating with correct cables. Test connectors, located in the rear of the control, are equipped with protective caps for on-engine protection. The pressure transducer pneumatic lines and the fuel inlet and outlet hydraulic lines are polarized with the male insert which is normally installed by the engine manufacturer. The chassis is supplied with a bond strap in accordance with MIL-B-5087B, Class L, to provide effective grounding of the control against lightning.

The bond straps attach to the engine with No. 10-32 hardware. Installation and transport of the control is facilitated by the integrally cast handle. Fuel connections are made in the rear of the package.

PHYSICAL DESCRIPTION

The FAFTEEC Control employs modular construction throughout, as shown in Figure 63, all modules plug directly into a central Interconnect Printed Circuit Board Module. This modular design approach facilitates sequential testing of all subassemblies at critical stages throughout the build to assure a reliable end assembly. Each unique module has been standardized as much as the package restraints would allow. This feature is directed to the benefits of automated assembly techniques and attendant increased reliability.

Module Description

Removal of the housing cover gives access to all electronic modules. The basic controller (A or B) consists of the submodules shown in Table 27.

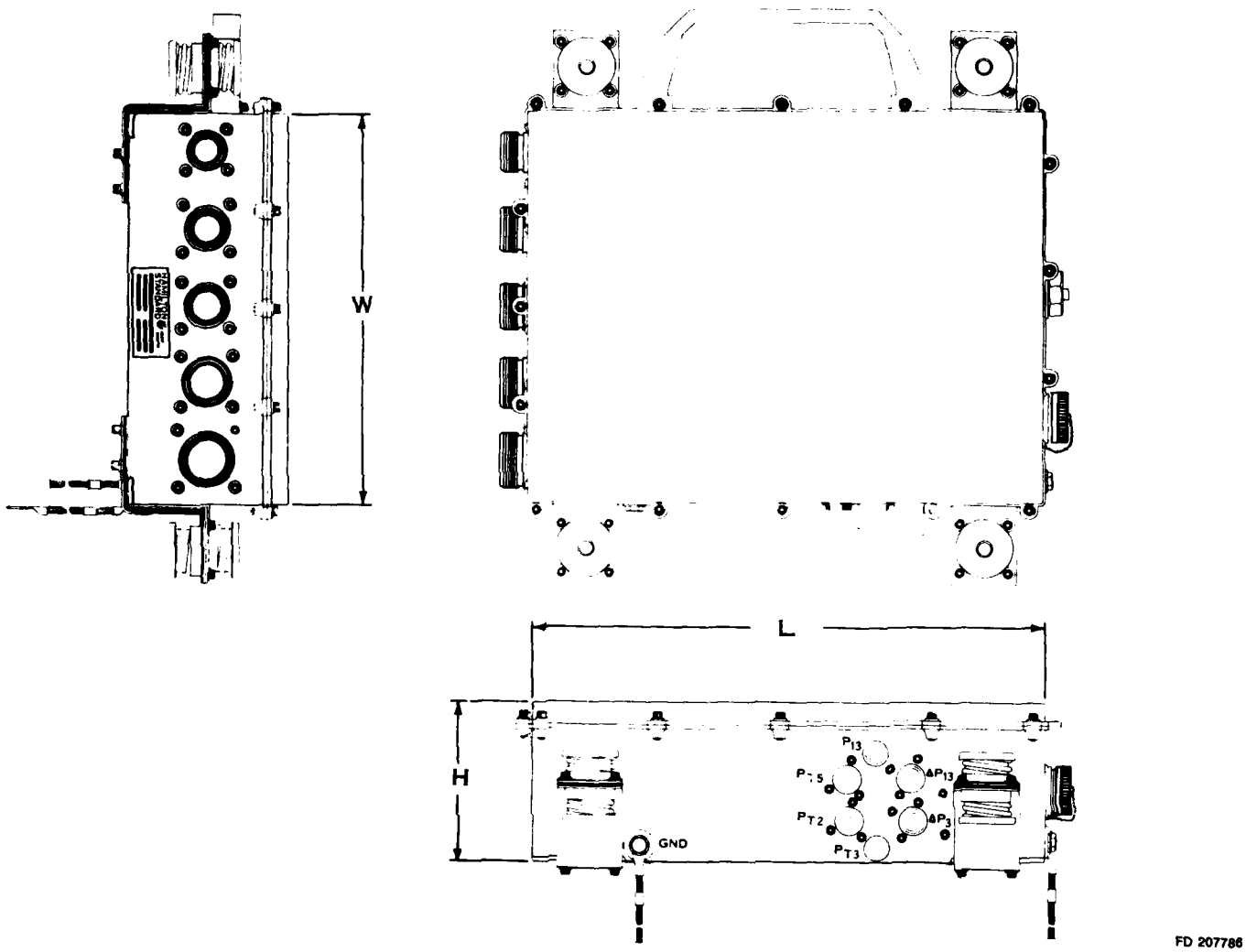


Figure 62. FAFTEEC Package Outline

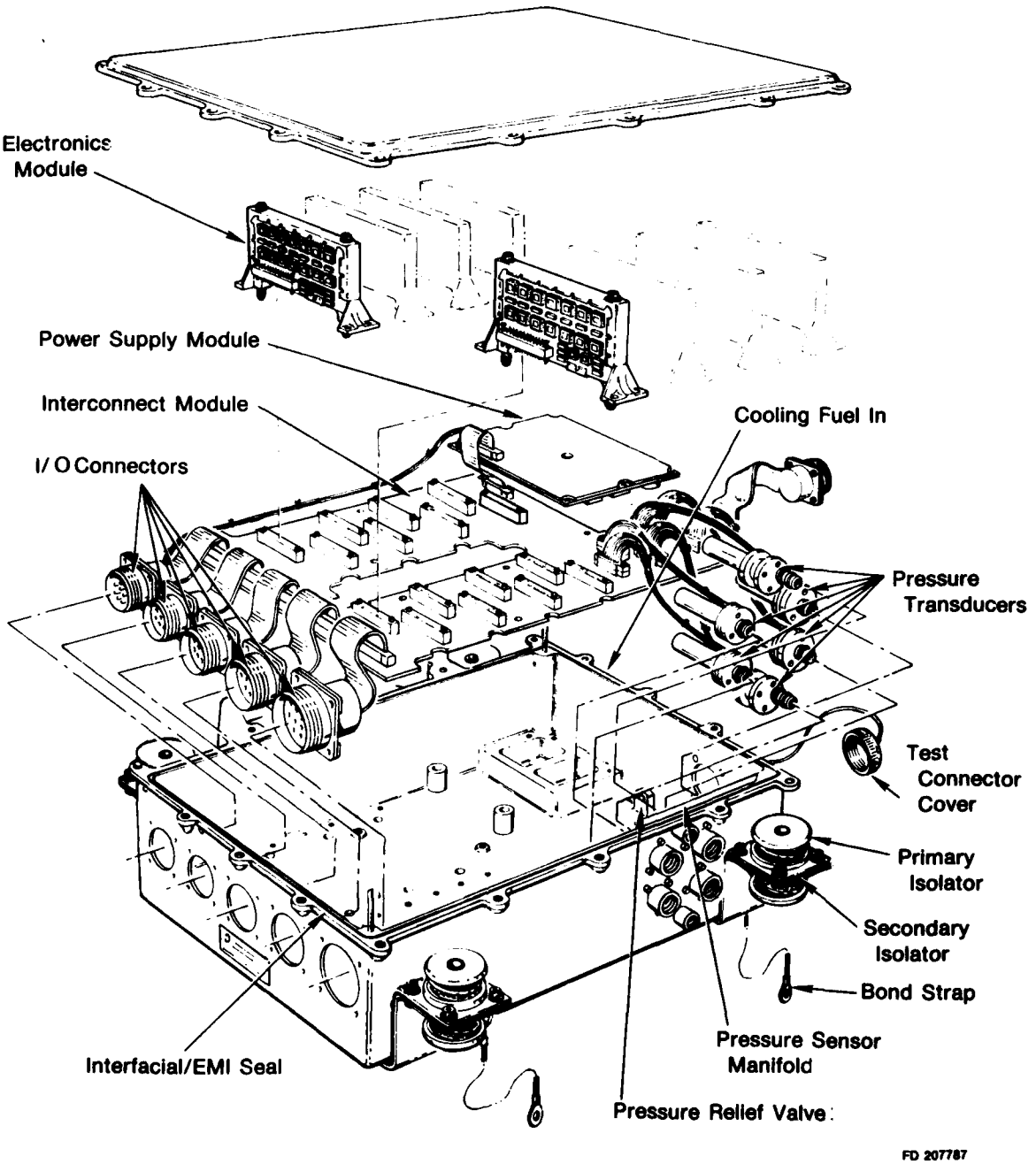


Figure 63. FAFTEEC Exploded View

TABLE 25. FAFTEEC PACKAGE CHARACTERISTICS

	Electronic Controller Configuration									
	A1		*A2*		*A3*		*A4*		*A5*	
Item	*A*	*B*	*A*	*B*	*A*	*B*	*A*	*B*	*A*	*B*
L (in.)	11.0	~	11.0	11.0	12.2	11.0	12.2	12.2	13.6	13.6
W (in.)	10.9	~	10.9	10.9	10.9	10.9	10.9	10.9	10.9	10.9
H (in.)	4.2	~	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
Volume ($in.^3$)	504	~	504	504	559	559	559	559	623	623
No. of I/O Conn	4	~	5	5	5	5	5	5	5	5
No. of Test Conn	1	~	1	1	1	1	1	1	1	1
Power (Watts)	28.9	~	28.8	28.3	36.5	28.9	35.9	35.9	69.8	69.8
Component Quantity	999	~	954	963	1070	943	1074	1074	1348	1348

TABLE 26. FAFTEEC WEIGHT BREAKDOWN

	Electronic Controller Configuration									
	A1		*A2*		*A3*		*A4*		*A5*	
Item	*A*	*B*	*A*	*B*	*A*	*B*	*A*	*B*	*A*	*B*
Housing	6.4	~	6.4	6.4	7.1	6.4	7.1	7.1	8.0	8.0
Interconnect Module	2.6	~	2.6	2.6	2.9	2.6	2.9	2.9	3.1	3.1
Electronic Modules	3.9	~	3.9	3.9	4.5	3.9	4.5	4.5	5.6	5.6
Power Supply Module	0.5	~	0.5	0.5	0.6	0.5	0.5	0.5	0.5	0.5
Pressure Transducers	1.2	~	0.6	0.8	1.2	1.2	1.2	1.2	1.2	1.2
Isolators	2.0	~	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0
Misc Hardware	0.5	~	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
Controller Weight (lbs)	17.1	~	16.5	16.7	18.8	17.1	18.7	18.7	20.9	20.9

Electronic Module

The configuration of a basic Electronic Module is shown with mounting platform and detail parts in Figure 64. The heart of this module is the alumina (AL_2O_3) circuit substrate with a multilayer thick film interconnect system. The Electronic Modules were designed to use leadless chip carriers to carry the active circuit chips. This electronic packaging approach provides size and weight advantages; good repairability and component replacement; preassembly testing and burn-in capability; package ruggedness; improved thermal dissipating properties; and improved reliability. Reliability is further enhanced by the capability of testing at both the component preassembly and post-assembly levels.

The alumina substrate in the Electronic Module is one standard size (3.0 in. × 4.5 in.). The base substrate is 0.062 in. thick 96 percent AL_2O_3 available from several manufacturers. Low substrate camber is required to obtain intimate contact between the substrate and LCC as well as the substrate and aluminum heat exchanger.

Electronic modules are mounted in pairs and clamped in place using a specially designed spring frame. Constructed of a phosphorous bronze material, the spring frame exerts only enough force on the ceramic substrate assembly to sufficiently secure it in the projected vibration environment, and to provide good heat transfer while minimizing the stresses in the ceramic itself. The spring frame slides over the two ceramic substrates and is held in place by two fasteners. An elastomeric heat transfer pad is molded to the back side of the ceramic substrate to optimize the thermal path from the ceramic substrate assembly to the module heat exchanger. The material hardness and pad size of the elastomer is designed to minimize the applied forces deflecting the ceramic substrate to a level consistant with the clamping forces of the spring retainer. An elastomeric material is used because with a minimum of pressure, it flows and fills the microsurface imperfections on the metal heat exchange surface with a resultant minimal thermal resistance.

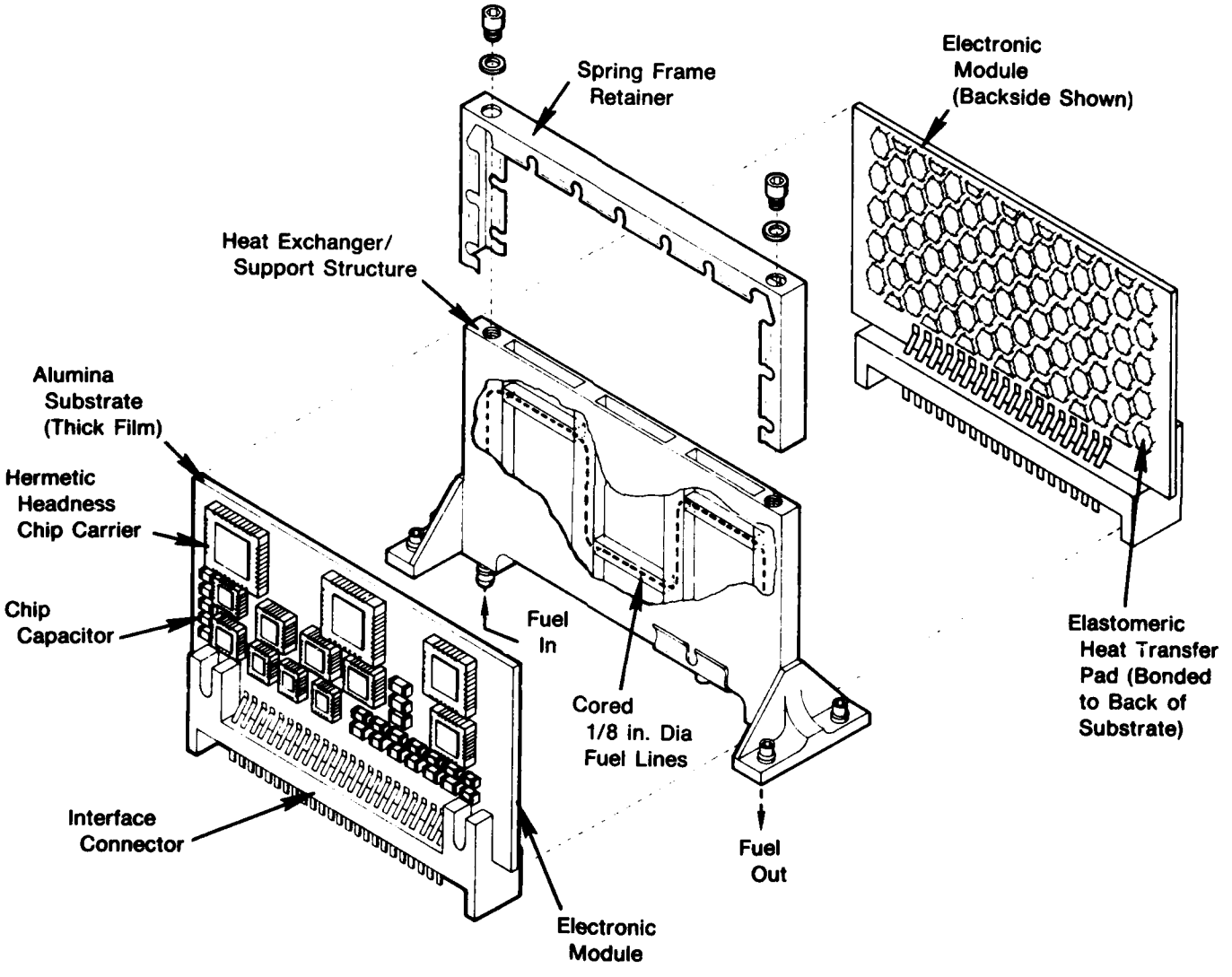


Figure 64. Electronic Modules With Coded Mounting Platform

TABLE 27. FAFTEEC MODULE POPULATION FOR FIVE SYSTEM CONFIGURATIONS

	Electronic Controller Configuration									
	A1		*A2*		*A3*		*A4*		*A5*	
Modules	*A*	*B*	*A*	*B*	*A*	*B*	*A*	*B*	*A*	*B*
Electronic Module	12	~	12	12	14	12	14	14	17	17
Sensor Electronic Module	2	~	2	2	2	2	2	2	2	2
Pressure Transducer	6	~	3	4	6	6	6	6	6	6
Power Supply Module	1	~	1	1	1	1	1	1	1	1
Interconnect Module	1	~	1	1	1	1	1	1	1	1

The module heat exchanger doubles as a module support structure. The basic supporting structure is a lightweight, cast aluminum heat exchanger with 1/8 in. diameter cored fuel passages. This structure provides the mechanical mounting accommodations used to secure the Electronic Module rigidly to the housing and connect it to the parallel fuel passages within, via two standard "O" ring sealed bosses.

Sensor Electronics Module

The Sensor Electronics Module uses the same design approach as the basic Electronic Module and contains all of the pressure sensor electronics.

Pressure Transducers

The Pressure Transducer design is similar to the Hamilton Standard miniature pressure transducer product line used in HSD engine mounted hardware. The transducers are mounted to the fuel cooled control housing and electrically interconnect to the adjacent Interconnect Module. The transducers utilize hard-wire harnessing and plug-in connectors which are equipped with jackscrews for ease of mating and separating without contact damage, while providing good mechanical retention. Severe engine control environments and strict accuracy requirements have limited the use of many types of pressure transducers whereas the vibrating cylinder type used in this design has demonstrated on-engine capability in a number of engine control applications.

Power Supply Modules

The Discrete Power Supply Module contains all the electronics associated with the power supply and LOD circuit. Conventional printed circuit board technology is utilized here because of the style of the power components presently available. A high performance polyimide laminate is used for the power supply module multilayer interconnect system. Electronic components are physically and thermally mounted to a metal heat sink and electrically attached to the printed circuit board. The heat sink is etched aluminum, coated with a dielectric material and laminated to the printed circuit board.

Interconnect Module

All of the individual submodules contained within the control are interconnected by the Interconnect Module, the heart of which is a polyimide multilayer board. The Electronic Modules and Sensor Electronic Modules plug directly into the Interconnect Module using two-piece connectors equipped with *Hypertac® contacts which feature low contact insertion force, low contact resistance and assured electrical continuity under shock and vibration. The pressure transducers have a hard-wire harness and Hypertac® connector which mates with a corresponding connector on the Interconnect board. A flexible molded cable soldered to the Interconnect Module is provisioned with a Hypertac® connector mating it to the Discrete power Supply Module. The I/O connector/cable assemblies include flexible molded cables terminated and potted to a severe environment resistant MIL-C-38999, series III, connector.

The alternator power and control lines are hard-wire twisted shielded triplets and twisted shielded pairs, respectively. These harnesses mate to the Power Supply Module through its own plug-in, Hypertac® connector.

Housing Description

The controller housing is a one-piece casting with stiffening as required to minimize deflections, and with an integral, forced fuel heat exchanger in the outer walls to cool the internal electronics. The housing material is an AMS 4218 (A356-T6) premium strength structural investment casting having a MIL-A-B625, type 1, anodize finish. Where required for electrical continuity and EMC closure, machined surfaces are conversion coated per MIL-C-5541 class 3. Gun drilled fuel passages, sealed with pin plugs, are strategically located to optimize the cooling of the electronic modules, power supply modules and sensors. Other housing features include internal mounting platforms for all modules, isolator mounting pads, fuel ports and raised cast letters for identifying all external interfaces. Also included are an integrally cast electrical bond lug, a sensor pneumatic manifold, and a handle for aiding installation and transportation. The sensor manifold is an integrally cast part of the housing and provides the sensor mounting platform, drilled pneumatic lines and external pressure port bosses, which are machined in accordance with MS 33649.

THERMAL DESIGN

Heat transfer to and from the exterior of the package is primarily by natural convection and radiation, with some effects of conduction though the mechanical interfaces. Cooling paths include radiation to and from the engine case and nacelle metal, as well as conduction through the mounting, plumbing and wiring interfaces. While these paths are mostly beneficial, that is they tend to cool the package further, in those instances where heat is added to the control, it is directed to the fuel sink through the housing and thus negligible heat is transferred to the components. Internal cooling encompasses all three modes of heat transfer; conduction, the most dominant of the three, is heavily utilized. Effective conductive cooling has been achieved with every module being directly tied to the central housing heat exchanger. Optimum thermal paths are attained by using individual, forced fuel, heat exchangers mated in parallel fuel paths with the housing heat exchanger. Also, the power supply module is supplemented with an aluminum alloy heat transfer plate mounted in direct contact with the main housing forced fuel heat exchanger. Components are strategically located to match the resultant thermal resistance with each component's power dissipation to minimize hot spots and maintain a close average temperature between components. The close proximity of the components to the fuel minimizes the thermal resistance, and consequently keeps the temperature rise from the component to the fuel low.

*Hypertac® is a trademark of Industrial Electronic Hardware Corporation

Power Dissipation

Total power dissipation for each system configuration is summarized in Table 25.

VIBRATION DESIGN

Isolation Design

The primary isolator is a low damped, low frequency system designed for maximum attenuation of vibration inputs at engine frequencies. The higher amplification at natural frequencies is acceptable since it is only experienced at startup and shutdown. The isolator is a steel spring with wire mesh construction. The spring proves most of the spring rate with some added by the wire mesh. The wire mesh, however, provides all of the damping.

The secondary isolator is a high damped, high frequency system for minimum amplification at resonance with agreeable attenuation at higher frequencies. It is a laminated spring steel construction with viscoelastic inner layers. The secondary isolator system is designed to work only in the X and Z axis to reduce complexity. The axial (Y-axis) inputs are normally only half those of the tangential (X-axis) and radial (Z-axis) input levels, therefore the benefits of a secondary isolation system in the Y-axis would be negligible. The secondary isolator frequency is selected between that of the external interfaces/plumbing and the engine blades for maximum effect. All other features are frequency tuned based upon their inherent capabilities. The electronic modules are supported in the center of the printed circuit assembly. The ceramic substrates are relatively rigid and have a flexural modulus several times greater than most plastics. The results are that very low deflections and low dynamic stresses are exerted on the components. In addition, the leadless chip carrier packages themselves are considerably more capable of withstanding vibration than dips because of the inherent stiffness of the package and its mounting.

FAFTEEC MAINTENANCE

The Full Authority Fault Tolerant EEC (FAFTEEC) has been designed to facilitate maintenance at all levels of activity. Modular design, extensive BITE self-test, EAROM fault storage, diagnostic program down loading capability, MIL-STD-1553B Avionics Data Bus Communications are part of the maintenance features incorporated into the FAFTEEC. The unit is designed for rapid maintenance at the various maintenance levels as outlined in the following sections.

On-Aircraft-Organizational Levels

(a) Maintainability Features

- Four bolt mounting at shock-mount fittings.
- Four or five electrical; three, four, or six pressure, and two fuel disconnects depending upon configuration.
- Keyed connectors to preclude incorrect connections.
- LRU interchangeability, no retrim required.
- Extensive self-test and system test to isolate at a greater than 90% confidence level all faults to itself or to a system component.

- Continuous health output information per channel.
- External fault flagging capability identifying applicable FAFTEEC redundant channel malfunction.
- EAROM nonvolatile storage memory for in-flight fault detection to storage.
- Fault information via MIL-STD-1553B Communications can assistcation and maintenance decisions.
- External test connector provides on-aircraft system test capability utilizing suitcase type test unit.
- No scheduled maintenance - There will be no scheduled maintenance for the FAFTEEC.

(b) Maintenance Procedures - on A/C

- Identify fault through EAROM interrogation and external fault flag indications.
- Remove/replace FAFTEEC
- Check-out utilizing EAROM interrogation and external fault flag indications.

(c) Personnel level - semi-skilled, one person

(d) Tools required - normal aircraft maintenance tools.

(e) Test equipment - on board A/C equipment for monitoring.

- Flight line tester for on-engine system test/diagnosis

Off-Aircraft Maintenance - Intermediate (Module Level Replacement)

(a) Maintainability Features:

- All modular assemblies interconnect through plug-type disconnects.
- External test connectors allow closed box functional test and fault isolation to the module level.
- Modular ATE test compatibility. Atlas language for fault isolation to board level to be provided.
- MIL-STD-1553B RT interfaces enable in-flight fault information retrieval.

Maintenance Procedures - Module Level

Maintenance tasks will consist of functional tests, fault verification and isolation to the module replacement level, and final acceptance tests prior to delivery to service pool area.

The external test connector, in addition to the signal and power input connectors, will permit fault isolation to the module level in a closed box configuration.

Normally all faulty boards will be replaced by repaired boards which have been environmentally screened.

SECTION 9

FAFTEEC COST-OF-OWNERSHIP

INTRODUCTION

The FAFTEEC cost of ownership was assessed by compiling costs associated with system ownership. These costs included system aquisition costs and weight, development costs, system life cycle costs, and cost savings associated with improved control system mission reliability and safety. Development costs were estimated based on the engine development costs projected for an advanced engine by the ATES Phase I studies and included engine development costs through flight test costs. Based on F100 historical data control, system development costs amount to 15% of engine development costs.

COMPILING SYSTEM COSTS AND WEIGHTS

The system cost and weights were compiled for each system and include all elements of the system as shown in Table 28. These system cost and weights were used to evaluate the impact of system redundancy and were also used for input to the life cycle cost study.

TABLE 28. ACQUISITION COST AND WEIGHT SUMMARIES

	Acquisition Cost — $K					*Weight — lb*				
System	*Total Sensor*	*Effector*	*Pumps*	*EEC*	*Total System*	*Sensors*	*Effectors*	*Pumps*	*EEC*	*Total System*
1	21.5	160.5	38	40	260	32.5	248.5	64	17.1	362.1
2	29.5	184.3	58	64	335.8	40.5	292.5	73	33.2	439.2
3	40	260.9	76	64	440.9	60.5	421	100	33.2	614.7
4	40	218	32	64	354	60.5	299	65	33.2	457.7
4A	40	218.2	32	63	353.2	60.5	299.5	65	33.2	458.2
5	40	218.2	32	66	356.2	60.5	299.5	65	35.9	460.9
6	40	218.2	32	70	360.2	60.5	299.5	65	37.4	462.4
6A	40	218	32	71	361	60.5	299	65	41.8	466.3
7 No BUC	42.1	175.7	32	70	319.8	64.5	255.5	65	49.8	434.8

The components required for each system were conceptually configured to allow cost and weight estimating. The electronic control costs and weights were estimated based on controller studies made during the Reliability Advancement for Electronic Engine Controllers (RAEEC) program. Acquisition costs and weights for the other system components were estimated based on experience gained from the F100 program and other control system studies such as the Full Authority Digital Electronic Control (FADEC) Program. The costs were scaled to reflect FAFTEEC system implementation and complexity differences.

LIFE CYCLE COST APPROACH

The procedure used to assess the cost-of-ownership for the FAFTEEC systems is summarized below. The FAFTEEC Life Cycle Cost (LCC) Methodology Flow Chart (Figure 65) shows the interrelationship between successive steps in the analysis and the mathematical models which were used.

Constant fleet size was used throughout the FAFTEEC life cycle cost modeling.

Output from the reliability model and engine maintainability data were input to the AFLC Logistics Support Cost (LSC) model to determine hardware support costs for each control system being considered. Each control system architecture was compared with the baseline in order to determine engine operating and support (O&S) cost differences. The LSC model is described later in this section.

The number of spare FAFTEEC system components, line replaceable units (LRU's), needed was determined based on maintenance requirements and MTBF by the LSC model. The acquisition cost of the FAFTEEC system was determined by summation of the cost of the system components.

The components required for each system were conceptually configured to allow cost and weight estimating to be made.

Development Costs were estimated based on the engine development cost projected for an advanced engine during the ATES Phase I studies and included engine development through flight test.

The major impact of the engine control system on airframe LCC is due to differences in weight between the individual configurations. Since the study was conducted using a "rubber" or scalable aircraft, engine weight differences affect aircraft size, gross weight, and cost. Weight sensitivity factors generated during the Advanced Technology Engine Studies (ATES) were used to determine the airframe (delta) LCC due to differences in engine weight. This program, under joint Navy/Air Force cognizance, is a technical evaluation to establish long-range plans for future airbreathing propulsion systems, and included an advanced fighter aircraft suitable for the FAFTEEC baseline. Engine cost information was supplied to the ATES airframe subcontractors for generation of the sensitivity factors in Customer Computer Deck (CCD) 1165, described later in this section.

LOGISTICS SUPPORT COST (LSC) MODEL

The LSC model is an analytical accounting model used to estimate unscheduled maintenance costs. The model addresses the support elements shown in Table 29. Cost, reliability, repairability, and maintenance parameters are input for each engine component considered.

Equations 1 through 10, with a description of each input parameter required to exercise the mode, are presented in Figures 66 through 73.

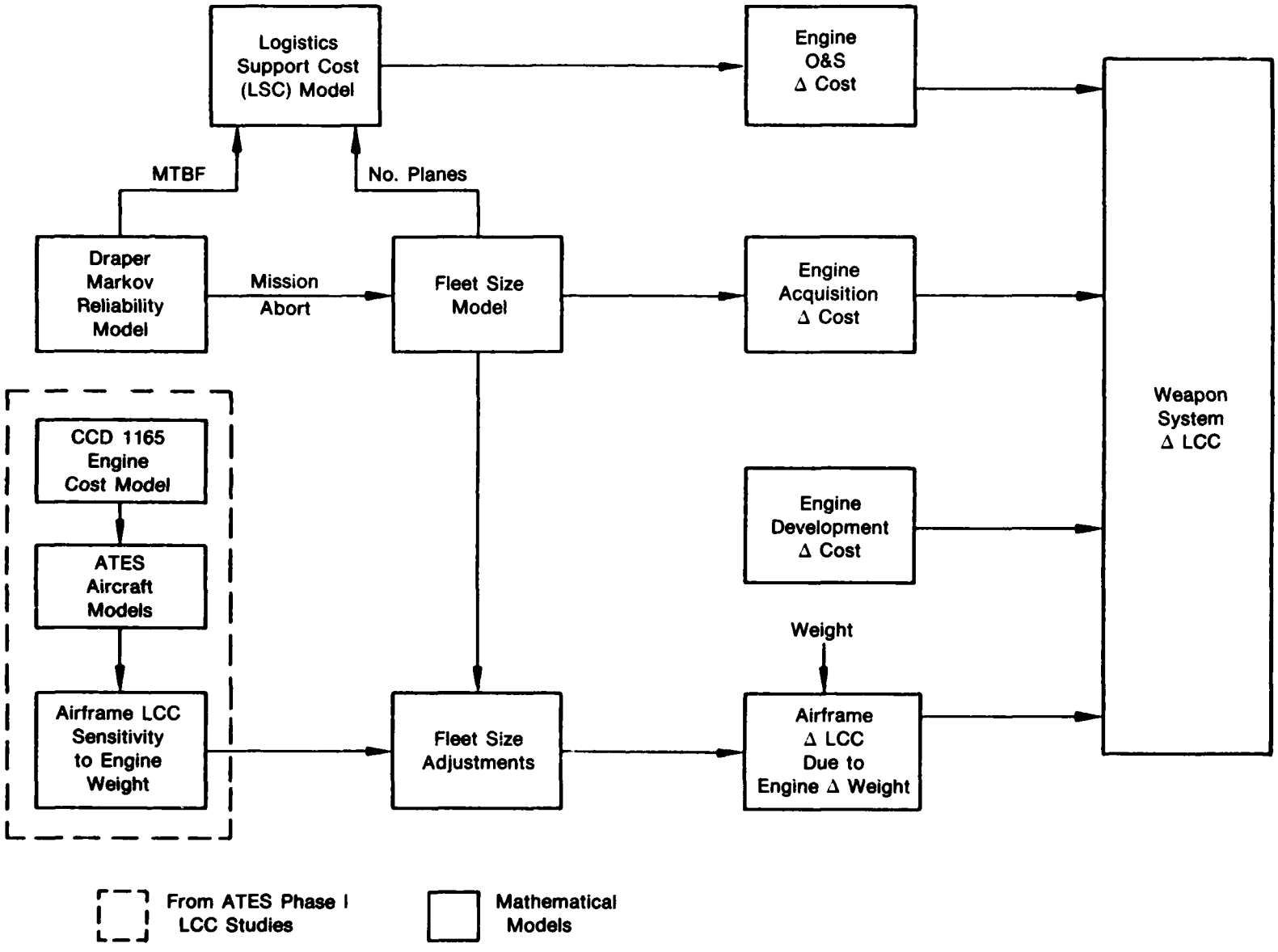


Figure 65. FAFTEEC Methodology Flow Chart

TABLE 29. LOGISTICS SUPPORT COST MODEL

Equation	*Cost Element*	*Drivers*
1	Pipeline Spares	MTBF, Cost, Flight Hours
2	On-Equipment Maintenance	MTBF, Flight Hours, Labor Rate
3	Off-Equipment Maintenance	MTBF, Flight Hours, NRTS, Labor Rates
4	Inventory Management	Parts Count, Number of Bases
5	Support Equipment	MTBF, Flight Hours, Repair Time
6	Personnel Training	MTBF, Flight Hours, Repair Time
7	Technical Data	MTBF, Flight Hours, No. Pages
8	Facilities	Cost, Number of Bases
9	Fuel	Fuel Cost, gph, Flight Hours
10	Spare Egines	MTBF, Cost, Flight Hours

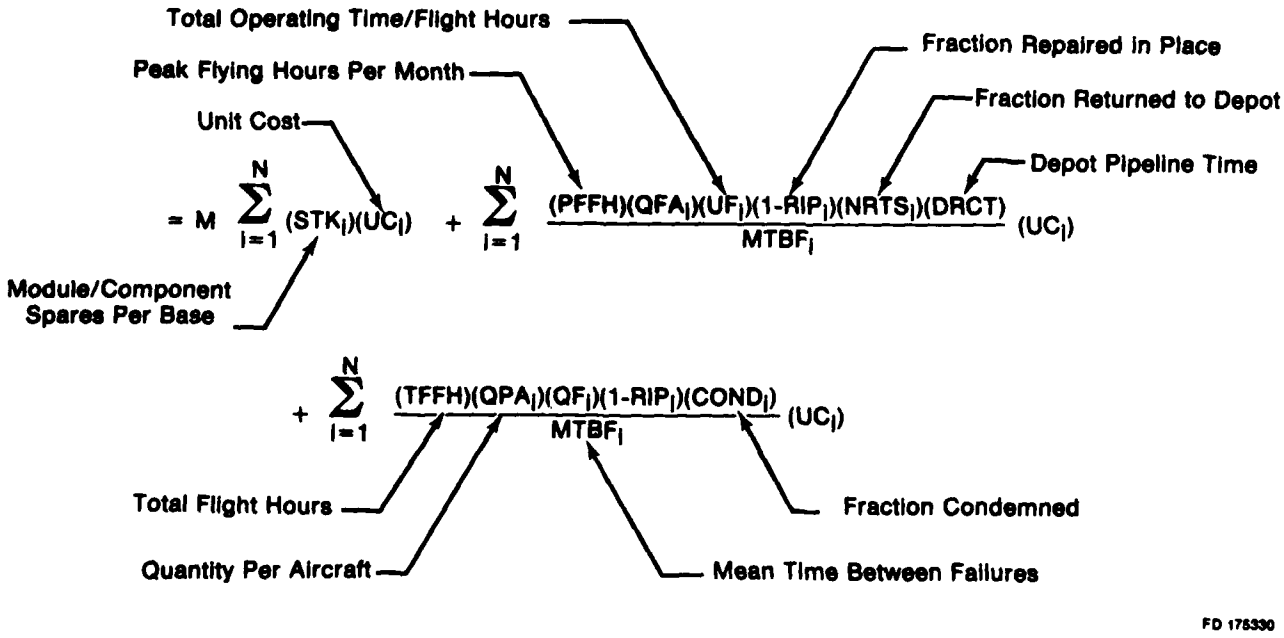


Figure 66. Equation 1: Pipeline Squares

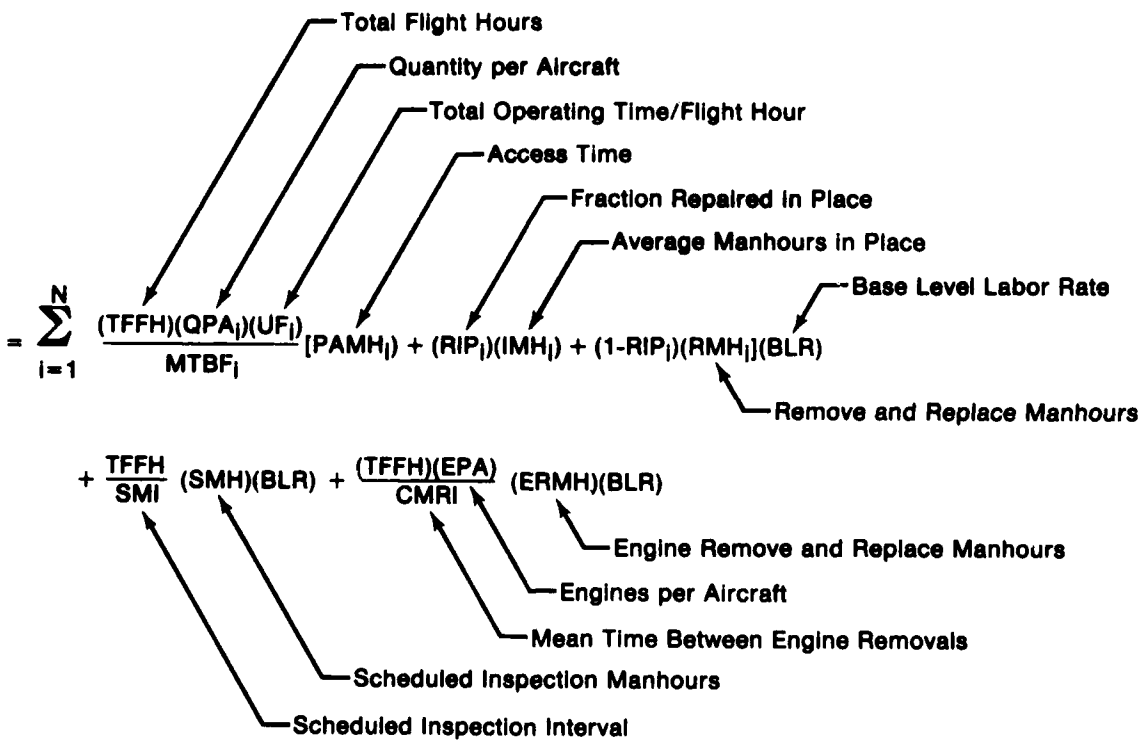


Figure 67. Equation 2: On-Equipment Maintenance

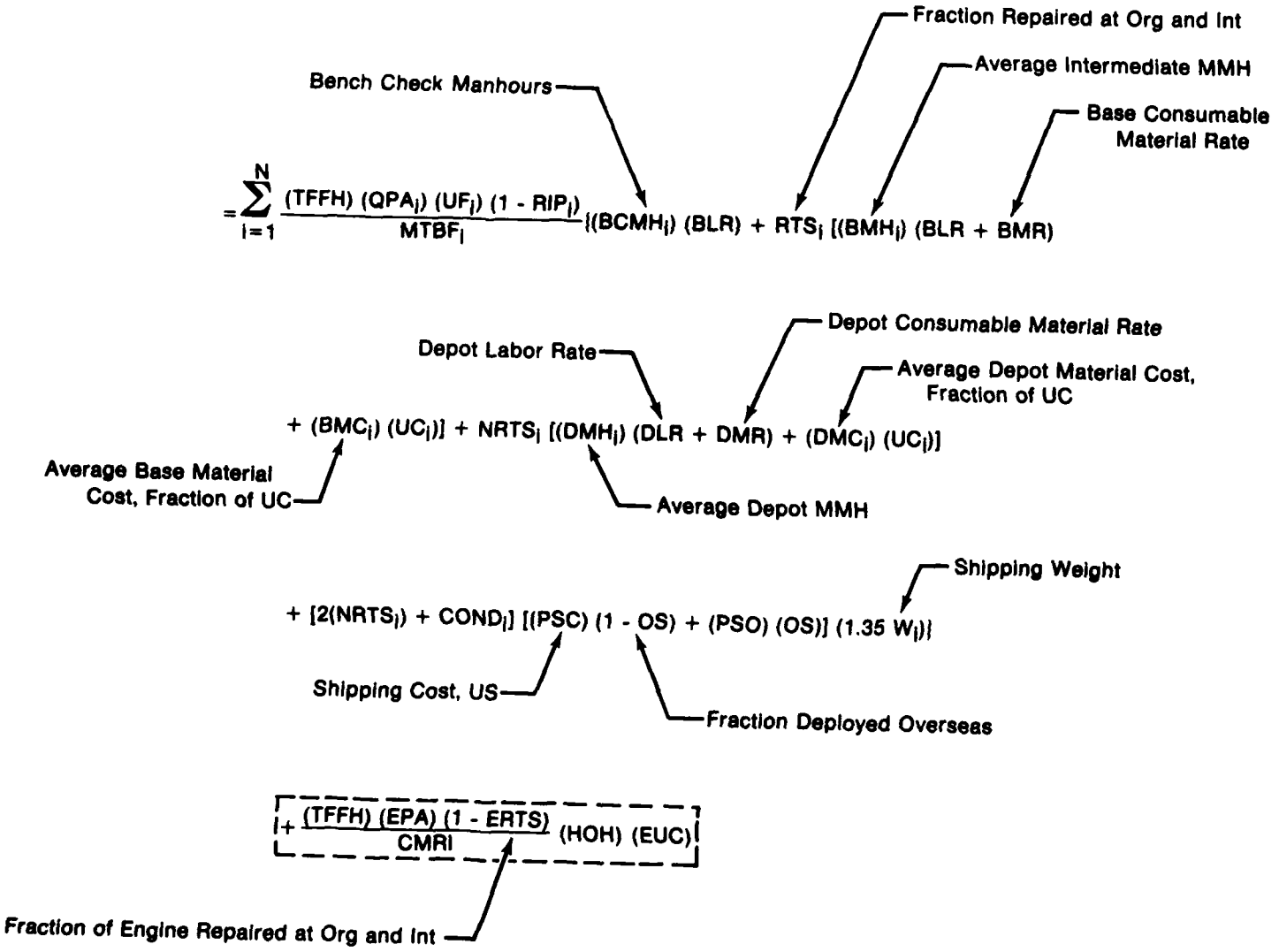


Figure 68. Equation 3: Off-Equipment Maintenance

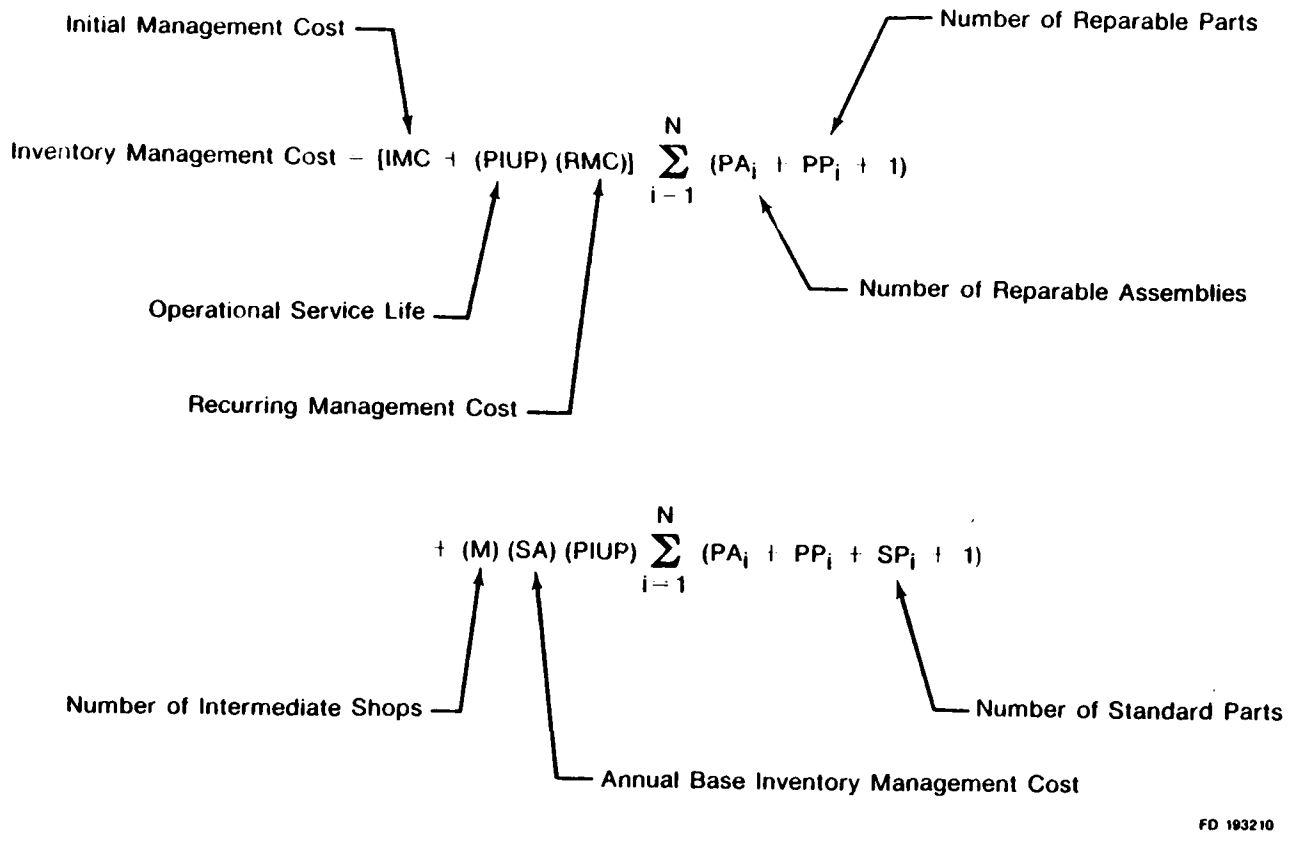


Figure 69. Equation 4: Inventory Management Cost

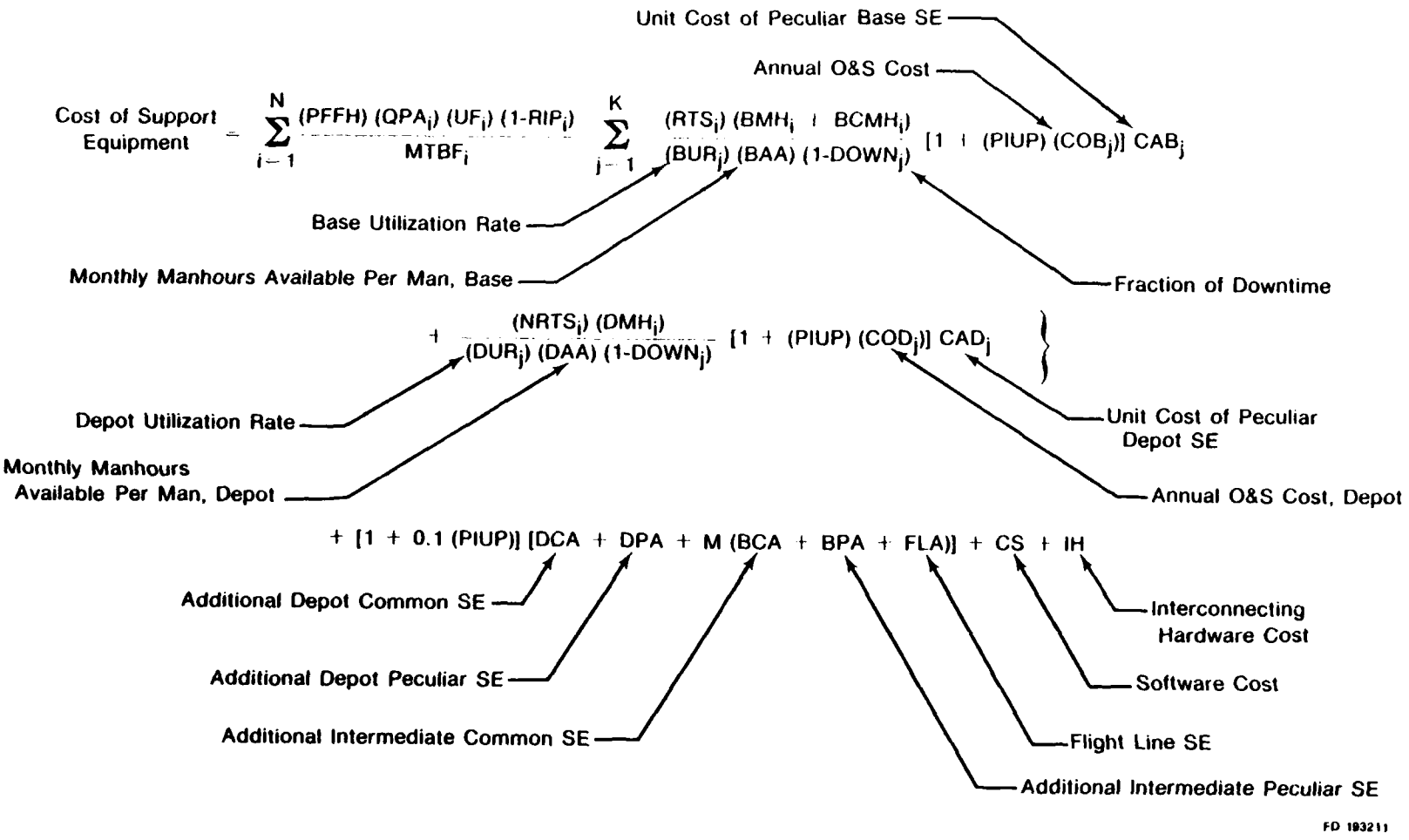


Figure 70. Equation 5: Cost of Support Equipment

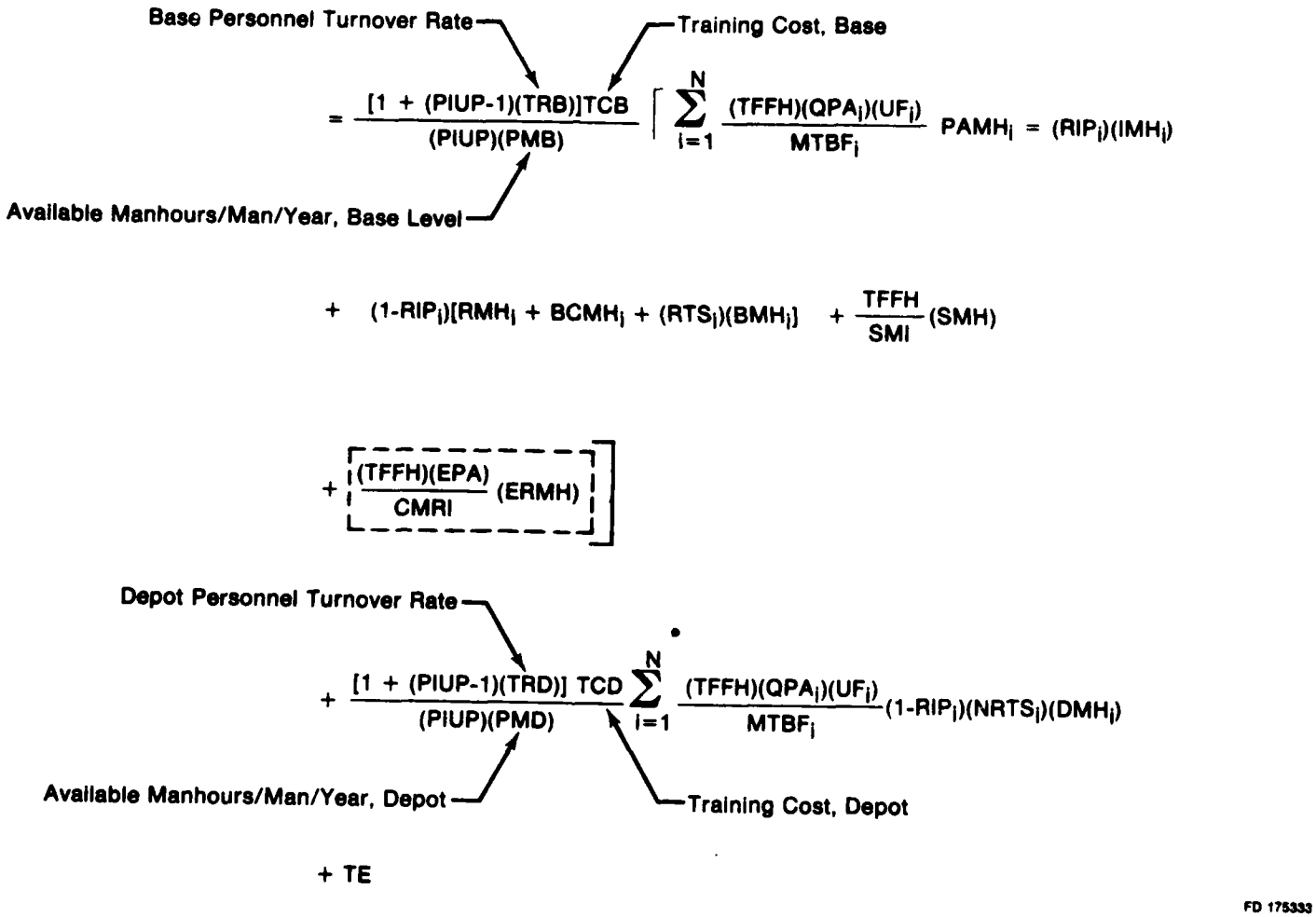
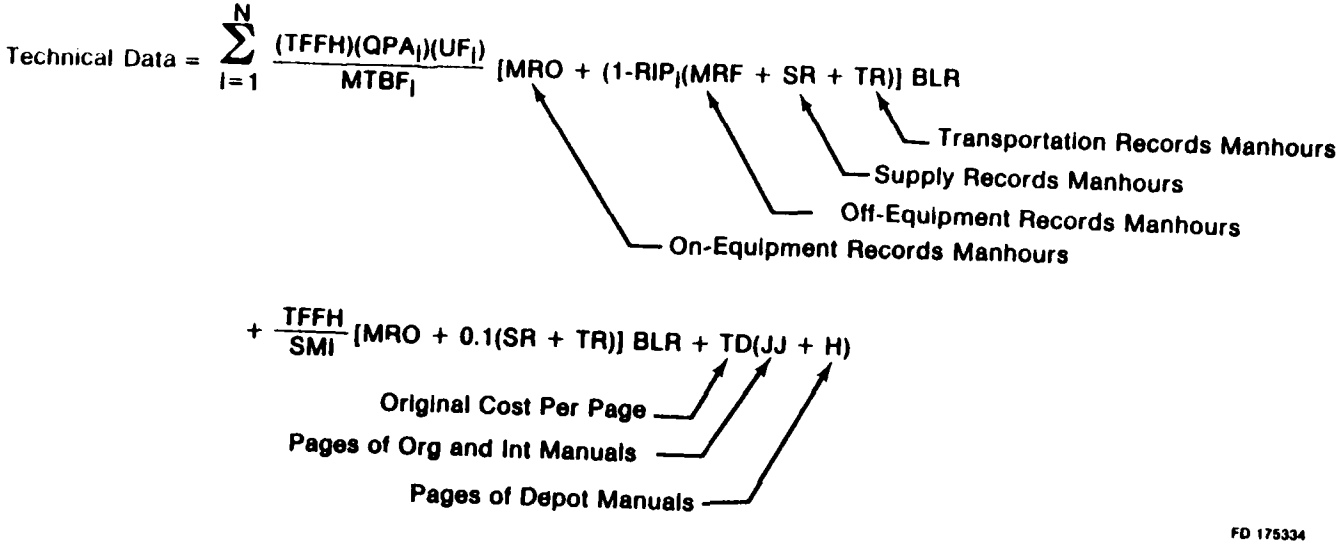


Figure 71. Equation 6: Personnel Training



Equation 7: Technical Data

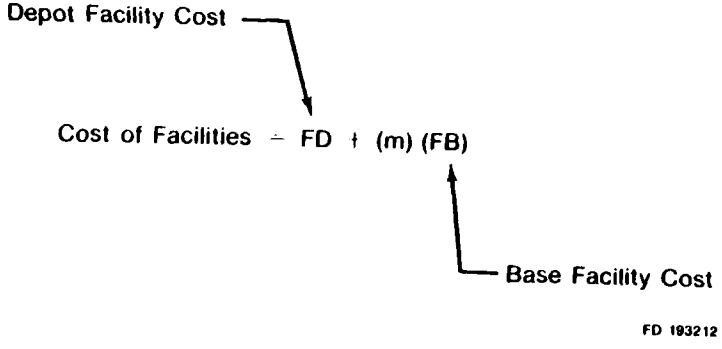
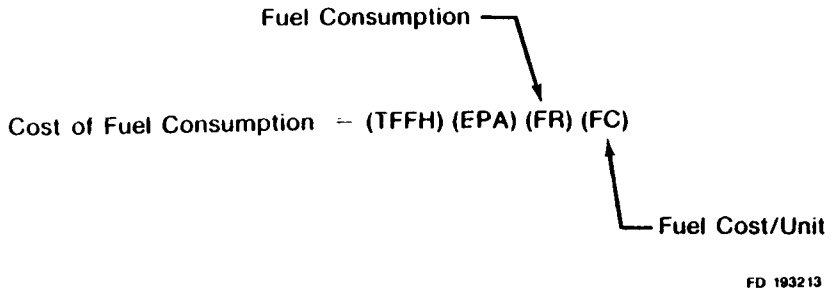


Figure 72. Equation 8: Cost of Facilities



Equation 9: Cost of Fuel Consumption

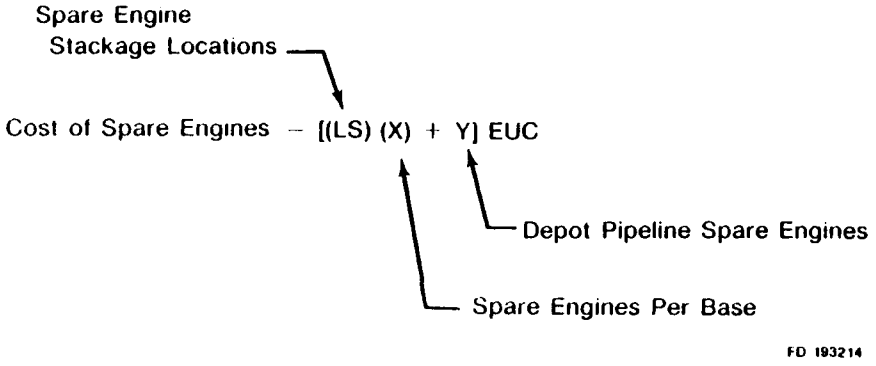


Figure 73. Equation 10: Cost of Spare Engines

CCD 1165 COST MODEL

General

CCD 1165 calculates engine development costs, engine acquisition costs, engine maintenance costs, and component improvement program (after qualification) costs for the P&WA JT69 engine family. Each type of cost is printed out separately. All costs are in 1980 dollars. These four elements include all of the costs directly attributable to the engines in aircraft system life cycle costs.

The program is parametric in nature and uses Cost Estimating Relationships (CER's) which are a function of input parameters to generate these costs for the P&WA JT69 engine family. Because of the wide range of JT69 engine configurations covered by this program, there has been some sacrifice of detail. The intent of CCD 1165 is to provide cost information which can be used in engine screening studies for advanced aircraft systems. All elements are calculated in accordance with standards specified by the Joint AF/Industry Turbine Engine Life Cycle Cost Model. Per these standards, all quoted costs represent the cost to the Government excluding P&WA profit.

LCC Ground Rules

The scenario chosen for the FAFTEEC cost-of-ownership study is an Advanced Tactical Attack Manned System (ATAMS) aircraft with an IOC date of 1990. Baseline aircraft and engine quantities, missions, and utilization are the same as those used in the current Advanced Technology Engine Studies (ATES) contract, which is under joint Navy/Air Force cognizance.

The weapons system life cycle is 15 years per operational aircraft consisting of a 9-yr buildup, 6 years of full force operation, and a 9-yr phaseout. The aircraft utilization rate over this cycle averages 300 flight hours per year with an attrition rate of 6.0 aircraft per hundred thousand flight hours. The weapons system force structure consists of 24 aircraft per squadron, three squadrons per wing, one wing per base, and 9 bases for a Primary Aircraft Authorization (PAA) of 648 aircraft. Based on a 10 percent ratio of pipeline spare aircraft to PAA aircraft, and also on the aircraft attrition and utilization rates, the total buy is 888 aircraft including 65 pipeline and 175 attrition replacement aircraft. Based on a 20 percent engine spares requirement, there are 1018 total engines required to support a single engine aircraft, and 2035 for a twin engine aircraft, both of which were considered in this study. These and other ground rules are summarized in Table 30.

TABLE 30. LCC GROUND RULES

	Single Engine Aircraft	*Twin Engine Aircraft*
Life Cycle Per Aircraft	15 yr	15 yr
Aircraft Flight Hours Per Year	300	300
Total Aircraft Flight Hours	2.916×10^6	2.916×10^6
Total Engine Flight Hours	2.916×10^6	5.832×10^6
Operational Aircraft	648	648
Pipeline Spare Aircraft	65	65
Attrition Replacement Aircraft	175	175
Total Aircraft Produced	888	888
Installed Engines	888	1776
Pipeline Spare Engines	130	259
Total Engines Produced	1018	2035
Maximum Aircraft Production Rate	12/Month	12/Month
Number of Flight Test Aircraft	12	12
Baseline Fuel Cost/Gallon	$1.80	$1.80
Dollars	FY 1980	FY 1980

BASELINE WEAPON SYSTEM LIFE CYCLE COST

ATES LCC For Twin Engine ATAMS

Results from Phase I of the ATES study were used to generate the baseline weapon system LCC for the FAFTEEC control study. The LCC for a twin engine Advanced Tactical Attack Manned System (ATAMS) aircraft is $29.231 billion for 648 operational aircraft, each flying 15 years from date of delivery.

Adjusted LCC for Single Engine ATAMS

The ATES study LCC for a twin engine aircraft was adjusted for a single engine configuration with the same total thrust as the twin engine aircraft, in order to keep aircraft size, mission and capability constant. Airframe and avionics costs remain unchanged and engine R&D, acquisition and O&S costs were scaled for the size increase using historical cost scaling relationships. A system LCC of $28.568 billion was estimated.

The control system development cost were estimated based on the engine development cost projected for an advanced engine during the ATES Phase I studies under Section 9. Historical data on development costs show control system cost to be 15 percent of the total engine development cost. Therefore the total control system development cost for the baseline system is projected to be $117 million based on a total engine development and flight test cost of $778 million. This can then be broken down by percentage of total control system cost for each group of components for the baseline system including vendor development cost for components and P&WA development cost for system integration and development components used during engine test and flight test. The percentages used are based on historical data for gas turbine control system. Table 31 lists the development costs for component groups for the various systems.

TABLE 31. DEVELOPMENT COSTS FOR FAFTEEC COMPONENT GROUP

Total Engine Development Cost = $778M
Total Control System Development Cost = $117M

Component Group	*% of Total*	*Systems 1,2,3*	*Systems 4,5,6*	*System 7*
Electronic Control	11	13M	13M	13M
Fuel Valves	9	10	10	10
Back-Up Control	17	20	20	0
Pumps	12	14	4	4
Actuation and Miscellaneous	17	20	20	20
P&WA Development	34	40	35	25
Totals	100	117M	102M	82M

LCC Sensitivity to Engine Weight

ATES Phase I trade studies for a twin engine aircraft show that 1% in engine δ weight causes a 0.07% change in weapon system LCC. This converts to +1.0 lb engine weight causing +$1.11 million change in weapon system LCC for the twin engine aircraft.

For the single engine configuration, weight and price adjustments for the larger engine result in a trade factor of $0.624 million per pound of engine weight.

CONTROL SYSTEM O&S COST USING LCC MODEL

Use of LSC Model for Control System Cost Resolution

The baseline weapon system LCC used for the study is based on parametric equations which do not provide the sensitivity or resolution required to examine small changes in control system characteristics.

For this reason, the AFLC Logistics Support Cost (LSC) model was used to determine operating and support cost differences between the baseline FAFTEEC system and the various configurations being evaluated.

LSC Model Input

Input for the model included reliability, cost, weight and maintenance data for each major control system component for the various systems. The input data for the baseline system is shown in Table 32, with complete input data for all of the FAFTEEC systems in Section 9.

TABLE 32. FAFTEEC INPUT PARAMETERS — CONTROL SYSTEM 1 BASELINE CONTROL SYSTEM

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	300	0.5	37037	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	11000	9.0	22831	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	700	1.0	76923	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	4000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1 00	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	600	0.5	25641	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	300	0.5	37037	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	3500	3.0	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	3500	3.0	32258	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	30000	30.0	7610	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.08
FIGV	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	5700	13.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	5000	10.0	145000	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	14000	15.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	13000	10.0	145000	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	900	1.5	83333	1.0	0	0	0	2.0	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	28000	27.0	3000	1.0	0	0	0	6.9	4.8	80	20	9.0	2.0	0.12	0.08
Aug Pump	10000	16.0	7042	1.0	0	0	0	6.8	4.8	80	20	12.0	2.5	0.02	0.02
Hyd Pump	8000	16.0	10000	1.0	0	0	0	6.8	2.5	80	20	10.0	2.5	0.08	0.05
GG Ign (2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer	39900	17.1	5000	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	2800	7.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.03
Cables	8000	25.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	12500	25.0	138889	1.0	15	1.0	100	2.0	0.5	—	—	—	—	—	—

O&S Costs for FAFTEEC Configurations

The absolute costs for the baseline system are shown in Table 33. It should be pointed out that these costs are included in the weapon system costs. All of the control systems had O&S costs above the baseline system. This is mostly due to component redundancies that outweighed individual increases in mean time between failure (MTBF) for other components. The LCC cost for all systems are shown in Table 34.

TABLE 33. ABSOLUTE BASELINE COSTS

	Dev. Costs	*Acquisition Costs*	*Pipeline Spares*	*Engine Maintenance & Inv. Mgt.*	*Total O&S*	*Total LCC Costs*
Single Engine Aircraft	117M	259	10	17	27	430
Control System Weight ≈344 lb						

COST OF OWNERSHIP RESULTS

The results shown in Figure 74 illustrate that the significant driver for the Weapon System LCC is acquisition cost due to control system redundancy. The increased O&S costs for the various systems range from 9 to 16% of the total LCC increase. None of the systems evaluated cause more than a 1.4% increase in total weapon system life cycle costs for a single engine aircraft. The life cycle cost results show no savings due to a higher reliability control system, however the life cycle cost analysis does not include costs attributed to loss of aircraft due to low mission reliability or costs due to reduced fleet size requirements. These areas will be treated in the following section as part of the cost-of-ownership.

MISSION ABORT COST SIGNIFICANCE

The basic Life Cycle Cost (LCC) Analysis does not consider the cost impact of improved mission reliability since the reliability input to the life cycle cost deck is maintenance reliability or Mean Time Between Failure (MBTF). In an effort to quantify the cost effect of mission reliability a cost was compiled for loss of aircraft due to mission abort.

This analysis was done by making a comparison of the baseline system with an abort rate of 700 per million operating hours and an enhanced dual system such as system 7 with a coverage of 0.999 which has a mission reliability of 0.23 failure per million operating hours. In this case it was assumed that the dual system with such high mission reliability would not require a back-up control. Therefore, the loss of the electronic control system would normally result in a loss of aircraft. This compares to an estimated loss of 1 of a hundred aircraft due to failure of the baseline to successfully transfer from the baseline system to the hydromechanical back-up system when the baseline electronic control fails. As indicated in Table 35 the baseline system contributes to a $500 million loss in aircraft which would not occur with an enhanced dual system without BUC.

This mission reliability cost may now be compared to the total life cycle cost of the system. The savings due to decreased loss rate of aircraft due to increased controller reliability could potentially offset the added life cycle cost of the redundant system and actually result in a savings in overall system cost-of-ownership.

TABLE 34. FAFTEEC CONTROL SYSTEM ΔLCC (1980$M) SINGLE ENGINE AIRCRAFT

Control System	Total Acquisition ΔCost	Development ΔCost	Control System O&S ΔCost: Pipeline Spares	Control System O&S ΔCost: Engine Maintenance $ Inv. Mgt.	Control System O&S ΔCost: Total O&S ΔCost	Weapon System ΔCost Due To Control System ΔWt	Total ΔLCC	Percent Increase In Weapon System LCC*
1			Baseline System				+0	+0
2	94.3	—	14.7	6.2	20.9	74.3	189.5	0.7
3	195.2	—	21.5	12.9	34.4	164.4	394.0	1.4
4	107.0	10	21.4	7.8	29.2	78.0	204	0.7
4A	99.8	10	21.3	7.6	28.9	78.0	197	0.7
5	117.1	10	21.9	8.9	30.8	84.2	222	0.8
6	99.8	10	21.7	9.6	31.3	84.2	205	0.8
6A	93.7	10	21.8	10.5	32.3	81.1	197	0.7
7	58.8	35	21	1.5	22.5	55	95	0.4

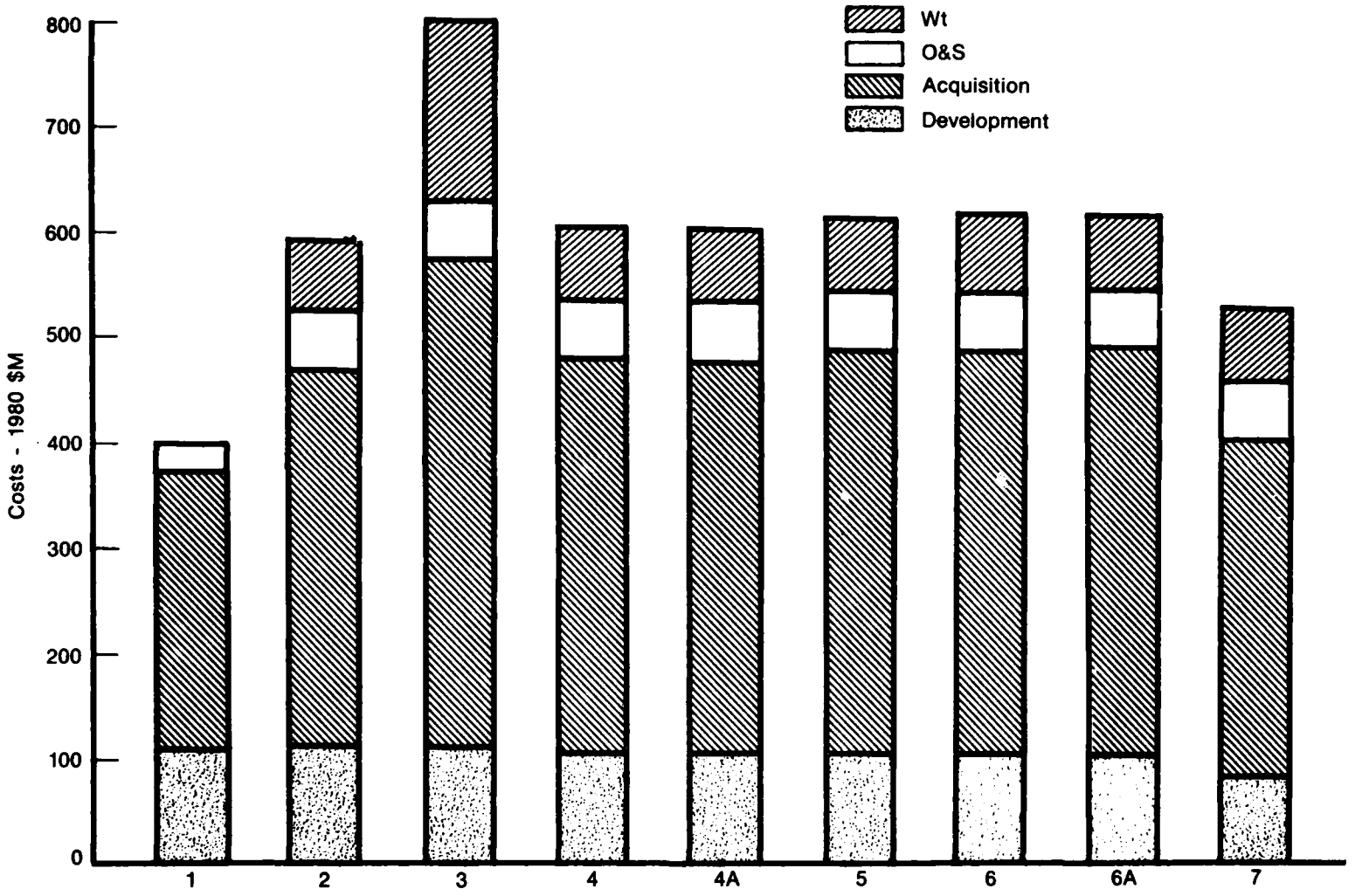


Figure 74. Life Cycle Cost Results

TABLE 35. MISSION ABORT SIGNIFICANCE

Baseline System	
700 Aborts/M Hours	
Assume 1% Cause A/C Loss	7 Aircraft/M Hours
In 5M Operating Hours	35 Aircraft = $525M
Enhanced Dual System	
0.23 Aborts/M Hours	
Assume All Cause Loss of A/C	0.23 Aircraft/M Hours
In 5M Flight Hours	1.1 A/C = $16M
Total Savings ≈ $500M	

FLEET SIZING

A preliminary analysis of the effect of redundant engine control systems on fleet size was completed using the Air Force memo on "Cost Analysis for Improved Engine Control Systems."

The parameter which relates FAFTEEC abort rate to fleet size is the probability of mission success. In order to calculate mission success, an average mission time was set at two hours. The first half of a mission is spent getting to the combat zone and in engagement. The second half is spent returning to base and loitering before landing. The flying time in the second half of a mission is not used in calculating the probability of mission success as the primary mission has been completed and cannot be aborted.

Once the fleet sizing parameters were chosen, an initial number of airplanes was calculated. Keeping all the parameters constant, except for the probability of mission success, a comparison was made of the results when using the reliability of a baseline control system and an enhanced dual redundant control system. While fleet size differnces are small, on the order of 6 to 7 aircraft, this fleet size increment is significant when compared to the cost increment due to redundancy in the control system. An LSC of 6 to 7 aircraft is in the vicinity of $300 million which is comparable to the entire life cycle cost increment of the redundant control systems.

SECTION 10

FAFTEEC STUDY RESULTS

The FAFTEEC study evaluated several alternate configurations for gas turbine control systems. The primary difference between these systems was the level or degree of redundancy used in achieving high mission reliability. The results of Section 7, System Reliability Modeling, indicate that there are no components where adequate reliability can be achieved by a simplex or single string design. Simplex technology would require an average improvement in component reliabilities by a factor of 1,000 to 10,000 to meet program goals. This is deemed to be impractical or impossible. Several alternative designs, using redundancy in differing degrees were modeled and evaluated to determine system mission reliability, maintenance reliability (MTBF), acquisition cost, weight, and life cycle cost. Each of the alternative designs can now be compared using the results of this evaluation process. Table 36 summarizes the primary features of each of the alternate designs.

TABLE 36. FAFTEEC CANDIDATE CONTROL SYSTEMS

System	*Sensors*	*Computer*	*Output I/F*	*Servovalve*	*Actuator*	*Pumps*
System 1	Single	Single	Single	Single	Single	Single
System 2	Shared/Dedicated	Dual	Dual	Single/Dual[1]	Single/Dual[1]	Dual-Fuel Single/Hyd
	0.99	0.95	1.0	1.0	1.0	1.0
System 3	Dual	Dual	Dual	Dual	Dual	Dual
	0.99	0.95	1.0	1.0	1.0	1.0
System 4	Dual	Dual	Dual	Dual	Dual	Dual
	0.99	0.95	1.0	1.0	1.0	1.0
System 4A[2]	Dual	Dual	Dual	Dual	Dual	Dual
	0.99	0.90	1.0	1.0	1.0	1.0
System 5	Dual	Triplex	Dual	Dual	Dual	Dual
	0.99	1.0	1.0	1.0	1.0	1.0
System 6	Dual	Dual/Dual	Dual	Dual	Dual	Dual
	0.99	1.0	1.0	1.0	1.0	1.0
System 6A	Dual	Dual/Dual Microcomp.	Dual	Dual	Dual	Dual
	0.99	1.0	1.0	1.0	1.0	1.0
System 7	Dual	Triplex or	Dual	Dual	Dual	Dual
	1.0	Dual/Dual	1.0	1.0	1.0	1.0

[1]Dual in the areas where a failure causes a transfer to HMBUC
[2]Same as System 4 except computers are not cross strapped
Note: All 1.0 numbers represent coverage values.

Systems 1, 2, and 3 employ simplex actuation technology which is essentially unchanged from current gas turbine engine control. System 4 through 8 employ dual actuation and pumping technology. That is, the actuation and pumping designs were optimized to exploit the advantages of dual system design. This entails actuation designs and pumping concepts which are different than the existing simplex actuators which will provide considerable benefits in the system cost, weight, MTBF, and mission reliability over the current technology designs.

MISSION RELIABILITY

The mission reliability and transfer to hydromechanical back-up control reliability for each system were discussed in detail in Section 7. The results are summarized in Figures 75 and 76. The transfer to HBUC reliability is improved significantly in all the redundant systems when compared to the baseline. Systems 5 and 6 meet the minimum acceptable goal of 2.5 per million, however, they fall short of the desired goal of 0.25 per million. This goal can only be met by an enhanced dual system such as System 7 where 100 percent first failure coverages are achieved by selective redundancy, analytic techniques and improved fault self-detection for sensors. The mission reliability is also significantly improved by all redundant systems. The minimum goal of 2.5 is met by systems 3, 4, 5 and 6; however, the desired goal of 0.25 is again only met by System 7.

In considering the results depicted in both Figures 75 and 76 it should be noted that once redundant components are added to a system so that the resources or means of tolerating a fault are present, then the strongest driver limiting reliability is the coverage value. The resources to tolerate a fault are of no use if the fault's presence is undetected or its source indeterminant.

MEAN TIME BETWEEN FAILURE (MTBF)

When the redundant systems are compared to the baseline single string system there is a decrease in system MTBF. The system MTBF is a function of system parts count. This penalty in mean time between failure purchases a thousand fold increase in mission reliabilities. The MTBF predicted for all the digital electronic control systems was significantly better than that demonstrated by current hydromechanical systems. Figure 77 summarizes the projected MTBF numbers for all of the alternate designs and contrasts them with current hydromechanical control experience.

SYSTEM COST AND WEIGHT

The initial approach taken in the study was to replicate system components where required to improve mission reliability. The technique was then extended to full replication in system 3. This straightforward replication increased cost and weight of the system to an excessive level. An evaluation of the technology being used was then made. In several areas such as fuel pumping and actuation, redundant assemblies or subsystems were being used in an inefficient fashion. The system was then reconfigured to utilize components in an optimized fashion and to introduce the direct drive valves as the actuator interface. The results of these changes are shown by Figure 78. If the cost and weight of the BUC are eliminated as was done in System 7 then the FAFTEEC control increases system cost and weight by only 20 percent.

SYSTEM OVERHEAD

The term "overhead" is sometimes defined as the additional items required by redundant systems such as voter circuitry, line monitors, additional modules/channels. The impact on reliability and cost of these overhead elements were evaluated during the evaluation phase of the program. As was pointed out in Figure 77 and Figure 78 the addition of redundant parts using conventional gas turbine control components, as was done with System 2 and 3, did have a negative effect on system cost and weight. This was the reason for investigating alternative architecture and technologies for the system components. After reconfiguring the system architecture as was accomplished for System 4, Advanced Dual Control System, the impact was significantly reduced, and in fact as was stated in the preceeding paragraph, the increase in mission reliability with the redundant system would reduce the overall life-cycle-cost of the system.

The issue of software overhead associated with redundant electronic controls was also addressed and is discussed in the following paragraph.

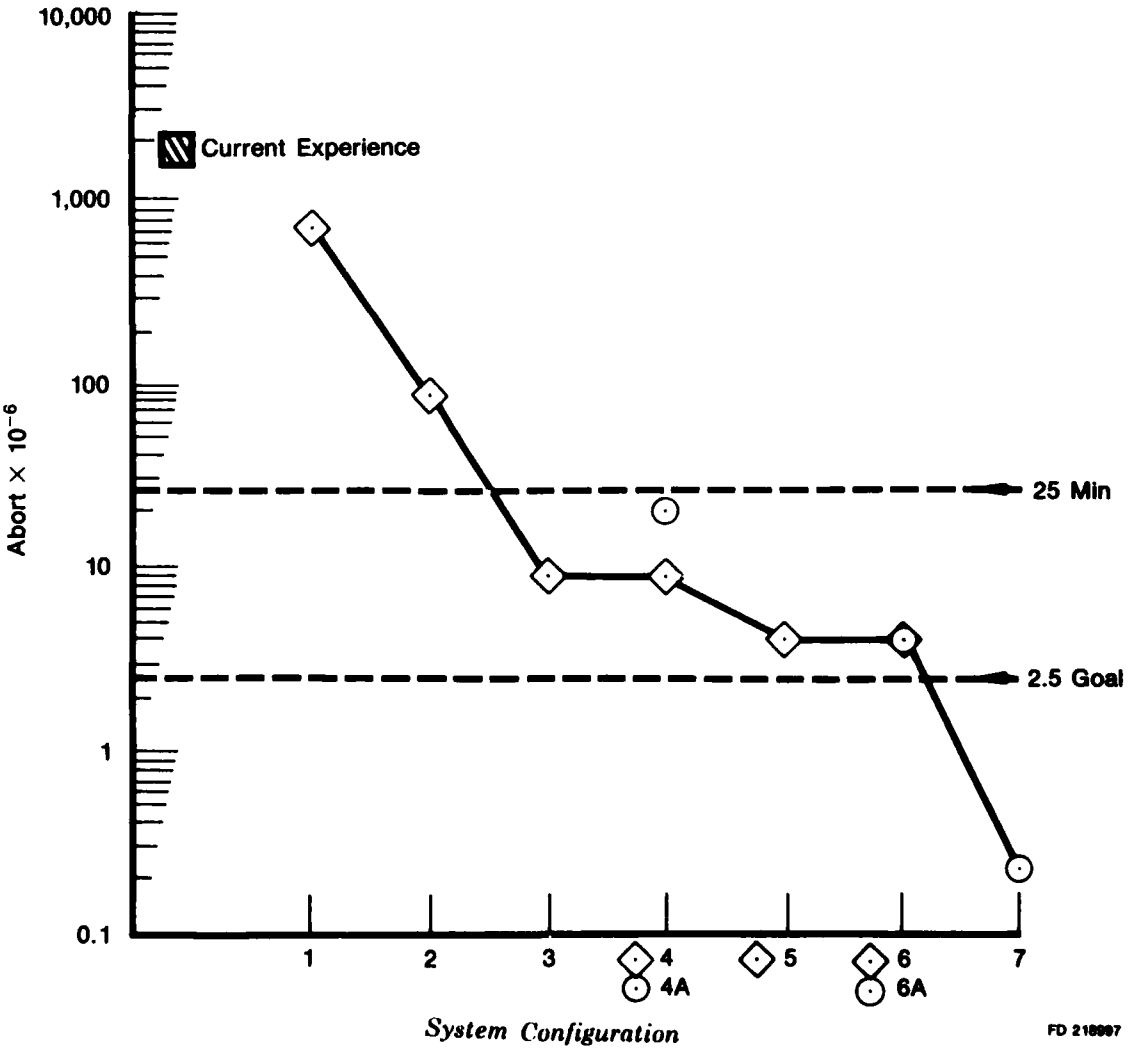
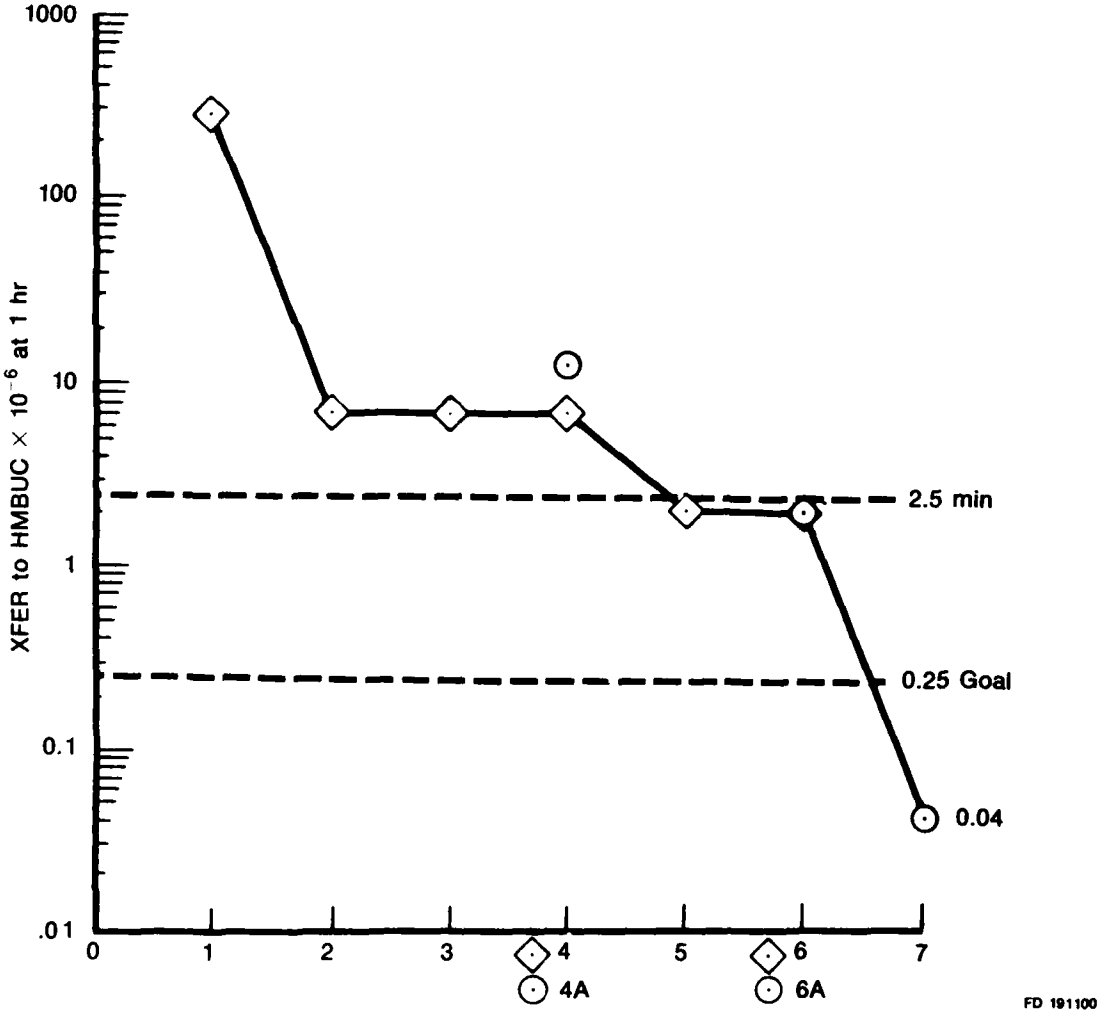


Figure 75. Mission Abort Reliability



System Configuration

Figure 76. Transfer to HBUC Reliability

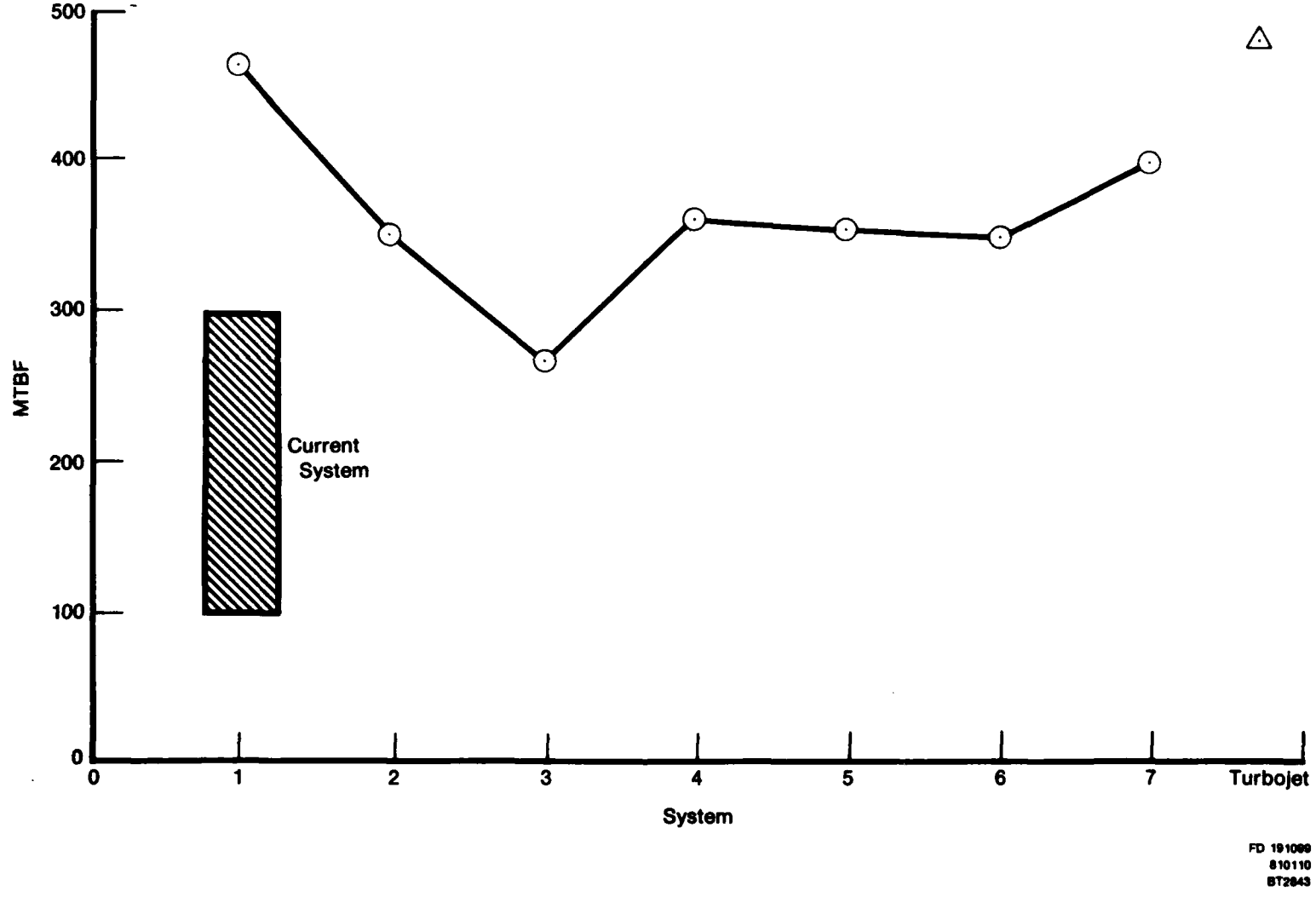


Figure 77. Mean Time Between Failures

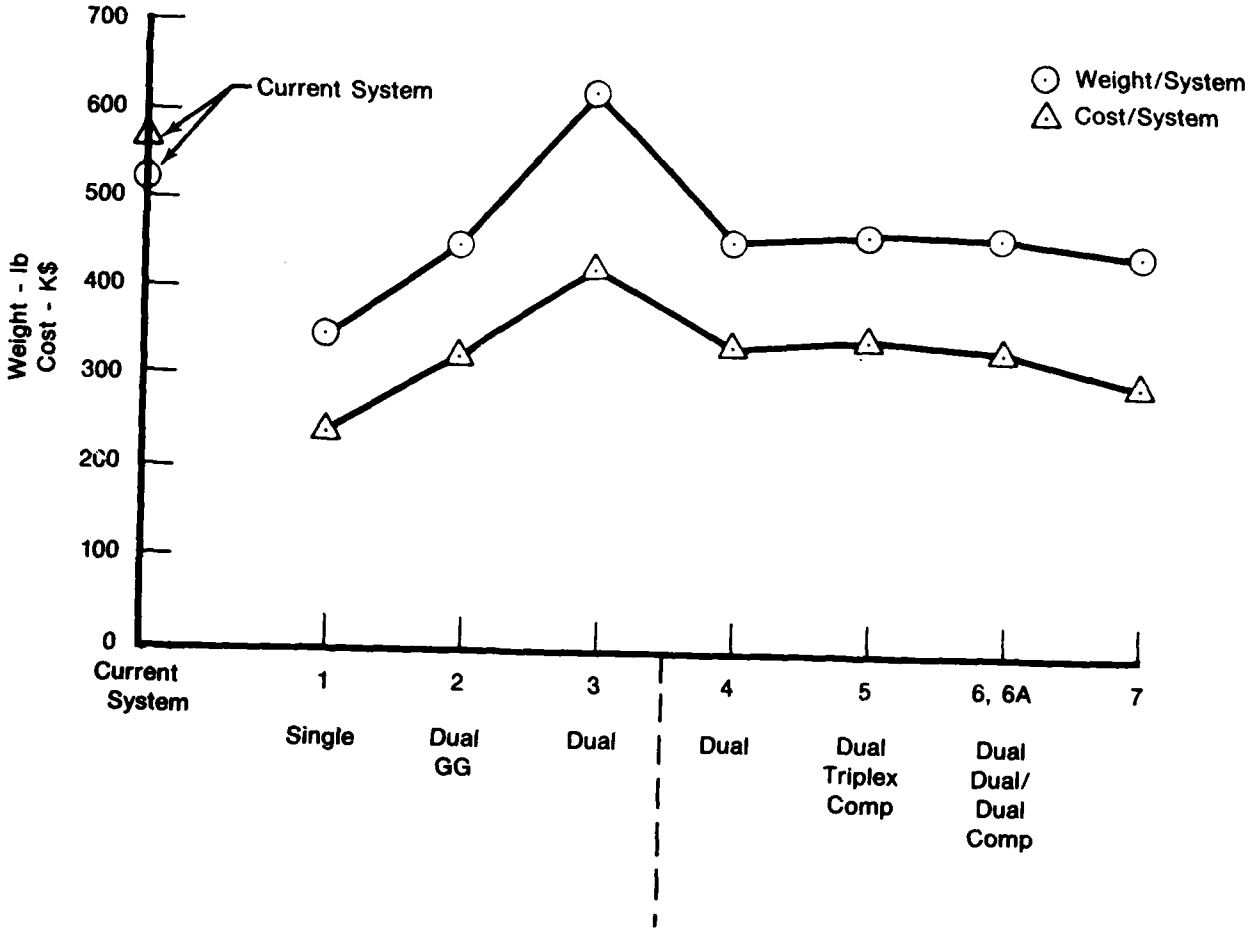


Figure 78. Cost and Weight

FD 218008

SOFTWARE COMPLEXITY

An issue which must also be addressed is the software required to implement the redundancy. This was assessed and is summarized by Figure 79. A basic computer size was selected for engine control logic and data I/O handling. This normally required approximately 6000 words of storage capability to implement conventional gas turbine control laws. To this additional memory, code is then added to handle fault accommodations. Even in the baseline system there is a requirement for fault accommodation software since the single string computer must be protected against faults which would cause active failures and prevent transfer to the back-up control. The additional software burden is reflected in development cost to write the code and additional throughput requirements on the processor to assure timely execution of this code. As shown by the chart the additional hardware redundancy added to the triplex and dual/dual systems has a benefit in reducing the software self test requirements since the selection of the good computer is accomplished via a hardware vote. In addition to reducing the software required the hardware vote also increases the computer coverage.

COST-OF-OWNERSHIP

A formal life-cycle-cost model was exercised with input data for all of the alternative designs. This LCC model is limited in its ability to accurately project cost-of-ownership in that there were several areas where design choices will have a cost impact but the magnitude of that impact is too subjective to input into LCC model calculations. Examples of these subject cost factors are the costs associated with variation in control system reliability and those associated with fleet size changes due to changes in engine control system reliability.

The formal LCC study indicates that all alternate designs exhibit a negative cost impact. Quantitatively the LCC penalty could be expected to be roughly 25 percent. The primary contributor to this cost penalty is acquisition cost. Increases in MTBF, while favorably impacting cost, were not a major driver.

An estimate was made of aircraft loss rates for alternate controller designs. This indicates that under one set of subjective assumptions, the baseline control would contribute to the loss of about $500M dollars (purchase price) of aircraft which would not have occurred with the System 7 controller without backup. This should be interpreted as a qualitative estimate as the inputs are sensitive to operational assumptions. The magnitude of this number is larger than the formal LCC impact of the redundant designs and this factor alone might produce a positive LCC project if it could be more accurately quantified.

An estimate of required fleet size was also made. For an example scenario it was determined that increased controller reliability could reduce fleet size requirements by 1 percent. While a 1 percent reduction is a small number, it implies a 1 percent reduction of total weapons system cost. This multiplicative factor is large enough that the resultant savings implied is again of the same magnitude as the total negative cost impact projected by the LCC model. This estimate is, however, very subjective as fleet size calculation depends heavily on an assumed mission scenario with assumed combat loss rates and mission success rates.

While exact quantitative evaluation is not possible, the total cost-of-ownership is likely to be smaller for the redundant alternatives.

Computer Configuration	Engine Control Logic K Word	Fault Logic K Word	Total	Coverage	Failure Accom
Baseline (Simplex)	6	4	10	85	Fail Safe
Dual Crosstrapped	6	10	16	95	Fail Op
Triplex Crosstrapped	6	2	8	100	Fail Op
Dual/Dual	6	1	7	100	Fail Op

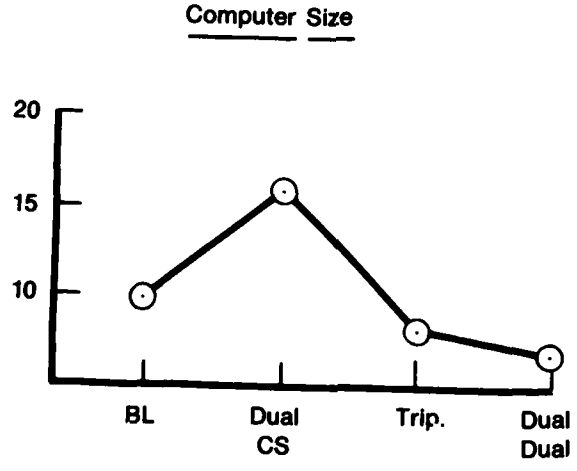


Figure 79. Software Complexity

AUTOMATIC RETRY AND MANUAL RETRY

The FAFTEEC configurations were evaluated with respect to automatic or manual retry cpability to recover from transient "glitches" or temporary faults and restore the system to original status.

The Baseline System which utilizes the hydromechanical backup control to back-up the system for first failures has no automatic retry capability. Typically hydromechanical back-up systems operate on a reduced capability control mode from the primary full authority electronic control. The transfers from electronic control to hydromechanical back-up requires extensive system integration testing to eliminate engine transients during transfer. There is no capability to automatically retry the primary control as this could result in switching back and forth between full authority electronic control and hydromechanical back-up which are different control modes and operate differently.

The systems which use dual or better electronic control channels operate such that there are dual full authority control channels which are identical in function. After a failure in one channel the other channel continues to operate the engine with the identical control mode. The faulty channel would be monitored for health and could be retried if so desired. These control channels would be operated with a dual active mode so there would be no difference between operating on one channel versus two channels, therefore there could be an automatic or manual retry with no interruption in engine operation.

SECTION 11

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

The analysis provided by the FAFTEEC program allows the following conclusions to be reached in regard to the FAFTEEC system architectures.

- FAFTEEC goals are reasonable and obtainable
- Redundant systems are required
- Single string technology is not cost and weight effective
- Coverage of dual systems is extremely important
- Coverage via software is complex, costly, and will not provide 100 percent coverage.
- Dual system technology must be included throughout all system components

Elimination of the hydromechanical back-up control from System 7 merits consideration of this system. Pratt & Whitney Aircraft feels elimination of the back-up control is made possible by a high reliability FAFTEEC system.

The future military gas turbine engines will be used in aircraft which will use integrated flight propulsion control systems. These integrated systems will require the propulsion control system to meet a high level of reliability consistent with that of flight controls and to be fail-operational. Therefore, the FAFTEEC goals are reasonable to project as requirements for these propulsion control systems.

There is an extremely significant improvement in the mission reliability of the best FAFTEEC system (0.23×10^{-7}) which exceeds the study goal of 2.5×10^{-6}. System No. 7 improves the baseline mission reliability by a factor of 3000. The system cost and weight evaluations show that system cost and weight will increase by about 30% compared to the baseline system. However, it should be remembered that the baseline system fails to meet the FAFTEEC goal by a factor of 300. The overall cost-of-ownership can be put into perspective by including the cost and weight in the life cycle cost analysis and comparing this to the cost savings which can be attributed to airplanes lost due to mission abort reliability. The results show an actual cost savings in the cost-of-ownership of the best FAFTEEC system.

As shown by the reliability modeling of the FAFTEEC systems, once the dual system redundancy has been incorporated, the mission reliability obtained is then very much a function of coverage. To reach the goal set forth by the FAFTEEC program the system coverage must approach 100% for the entire system. The methods recommended for doing this can be best explained by breaking the total system into the subsystem elements of computers, fuel management system, actuation, and sensors.

Computers

The dual systems, like system 2, 3, and 4 using our self-checking computer per channel, do not provide the necessary level of coverage to meet the FAFTEEC goals. These configurations must depend on individual computer self-test to decide when a computer is malfunctioning and remove the bad computer from the system. Analysis has shown that a coverage of greater than 95 percent is not obtainable by self-test methods alone. This level of coverage through self-test increases the software requirement by 100 percent over that needed to run the engine which significantly impacts computer design. This typically requires custom computers to be used to meet the speed requirements, thus driving down the reliability and increasing the cost, both of which are unacceptable. In contrast, a coverage of 100 percent can be obtained by using computer redundancy within each channel. In this architecture the failed computer is identified by a hardware vote. This technique has been used in other industries such as flight control and missile control, and is a demonstrated method of achieving computer coverage. The impact on future computer hardware cost is low.

Fuel Management

The components which are among the fuel management subsystem are also required to be redundant to meet the reliability goals as they are the most critical components on the engine both for mission abort reliability and flight safety. Current single engine systems typically employ two fuel pumps, one for the gas generator, and one for the augmentor. The hydraulic servo pressures for the metering valves, also typically supplied by these pumps, require a high fuel pressure at low speeds. A FAFTEEC fuel management scheme has been identified which uses dual centrifugal pumps, and dual fuel throttling valves and servo system. This provides a total dual fail-passive fuel management subsystem with a minimum of components.

Hydraulic Direct Drive Actuation

Dual hydraulic pumping subsystems are an established technology in the actuation of highly reliable flight control systems. The components for a 100 percent fail-passive dual hydraulic pumping system were established along with mechanical flight controls and have been continued in use with the fail-operational redundant electronic flight control systems. The electrical interface or servo valve has typically been at least triplex to provide fail-operational capability. The complexity which accompanies this interface is too complicated and costly for use in the gas turbine area. The use of a direct drive hydraulic servo valve has identified for FAFTEEC. This interface will provide a fail-passive interface between the hydraulic and electronics.

Engine Sensors

The engine sensors provide a challenge for the engine control system designers, since it is not obvious how to provide the required coverage without using total sensor replication. The addition of sensors beyond dual redundancy, presents an unwanted increase in system cost and weight in that they impact the cost of probes, cables, and electronic control interface equipment thus impacting electronic control cost, weight, and MTBF. There are means under study which can provide the required coverage through sensor self-tests, hard failure tests, and analytic redundancy techniques. The sensor coverage assumptions account totally for the mission reliability differences between systems 5, 6 and 6A which do not reach the required FAFTEEC mission reliability goal and system 7, which does meet the goal.

Using a "single string" electronic control results in a failure rate which is unacceptable for flight safety without a hydromechanical back-up control. However, the reliability modeling done for system 7 projects transfer to hydromechanical back-up control failure rate of 4×10^{-8}. When a reliability level of that magnitude can be obtained, it may be unnecessary to carry along the hydromechanical back-up control. Elimination of this unit can save cost, weight, and significantly reduces the development effort required for the system by eliminating the difficulties associated with developing a hydromechanical computer for the engine. Elimination of the back-up control also eliminates those reliability problems associated with transferring from full-up electronic control of the engine to the reduced fidelity of a simplified hydromechanical unit.

RECOMMENDATIONS

The following recommendations are made based on the FAFTEEC study.

- Develop a dual hydraulic actuation system
- Develop a dual centrifugal pumping system
- Build and evaluate a FAFTEEC computer architecture with triplex and dual/dual concepts with compatible engine sensors
- Development schedules should support next new engine program
- Development cycle for engine controls should be revised to reflect redundant system vs single channel prime reliable components.

SECTION 12
TECHNOLOGY TRANSFER

INTRODUCTION

The Full-Authority Fault Tolerance Electronic Engine Control System for Variable Cycle Engines (FAFTEEC) program presented the unique opportunity for members of the propulsion control community to study what was being done in other parts of the industrial control community. The telephone industry and the automotive industry were originally included in the proposal. In addition, the study was expanded to include an airframe manufacturer, to allow an overview of high reliability digital flight control systems, and a visit with Dr. Harold E. Ascher of the Naval Research Laboratory to discuss reliability estimation techniques. Each of these diverse industries and individuals will be presented in detail in this report through the discussion of ideas and trends these people projected for their own areas of expertise.

In general, these "technology exchange visits" took the form of a brief FAFTEEC presentation and then presentations, discussions and tours by each industrial host. The FAFTEEC presentation was given in three parts, the first of which gave an overview of modern gas turbine propulsion systems and their control requirements. The second was the evolution of aircraft engine control system hardware from hydromechanical through full authority digital electronic control. Finally, FAFTEEC was discussed to put into perspective what was expected to be accomplished in the program, where we currently stood, and the methods and models which were used in the program. The form of the industrial presentations was much less structured than the FAFTEEC presentation but may be generalized as presentations of the particular control area, tours of the facility where it was germane to the meeting and across the table engineering discussions. These meetings were open and frank discussions of ideas and problems which are part of designing a modern digital electronic control system.

All of the people we met on these technology exchange visits were of great help in this phase of the FAFTEEC program. Particular thanks go to the following gentlemen who coordinated our visit and smoothed the path in their company:

Dr. Wing Toy -- Bell Laboratory
Mr. John L. Ruby -- Ford Motor Company
Mr. John L. Webster -- Chrysler Corporation

TECHNOLOGY EXCHANGE TOPICS

In the course of the technology exchange visits with Ford and Chrysler an agenda of topics was used as a springboard into the current and future plans and practices of the automotive industry. A list of these topics is shown in Table 37. This list was supplemented by a more detailed set of questions within this broad framework. The trip reports to Ford and Chrysler included in Section 13 of this report contain an overview of these discussions.

The technology exchange visits with Bell Labs and General Dynamics present material that is very diverse and yet in line with the ideas being studied in the FAFTEEC program and the aircraft engine control community in general. Bell Labs is a user of large main frame type computers with an established reputation for high reliability testing, design, and hardware implementation. General Dynamics presents a view of high reliability electronics operating under many of the constraints and requirements imposed on the aircraft engine control.

TABLE 37. AUTOMOTIVE INFORMATION ITEMS

• Reliability
• Failure Accommodation
• Design
• Hardware
• Testing
• Specifications
• Maintenance

The visit to the Naval Research Center opens the avenue of the statistical study of high reliability devices, in particular, the acquisition of valid data given a relatively small sample size and long period required to acquire data. Material from these visits may be found in Sections 2 and in the trip reports of Section 13.

With the above information as a starting point the discussion topics with the automotive industry will be addressed. Information is mixed and does not reflect either the ideas of Ford or Chrysler, but rather is a compendium of the viewpoints of the FAFTEEC participants.

FORD AND CHRYSLER TECHNOLOGY EXCHANGE VISITS

The automotive industry is in the process of introducing a new generation of smaller, cleaner and more fuel efficient engines. Currently, automakers use electronics to perform pollution and fuel economy related functions as well as improving safety and operating sophisticated dashboard displays. Electronics have been used since the late 1970's to help meet federal government emissions and fuel economy standards. These automotive controls are based on microprocessor systems which control vital engine parameters such as air/fuel ratio and ignition timing. Figure 80 shows a block diagram of the first Ford electronic control system which puts spark timing and exhaust gas recirculation under the control of a 12-bit microprocessor. This system uses seven sensors and two outputs, the spark-ignition and module, and the EGR valve actuator. This system is designed to meet current regulations for emissions and provide a building block for future systems.

Reliability

As one of the main thrusts of the FAFTEEC program the automotive companys' views on reliability was of particular interest. The reliability goals are set by the individual company is based on the past history of the product, the operating environment, specifications (both in-house and industry-wide) and the expected failure mode of the electronic device. Reliability growth models, such as Duane plots are not in general use throughout the industry. This is due to several factors such as the large number of different models of components and their general nontraceability. This is expected to change in the future if automotive controls move from nonrepairable to repairable units. For now, when a new product is introduced, all returned units are inspected to first determine if the unit has really failed and secondly the cause of a verified failure.

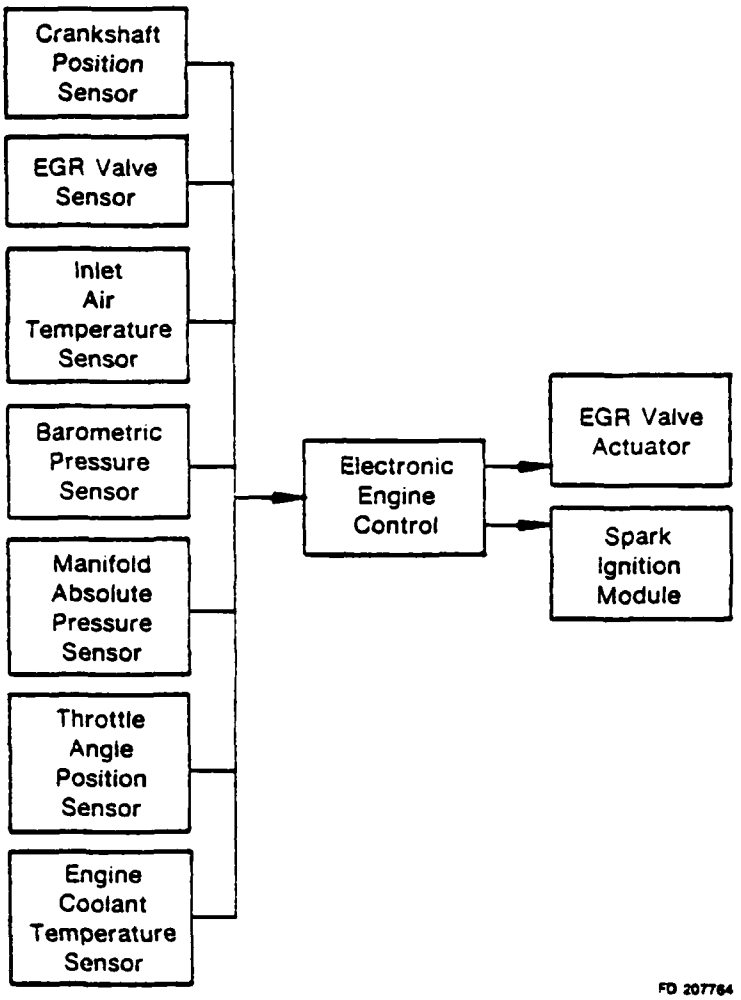


Figure 80. *Electronic Engine Control System Ford*

The reliability of the electronic portions of the engine control systm is enhanced by several methods. Higher quality parts are used to reduce the incidence of failures during predelivery tests. These parts then undergo extensive screening at both the vendors and during module assembly. Parts are derated to enhance the possibility of operating for a long period of time with no failures. It is expected that the costs associated with high reliability electronics will result in fewer returns and field repairs and will more than compensate for the initial higher cost of the electronic parts.

As the systems are configured today the engine electronic control does not contribute significantly to breakdowns of the system. The major problems are with the electro-mechanical devices such as actuators and solenoids and with engine sensors.

Failure Accommodation

The basic concept for fault accommodation is the idea of "limp home" capability. In the event of an electronic control failure the car will run well enough to get the driver home. In general, this backup control is a reduced capability electronic control. The failure of the primary electronic control is indicated to the driver on a dashboard display or simply by deteriorated vehicle performance.

Electronic Engine Control System Design

The FAFTEEC participants had a particular interest in the hardware and software design constraints and system drivers which govern the automotive industry in engine control system design. The number one consideration for the design of the systems is reliable operation over an extended period of time in the automotive environment. Components must be qualified to operate over the temperature, vibration, and EMI expected in the car. Table 38 is a comparison of a typical automotive and military aircraft engine environment. As can e seen from this table the environment in which electronic controls as expected to operate is only slightly less severe in the automotive system than the aircraft system.

TABLE 38. ENVIRONMENT COMPARISON

	Automotive Engine Control	Aircraft Engine Control (1)
Temperature	-40 to +125°C Engine compartment -30 to +80°C Passenger compartment	-56.7 to 182°C
Vibration	5 to 200 Hz 10 to 15g	10 to 2500 Hz 0.5 to 20g
EMI	200 V/M 10 MHz to 0.5 GHz	200 Volts/meter 14K to 40 GHz

(1) Values for the aircraft engine environment are as described in the appropriate Military Standard as listed in PWA Document FR-9621, Reliability Advancement Study for Electronic Engine Controllers, Definition of Controller Environment

The other major, and perhaps even most important, driver in the design of automotive engine control systems is the requirement to meet the emissions requirements established by the Federal Government. These requirements impose a need for a complex control system which can ony be reasonably accomplished with electronics. The accuracy of electronic control limits polluting emissions while helping to improve fuel economy. The two major contributors to these improvements are electronic spark advance and electronic fuel metering. Without the use of the electronic engine control the opposing standards, emissions and fuel economy, would be difficult, if not impossible to achieve.

Software design verification is achieved through various test methods to ensure that the program allows operation of the engine within acceptable tolerances. These verification methods include system emulation, time shared simulation/emulation comparison, bench testing and vehicle testing. The benefits of each of these test levels is described in Reference 1, "Software Design Verification in Real Time for Microprocessor Based Electronic Engine Control."

1. Durrett, C. D., Jr., Ford Motor Company, "Software Design Verification in Real Time for Microprocessor Based Electronic Engine Control," SAE Technical Paper 790174, 2 March 1979.

Automotive Engine Control System Hardware

The hardware of engine controls systems is made up of three parts: sensors, computers and actuators. The sensors employed in both the automotive and aircraft engine control systems are used to measure operating positions, pressures, temperatures and speed. In general, the sensors employed in the automotive engine control system are analog devices with no tendency toward the redundant direct digital devices, such as surface acoustic wave pressure sensors, which are being studied for aerospace applications. Table 39 is a general comparison of the types of sensors used in both engine applications. The aircraft engine devices are those employed on the P&WA Full Authority Digital Electronic Engine Control (FADEC).

TABLE 39. SENSOR COMPARISON

	Automotive Engine	*Aircraft Engine*
Position	Linear Potentiometers	Resolver, LVDT
Pressure	LVDT, piezoelectric, variable capacitor and strain gage	Vibrating cylinder Quartz crystal
Temperature	Nickel wire T/C	Chromel-alumel thermocouples
Speed	Magnetic pulse pickups	Magnetic pulse pickups

Actuators for automotive engine control systems are generally either solenoids, DC motors or stepper motors. These devices are similar in concept to the actuation devices found in a modern digital electronic aircraft engine control. FADEC employs torque motors and solenoids as actuators. (The production F100 engine control system is stepper motors and solenoids.)

The interest in microprocessors for control computers focused on three areas: reliability, memory size, and microprocessor technology. The favored technologies in the automotive industry are N-MOS, H-MOS and CMOS. On the other hand, FADEC employs a custom CMOS microprocessor. Where the automotive industry attempts to employ off-the-shelf computer components the trend in the aerospace industry has been toward custom chips. In the future, however, the two industries may meet as both are using or investigating the use of the computer on a chip, such as the TI 9940 and Mostek Rainbow. The reliability of the computers has been excellent in the automotive application with failure rates as low as two confirmed failures in 100,000 units. The memory size in the automotive appliation is growing just as it is in the aircraft engine control computers. The automotive applications range from 2500 words up to projections as high as 65,000 words. Current aircraft engine controls such as DEEC operate with 10,000 words of memory. As hardware redundancy is introduced into aircraft engine control this requirement is expected to decrease significantly.

Testing

Both Ford and Chrylser have extensive test facilities for both the development and production testing of their respective automotive controls. A description of the Chrysler test practices and procedures may be found in the paper "Production and Automated Testing of Chrysler's Engine Contrl Computer," Reference 2. This paper describes the various levels of testing employed to ensure "full compliance to the electrical, environmental and durability requirements included in individual component specifications." Production testing is accomplished at board, module and unit levels including a 7-hr post test burn-in of the units at temperatures up to 85°C.

Specifications

The automotive manufacturers establish their own specifications to control the quality of vendor supplied hardware. The quality of the automotive electronic control system is determined through the specifications they impose on vendors and the actual vendor selection procedure. Since the automotive industry is a large user of electronic hardwre it is able to set requirements which the vendors strive to exceed or they will be displaced in the market.

Maintenance

The maintenance practices for both Ford and Chrysler are similar for the automotive electronic controls. Current service center diagnostic equipment attaches to test points in the vehicle electrical system and checks out starting circuit, primary and secondary ignition and no load operation of the engine. Future electronic controls will be designed with on-board diagnostics which will be read out directly by the service center diagnostic equipment.

BELL LABS TECHNOLOGY EXCHANGE VISIT

As with the visits to the automotive industry an agenda of topics was prepared for discussion with Dr. Wing Toy of the Bell Labs. These items are:

- System Architectural Issues
- Failure Modes
- Software/Architectural Issues

These topics will be discussed individually in the sections that follow and in detail in the trip reports. A paper describing the design details of the Bell System Electronic Switching System (ESS) may be found in Reference 3, "Fault Tolerant Design of Local ESS Processors."

System Architecture Issues

A major area of interest to the FAFTEEC participants is the synchronized operation of the ESS system. This is a different mode than the current practice of frame syncronism or asynchronous operation currently employed in dual systems for aircraft engine control such as FADEC. These synchronized parallel ESS channels operate on identical input signals and produce identical output commands. In addition, the control computations are synchronized down to the processor instruction level. This makes the problem of failure detection of the computational core a matter of simple comparison on a bit by bit level.

2. Webster, J. L., and W. F. Henley, Chrysler Corporation, "Production and Automated Testing of Chrysler's Engine Control Computer."

3. Toy, W. N., "Fault Tolerant Design of Local ESS Processors," Proceedings of the IEEE, Volume 66, No. 10, October 1978.

Failure Mode

The ESS systems are designed and tested so that no single failure can cause the whole system to failure. The system does not take multiple failures into consideration. The failure detection logic for the ESS system is designed to activate only during a diagnostic check. The philosophy here is that as long as the system is operating at some level of efficiency long enough to maintain it and keep it working. This is consierably different from the safety considerations for aircraft engine controls where diagnostics are run continuously to catch and correct the failure at the time of occurrence.

There are several possible causes of system failures along with hardware failures. Dr. Toy, in Reference 3, breaks the outages down into hardware reliability, procedural errors, recovery deficiencies and finally software deficiencies. Figure 81 shows the percentages of each type failure.

Software/Architectural Issues

The software involved with the telephone computer system is far more complex than that of an aircraft gas turbine control computer. The software is typically developed and implemented using a high level language with automated compiler and translator for machine language programming. Even with extensive documentation and software control procedures an appreciable number of system failures are attributed to software errors.

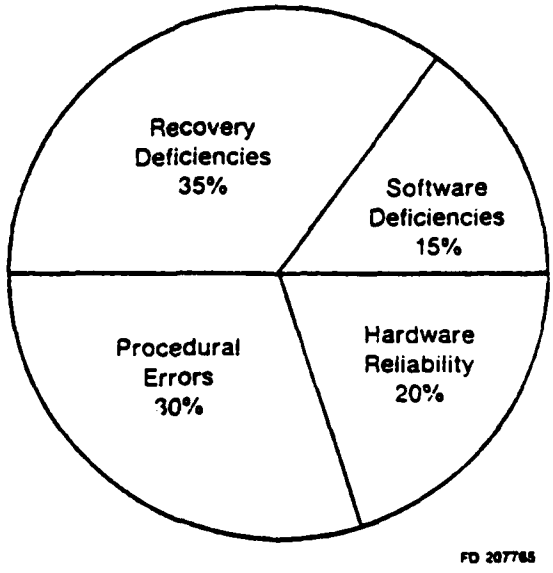


Figure 81. System Outage Allocation

As presented in Figure 81, Software Deficiencies account for about 15% of the problems with the ESS systems. These softwre problems include errors that wipe out the system memory and program loops that can only be cleared by shutting down and reinitializing the system. Software faults in the ESS may be traced to sources which aree common to all control system software, that is, incorrect initial algorithms or improper translation of the algorithm into code. Corrections and program changes may be made continuously to any operating system.

GENERAL DYNAMICS TECHNOLOGY EXCHANGE VISIT

The General Dynamics participation in the FAFTEEC Technology exchange presents the opportunity to exchange information with an industrial partner familiar with highly reliable, redundant electronic control systems operating in the military aircraft environment. The discussion centered on the General Dynamics AFTI F-16 program which employs a multimode triplex digital Fly-By-Wire flight control system, Figure 82. This figure is based on information contained in Reference 4, "Design Considerations for AFTI/F-16 Digital Flight Control System."

The major technical thrusts of the AFTI/F-16 program include the development of: task-tailored multimode control laws, a triply redundant digital flight control computers, advanced redundancy management techniques, integrated crew station controls and displays and an interface compatible for integration with other aircraft subsystems. The control system is projected to provide a two fail operational capability which will exceed a loss of control reliability of 10^{-7} failure/flight hour.

4. Ramage, J. K., AFWAL and J. H. Watson, General Dynamics, "Design Considerations of AFTI-F-16 Digital Flight Control System," 13 November 1980, SAE Aerospace Control and Guide Systems Committee, Meeting No. 46 Presentation.

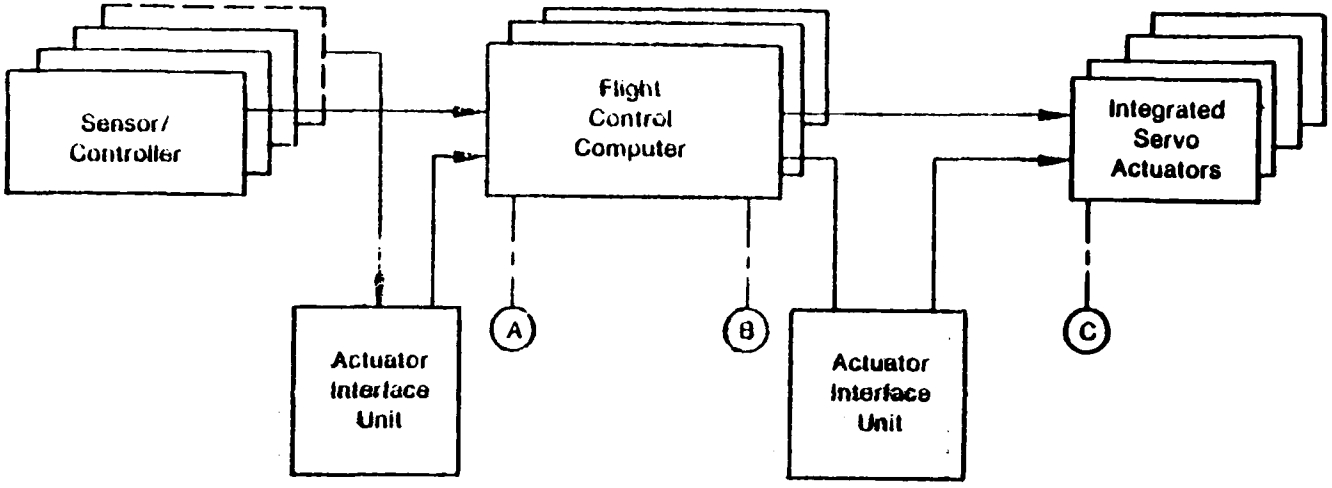


Figure 82. APTI/F-16 Flight Control System Redundancy Management Scheme

SECTION 13
TRiP REPORTS

TECHNOLOGY EXCHANGE VISITS

During the course of the technology exchange task, visits were conducted to several industrial users of microprocessor board control systems. Trip reports were written to document these trips and are included in this section as follows:

- Bell Laboratories
- Dr. Harold Ascher, Naval Research Laboratory
- Ford Motor Company
- Chrysler Corporation
- General Dynamics.

BELL LABORATORIES

Trip Report on Technology Exchange Visit to the Bell Laboratories, Naperville, Illinois, 5 December 1979, M. E. McGlone

Summary

The initial trip for the FAFTEEC technology exchange task was made to Bell Laboratories, Naperville, Illinois. The trip was hosted by Dr. W. Toy of Bell Labs and attended by the following:

C. E. Ryan, Jr.	AFAPL
M. E. McGlone	P&WA
W. J. Davies	P&WA
T. B. Smith	CSDL
J. H. Lala	CSDL
W. C. Peck	HSD
A. Martin	HSD

An overview of the FAFTEEC program was presented along with the first Quarterly oral review of the program. An agenda of topics for discussion was provided by P&WA and Draper and an informative dialogue followed. Some observations relevant to the FAFTEEC program are included below.

1. The Electronic Switching Systems (ESS) developed by Bell Labs are under control of fault tolerant ESS processors which have been under development since 1953. The ESS processors fall into three categories. The large capacity No. 1 ESS serves metropolitan offices, the medium capacity No. 2 ESS was designed for suburban offices, and the No. 3 ESS supports rural offices. The architecture of all the systems in duplex; however, the implementation of the duplex structure differs in each system. The No. 1 processors are duplicated and switched on a small block basis while the No. 3 processors are duplicated on a system basis and switched as a system. This is possible with the No. 3 processors because the number of components in the No. 3 processor is considerably less. Also the No. 1 processor was designed in the early 1960's and the No. 3 processor was designed and developed in the late 1960's and took advantage of the small scale integration (SSI) technology available.

2. Experience with the ESS systems has shown fault detection and recovery to be the biggest contributor to system down time. By design the processor is allocated two-thirds of system down time with fault detection and recovery problems accounting for 35 percent of processor down time. Processor hardware only accounts for an additional 20 percent of system down time with the rest going to software and procedural problems. It appears this is one reason Bell Labs leans more toward duplex systems than TMR systems. That is, to keep the complexity of fault tolerant software and hardware to a minimum.

   The magnitude of the software job required to operate the ESS systems has led Bell Labs to the use of structured software using higher level language programming. The UNIX operating system was developed by Bell Labs and is marketed by Western Electric. The impact of the structured software, along with the fault tolerant capability, has been to double the requirement for processor speed and memory size.

3. The problem of evaluating the fault tolerant capability of the design before introducing the equipment into the field is addressed with two techniques. These are by simulation of the systems and the faults and by actually introducing faults into a hardware model of the system. The digital simulation method can precede the hardware method since the hardware method requires the equipment to be operational. It was felt that since both methods have individual restrictions and advantages both were required for a comprehensive evaluation.

4. The impact of technology developed since the No. 3 processor was also discussed. The trend of electronics toward large scale integration (LSI) has pushed the processor to a smaller board area which would favor triplication of the processor; however, other areas of the system would be much more difficult. The discussion touched briefly on distribution processing. Comments indicated distributed processing would create an even larger software management problem when redundancy is involved.

It appeared the overall philosophy was to keep it as simple as possible and still meet the reliability requirements.

Trip Report on Technology Exchange Visit to the Bell Laboratories, Naperville, Illinois, 5 December 1979, T. Basil Smith

Jay Lala and I attended a joint technology exchange and quarterly oral report meeting at Bell Labs' Indian Hill Facility. Our visit was hosted by Dr. W. Toy of Bell Labs. The meeting was a useful exchange of information, and provided Jay and me with an opportunity for updating our knowledge of the ESS switching computer developments. Some observations which might be relevant to this program are included below.

First, I would like to comment on the complexity of the task ahead. Toy indicated that over half of the circuitry of each processor of the dual ESS processor is devoted to error detection or maintenance functions. The basis system is, of course, dual. Thus an overhead factor of four is probably representative of the hardware price paid for the degree of fault tolerance exhited by ESS systems. This is remarkably close to the overhead/complexity curve first presented by Steve Osder in April of 1977*. It should also be noted that this degree of fault tolerance may be inadequate to meet FAFTEEC program goals. Triplex or dual-dual flight control systems operate with overhead factors of 10 to 12. Thus the message should be to prepare oneself for what could be a disappointing reaction to the FAFTEEC program should FAFTEEC discover that it falls on this same historical curve. A second message should be to view any systems which purport to fall significantly below this curve with some suspicion.

The use of a higher level language and structured code will have even further implication on perceived FAFTEEC overheads. Toy indicated that these software techniques reflect into the hardware so as to require a speed/performance enhancement by a factor of two and a memory size expansion by a factor of two over unstructured assembly language.

The composite message is again that any viable FAFTEEC system is apt to have a complexity which may be substantially higher than current expectation, or hopes. This complexity should not be unmanageable; however, the VLSI trends should make it fairly affordable.

A second observation deals with the technology changes which have taken place since the design of the ESS systems, and the impact these changes might have on system architecture. The ESS No. 3A processor employed SSI parts. The implications of this are twofold. First, at this level of integration hardware costs are a dominant concern. The difference between dual and triplex systems is large from a cost viewpoint. Clever encoding and error checking schemes have a fairly large hardware cost base with which to leverage even relatively minor gains in efficiency. Second, since the circuit implementation is SSI, certain assumptions as to fault independence, propagation paths for faults, stuck at one or stuck at zero models for faults are reasonable approximations. These assumptions provided the theoretical base for the clever encoding and error checking systems.

The situation is largely changed relative to LSI architectures. The cost of the computational core is not likely to be large because of the economics LSI will bring to bear. Thus the savings of a dual system over a triplex or quad is not likely to be large in absolute terms. Additionally, since the fault propagation paths across a single chip can be fairly arbitrary, many of the clever techniques developed in the past are not apt to work. Toy confirmed that he also believes that one must assume arbitrary behavior of a failed chip. Future designs are thus likely to take substantially different architectures. For example more extensive use of outright replication of critical functions for purposes of error detection and fault masking may be used.

A third observation deals with the issues of coverage. Toy confirmed the intuitive feeling that the error detection coverage of the synchronized and match systems of the 1, 1A and 2 ESS computers does provide very good coverage. The problem of isolating which side of the dual system has sustained an error, as might be expected, is somewhat more difficult. It seem particularly true that the concept of running quick diagnostic tests after discovery of an error is easily frustrated by intermittent or transient errors.

**Osder, S. S., "Chronological Overview of Past Avionics Flight Control System Reliability in Military and Commercial Operation," in AGARDograph No. 224, Integrity in Electronics Flight Control Systems, April 1977.

If I read what Toy said correctly, the ESS systems fail to recognize or diagnose a problem correctly in about 5 percent to 10 percent of the situations. Thus coverage of the first error from detection to selection of the unfailed channel would appear to be in the range of 90 percent to 95 percent. Since the real-time constraints of the phone system are less severe than those imposed on an engine controller, the self-check procedures will therefore be shorter for the engine controller, one might expect that first error coverge for a dual engine controller to be less than 90%. It might also be observed that the impact of incorrect diagnoses for the case of a transient error is much less severe for the phone system than the engine. The phone system can afford to drop all calculations in progress. This results in only the loss of a few calls. The caller recycles the system by redialing the call. If the error was indeed transient, it is unlikely that the caller will be further impacted even if the faulty channel was left in control. Even repeated occurrences of the same transient can leave the system functioning at nearly normal levels. It is unlikely that the engine controller will be faced with such a forgiving environment.

A fourth observation deals with the problem of maintenance. Fault tolerance allows the system to continue functioning despite failures. In order to achieve the high degree of reliability predicted for these systems, it is necessary to follow the maintenance philosophy on which the reliability modeling was based. I have observed that many fault tolerant systems tend to deteriorate to a point where maintenance is done on a fix-after-system-failure basis. This was the case to some extent with the computerized controls of the Morgantown rapid transit system. It appears to be the case to some extent with the ESS systems, and observed to have been the case in certain situations in nuclear power plant control. It is even regretably the case with our own fault-tolerance multiprocessor breadboard. As a warning, one should not underestimate the degree of discipline which will be required to enforce a maintenance philosophy.

A fifth observation concerns the necessary software support tools for reliable softwae. The hardware cost of using a higher level language and structured programming does not truly reflect the total cost of developing reliable software. This is merely the recurring cost to be paid for each system produced. If the numbers to be deployed are large, this recurring cost is the dominant cost. This may not be the case for engine controllers. Specifically one must consider the costs of compilers, program analyzers, statement level simulators, interface verifiers, version control software, and other aspects of the whole framework of software support. All of this support software costs a great deal of money and it is desirable to spread this cost over as many units as possible. This may dictate the choice of processor and/or certain architectural features so as to achieve some commonality with another program or project. Most desirable of all would be a situation in which support tools could be captured intact from another effort with someone else bearing the development costs. It is exactly this phenomenon which has made the Bell Labs UNIX operating system and programmers workbench so successful.

My final observation deals with the problem of verification. Verification will be done by direct fault injection and by simulated fault injection. LSI technology has greatly reduced our ability to actually inject hardware faults into a system. Such faults are really limited to device pin faults. As the complexity of each device increases, this becomes a cruder and cruder mechanism. There are an unlimited number of faults which cannot be so injected, and as LSI densities increase, the fraction of faults which can be emulated by pin faults drops. The problem with simulation is even worse. The ability to economically increase the numbers of active devices on a chip is outstripping the ability to economically simulate differing faults in that chip. Indeed, the ability to simulate the single device which is the correctly functioning chip has barely kept pace with the complexity of these devices and is a factor in limiting future complexities. Verification is thus likely to be an arduous task at best.

PROPOSED ISSUES FOR DISCUSSION

SYSTEM ARCHITECTURAL ISSUES

- Using synchronous and match mode operation of the No. 1, No. 1A and No. 2 ESS processors has the error detection coverage been perfect?
- Have there been any error events which were not detected, were these problems, if any, a result of latent errors resulting in simultaneous manifestations of errors or simply uncovered single point faults?
- Has this trend been toward less extensive matching because it was deemed unnecessary to the desired coverage or simply because of cost?
- How often following the detection of a fault, is the diagnosis of the unit at fault incorrect and the failed unit is left in service and the other unit disabled?
- What has been the coverage experience for the No. 3A processors?
    - How many 3A processor faults go undetected?
    - How many 3A processor faults are associated with the checking circuitry (that is, they would not have occurred if the complexity of the checker were excluded from the design)?
    - How has this compared to synchronous operation experience?
- Impact of LSI
    - What do you see as the usefulness, if any, of totally self-checking circuits in the LSI environments?
- What assumption do you make/think reasonable on chip failures?
    - Arbitrary behavior?
    - Stuck at "1" "0" of internal logic of output pins?
    - Too complex to characterize?
- Does LSI favor 3A or 1 type of architecture? Yet another architecture?
- Does LSI make triplex processors look more attractive?
    - Coverage of faults and diagnostic simplicity?
    - Triplex processors/encoded memories?

FAILURE MODE

- How many of your errors are intermittent or transient?
- How many are hard failures?

- How long to recover from an identified fault?
- How does this affect complexity/effectiveness of recovery algorithms/fault location algorithms?
- What about models of intermittent and transient modes of failures? What is the degree to which they degrade reliability projections over hard faults?

SOFTWARE/ARCHITECTURAL ISSUES

- Since large percentage of errors are software, what hardware assists are deemed necessary to limit authority of pieces of code to do damage.

  Example: Write protect
  Supervisor call/user modes
  Memory mapping
  Watchdog timers
  Security kernels
  Etc.

- Role of structured programming/higher level languages/modern architectures.
- Role of debugging tools, online trace and monitoring.

TRIP REPORT ON TECHNOLOGY EXCHANGE VISIT TO DR. HAROLD ASCHER, NAVAL RESEARCH LABS, 28 FEBRUARY 1980, T. BASIL SMITH

On 28 February 1980, a technical exchange and discussion was held between Harold Ascher of the Naval Research Laboratory and the P&WA/CSDL FAFTEEC team. Pratt & Whitney Aircraft was represented by Mike McGlone, and Draper Laboratory by Basil Smith.

Mike McGlone presented a brief overview of the P&WA/CSDL FAFTEEC effort. Basil Smith then summarized the Markov Modeling techniques and the available tools, which are to be employed by this effort. Particular attention was given to CSDL's belief that these modeling techniques, and particularly the use of fixed hazard rate exponential failure assumptions, will be adequate to the needs of this program. Ascher was in general agreement that the exponential failure rate distribution assumption was satisfactory, given the difficulty in projecting failure rates for future components. He did express a healthy skepticism as to the need to so accurately model the dynamics of the proposed systems, given this difficulty. In absolute terms, uncertainty in failure rate projections can easily swamp many of the finer detail and subtle failure modes and their effects represented in such models. Such uncertainty could produce in excess of order of magnitude uncertainties in the reliability projections. The value of such detailed modeling is therefore in its ability to measure relative differences in reliability between alternatives, given similar input assumptions.

Mike McGlone presented some sample failure rate data from F100 engine experience. Dr. Ascher was interested in this data based approach to reliability projection. He observed that the standard extraction or curve fitting programs repeat what he believes is an all too common blunder of assuming a particular distribution and then fitting a curve to it without regard to the validity of the original assumption. Duane plots for the same components in fact, clearly

show that their failures are not homogeneous Poisson processes, despite reasonably good curve fits. Dr. Ascher expressed further interest in seeing other elements of the F100 data base and in helping in its proper interpretation.

It became clearer as the discussion progressed, that reliability modeling, and reliability analysis of failure data are two distinctly differing areas of concern, joined by a common vocabularly of terms, but not necessarily joined by common definitions or understanding for those terms.

Part of the problem then becomes one of recognizing that the two activities are different. For example, of particular interest in any real life analysis of failure rate data should be a concern for whether the system being studied is getting more reliable or less reliable with time. Basically, one studies the data to detect anomalous behavior, that is behavior that differs from expected performance. Presumably, if the system is unexpectedly growing less reliable, then some corrective action should be identified. In contrast, a priori, mission reliability is not critically concerned with trends (except for the ultimate end points to which a system is driven) because the rates of degradation or improvements are slow compared to mission times. It is not even clear whether life cycle cost projections can usefully utilize trend information of this type as the impact of the absolute uncertainties in the a priori projections can be large compared to the impact of any trends.

In summary the discussion with Harold Ascher did not reveal any significant problems in the basic reliability modeling technique to be employed by this project. Ascher did express an interest in studying the reliability data available on the F100 engine, and if possible, arrangements should be made to coordinate with the failure rate data collection and analysis projection phases of this project with him.

TRIP REPORT ON TECHNOLOGY EXCHANGE VISIT TO THE FORD MOTOR COMPANY, DEARBORN, MICHIGAN, M. E. MCGLONE

Summary

The visit to Ford provided a very congenial, open discussion of the problems, philosophy, and practices of designing and developing digital electronic control systems for aircraft gas turbine or automotive engine control. Although each application has its own specific requirements and goals there were many parallels in system design drivers and component technology base. Overall the visit provided an excellent opportunity to exchange information pertinent to both applications and a dialogue should be continued.

Discussion

The morning session consisted of an introductory briefing by Chuck Ryan discussing the origins of the FAFTEEC program and why fault tolerant electronic control systems are of interest to the Air Force and to the industry. Ford felt they were in accord with the FAFTEEC programs as they had the only total digital system in the automobile industry, the other manufacturers using analog and hybrid systems.

Pratt & Whitney Aircraft then presented the FAFTEEC program and the role of each of the program participants. A brief overview of the program plan was also discussed. Pratt & Whitney Aircraft and Hamilton Standard discussed gas turbine control historical development from early hydromechanical controls to the current technology programs involving full authority digital electronic systems.

In answer to Ford's questions, technology drivers were pointed out to be performance, cost, and weight during early electronic control programs evolving to a strong desire for reliability in the current FAFTEEC program.

Ford was interested that our current update rates for a computer cycle were operating at 20 msec. Current update times for their systems are 5-10 msec and they hope to progress to 2-3 msec.

The use of the Markov modeling techniques used by Draper Labs was discussed. Ford was interested that reliability failure data used in the FAFTEEC program was based on field failure data rather than handbook and felt the field data was the preferred method.

Ford was in agreement that extreme temperature (above 150°C) should be avoided for best reliability of electronics. Ford designs electronics for a max ambient environment of 125°C and feels thermal cycling also presents a problem to overcome.

The meeting was adjourned for lunch and reconvened at the Ford Electronic Control Development Facility where the meeting was attended by additional Ford stall engineers.

The afternoon session was led off by Ford describing the evolution of electronic control systems at Ford. Their discussion revealed a dedicated effort to develop reliable cost-effective digital electronic computer based systems. These programs involved design, development, and extensive laboratory and field test experience. Future plans show an agressive effort to push the microcomputer industry to develop products for their systems.

The meeting then proceeded to an open discussion of information items provided by P&WA Controls Technology Group. These items covered EMI, Reliability, Failure Accommodation, Design, Hardware, Testing, Specifications and Maintenance.

EMI

Ford gave a description of what is expected for an EMI environment and how they plan to test for it using a new anechoic enclosure equipped with a dynamometer. This facility was designed by Boeing and can test vehicles made by Ford under operating conditions for EMI levels up to 200 volts/meter.

Reliability

Ford was in agreement that field data was an excellent source for reliability data to be used for future projections. Ford used a system to track field failures which were statistical plotting techniques. These differed from Duane plots, but accomplished the same goal of tracking field reliability.

Ford felt the track record of their electronics to this point has been very good. They listed actuators as their number one problem with sensors as second. They were in agreement that the best approach to reliability was to take a system approach.

Fault Accommodation

The Ford system will be fault accommodating from the aspect that after a failure the driver will have get home capability, but will require maintenance action to regain full performance. Electrical backups are provided for critical items which could cause the vehicle to stop entirely.

Failure indication is identified by degraded vehicle performance and no pilot (driver) flags or lights are provided. However, the electronic controller does provide built-in-test to provide fault diagnostic information for maintenance personnel. Built-in-test and computer automated test units are also used to diagnose failures during controller screening tests performed during incoming inspections.

Design

The major drivers for system design are reliability, cost and control accuracy. Emission and certification standards make acuracy of control of prime importance. Emissions and mileage requirements lead to increased design complexity which require electronics for adequate control.

Ford acts as the system designer as well as overall system integration manager. Ford has people in all system disciplines and crosses all technical areas contained both in Pratt & Whitney Aircraft and Hamilton Standard. They do the whole job with exception of design and manufacture of the IC's.

The environment in which the automotive electronics unit must live is very similar to the gas turbine environment after we cool and isolate. Electronics are designed to withstand an ambient temperature of -40 to 125°C with vibrations of 10 — 15g7s over 5 — 2000 Hz.

Hardware

Ford is currently using custom N-MOS with H-MOS (dense N-MOS) predicted for the future. Current technology reflects 16 Bit, 4 K-word (expandable to 64K-word) microcomputers. Current cycle times are on the order of 10 μsec with reductions to 7 μsec in the near future (driven by spark and fuel control requirements).

Sensors designs are stressing reliability by driving toward reduction of accuracy requirements to reduce cost. Actuators are generally DC or stepper motors with potentiometer feedbacks.

Testing (Screening)

Ford has no plans to utilize accelerated stress testing. They are familiar with the Bell Lab work in this area, but economics rule out its use for their products. P&WA commented we share the same problem.

Burn-in at the subassembly level and final assembly are used 100% at the present time. It is planned to transfer this testing to the vendors as electronics are used more widely in their industry.

Specifications

Ford limits their electronic vendors to only those who produce quality products. They have in place extensive quality review programs for their vendors. These parts are purchased [illegible] specifications (Q101).

TRIP REPORT ON TECHNOLOGY EXCHANGE VISIT TO THE CHRYSLER CORPORATION, HUNTSVILLE, ALABAMA, W. J. DAVIES

Summary

The visit to Chrysler provided the opportunity for open discussions of the similarities and differences between aerospace and automotive electronics. This dialogue covered aspects of electronic reliability, design, testing and control requirements in general. A plant tour put into perspective the magnitude of the automotive operation that manufactures electronics for the Chrysler Corporation cars, and the planning and testing required to ensure delivery of a reliable product.

Discussion

The first order of business in the morning was a tour of the production facility for automotive electronics for all Chrysler cars. These products include spark controls, engine controls, radios and dashboard electronic assemblies.

The incoming inspection of parts is conducted on various percentages of parts depending on the previous history of the part and its vendor. For instance, resistors may be accepted with no incoming inspection, accepting the vendor's test data. IC's, on the other hand, are tested 100% using a Fairchild Sentry VII Tester; some of these IC devices are tested at an elevated temperature.

Components are automatically inserted into the various printed circuit boards, except for a few expensive devices which must be inserted in the board by hand. After assembly all boards are visually inspected for missing or damaged components. One of the last components installed on each board is the PROM which has been burned in and tested for the designated final application. PC boards are then soldered and cleaned prior to final testing as a unit.

Testing is conducted on 100 percent of all engine control and spark control units. This includes board tests and module tests. The module tests are conducted before and after potting. The post-potting burn-in test is conducted in cycles of 7 hours, one hour on/one hour off. Reliability Engineering selects units each week for a long term, 5-week, endurance test in a facility which simulates the engine compartment environment. This facility is similar to the CERT facilities being developed at Pratt & Whitney Aircraft and Hamilton Standard.

One of the topics that was discussed during this tour was the use of PROM's compared with a computer on a chip with ROM. Chrysler has been working with both concepts and prefers PROM's for their relatively high volume application. They fell that if a change is required in module software, a common occurrence, it is most cost effective to change just the PROM and not the CPU and ROM on a single chip.

Discussion

After the plant tour the general meeting was joined by members of the Chrysler Engineering and Reliability Staffs. Chuck Ryan started the meeting with a description of the origins of the FAFTEEC program and the need for increased reliability in aircraft engine control systems.

Pratt & Whitney Aircraft described the program plan for FAFTEEC and the role of each of the participants. Prior to the Draper presentation on Markov modeling techniques P&WA described the engine system and the various control systems being studied. Chrysler was

interested in configurations with high levels of redundancy and questioned whether a mission would be started with one of the systems not operating. This led to a brief discussion of the Life Cycle Cost portion of the FAFTEEC program which had just gotten underway in October.

Hamilton Standard gave an overview of electronic control development. Chrysler was particularly interested in the use of fuel for cooling the electronic circuits. Bill Peck also made a short presentation showing the HSD CERT facility. This was most appropriate since during the plant tour we had been shown the Chrysler version of this type test equipment.

The use of Markov modelling techniques was presented by Basil Smith of the Draper Labs. Chrysler reliability personnel were interested, and, although they do not currently use this type technique, they are familiar with its application.

The afternoon activity was devoted to presentations by Chrysler covering their reliability activity, component testing and analysis program, and engine control failure detection and accommodation.

Chrysler's goal for reliability, by 1986, is for a 250 percent reduction in the number of warranty occurrences chargeable to the engine control system. They plan to accomplish this through the use of a proven microprocessor, the RCA 1802, combined with improved selfcontained diagnostics, and the relocation of the computer module from the air cleaner to the firewall. The Chrysler in-house effort toward this goal is placed by programs for component test, reliability and failure analysis.

The component test effort includes topics covered during the plant tour portion of this report. In addition, they are using 1000 hr, 5 yr of operation, life tests with some of their vendors. Accelerated life tests are run at 125°C.

Chrysler controls the reliability of their vendor supplied hardware by being completely involved in the vendor quality program. They are involved with all vendor specifications and design processes. Chrysler maintains control of chip design by designating what must be done and how it is to be accomplished to meet their specifications.

In the event of a failure, Chrysler performs an analysis of the field component rather than returning it to the vendor. This is done to get a quick turnaround to ensure that the problem will not be recurring. Failure analysis also involves evaluation of vendor process control, techniques and requirements.

The engine control phase of the Chrysler discussion centered on the computer hardware and its potential failure modes and their detection. As mentioned previously, the CPU is an RCA LSI COS/MOS (C/MOS) 1802. This unit is an 8-bit registered-oriented central processing unit with high noise immunity and a wide operating voltage range. The 1802 chip has DMA capability but Chrysler currently uses this feature only for control development. The control operates on a 2.5 to 5.0 millisecond update time, which is set by the fuel injection system requirement. The system has an I/O complement of ten inputs and eight outputs.

Chrysler considers four possible failure modes for the engine control system; disabling failures, detectable degradation, undetectable, and no normal effect. This last failure mode occurs only under certain specific operating conditions, and, if these conditions are not met exactly, the unit operates normally. Needless to say this is considered a difficult failure to analyze and correct. The disabling type failure requires some type of engine backup control to provide what Chrysler terms "limp-in" capability. This is operation with a minimum amount of electronics and a battery backup memory. Failure detection and accommodation is accomplished in software as Chrysler feels this is a more cost-effective approach than redundant hardware.

CHRYSLER CORPORATION/AIR FORCE, PRATT & WHITNEY AIRCRAFT, DRAPER LABORATORIES, HAMILTON STANDARD MEETING 21 OCTOBER 1980

Attendees

C. E. Ryan	Air Force
W. Davies	Pratt & Whitney Aircraft
W. Peck	Hamilton Standard
B. Smith	Draper Laboratories
J. Webster	Engine Controls Chrysler Corporation
J. Butler	System Reliability Chrysler Corporation
J. Lappington	Advanced Chassis Electronics Chrysler Corporation
A. Seitz	Reliability and Failure Analysis Chrysler Corporation
D. Shallenberger	Reliability Chrysler Corporation
G. Thornton	Engine Control Product Support Chrysler Corporation

MEETING 6-9-81 GENERAL DYNAMICS, FORT WORTH WITH PRATT & WHITNEY AIRCRAFT

John H. Watson	GD Flight Controls
J. V. Clifton	GD Propulsion
C. S. Droste	GD Flight Controls
H. Z. Scott	GD Flight Controls
Paul C. Leamer	GD Propulsion
Gordon Fenn	GD Propulsion
W. R. Fuchs	GD Flight Control Design
Tom Daugherty	P&WA Texas Office
Ron Miller	Control Technology Manager
E. E. Ammons	GD Flight Control Design
E. C. Livingston	Products Digital Flight Controls
P. H. Lang	Products Digital Flight Controls
M. E. McGlone	P&WA

ATTACHMENT A
FAFTEEC TECHNOLOGY EXCHANGE VISIT
FORD MOTOR COMPANY
DEARBORN, MICHIGAN
FORD MOTOR COMPANY/AIR FORCE, PRATT & WHITNEY AIRCRAFT, DRAPER LABS, HAMILTON STANDARD MEETING
12 MARCH 1980

Attendees

C. E. Ryan	Air Force	
Bill Peck	Hamilton Standard	x4544
Pete Ansbro	Advanced Engine Electronic Controls Ford Motor Company	
Dieter Forberger	EEC Subsystems and Applications Ford Motor Company	
John Ruby	Powertrain Electrical Electronics Ford Motor Company	
Ken Dabrowski	Engine Engineering Ford Motor Company	
Jack Paulus	Engine Engineering Ford Motor Company	
William Davies	Pratt & Whitney Aircraft	
Basil Smith	Draper Labs	
Mike McGlone	Pratt & Whitney Aircraft	
Joe Gormley	Engine Electronic Engineering	

APPENDIX A

RELIABILITY MODELING BACKGROUND

1.0 INTRODUCTION

To help evaluate the reliability of the baseline FAFTEEC controller a general set of modeling tools have been developed. The overall modeling methodology consists of partitioning the system to be modeled into smaller, more tractable subsystems, developing models from FMEA tabulation for each subsystem and finally combining the results of submodels to obtain the reliability of the complete system. The tools that have been developed include a procedure for partitioning the system into subsystems, a method for developing models for subsystems from FMEA tables, a specification language for translating the model description into an input file for a computer program. The computer program then numerically solves the specified models of subsystems, combines the results from these models to obtain overall system reliability and other reliability parameters of interest. These tools are sufficiently general enough so that they will adequately handle all the candidate architectures to be evaluated under the FAFTEEC contract.

The purpose of this Appendix is to acquaint the reader with the fundamental mathematical concepts underlying the chosen modeling methodology, to describe the model specification language for the use of the computer programs and to illustrate the procedure for doing the combinatorial analysis of the subsystem models. These procedures are illustrated where necessary with the aid of simple examples. A step-wise procedure has also been included that shows the important steps in going from a system description to the final stage of obtaining the numerical results, using a simple system as an example.

The overall modeling methodology is summarized in Section 2.0 of Appendix A. Section 3.0 explains the concepts of 'state' and 'state transitions' and their relationship to the failure modes and effects

analysis (FMEA), which enumerates the basic fault interactions and impacts on the control system. These state transition diagrams form the basis for all Markov model analyses. Section 4.0 describes the basic algorithm used to numerically solve a single Markov model. Section 5.0 enumerates the steps outlined above with the help of a numerical example. Section 6.0 illustrates the procedure for partitioning a system into segments, each represented by its own Markov model, and the procedure for combining results obtained from these separate subsystem models to compute the overall system reliability. Section 7.0 is an overview of the reliability modeling program and a description of the input specification language. Section 7.0 also includes an example application of the program using a simple control system and proceeding from the system description through to numerical and graphical results.

2.0 MODELING METHODOLOGY

During the span of the past few years Draper Laboratory has carefully examined various modeling techniques for estimating the reliability of redundant systems. This effort has included examination of most of the packaged computer models such as CARE I and II, TASRA, CAST, CARSRA, and others. All of these techniques suffer from a variety of deficiencies. The number of architectures that can be modeled is limited. These models do not treat the sequential nature of failures in a complex redundant system where the order of failure events is important; they do not have any capability for handling time varying failure rates; and they do not produce predictions on mean time to maintenance, availability, or average times in degraded states. All of these vital parameters are required in judging redundant systems. Additionally, the concept of coverage is only partially treated.

The mathematical approach developed and used by the Draper Laboratory during the past several years is discrete-state, continuous-time Markov modeling. The Markov process was first defined by A. A. Markov in a paper in 1907 (Ref 1). It is a mathematical technique that has been thoroughly analyzed and understood. Markov modeling has been used extensively in a number

[1] Markov, A. A., "Extension of the Limit Theorems of Probability Theory to a Sum of Variables Connected in a Chain," The Notes of the Imperial Academy of Sciences of St. Petersburg, VIII Series, December 1907.

of complex and uncertain systems. Examples range from supermarket queues to machine maintenance and inventory control. The use of Markov modeling for modeling of reliability in complex redundant systems was suggested by Avizienis (Ref 2). The Draper Laboratory expanded upon this work, and combined many of the concepts of Avizienis with computer and mathematical tools developed previously at Draper for performance prediction using Markov modeling. Draper was able thereby to synthesize an extremely powerful reliability model, which was applied to the task of reliability prediction for the Fault-Tolerant Multiprocessor (FTMP) under development at Draper for NASA. It was also used to support reliability projections for the Advanced Group Rapid Transit (AGRT) control system of the Boeing Aircraft Company and in a similar effort for an enhanced reliability control system for a Personal Rapid Transit (PRT) system of the Transportation Technology Division of Otis Elevator. The variety of architectures modeled have ranged from simple TMR to the highly complex parallel-hybrid redundancy of the NASA-sponsored FTMP. Overall system failure rates have varied from 10^{-4} to 10^{-11} failures per hour. It has also been used to study the effects of intermittent and transient faults on digital systems and the suitability of various redundancy techniques in combating these faults. In the case of the FTMP modeling, the resultant reliability predictions were independently verified using alternate means by a consultant to the NASA Langley Research Center. The modeling techniques are mature and in place, and have been verified to a high level of confidence.

The Markov model methodology can be summarized fairly simply. The first task is to identify and define the various states of the system under study. This corresponds exactly to the definition of state transition diagram. The number and nature of these states is, of course, dependent upon the exact nature of the design of the system being modeled. In this case the state transition diagrams will have been developed as part of the basic description of each system to be modeled.

[2] Avizienis, A., "A Unifying Reliability Model for Closed Fault-Tolerant Systems," Presented at the Fifth Annual Fault-Tolerant Computer Conference, Paris, France, June 1975.

The second task is to compute transition rates from one state to another. One assumes that the events which would carry the system from one state to another are failure rates which occur with an exponentially-distributed probability density function. The estimation of failure rates can be made using reliability projections or by directly measuring the failure rate of similar components or modules.

The states of the system are numbered, and the transition rates are used to fill a two-dimensional transition matrix. Note that many entries of the transition matrix are zero, as it is impossible to directly transit from many states to many others. Thus, while the apparent difficulty of setting up the transition matrix of N^2 state transitions seems to grow rapidly with the number of states, N, the fact that most of the entries are zero means that this difficulty increases in a fashion which is more nearly linear with N.

The third step is to initialize the system. The system may be initialized with all of the probability being assigned to one state, generally the no-failures state; or the likelihood of being in any one state may be spread over any number of initial states, providing they sum to one. This initial state corresponds to the time zero situation. Once the initial state is known and the state transition matrix is known, the time history of the probabilities of being in any state can be calculated by solving a differential equation that relates the rate of change of state probabilities to the state transition rates and the state probabilities.

Although a single model of the type outlined above can be theoretically applied to a system of any complexity, in practice, the number of states, which increase in geometric proportion to the complexity of the system, limit model size. The number of states and the transitions between them can quickly become intractable. This intractability of a single large model is attacked by partitioning a large complex system into small segments and developing a Markov model for each segment independently. The individual models are each solved independently of all the other models. The results from each segment are then 'added' using combinatorial equations to obtain results for the system as a whole.

3.0 STATE TRANSITION DIAGRAMS

In order to better understand the exact nature of state transition diagrams, they are briefly described here with examples as necessary.

The analysis of fault-tolerant control systems becomes more complex as the level or degree of fault tolerance increases. Single-string systems have essentially one operating state or condition. Generally, any fault will cause the system to fail to a safe state. A system of this simplicity generally does not require explicit documentation to understand the state dynamics of its operation. Such dynamics are so simple as to be easily inferred from the block diagrams and control law documentation. A fault-tolerant system in contrast may have many operational states, each state being uniquely defined by the number of faults present in the system and the sequence in which they appeared and in which corrective action was taken. A convenient means of documenting and describing this dynamic interaction between the operating states of the system and events, such as the onset of a fault, is the state transition diagram. State transition diagrams will be used by this program for this purpose.

Each operating state of the system is represented by a node. An event causes a transition from one state of the system to another. Such a transition is represented by a vector drawn from one node of the system to another. The source node represents the state of the system before the event, the vector represents an event, and the destination node represents the state of the system after the event.

For example, consider the case of a simple control system as pictured in Figure A-1. There are three types of sensors, A, B, and C, each of which is dual redundant. These sensors can be read by three computers, X, Y, and Z. X can read an A and a B, Y can read a B and a C, and Z can read an A and a C. The information obtained from sensor types A, B, and C is such that the output of any one sensor type can be synthesized from the other two with sufficient accuracy to operate the controlled plant in a degraded state. The computers each have communication channels to each other so as to allow exchange of sensor values. The output of each computer is used

to drive a voting actuator. If any computer should fail it outputs a null signal. The voter/ actuator functions by averaging the non-null inputs. The system is intended to be fail-safe. This is assured for computer failures because any computer failures will produce a null output. When all computers have failed, the actuator will drive to its null or fail-safe position. In order to assure fail-safe operation despite sensor failures, each computer will produce a non-null output only when it has adequate information on sensor inputs to verify correctness. A single sensor reading will not be trusted unless verified by another reading from that same type of sensor or by a consistency check which employs readings from the other types of sensors.

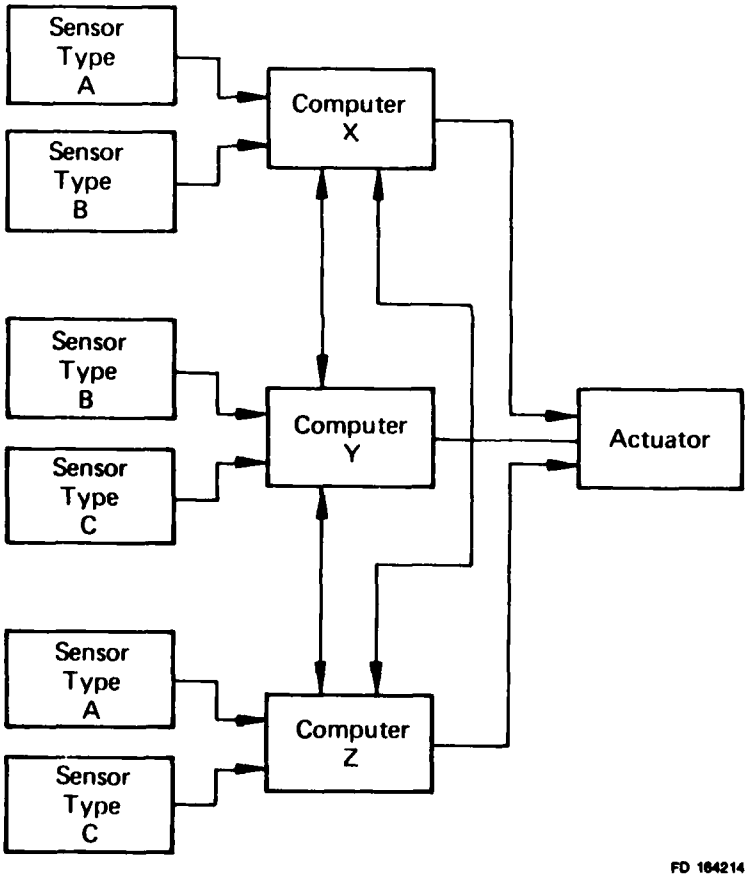


Figure A-1. Control System Example

Figure A-2 is a state transition diagram for such a system. The states and events are briefly elaborated below.

State 1 corresponds to all sensors and computers functioning correctly. A computer failure, event "a," would cause a transition to state 2. A sensor failure, event "b," would carry the system into state 3 where only one sensor is unavailable.

State 2 corresponds to a state in which one computer has failed or both sensors of one computer have failed. Because of the simplicity of this system, each of the above has equivalent impact on the system. Now, if another computer fails, or another sensor of a type which already is unavailable fails, then the system fails safe. Such an event is designed "c" and causes a transition to state 8, the fail-safe state. If a sensor fails which does not leave an unverifiable sensor set, event "d," then the system is carried to state 4. A sensor is verifiable if it can be compared to another sensor of similar type or its value can be compared to a value synthesized from dissimilar type sensors.

State 3 corresponds to the system with a single sensor failed. If the computer to which that sensor is attached fails, or the other sensor of that computer fails, event "e," then the system is carried to state 2. If the computer which is not interfaced to the same type sensor as the failed sensor fails, event "f," then the system is carried to state 4. For example, if sensor A of computer X is failed, then the failure of computer Y corresponds to event "f," while failure of computer X constitutes event "e" and failure of either sensors B and C in Y or Z constitutes event "g," as explained below. If a type of sensor other than the already-failed sensor fails, event "g," then the system is carried to state 5. If the other sensor of the same type as the failed one fails, event "h," then the system is carried to state 6. In the present example, note that in state 6 two sensors of the same type have failed and it is therefore necessary to synthesize that sensor reading. Event "i" corresponds to the computer failure which leaves an unverifiable sensor set and thus carries the system to the fail-safe state, state 8. In the example above, event "i" is the failure of computer Z.

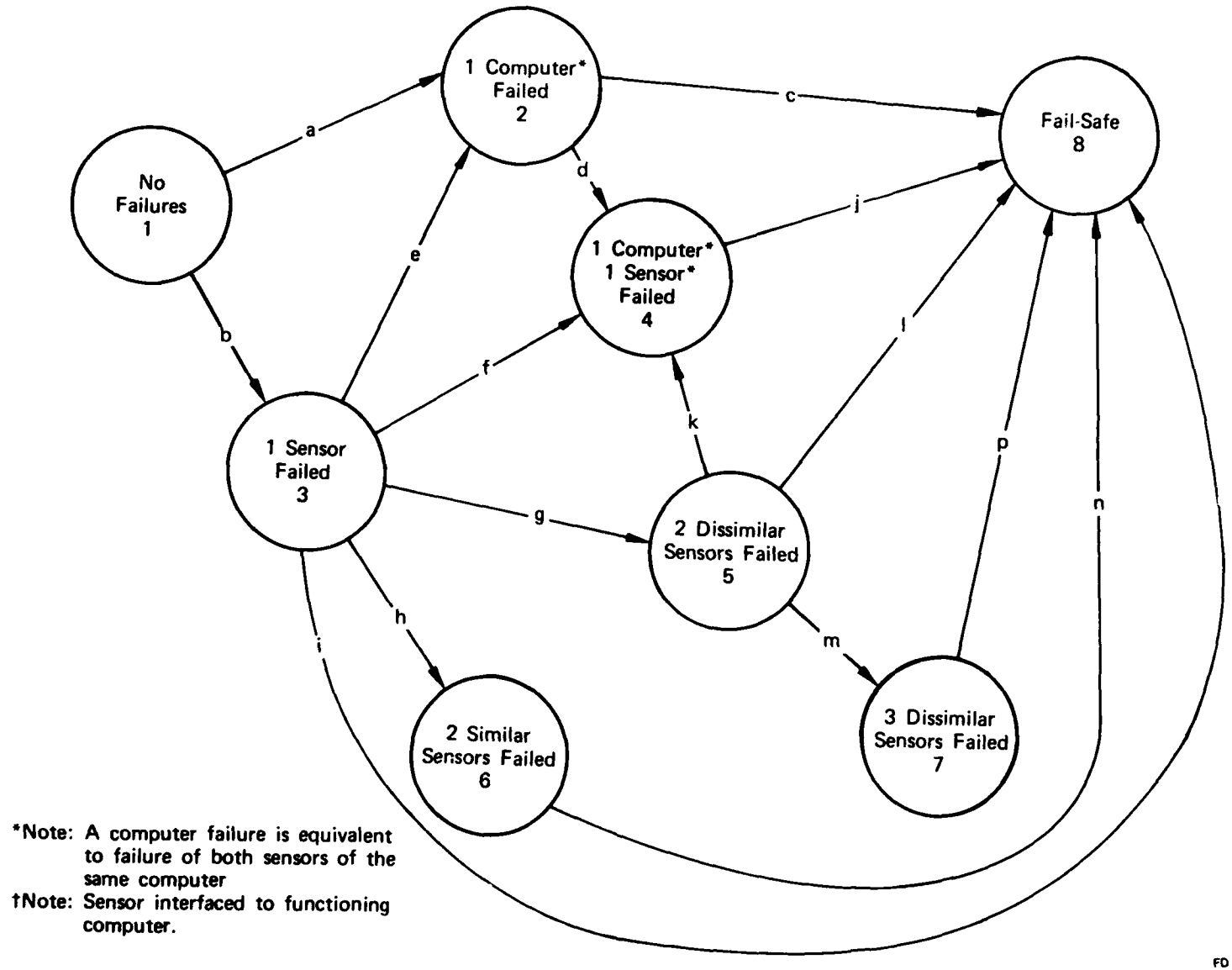


Figure A-2. Example of a Static Transition Diagram

State 4 corresponds to a state in which one computer (or its sensors) has failed, and one other sensor has failed. Another additional sensor failure or computer failure, event "j," will carry the system to the fail-safe state.

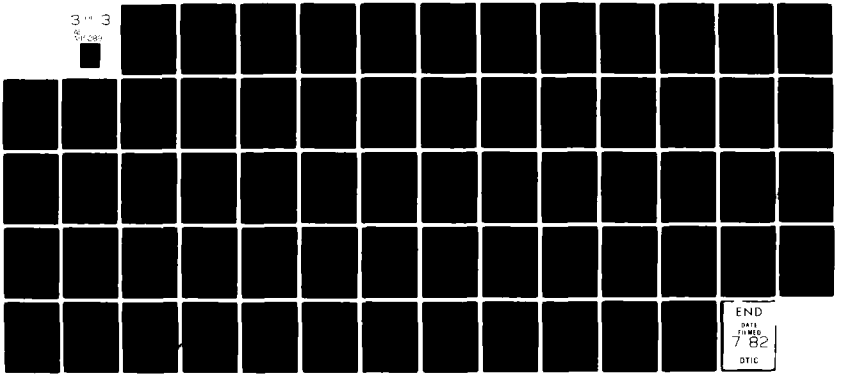
State 5 corresponds to a state in which two sensors, not of the same type, and not attached to the same computer, have failed. If a specific sensor should fail or specific computer should fail, event "k," then the system could be carried to state 4. For example, if sensor A of X is failed and B of Y is failed, then the failure of either C of Y or Y itself would carry the system to state 4. If either of the other computers fails or another sensor of the same type as one of the already failed sensors fails, event "l," then the system is carried to state 8. If the sensor which is not of the same type as one of the failed sensors and not attached to the same computer as one of the failed sensors fails, event "m," then the system is carried to state 7.

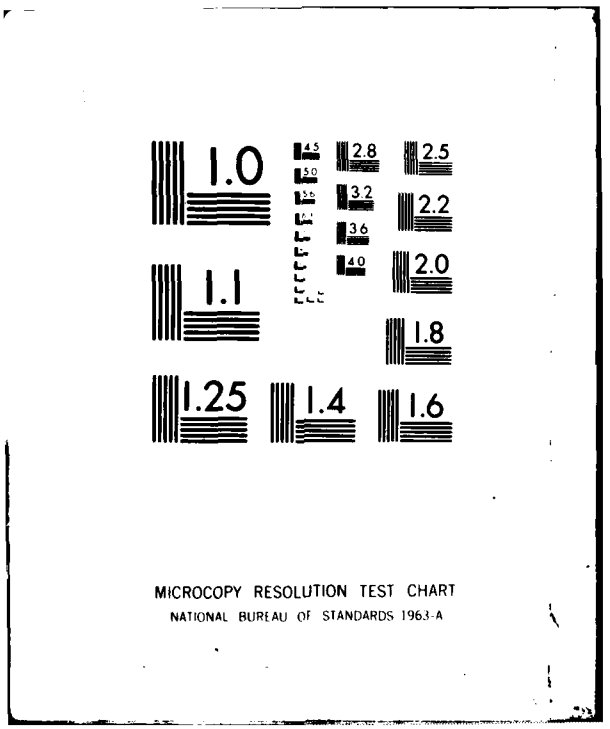
State 6 corresponds to the situation where two identical type sensors have failed. Any additional sensor failure or computer failure, event "n," will cause a transition to the fail-safe state, state 8.

State 7 corresponds to the situation where one of each of the three types of sensors has failed and they are spread equally among each of the three computers. Any additional failure, event "p," would cause transition to state 8.

State 8 is the fail-safe state. There are no transitions out of 8 and it is therefore called a trapping state.

AD-A115 289 PRATT AND WHITNEY AIRCRAFT GROUP WEST PALM BEACH FL G--ETC F/G 21/5
FULL-AUTHORITY FAULT-TOLERANT ELECTRONIC ENGINE CONTROL SYSTEMS--ETC(U)
DEC 81 M E MCGLONE, W J DAVIES, T B SMITH F33615-79-C-2082
UNCLASSIFIED PWA-FR-15054 AFWAL-TR-81-2121 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

4.0 MARKOV MODEL SOLUTION

Solving a Markov state model of a system is equivalent to determining the state of the system at a future time given the state of the system either at the present time or at some initial time instant. The initial state of the system may be known with certainty; for example, all system components may be known to be in good operating condition at take-off, or the initial system state may be a distribution of probabilities amongst various states. In any event, the initial system state can be specified by a state probability vector $\bar{P}_n$ where n is the number of states in the model. The rate of change of the state vector $\bar{P}$ is related to the state transition rates by the following vector-differential equation

$$\frac{d\bar{P}}{dt} = (Q-I)\,\bar{P}$$

where

$\bar{P}$ = state probability vector (n elements)

Q = state transition matrix (nxn elements)

Q_{ij} = transition rate from state i to state j

$Q_{ii} = 1 - \sum_{j \neq i} Q_{ij}$

$P_i(t)$ = probability of being in state i at time t

I = identity matrix.

The above equation seldom has an analytic solution which is tractable, particularly if time varying transition rates (failure rates) are used. Fortunately, numerical solutions can be obtained using modern computers. To integrate the equation numerically, it is helpful to rewrite it as a vector-matrix difference equation as follows:

$$\bar{P}(k+1) = Q \cdot \bar{P}(k)$$

where

$\bar{P}(k)$ = state probability vector after k time increments of Δt

Q = modified state transition matrix

$Q_{ij} = T_{ij} \Delta t \quad i \neq j$

$Q_{ij} = 1 - \sum_{i \neq j} T_{ij} \Delta t$

Δt = integration time-step

T_{ij} = transition rate from state i to j per unit time

To obtain good accuracy, the time-step Δt should be chosen to be small. However, iterative application of this stepwise integration using a small time-step can be very costly. Therefore it is necessary to increase the time-step dynamically as a function of time. This can be done without losing accuracy if the Q matrix is modified appropriately for the chosen time-step. In particular, the time-step can be increased n-folds if the nth power of the transition matrix is used as shown in the following equation.

$$\bar{P}(k+1) = Q^n \cdot \bar{P}(k).$$

For practical reasons related to the display of the results on a long (time) axis, n was chosen to be 10. After ten such iterations (at the edge of a new decade) Q' then replaces Q. Thus each iteration of the process involves two steps:

i. A vector-matrix multiplication (P times Q), and

ii. A matrix-matrix multiplication (Q' times Q).

5.0 MODEL EXAMPLE

The example of Section 3 can be used to illustrate this entire process. Referring again to Figure A-1, it can be seen that in order to convert this state transition diagram to a Markov model diagram it will be necessary to compute transition rates for the various transitions "a" through "p." The basic physical events which contribute to the transitions "a" through "p" are either sensor or computer failures. Assume that reliability data has been collected which enables one to project a failure rate for a single sensor at:

$\lambda_s = 2 \times 10^{-5}$ failures/hr.

Assume that similar data collection efforts enable one to project a failure rate for a single computer at:

$\lambda_c = 10^{-4}$ failures/hr.

Transition rates "a" through "p" can be computed.

Event "a," which is a failure of one of three active computers, will occur at rate,

$\lambda_a = Q_{1,2} = 3\lambda_c = 3 \times 10^{-4}$

Event "b," which is the failure of one of the six sensors will occur at rate,

$\lambda_b = Q_{1,3} = 6\lambda_s = 1.2 \times 10^{-4}$

Event "c," which is the failure of one of the remaining two computers, or of one of the remaining sensors of the type attached to the failed computer, will occur such that,

$\lambda_c = Q_{2,5} = 2\lambda_c + 2\lambda_s = 2.4 \times 10^{-4}$

Event "d," which is the failure of one of the remaining two sensors which are of a type different from those attached to the failed computer, will occur at rate,

$\lambda_d = Q_{2,4} = 2\lambda_s = 4 \times 10^{-5}$

Event "e," which is the failure of the computer to which the failed sensor is attached or of the other sensor of that computer, will occur at rate.

$$\lambda_e = Q_{3,2} = \lambda_c + \lambda_s = 1.2 \times 10^{-4}$$

Event "f," which is the failure of the computer which is interfaced to the two-sensor set which differs from the failed sensor (leaving one of each type of sensor and two computers functioning), will occur at rate,

$$\lambda_f = Q_{3,4} = \lambda_c = 10^{-4}$$

Event "g," which is the failure of a sensor which is different from the failed sensor and attached to a different computer, will occur at rate,

$$\lambda_g = Q_{3,5} = 3\lambda_s = 6 \times 10^{-5}$$

Event "h," which is the failure of the remaining sensor of the same type as the failed sensor (leaving the system with no sensor of one type, thereby requiring synthesis of that sensor reading), will occur at rate,

$$\lambda_h = Q_{3,6} = \lambda_s = 2 \times 10^{-5}$$

Event "i," which is the failure of the computer which is not interfaced to the failed sensor, but which is interfaced to the other sensor of the same type as the failed computer, will occur at rate,

$$\lambda_i = Q_{3,8} = \lambda_c = 10^{-4}$$

Event "j," which is the failure of any remaining functioning component of state 4 (two computers and three sensors) will occur at rate,

$$\lambda_j = Q_{4,8} = 2\lambda_c + 3_s = 2.6 \times 10^{-4}$$

Event "k," which is the failure of the computer which leaves two computers and three dissimilar sensors functioning or the sensor failure which produces an equivalent result, will occur at rate,

$$\lambda_k = Q_{5,4} = \lambda_c + \lambda_s = 1.2 \times 10^{-4}$$

Event "l," which is the failure of either of two computers or of either of the two sensors which would lead to an unverifiable sensor set, will occur at rate,

$$\lambda_l = Q_{5,8} = 2\lambda_c + 2\lambda_s = 2.4 \times 10^{-4}$$

Event "m," which is the failure of the single sensor that is of a different type and attached to a different computer than either of the two previously failed dissimilar sensors (leaving the system with three computers, each with only one sensor and all sensors dissimilar), will occur at rate,

$$\lambda_m = Q_{5,7} = 2\lambda_s = 2 \times 10^{-5}$$

Event "n," which is the failure of any three functioning computers or four functioning sensors of state 6, will occur at rate,

$$\lambda_n = Q_{6,8} = 2\lambda_c + 4\lambda_s = 3.8 \times 10^{-4}$$

Event "p," which is the failure of any of the three functioning computers or three functioning sensors of state 7, will occur at rate,

$$\lambda_p = Q_{7,8} = 3\lambda_c + 4\lambda_s = 3.6 \times 10^{-4}$$

All other $Q_{i,j}$, where $i \neq j$, are zero. The Q' matrix pictured in Figure A-3 can then be used to solve the Markov model. Figure A-4 graphs the probability of the fail-safe state (likelihood of being in state 8) as a function of time for a 100-hr period assuming an all-functioning state at time zero. The probability that the system is operating with one failure (in state 2 or 3) or operating with multiple failures (in state 4, 5, 6, or 7) is also shown as a function of time.

$$
\begin{bmatrix}
* & 3 & 1.2 & 0 & 0 & 0 & 0 & 0 \\
0 & * & 0 & 4 & 0 & 0 & 0 & 2.4 \\
0 & 1.2 & * & 1 & 0.6 & 0.2 & 0 & 1 \\
0 & 0 & 0 & * & 0 & 0 & 0 & 2.6 \\
0 & 0 & 0 & 1.2 & * & 0 & 0.2 & 2.4 \\
0 & 0 & 0 & 0 & 0 & * & 0 & 3.8 \\
0 & 0 & 0 & 0 & 0 & 0 & * & 3.8 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & *
\end{bmatrix} \times 10^{-4}
$$

*diagonal computed by model

Figure A-3. Input Q Matrix

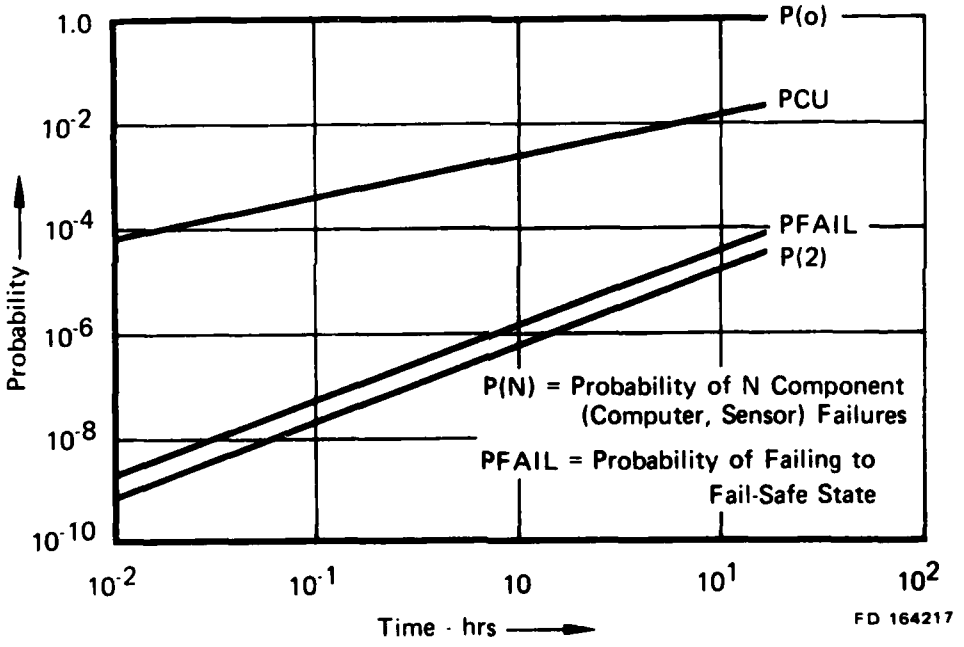


Figure A-4. Reliability Model Results for Sample Case

FD 164217A

Note, that in actual practice, repair might be undertaken before system failure with the system being restored to full health from an operational but partially failed state. This would correspond to the addition of repair transitions, as shown in Figure A-5. There is a mean time to removal from service for the unit once the repair point has been reached. This would be approximately equal to half the mission time, reflecting the fact that the unit would continue in service at least to the end of a mission and a failure could occur duing this time. The mean time to repair is simply a measure of the time required to repair the unit after it is removed from service. The time spent in the repair state vs time spent in service is a good measure of unit availability and can be useful in computing life cycle costs and spares requirements. Note, also, that not all failure states need trigger a repair action. The unit can be left in service with particular types of failures and repair would not be triggered until another failure event. By varying the maintenance policy for the unit, and running the Markov model with maintenance transitions for that policy, an optimum balance can be reached between maintenance activity and reliability considerations. In this example, mean time to removal from service is constant for all states which will trigger repair. This also need not be the case as some of these transitions may correspond to a repair policy of removing the unit for repair at the end of the current mission and some could correspond to a repair policy to fix the problem at the next engine overhaul. This second policy would be equivalent to deferring maintenance on less serious problems to a convenient time.

Several advantages of the Markov approach should now be apparent. First, and most apparent, is the ability to handle time-varying failure rates. Since numerical integration is used, any expression defining transition rates as a function of time can be used. Secondly, since Markov modeling explicitly tracks sequences of events, it is relatively easy to differentiate one state from another by the sequence of events or ordering of the state transitions which brought the system to a given state. Thus, if it matters whether A failed before B or B before A, it is possible to create two states representing both A and B failed: one in which A failed first, the other in which B failed first. Since complex redundancy creates many situations in which the chronology of failure events is critical, this ability to handle sequenced events is deemed to be critical.

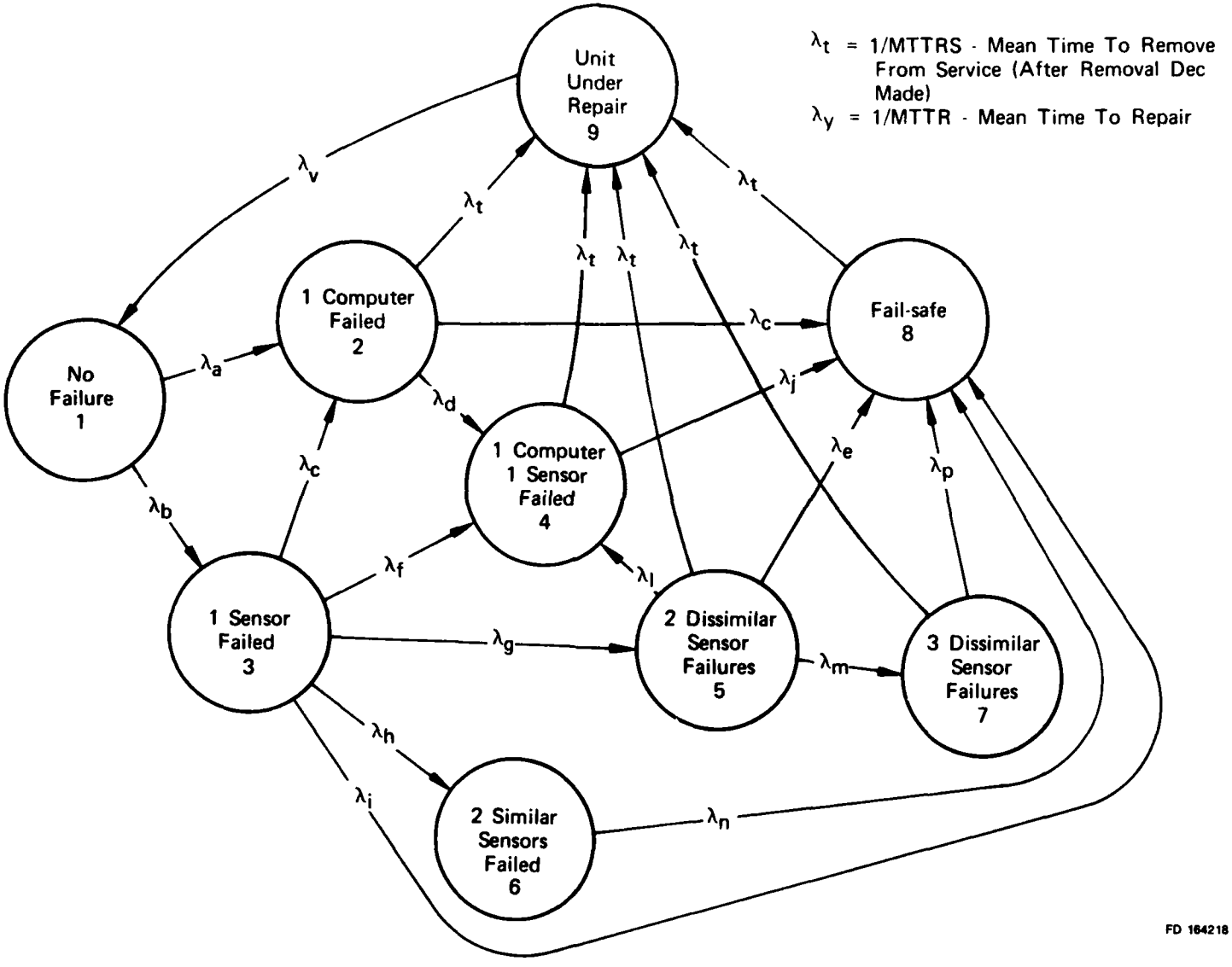


Figure A-5. Model Example With Maintenance States

Thirdly, since repair states or operational states can be incorporated into the modeling, direct measures of such parameters can be established. For example, estimates of how often the system must be repaired, how frequent are mission aborts, how available the system is, can all be computed with little additional effort by associating appropriate system states or groups of states with operational and maintenance action requirements. If, for example, it were operational policy to repair any controller faults as scheduled maintenance when convenient after the first fault, and redundancy was such as to allow operation with a number of faults, but to require unscheduled maintenance if certain combinations or numbers of faults occurred, then the model would generate predictions of frequency of scheduled maintenance, frequency of unscheduled maintenance, fraction of time spent operating in degraded states (with faults), the fraction of time the system was unavailable due to unscheduled maintenance, and other useful and valuable statistics as well as the system fail-safe rate (rate of inflight reversions to backup).

Finally, the Markov model handles coverage calculations and fault latency better than any competing models. Coverage involves the detection of a fault, isolation or diagnosis of its source, and reconfiguration. Models often combine this concept into a single number which is intended to represent the a priori likelihood of successful detection, isolation and recovery under a wide range of (often all) circumstances. In contrast, the Markov state approach can fully model the state of an undetected fault with the increased hazard associated with that state until the fault is detected. It can model the diagnostics state with its likely outcomes, both correct and incorrect diagnosis, and it can model the recovery phase dealing only with the likelihood of correct operation of the recovery mechanism given correct diagnosis and timely detection. It is possible to model these phases in numerous locations with the model using coverage segments which are tailored to the situation and linked closely enough to the physics of the situation to provide good guidance. Additionally, such phenomena as coverage of double faults, or triple faults, are explicitly treated by the Markov model as a result of its structure, and do not require special effort.

6.0 SYSTEM PARTITIONING AND SUBSYSTEM MERGING PROCEDURES

For modeling of complex systems it is best to divide the system into smaller, more tractable segments and model each segment independent of all the other segments. This can reduce the number of Markov states substantially and result in a lower computation cost as well as a cleaner, more comprehensible model. The best partitioning strategy is to divide the system into segments that do not interact with each other at all and have no interdependencies between them. However, in practice this is not always possible. The next best strategy is to choose the partitioning boundaries such that interdependencies between the segments are minimized. These interactions are eventually taken into account when the results of submodels are merged together. Therefore, this approach does not sacrifice any accuracy in the modeling process and the results would be identical to those obtained by solving a single Markov model representing the whole system.

To illustrate the concepts of partitioning a system and then merging the results consider a simpler version of an engine control system than that described in Section 3.0. Let us assume that there are three sensors in the control system A, B and C and that these are the only components which fail. Each sensor may be synthesized from the other two accurately. Therefore, a single sensor failure does not affect the control system and the engine performance is the same as if no failure had occurred. Let this state of the system be known as the 'Alert' state. Further assume that the controller continues to function, although in a slightly degraded mode, when any two out of three sensors fail and let this state of the engine be known as the 'Degraded Performance' or the DP state. Finally, let the state corresponding to three failed sensors be known as the 'Abort' state.

This hypothetical control system may be modeled as shown in Figure A-6. There are eight states in this Markov model corresponding to none, one, two or three failed sensors. When none of the sensors is failed, the system is in 'OK' state (state 1 in Figure A-6). States 2, 3 and 4 corresponding to a single failed sensor are the Alert states. States 5, 6 and 7 corresponding to double failures are the DP states and state 8 with all the sensors failed is the Abort state. This model has a fairly small number of states and transitions amongst the states; therefore, it is quite clear and comprehensible. However, for the sake of illustration, let us segment this system into three subsystems and model each individually.

The system of three sensors can be partitioned into three segments or models each of which represents one sensor. Each segment is modeled independently as shown in Figure A-7. The two states in each model correspond to the sensor being in the OK or the failed state.

It is possible to model each sensor independently of the other two sensors because the failure of each sensor is assumed to be independent of the state of the other two sensors. That is, there is no correlation whatsoever between the functioning of the three sensors. In general, different parts of a system may be modeled separately only if the events modeled within one partition or submodel are independent of the events of the other submodels. In terms of Markov models, that implies that a state transition in one submodel cannot cause a transition in any other submodel of the same system.

As a general rule the failure of various sensors and actuators in an engine control system may be assumed to be uncorrelated. However, care should be taken so as to avoid confusing independence of the failure events with equivalence of independent events in their effect or impact on the system. As an example, consider a triple redundant computer architecture where each computer reads a third of the sensors and exchanges this data with the other two computers. If each sensor can be read only by one computer then the failure of one computer would also imply a loss of one third of all the sensors.

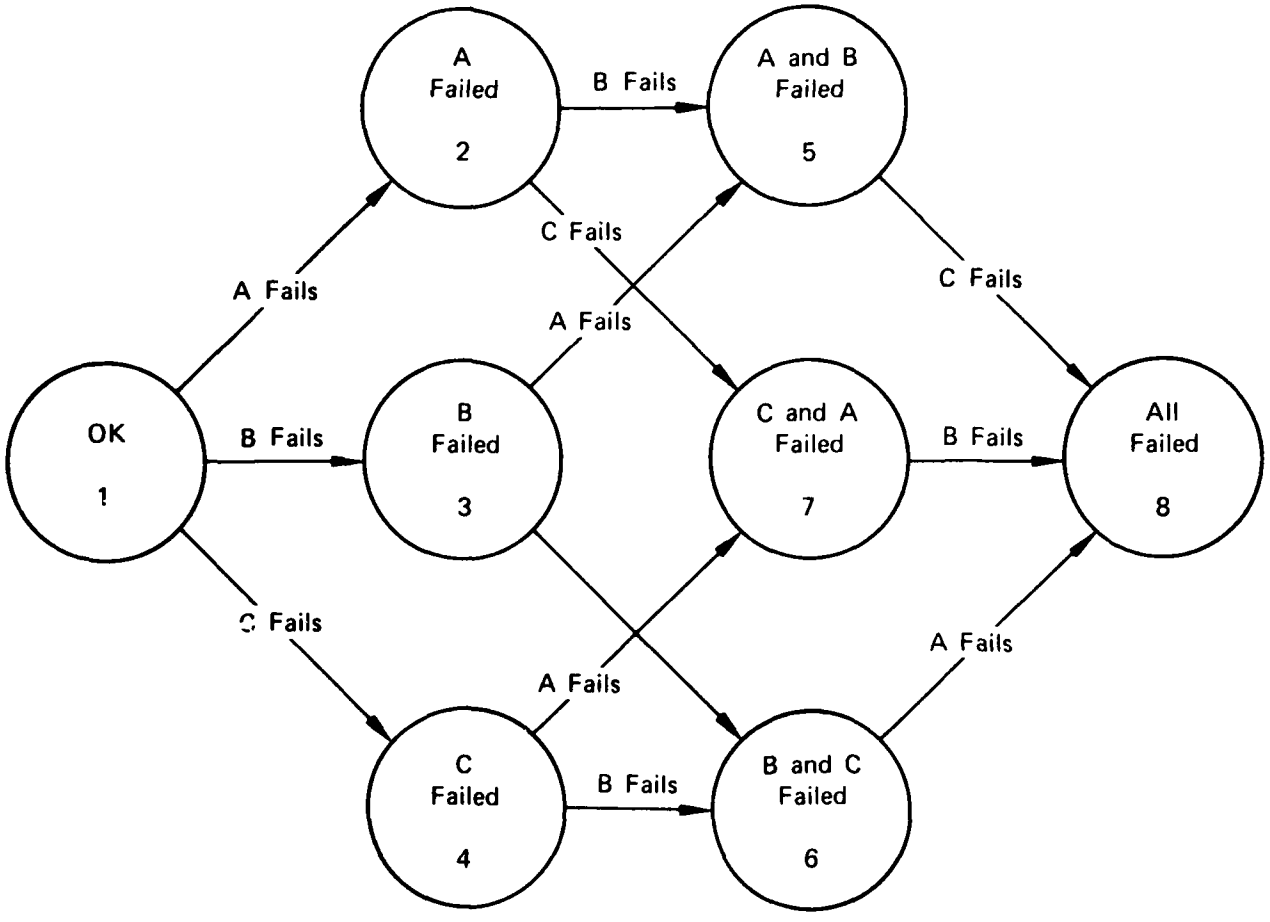


Figure A-6. Unified Example

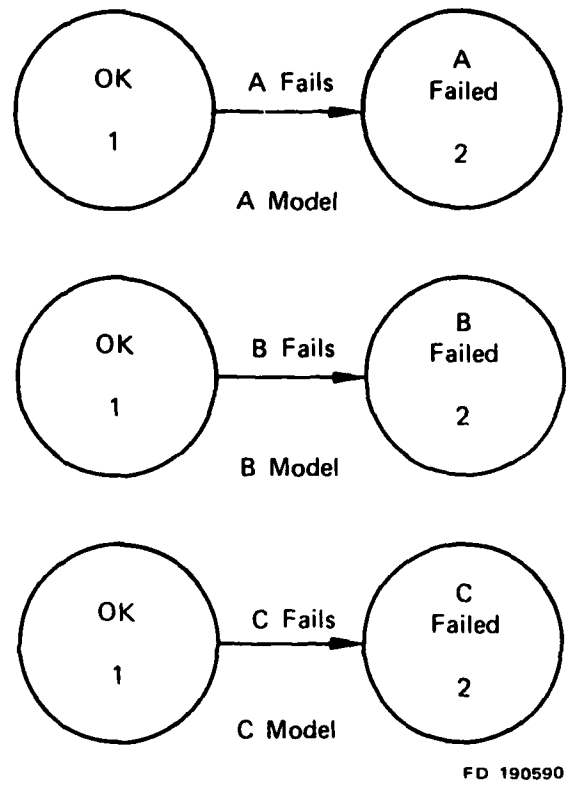


Figure A-7. Partitioned Example

In any case, it can be seen that one 8-state model has been replaced by three 2-state models. In general, the number of states in a single super model could be as high as the product of the number of states in each submodel. However, this number may be lower if some combinations of states from submodels map into a single state of the super model. For example, if the effect of all the double sensor failures was the same as that of the triple sensor failure then states 5 to 8 in the super model could all be merged into a single state and the total number of states would have then been only 5.

Having partitioned the system into three segments and modeled each segment independently, the next step is to solve the three models. This is quite straightforward. Each model is handled independently by initializing its state probability vector and computing its state probabilities as a function of time by using the transition matrix for that model alone. Once a numeri-

cal solution has been obtained for each model, one would like to map the submodel states into the super model states. The merging process can be illustrated with the same 3-sensor system used for the partitioning case.

Each of the three models of Figure A-7 represents the status of one sensor A, B or C. The super model of Figure A-6, on the other hand, shows the status of all the three sensors. Therefore, in order to establish the complete system state using the submodels, it is necessary to know the state of each sensor in each submodel. It is quite obvious that there are eight different combinations of states from the submodels. Each of these eight combinations maps into a unique state of the super model. This mapping is shown in Table A-1.

TABLE A-1

MODEL MAPPING

Model A State	*Model B State*	*Model C State*	*Super Model State*
1	1	1	1
2	1	1	2
1	2	1	3
1	1	2	4
2	2	1	5
1	2	2	6
2	1	2	7
2	2	2	8

Mathematically, the mapping is quite simple. The probability of being in a given state in the super model is simply the product of the probabilities of the three models being in the required corresponding states. For example, the probability of 'Mission Abort' (state 8 in the super model) is the product of the probabilities of all three models being in state 2. That is,

$$PROB(ABORT) = PROB(S8) = PROB(A2) * PROB(B2) * PROB(C2).$$

In the above equation PROB(S8) is the probability of the super model A being in state 8, PROB(A2) is the probability of model A being in state 2 and so on.

It is not necessary to have a super model in order to merge the models of system segments. It is only necessary to establish the criteria for various system states using the FMEA tables. As an example, we know in the present case that the system state is 'Degraded Performance' if any two of the three sensors are failed. The probability of this event can be written in terms of the probabilities of submodel states quite simply, as follows.

$$\begin{aligned} \text{PROB(DP)} &= P(A2) * P(B2) * P(C1) \\ &+ P(A1) * P(B2) * P(C2) \\ &+ P(A2) * P(B1) * P(C2). \end{aligned}$$

The mathematical principle underlying the procedure of merging multiple models can be illustrated with the help of Venn diagrams. The three models of Figure A-7 may be represented by Venn diagrams as shown in Figure A-8. Notice that the outer circle in each case represents the sum of all the states in that model. The circle of 'set' is segmented into various segments or 'subsets,' one segment for each type of state. To obtain an equation for the probability of the system being in a certain state, say all OK states, it is necessary to combine the three Venn diagrams. The subsets or segments from each circle can be combined with subsets from other circles in two ways. The first of these is called the 'intersection.' The intersection of two sets results in a segment or a set that is common to the two sets being combined together. This is analogous to the logical operation 'AND.' The second way is to add two subsets or segments. This is called a 'union' of sets and results in a segment that appears in either of the sets being added together. This operation is analogous to the logical operation 'OR.' Mathematically, the AND operation is equivalent to taking the product of two probabilities and the OR operation is the same as summing two probabilities. The AND and the OR operations can, of course, be extended to more than two operands.

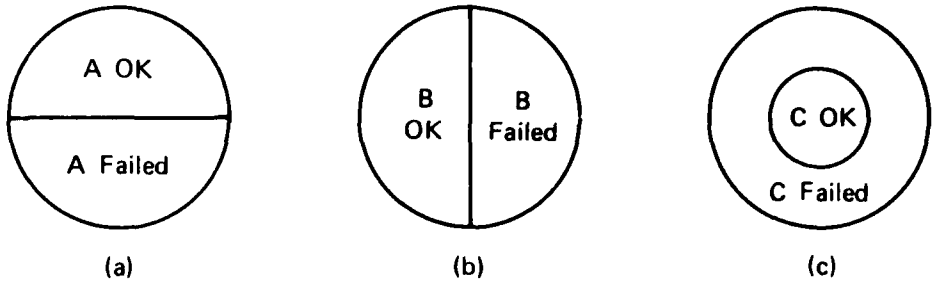


Figure A-8. Venn Diagram Representation of Partitional Example (Figure A-7)

Now, the system is with OK state if all the models are in the OK state, that is, none of the three sensors is failed. This is equivalent to obtaining the intersection of three sets: A1, B1 and C1. For the sake of clarity, this is broken down into two steps as shown in Figure A-9 (a, b). The Venn diagrams in Figure A-9 (a) show the interaction of A.1 (sensor A OK) with B.1 (sensor B OK). Figure A-9 (b) shows the intersection of C.1 (sensor C OK) with the subset resulting from step 1. This process could also have been accomplished simply by overlaying the three sets on each other as shown in Figure A-10.

To obtain the probability of the system being in DP mode, it is necessary that two of the three sensors be failed. There are three such combinations and the Venn diagram representation for each of these is shown in Figure A-11 (a, b, c). The union of these three sets as shown in Figure A-12 is the desired probability. Since the intersection and the union of two sets corresponds to the products and the sum of two probabilities respectively the relationship between the equation obtained earlier for the probability of degraded performance and the Venn diagrams shown in Figures A-11 and A-12 should become obvious.

One advantage of Venn diagrams is that they provide a visual representation of the mathematical equations. However, topologically these diagrams can get very complex with a large number of models and/or states and in general cannot be mapped into two dimensional diagrams as in this example. Indeed in this example, the complexity has been deliberately constrained to almost a trivial case in order that the Venn diagram be topologically tractable. Their utility is thus primarily one of tutorial aid.

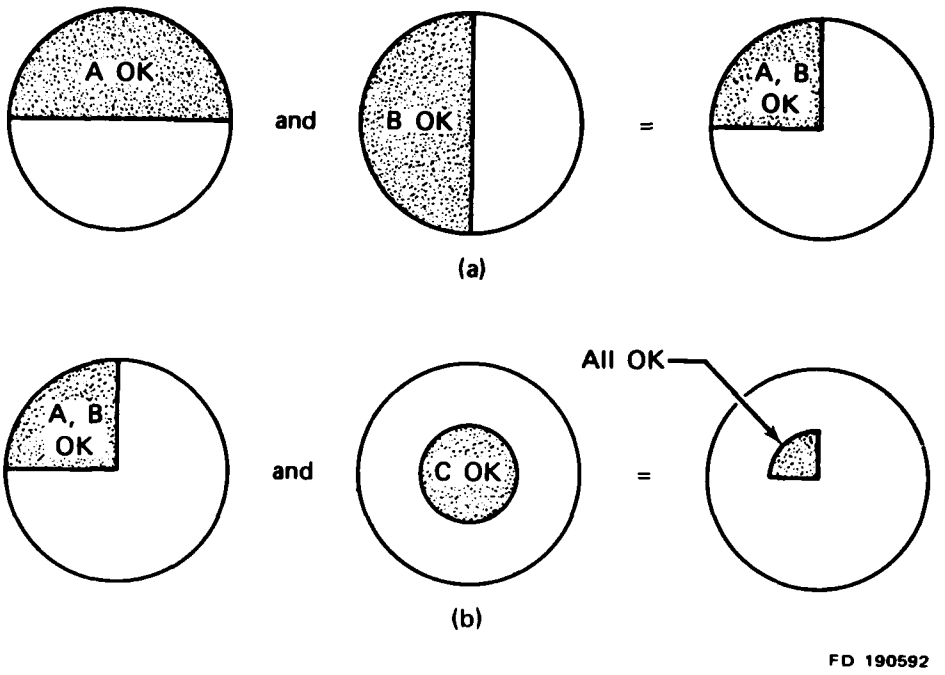


Figure A-9. Intersection of the Venn Diagrams

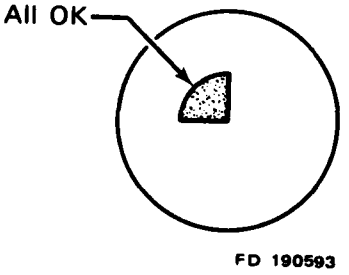


Figure A-10. Resultant Intersection of the Venn Diagrams

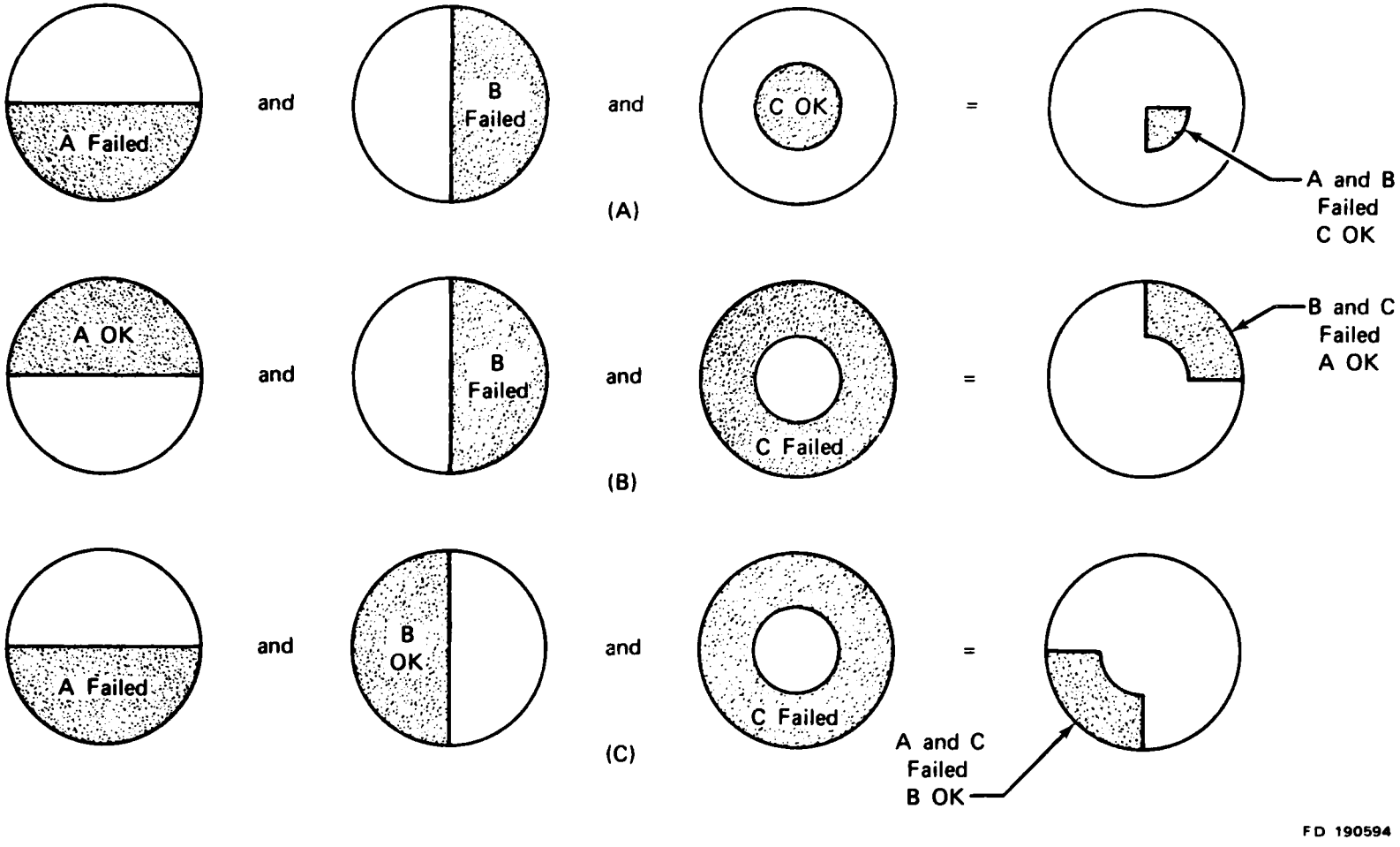


Figure A-11. Venn Diagram Representation With Two Sensors Failed

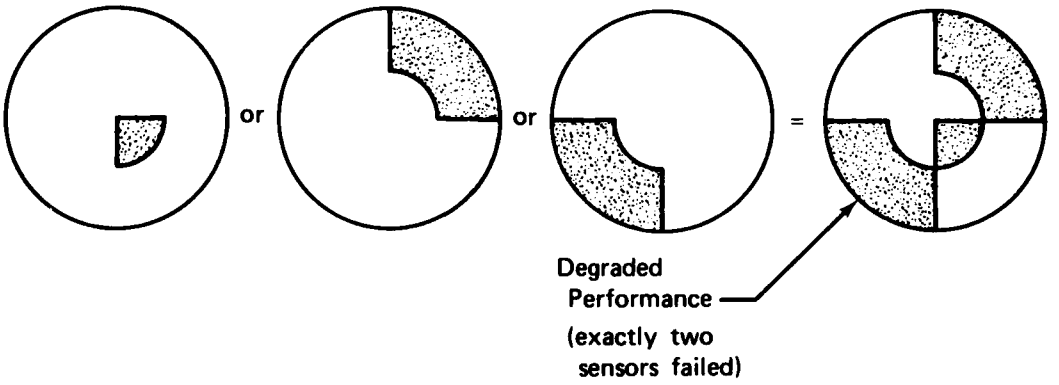


Figure A-12. The Resultant Union of the Three Sets Represented by Venn Diagrams

7.0 RELIABILITY MODELING PROGRAM

Program Overview

A numerical method to solve a Markov model was described in Section 4.0. To recapitulate briefly here, the method involves integrating the following vector-difference equation.

$$\bar{P}(K+1) = Q \cdot \bar{P}(K)$$

In the above equation, $\bar{P}(K)$ is the state probability vector of the system after K time-steps of, say, Δt and Q is the state transition matrix corresponding to the time-step Δt. To solve this equation numerically, the state probability vector $\bar{P}$ is initialized at some point in time where the probability of the system being in various states is known. The system state probabilities at a future instant in time may then be obtained by multiplying the vector $\bar{P}$ by the transition matrix Q. The only practical way of implementing this procedure is to do it with the help of a digital computer. Therefore, a general purpose program has been written in a high level language (PL/I) to perform the integration of the vector-difference equation described above. A number of features have been added to this basic program to facilitate a simple and straightforward interface between the user and the program. It is not necessary for the user, for example, to be conversant with the PL/I language or be a programmer. One only has to know the format of a few statements required to input the model specification and certain other data to obtain the required results from the program. The exact format and meaning of these statements, that is, the input specification language is described in the next section.

There are three sets of data that completely define a Markov model at a given instant in time. These are the number of states in the model, their occupancy probabilities at some initial time (i.e. the state probability vector $\bar{P}$) and the transition rates amongst the states. These are the parameters that are input to the computer program using the input specification language. As should be evident by now, there are no architectural limitations on the systems that can be modeled by this program. In fact, any system that can be represented by a Markov process can

be modeled using this program. Systems as diverse as engine controllers and supermarket queues may be modeled by this program. Unlike some other 'general purpose' reliability modeling packages such as CARSRA which also are based on Markov processes there are no preconceived restrictions on the interconnections between the states. That is, transitions from each state to every other state may be defined by the user. Additionally, a relatively large model can be easily handled by this program. Depending upon the computer memory size and the operating system under which this program is run, as many as 500 Markov states may be defined in a model.

One of the strong features of this program is its ability to handle several models in parallel. This allows the user to partition his system in several small segments and construct an independent model of each segment. A judicious partitioning of a complex system can result in several smaller models with far fewer total number of states than the number of states in a single Markov model that represents the complete system. There are two reasons for modeling a system through several small models rather than a single large model. First of all, the number of states in a single model, which increases in an exponential proportion to the number of state variables, may be well beyond the capabilities of the largest digital computers available today. Second, even if it were possible to solve such a model, the comprehensibility of such a model decreases rapidly as the number of states in the model are increased. To someone not directly involved in the modeling process the fidelity of the model and the correspondence between the system and the various states of the model may be totally obscured by the large number of states and state transitions. Therefore, a partitioning of the system just for the sake of clarity and tractability is justified. Eventually, of course, one must take into account the large number of states that have been eliminated by this process. Therefore, appropriate tools have been provided in this computer program to merge the results obtained from the solution of the several small models. The system state probability is a sum of a number of terms. Each of these terms is a product of one state

probability term for each model to be merged. (A detailed explanation of how to partition a system and how to merge the models back together and the mathematical principles underlying this process, is provided in Section 6.0.) These sums of products terms using standard algebraic operators and symbols identifying states in various models can be input to the computer program to define the system state probabilities. The details of all the valid operators, state identification symbols etc. are contained in the next section.

Once all the system state probabilities have been computed for the requested time span, the program formats the results as required. The user may request printouts of numerical data, that is, state probabilities and/or plots of them as a function of time. Algebraic combinations of various state probabilities may also be printed and plotted. As part of its documentation output the program summarizes each model by including a description of all the states and state transitions in the printout.

In summary, the reliability modeling program being applied to the FAFTEEC program is a powerful tool available to the control system designer to help evaluate alternate candidate architectures. This tool performs a number of helpful functions. First of all, it frees the designer from mundane programming details and helps him concentrate on the problem at hand. Second, it tells the designer whether or not various reliability goals will be met by a certain control system. Third, if the goals are not met, the reliability bottlenecks of the design are easily identified. This valuable feedback enables one to make appropriate system modifications and evaluate the impact of those changes by running the revised model through the program. Several such design iterations can quickly converge in an optimal control system that meets the reliability requirements.

MARK1 USER INSTRUCTIONS

All the input from the user to the program is contained in an input file. The input file is organized as an 80-column card deck image. The output generated by the program consists of a copy of the input file, summary descriptions of Markov models, state probabilities as a function of time and plots of probabilities as a function of time.

The input file is divided into three logical parts. The first part of the file is the model specification. The model is specified by the total number of Markov states in the model, the description of each state, the initial state occupancy probabilities and the interconnections between the states, that is, the transition rates between these states. If multiple models are to be solved simultaneously then all the models are specified sequentially in the first part of the input file. The second part of the input file is the time-span for which the Markov model should be solved, that is, numerically integrated. The last part of the user input to the program consists of commands to merge the results of the models, if there are more than one, to obtain the system state probabilities. In addition to the standard printed results generated by the program, plots may also be obtained by including appropriate plot commands in the Q_s portion of the input file. The exact sequence and format of each command in the input file is described in the following.

The general format of each card calls for a key word beginning in column 1. This key word identifies the type of data to follow on that card to the program. The format of the data

depends on the type of the card. Most model parameters such as initial state probabilities, the number of states in the model and the state transition rates are defined using assignment statement format. An assignment statement consists of the parameter identification followed by the assignment operator (=) followed by the numerical value to be assigned to the parameter. Each card may have comments following the data required on that card. The comments should be separated from the data by a colon.

Normally, the first input card should be the TITLE card. The key word TITLE should begin in column 1. This is followed by text. This text will be printed as the title on top of each page of result produced by the program. The text field is separated from the key word field by a colon. This card has no numerical data on it.

After the TITLE card, the user has the option of including a delta card. If no delta card is included the program uses the default value 1.E-5 for delta time. The delta card has the following format.

D = step

D is the key word in this card, 'STEP' is a floating point number in scientific notation that is the initial integration time step.

The next part of the input specifies the model parameters. The first of these cards defines the model number and the number of Markov states in this model. This card has the following format.

Mii=jjj:text

M is the key word in this card, 'ii' is the model number and 'jjj' is the number of states in this model. Models are normally numbered sequentially starting at number 1. Optional text may follow the assignment statement, separated by a colon.

The M card is followed by up to 'jjj' S cards, that is, one card for each state. The format of the S card is as follows:

Snnn=p:text

Here, S is the key word, 'nnn' is the state number and 'p' is the initial occupancy probability of this state. 'p' is a number between 0 and 1 in scientific notation and 'nnn' is an integer less than or equal to 'jjj'. Optional text may follow the assignment statement, separated by a colon. Normally, there should be an S card for each state in the model. However, those states for which there is no card are assigned an initial probability of zero. Since the program, as part of its output, produces a textual description of the model by compiling the text on S cards, one may wish to include a card and a description of each state in the input file for the sake of completeness.

The S card is followed by the L card. The L cards are used to define constants on various algebraic combinations of previously defined L's. These L values will be used later on the T cards to calculate transition rates. The format of the L card is as follows:

Li=exp:text

Where L is the key word and exp is an algebraic expression or a constant. Optional text may follow this statement. The following is the set of allowable operators for the L cards.

Operator	Meaning
*	Product
+	Sum
-	Difference
**	Exponentiation
/	Division
()	Parenthesis

An example of three L cards is shown below.

```
L1  =  7.5E-6

L2  =  2*L1

L3  =  L1 + L2
```

Failure rates (L's) and models (M's) should be sequentially numbered starting at 1 and without skipping any numbers, i.e., L1, L2, L3 etc. and M1, M2, M3 etc.

The next part of the model specification is the definition of transition rates. The state transitions are assigned numerical values using the assignment statement as shown below.

```
T1>j=rate: text
```

T is the key word, 'rate' is a constant or an algebraic expression that is assigned to the transition from state 'i' to state 'j'. 'i' and 'j' are intergers (state numbers) and are separated by the sign '>'. 'rate' is the transition rate per hour. Optional text may follow this statement. The default value for a transition not specified by a T card is zero. If rate is an algebraic expression all the previously defined operators and L values may be used to calculate the transition. An example of three T cards is shown below.

```
T1>2  =  10.9E-6

T2>3  =  L1+3*L2

T5>8  =  L3
```

The self-transition, that is, a transition from a state back to itself should not be included in the input since they are automatically derived by the program.

The M, S and T cards as described above specify a Markov model completely. A number of such models may be defined successively.

The model specification is followed by a RUN command in the following format.

```
RUN t1 t2:text
```

This causes the program to compute the system state from time t1 to t2. This is done for all the models. t1 should normally be zero. t2 is in hours and can be input using scientific notation. For example, 'RUN 0 1E4' is a command to solve all models from time 0 to 10,000 hours. The next section of the input file concerns outputting of the results.

The default output of the program is a listing of all the system states after each step of integration. The diagonal elements of the Q matrix are also displayed at time t1 for each model. This detailed reporting may be suppressed by the ABR (abbreviate) card. There is no other data on this card other than the key word ABR. This card should appear in the input file just after the RUN card. The abbreviated reporting consists of the state vector at the beginning of each new time-step, that is, every ten steps of integration. The Q-matrix is not displayed.

In addition to the printed results, the user can obtain plots of various state probabilities as of function of time. There are two cards that are used for this purpose.

The first card is the F card with the following format:

Fi=exp:Text

where i is an identification of the factor for later use on a F or Plot card, and exp is an algebraic expression combining states and other factors as follows:

F3=Sm.n+F1

Sm.n identifies the state of particular model. m and n are the model number and the state numbers, respectively. The F card is used to make it easier for the user to create the plot cards. F factors may be numbered in any order.

The second card is the PLOT card. The plot card can be used as follows:

PLOT Sm.n: Plot title

Plot is the key word on this card and Sm.n identifies the state for which the plot is desired. Sm.n is the general format for identifying a state of a particular model. m and n are the model and the state numbers, respectively. An optional text may follow this statement, separated by a colon. This text appears as the title on the plot.

It is also possible to plot various algebraic combinations of states within one model or combinations of models by using defining F cards and using a set of operators.

The following is the set of allowable operators for both the F card and the PLOT card.

Operator	Meaning
*	Product
+	Sum
-	Difference
**	Exponentiation
/	Division
()	Parenthesis
¬	Complement
>	From_To
,	Sequence

The meaning of the first six operators is obvious. The complement has the following meaning:

```
¬ S1.1=(1-S1.1)
```

The From_To operator has the following meaning:

```
S3.5>8=(S3.5+S3.6+S3.7+S3.8)
```

and the sequence operator has the following meaning:

```
S2.1,5,7=(S2.1+S2.5+S2.7)
```

The complement operator computes the probability of not being in the state that follows this operator.

The From_To operator sums the probabilities of all the states from the state number preceding the operator to the state number following the operator.

The sequence operator sums the probabilities of the states separated by the operator.

The user has the option of producing multiple plots on a single frame. This is done by separating each plot expression with a ";" as follows:

```
PLOT S2.3+F1:title1; S5.7,8+F2:title2
```

This card would produce two curves on the same set of axis. The program allows 10 plots to a frame.

An expression of state probabilities may be continued on more than one card. The statement may be broken anywhere after the key word PLOT or F and may continue on the next card starting in column 2 or thereafter. No continuation character is necessary on the preceding card.

A listing of the numerical values of each plot is also provided as part of the program output.

Results from multiple models may be merged to obtain the overall system state probabilities by using the algebraic expressions. This results in a plot and a numerical printout of that state probability, as outlined above.

The last card in the input file is the END card and all input after it is ignored.

The next section includes a sample input deck, printed output and the plots produced by MARK1 package.

Modeling Example

Consider the system shown in Figure A-13. This is a hypothetical digital engine controller. It consists of a simplex computer that reads a number of sensors and controls a number of actuators. The sensor set consists of pressure (P), temperature (T) and speed (N) sensors. There are two actuators, fuel flow (F) and vane angle (VA). Table II shows the failure modes and effects analysis (FMEA) for this control system. The reader should keep in mind that the control system components and the effects of their failures have been chosen purely for illustrative purposes. The assumptions made here have no relation to a realistic controller and its FMEA.

The effect of all the possible failure combinations is listed in the FMEA table, Table A-2. The effect may range from a maintenance alert to reversion to the backup controller (BUC). Other effects include a degraded engine performance and mission abort due to a lack of engine performance. Also tabulated with the FMEA are the hypothetical failure rates for these items.

The number of items in the control system are small enough so that a single Markov model could represent all the states corresponding to various failure modes. However, for illustrative purpose the control system could be partitioned into two models as shown in Figures A-14 and A-15.

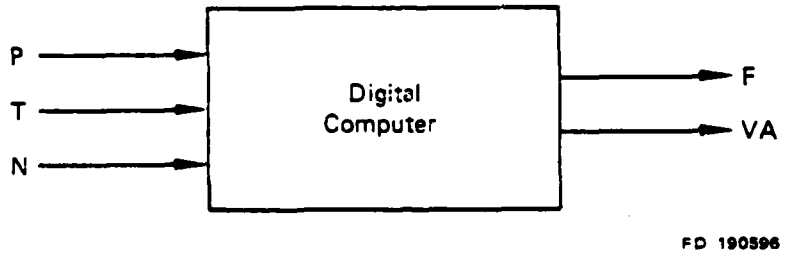


Figure A-13. An Example Engine Controller

TABLE A-2
FMEA FOR THE EXAMPLE CONTROLLER

Failed Item(s)	*Effect*	*Rate (Per Million hr)*
P	Alert	2
T	Degraded Performance	4
N	Degraded Performance	10
F	Mission Abort	6
VA	Degraded Performance	12
DC	BUC	10
Any two Sensors	Mission Abort	
All Three Sensors	BUC	
F, DC	BUC	
VA, DC	BUC	
F, VA	BUC	
F, VA, DC	BUC	
Any Sensor and Actuator	BUC	

Model 1 (Figure A-14) represents all the sensor failure combinations and model 2 (Figure A-15) represents all the actuator and computer failure combinations. In general, each item of the control system should appear in one and only one model. State 1 in model 1 corresponds to all three sensors functioning correctly, states 2, 3 and 4 to one sensor failure, states 5, 6 and 7 to two sensor failures and state 8 corresponds to all sensors being in the failed mode. In terms of effect of these failures on the engine performance, state 2 corresponds to a maintenance Alert, states 3 and 4 to degraded performance, states 5, 6 and 7 to mission abort and state 8 corresponds to reversion to BUC. Notice that model 1 tells us nothing about the status of the actuators and the computer. Similarly model 2 says nothing regarding the status of the sensors.

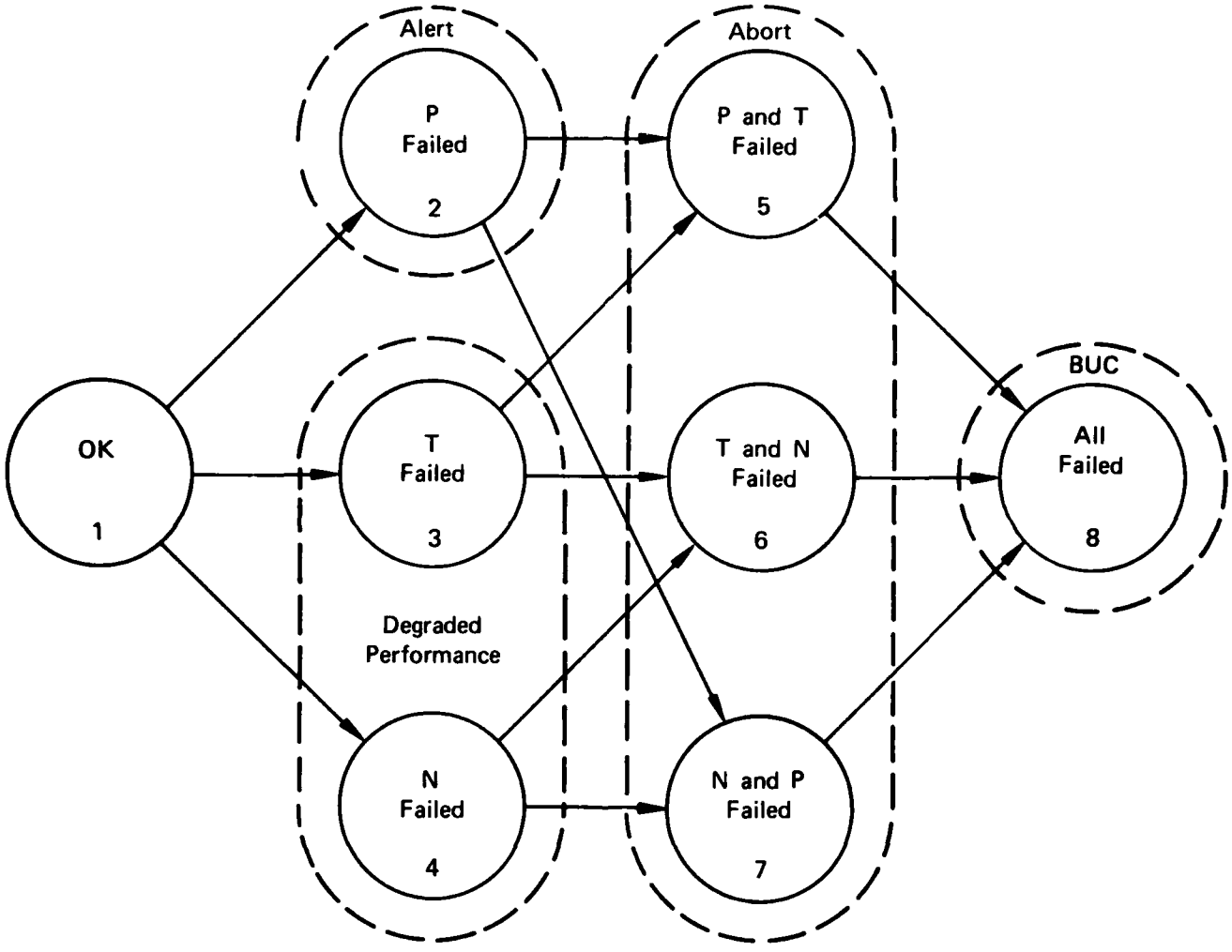


Figure A-14. Sensor Failure Model

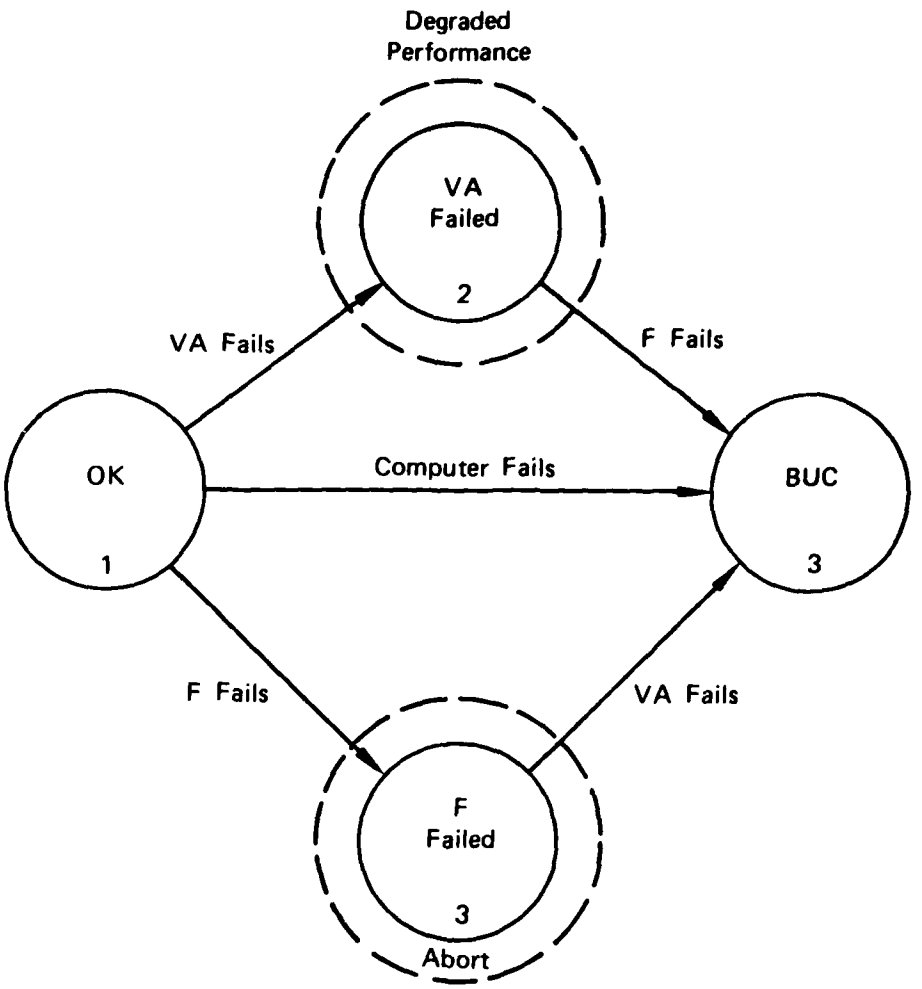


Figure A-15. Computer and Actuator Failure Model

The two models may be merged together to obtain the probabilities of the system being in various degraded modes due to a failure of any of the components as follows.

The probability that the system is in 'OK' state as a whole, that is, no failures have occurred at all is the product of the two following state probabilities.

i. S1.1 = prob (no sensors have failed)

ii. S2.1 = prob (no actuators or computer have failed)

Therefore Prob (system OK) = S1.1 * S2.1. (1)

Similarly Prob (system Alert) = S1.2 * S2.1. (2)

Prob (system deg perf) = (S1.3 (S1.4) * S2.1 + S1.1 * S2.2. (3)

Prob (mission abort) = (S1.5+S1.6+S1.7) * S2.1+S1.1 * S2.3. (4)

Prob (BUC) = S1.8+(S1.2-7) * (S2.2-3) + (S1.1.-7) * S2.4. (5)

Notice that in the above equations, the right hand side of each equation is the sum of a number of terms. Each of these terms is a product of two terms, a state probability from each model. Each of these product terms corresponds to a unique failure combination listed in the FMEA table. As an example of this, the right hand side of equation 3 has three such terms. The three terms correspond to the FMEA table entries as follows.

S1.3 * S2.1 Only T sensor failed

S1.4 * S2.1 Only N sensor failed

S1.1 * S2.2 Only VA actuator failed

Notice also from the FMEA tabulation that no failure combinations, other than the three listed above, result in the system degraded performance state.

Figure A-16 shows the input file for the reliability program to solve the two models. Figure A-17 shows the plotted results. Numeric tabulations of results are also provided by the program but are not illustrated here.

Reliability Modeling Computer Program

The computer program MARK1, written in PL/I, is composed of two modules. The first module, MARK1A, numerically solves specific models for state probability factors. The second module, MARK 1B, combines the results of these models, plots, states and combination of states of interest. The program is presently being run on Amdahl 470 computer under the MVS operating system. It can be run on any IBM compatible machine. The plotting is done, using calcomp plotting routines, on a calcomp and/or versatic plotter. With six megabytes of virtual memory, it is possible to process 50 models of 100 states each over a time period of 100 time points (10 decades).

MARK1A Functional Description

MARK1A reads and processes the input data set (deck). It makes two passes. On the first pass it determines the number of models, the number of states for each model, and the length of the run time. This is done by interpreting the 'M' cards and the 'RUN' card. After determining the run time it calculates the number of points that will be stored on disk for each state.

```
The following is the input data  set for the reliability model of
the example engine controller.
```

```
TITLE     : MARKOV MODEL OF AN EXAMPLE ENGINE CONTROLLER
M1=8      : MODEL 1 CONTAINS ALL THE SENSOR FAILURE STATES
S1=1E0    : ALL OK STATE (NO FAILED SENSORS)
S2=0      : SENSOR P FAILED (ALERT STATE)
S3=0      : SENSOR T FAILED (DEGRADED PERFORMANCE STATE)
S4=0      : SENSOR N FAILED (DEGRADED PERFORMANCE STATE)
S5=0      : P AND T FAILED  (MISSION ABORT STATE)
S6=0      : T AND N FAILED  (MISSION ABORT STATE)
S7=0      : N AND P FAILED  (MISSION ABORT STATE)
S8=0      : ALL 3 SENSORS FAILED (REVERT TO BACKUP CONTROLLER)
L1=2E-6   : P FAILURE RATE PER HOUR
L2=4E-6   : T FAILURE RATE PER HOUR
L3=1E-5   : N FAILURE RATE PER HOUR
T1>2=L1   : TRANSITION RATE FROM STATE 1 TO 2 PER HR. (P FAILURE)
T1>3=L2   : T FAILURE
T1>4=L3   : N FAILURE
T2>5=L2   : T FAILURE
T2>7=L3   : N FAILURE
T3>5=L1   : P FAILURE
T3>6=L3   : N FAILURE
T4>6=L2   : T FAILURE
T4>7=L1   : P FAILURE
T5>8=L3   : N FAILURE
T6>8=L1   : P FAILURE
T7>8=L2   : T FAILURE
M2=4      : MODEL 2 HAS ALL ACTUATOR AND COMPUTER FAILURE COMBINATIONS
S1=1E0    : ALL OK
S2=0      : VA FAILED (DEGRADED PERFORMANCE STATE)
S3=0      : F  FAILED (MISSION ABORT STATE)
S4=0      :COMP OR 2 ACTUATORS OR AN ACTUATOR AND COMP FAILED(BUC)
L1=1.2E-5: VA FAILURE RATE PER HOUR
L2=6E-6   : F FAILURE RATE PER HOUR
L3=1E-5   : COMPUTER FAILURE RATE PER HOUR
T1>2=L1     : VA FAILURE
T1>3=L2     : F FAILURE
T1>4=L3     : COMPUTER FAILURE
T2>4=L2+L3 : F OR COMPUTER FAILURE
T3>4=L1+L3 : VA OR COMPUTER FAILURE
RUN 0 1E3   : SOLVE ALL MODELS FROM TIME 0 TO 1000 HOURS
F1 = S1.1*S2.1 : DEFINE ITEMS FOR PLOTTING
F2 = S1.2*S2.1 : SYSTEM ALERT
F3 = S1.3,4*S2.1 + S1.1*S2.2 : DEGRADED PERFORMANCE
F4 = S1.5>7*S2.1 + S1.1*S2.3 : MISSION ABORT
F5 = S1.8 + S1.2>7*S2.2>3 + S1.1>7*S2.4 : REVERT TO BUC
THE FOLLOWING ARE INDIVIDUAL PLOTS, I.E., ONE PLOT PER PAGE
PLOT F1 : ALL OK
PLOT -F1: NOT OK (AT LEAST 1 FAILURE)
PLOT F2 : SYSTEM ALERT
PLOT F3 : DEGRADED PERFORMANCE
PLOT F4 : MISSION ABORT
PLOT F5 : REVERT TO BUC
        : THE FOLLOWING 3 PLOTS ARE ALL ON THE SAME PAGE
PLOT F2 : SYSTEM ALERT; F4: MISSION ABORT; F5: REVERT TO BUC
END
```

Figure A-16. Input Control Deck

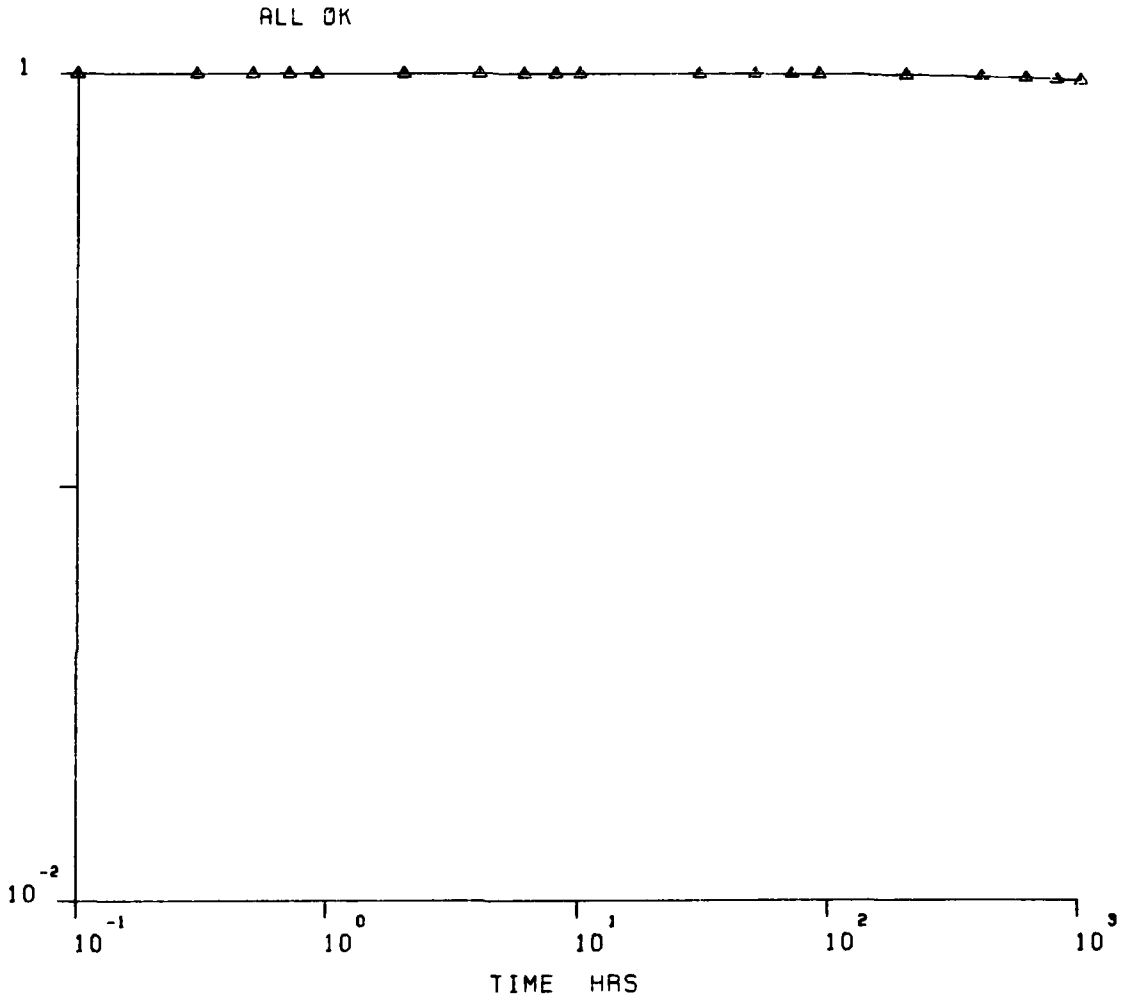


Figure A-17. Markov Model of an Example Engine Controller (1 of 7)

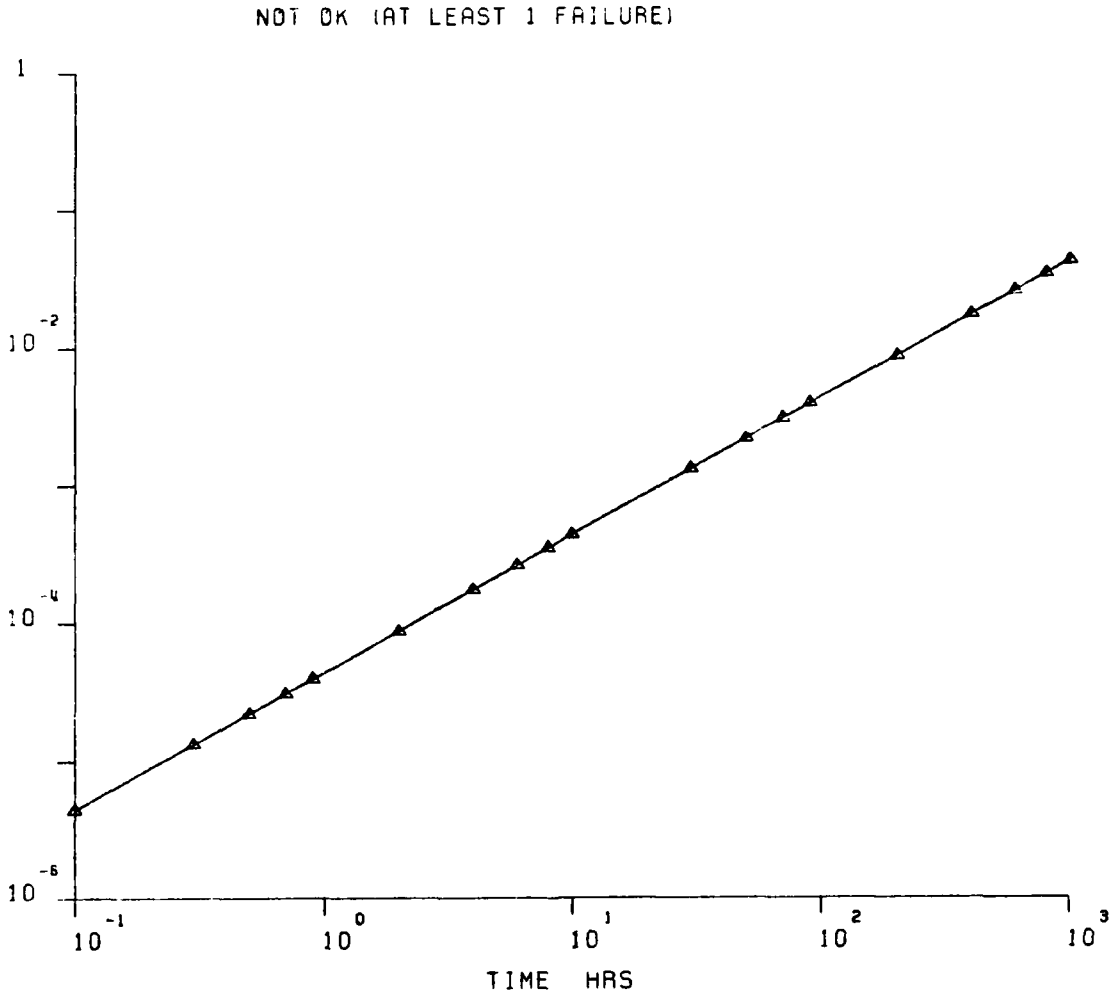


Figure A-17. Markov Model of an Example Engine Controller (2 of 7)

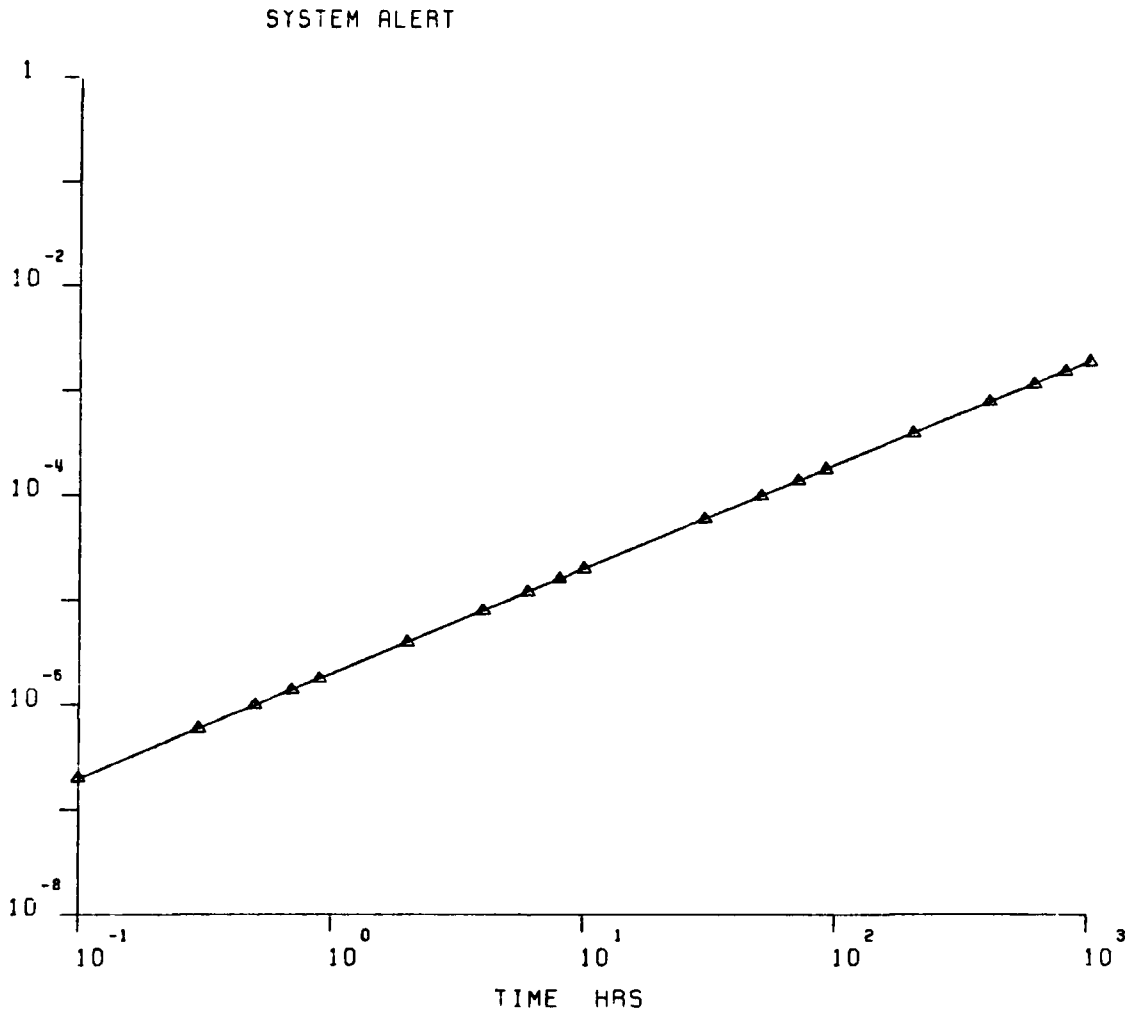


Figure A-17. Markov Model of an Example Engine Controller (3 of 7)

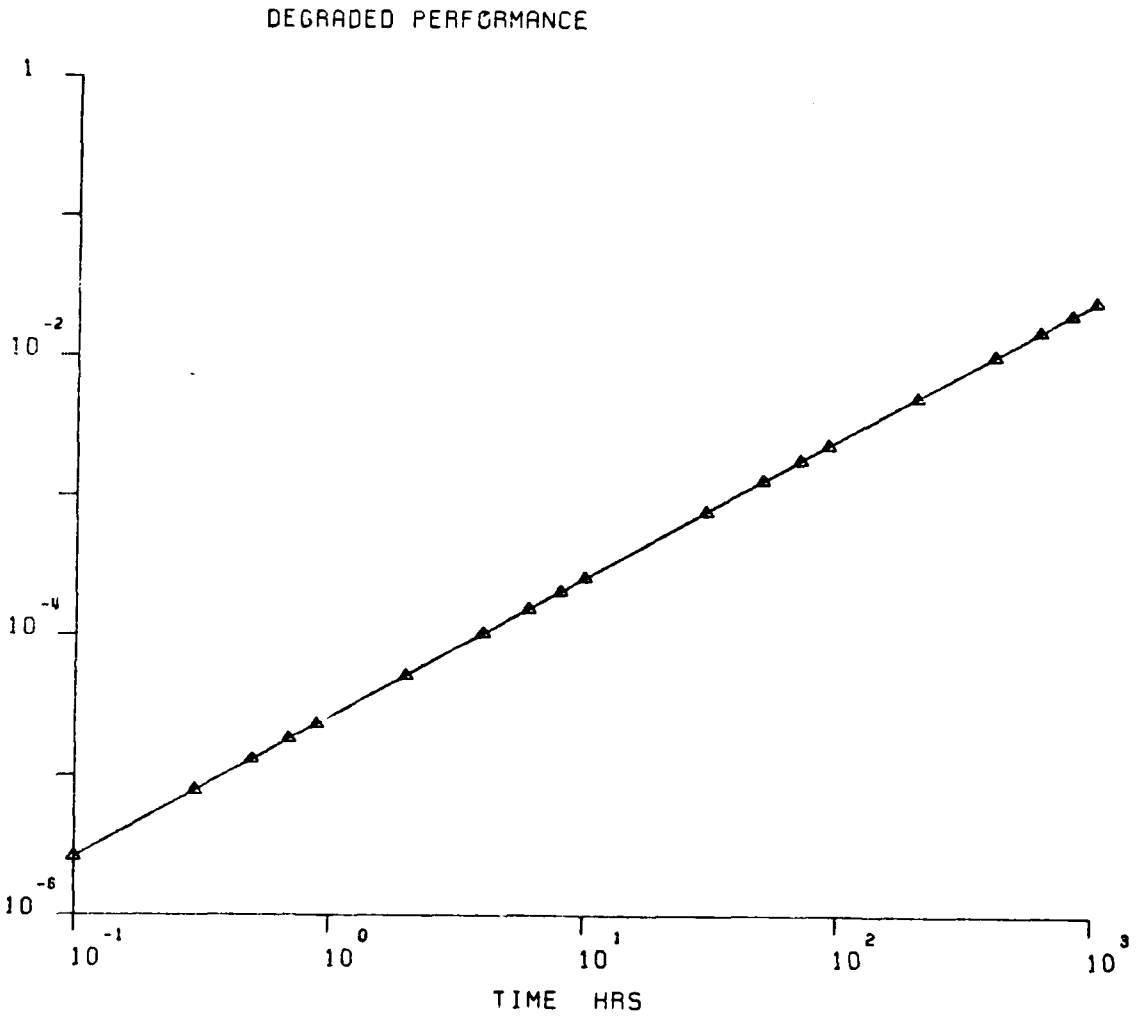


Figure A-17. Markov Model of an Example Engine Controller (4 of 7)

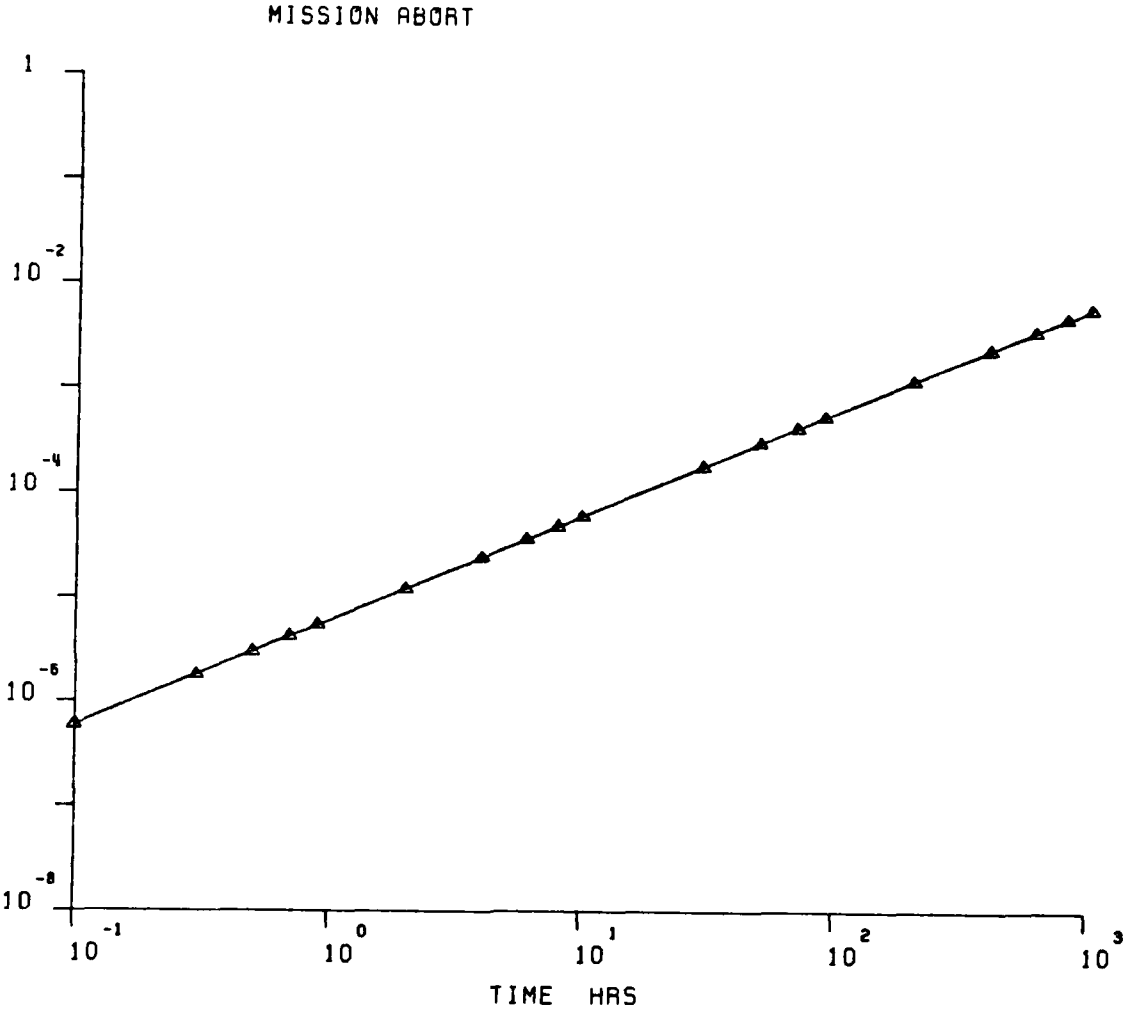


Figure A-17. Markov Model of an Example Engine Controller (5 of 7)

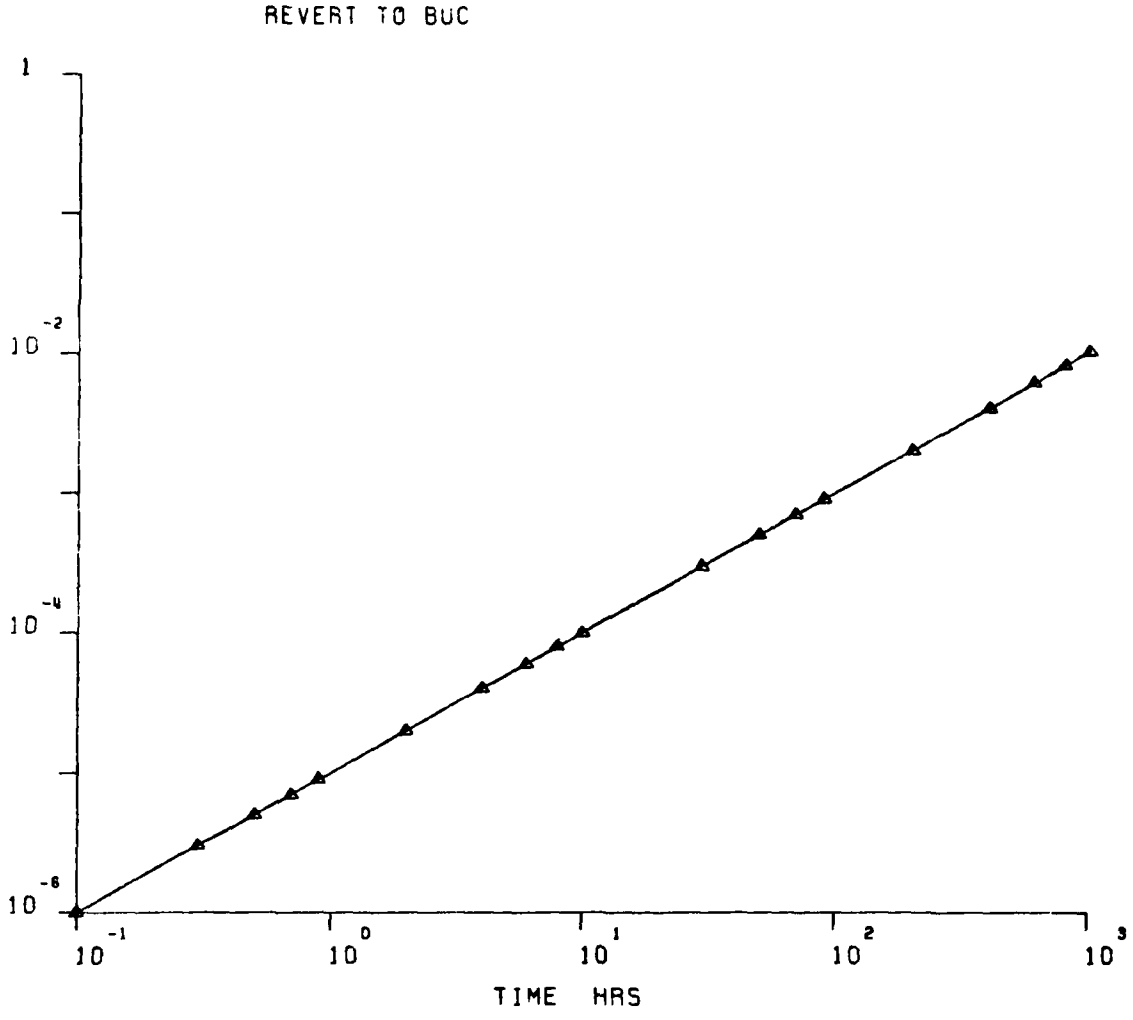


Figure A-17. Markov Model of an Example Engine Controller (6 of 7)

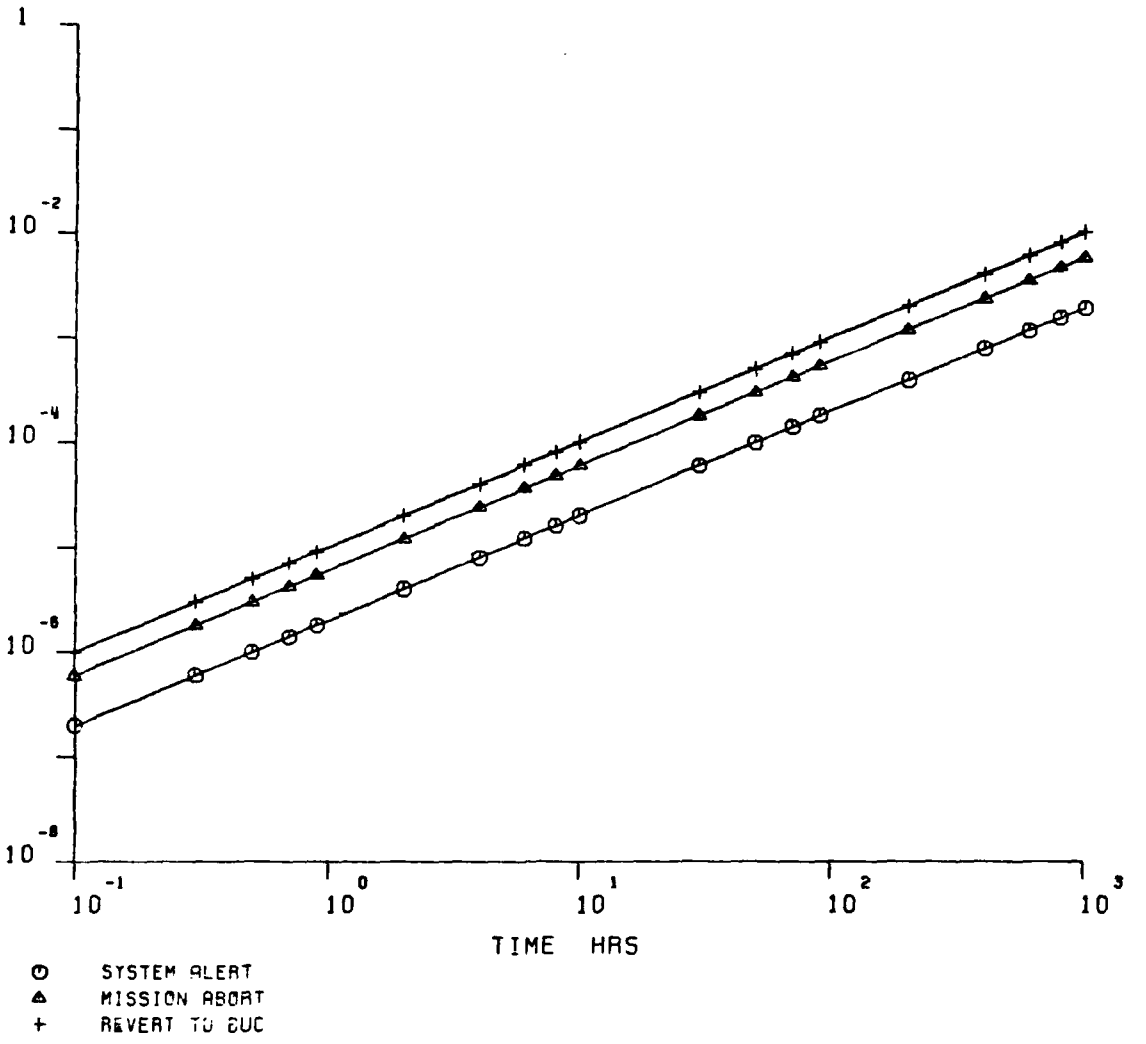


Figure A-17. Markov Model of an Example Engine Controller (7 of 7)

The program then makes a second pass through the input deck. At this point it reads and interprets the 'S' and the 'T' cards for the first model. The values on the 'S' cards are used in the program to initialize the state probability vector at time zero. The values on the 'T' cards are used to partially initialize the state transition matrix (Q-matrix).

The Q-matrix is fully calculated by multiplying the partially initialized matrix by a very small delta (1/1000) and then calculating the diagonal elements such that the rows sum to 1.

The state probability vector for each time point is calculated next. The program uses the simple algorithm:

SP (N+1) + Q * SP(N).

Delta (time) is increased ten-fold every ten iterations. The variations in Delta were chosen for compatibility with graphical display.

The program makes all of its calculations for each of the models *before* it reads and interprets the input deck for the next model.

After the state probability vector is calculated for each time point, these double precision numbers are written to disk to be retrieved and used by the second module, 'MARK1B.' These values are also to be printed on the printer. The input card 'ABR' will surpress this printed output.

The program will then continue to read the 'S' and 'T' cards for the next model and repeats the above steps until all the models are processed.

MARK1 FUNCTIONAL DESCRIPTION

The computer program MARK1, written in PL/I, is composed of two modules. The first module, MARK1A, numerically solves specific models for state probability factors. The second module, MARK1B, combines the results of these models, plots states and combination of states of interest. It can be run on any IBM compatible machine. The plotting is done, using calcomp plotting routines, on a calcomp and/or versatic plotter. With six megabytes of virtual memory, it is possible to process 50 models of 100 states each over a time period of 100 time points (10 decades).

MARK1A MODULE

MARK1A reads and processes the input data set (deck). It makes two passes. On the first pass it determines the number of models, the number of states for each model, and the length of the run time. This is done by interpreting the 'M' cards and the 'RUN' card. After determining the run time it calculates the number of points that will be stored on disk for each state. On the first pass the program also prints out the entire input file as part of the output.

The program then makes a second pass through the input deck. At this point it reads and interprets the 'S', 'L', and the 'T' cards for the first model. The values of the 'S' cards are used in the program to initialize the state probability vector at time zero. The values on the 'T' cards are used to partially initialize the state transition matrix (Q-matrix).

The Q-matrix is fully calculated by multiplying the partially initialized matrix by a very small delta (1/100000) and then calculating the diagonal elements such that the rows sum to 1. If a 'D' card is included in the input deck, its value is used for delta.

The state probability vector for each time point is calculated next. The program uses the simple algorithm:

SP(N+1)+Q*SP(N).

Delta (time) is increased ten-fold every ten iterations. The variations in Delta were chosen for compatibility with graphical display.

The program makes all of its calculations for each of the models before it reads and interprets the input deck for the next model.

After the state probability vector is calculated for each time point, these double precision numbers are written to disk to be retrieved and used by the second module, 'MARK1B'. These values are also to be printed on the printer. The input card 'ABR' will surpress this printed output.

The program will then continue to read the 'S', and 'L', and 'T' cards for the next model and repeats the above steps until all the models are processed.

MARK1B MODULE

Plots are produced by the MARK1B package using numerical results generated by the MARK1A package which stores these results on the disk. If these results are already available on the disk the model solution step (MARK1A) is skipped and only the MARK1B step is executed. This enables the user to change the plot equations without solving the models every time. This function is controlled by the JCL.

The MARK1B program is divided into six sections.

1. Reading the file created by 'MARK1A' and storing the state probability vectors.

2. Reading the 'F' cards in the input deck.

3. Reading the 'Plot' cards in the input deck.

4. Interpreting the 'Plot' cards.

5. Graphing the data.

6. Printing the data.

Section 1

Reading the state vector file: the program begins by reading the entire file of state probability vectors, created by the 'MARK1A' program, into core. The dimensions for each model are also read from this file, therefore the program can use the based storage feature of PL/I to set up the storage allocations for each model.

Section 2

Reading the input deck: the program then reads each line of the input deck until it finds an 'F' card. Each 'F' expression is stored in its entirety so that it can be retrieved when the 'PLOT' cards are interpreted in section 4. The program uses the based storage feature of PL/I to store and identify each 'F' expression. Each 'F' expression can be written on several cards.

Section 3

Reading the input deck: the program continues reading the input deck until it finds a 'PLOT' card. It then checks the 'PLOT' card for a ';' and sets the multi-plot flag when a ';' appears. Each plotting expression can be written on several cards. The program stores the entire plotting expression for interpretation.

Section 4

Interpreting the plotting expression: the plotting expression is parsed and translated according to a small translation table. This avoids the repetition of the parsing process for each time point. Each point to be plotted is then calculated by separating the operands from the operators and using a stack machine method of evaluation. During the interpretation phase of the program, the state probability vectors of various models are merged.

Section 5

Plotting the data: the data is then sent to the graphing routine which plots the data points on a log-log graph. One can plot several sets of data points on the same set of axes by use of the multi-plot feature.

Section 6

Printing the data: the plotted data points are also printed on the printer.

APPENDIX B

LIFE CYCLE COST INPUT PARAMETERS

- System 1 — Baseline — Single String
- System 2 — Dual Gas Generator Functions
- System 3 — Dual Control (Dual Actuators)
- System 4 — Dual Control
- System 4A — Dual Control — Non Cross-Strapped
- System 5 — Dual with Triplex Computers
- System 6 — Dual with Dual-Dual Computers
- System 6A — Dual with Dual-Dual Microcomputers
- System 7 — Dual with Triplex or Dual-Dual Computers and No Hydromechanical Back-Up Control

FAFTEEC Input Parameters — Control System 1 Baseline Control System

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	300	0.5	37037	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	11000	9.0	22831	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	700	1.0	76923	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	4000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	600	0.5	25641	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	300	0.5	37037	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	3500	3.0	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	3500	3.0	32258	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	30000	30.0	7610	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	5700	13.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	5000	10.0	145000	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	14000	15.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	13000	10.0	145000	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	2700	11.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	900	1.5	83333	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	20000	27.0	3000	1.0	0	0	0	6.9	4.8	80	20	9.0	2.0	0.12	0.08
Aug Pump	10000	16.0	7042	1.0	0	0	0	6.8	4.8	80	20	12.0	2.5	0.02	0.02
Hyd Pump	8000	16.0	10000	1.0	0	0	0	6.8	2.5	80	20	10.0	2.5	0.08	0.05
GG Ign (2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer	39900	17.1	5000	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	2800	7.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	8000	25.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	12500	25.0	138889	1.0	15	1.0	100	2.0	0.5	—	—	—	—	—	—

FAFTEEC Input Parameters — Control System 2 Dual Gas Generator Functions

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	20000	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	22000	18.0	11500	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	5400	21.5	12500	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	2000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	2100	4.0	125000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	300	0.5	37037	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	32258	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	30000	32.5	7610	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	3400	11.5	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	6400	14.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	5000	10.0	145000	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	15000	16.0	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	13000	10.0	145000	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	3400	11.5	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	3400	11.5	25063	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1200	2.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump(2)	40000	42.0	1500	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump	10000	16.0	7040	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump(2)*	16000	33.8	10000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer(2)*	68300	33.2	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3100	8.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	13600	42.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	12500	25.0	138889	1.0	15	1.0	85	2.0	0.5	—	—	—	—	—	—

*Cost, weight and MTBF for two individual units

FAFTEEC Input Parameters — Control System 3 Dual With Dual Actuators

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Dep Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	20000*	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	22000	18.0	11500	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSV[a]	5400	21.5	12500	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	2000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	4200	8.0	75000*	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	4200	8.0	75000*	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	4200	8.0	75000*	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	4200	8.0	75000*	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	4200	8.0	75000*	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	350	0.5	20000*	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	17500*	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	60000	60.0	3805*	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	5400	21.5	12500*	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	11000	26.0	12500*	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	10000	24.0	72500*	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	28000	30.0	12500	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	26000	28.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	5400	21.5	12500	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	5400	21.5	12500	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1800	3.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump(2)*	40000	42.0	1500	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump(2)*	20000	32.0	3524	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump(2)*	16000	33.8	5000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer(2)*	68300	33.2	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3100	8.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	16000	49.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	14500	30.0	138889	1.0	15	1.0	85	2.0	0.5	—	—	—	—	—	—

*Cost, weight and MTBF for two individual units

FAFTEEC Input Parameters — Control System 4 Dual Control System

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	20000	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	14300	11.0	17800	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	3500	13.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	2000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	350	0.5	20000	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	17500	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	47000	36.5	5950	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	3500	13.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	7400	15.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	6500	14.5	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	18400	18.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	16900	17.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	3500	13.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	3500	13.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1200	2.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump(2)*	16000	33.8	5000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer(2)*	68300	33.2	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3100	8.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	16000	49.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	26500	27.0	138889	1.0	15	1.0	85	2.0	0.5	—	—	—	—	—	—

*Cost, weight and MTBF for two individual units

FAFTEEC Input Parameters — Control System 4a Dual Control NonCross-Strapped

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	20000	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	22000	18.0	17800	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0 1
HMBUC	41000	42.0	2000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	350	0.5	20000	1.0	0	0	50	3.2	.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	17500	1.0	0	0	20	4.0	.5	80	—	.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	.5	—	—	—	—	—	—
WFD(3)	60000	60.0	5950	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	11000	26.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	10000	24.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	28000	30.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	26000	28.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1800	3.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump(2)*	16000	33.0	5000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	.8	—	10	5.0	1.0	0.02	0.01
Computer(2)*	67400	33.2	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3100	8.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	16000	49.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	14500	30.0	138889	1.0	15	1.0	85	2.0	.5	—	—	—	—	—	—

*Cost, weight and MTBF for two individual units

FAFTEEC Input Parameters — Control System 5 Dual With Triplex Computers

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	2000	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	22000	18.0	17800	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	2000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	350	0.5	20000	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	17500	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	60000	60.0	5950	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	11000	26.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	10000	24.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	28000	30.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	26000	28.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1800	3.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump(2)*	16000	33.0	5000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer(3)*	72800	35.9	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3200	9.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	16000	49.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	13000	27.0	138889	1.0	15	1.0	85	2.0	0.5	—	—	—	—	—	—

*Cost, weight and MTBF for two hydraulic pumps and three computers.

FAFTEEC Input Parameters — Control System 6 Dual With Dual-Dual Computers

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	20000	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	22000	18.0	17800	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	2000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	350	0.5	20000	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	17500	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	60000	60.0	5950	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	11000	26.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	10000	24.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	28000	30.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	26000	28.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1800	3.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump	16000	33.0	5000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer(2)*	77300	37.4	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3200	9.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	16000	49.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	13000	27.0	138889	1.0	15	1.0	85	2.0	0.5	—	—	—	—	—	—

*Cost, weight and MTBF for two hydraulic pumps and three computers.

FAFTEEC Input Parameters — Control System 6A Dual With Dual-Dual Microcomputers

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	20000	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	22000	18.0	17800	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
HMBUC	41000	42.0	2000	1.0	0	0	0	3.0	2.5	20	80	12.0	50.0	0.08	0.06
HMBUC Trans Vlv	1500	2.0	25641	1.0	0	0	0	2.5	1.5	80	20	4.0	1.0	0.08	0.06
P2	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	350	0.5	20000	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	17500	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	60000	60.0	5950	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	11000	26.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	10000	24.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	28000	30.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	26000	28.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1800	3.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump	16000	33.0	5000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer(2)*	79600	41.8	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3100	8.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	16000	49.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	13000	27.0	138889	1.0	15	1.0	85	2.0	0.5	—	—	—	—	—	—

*Cost, weight and MTBF for two hydraulic pumps and three computers.

FAFTEEC Input Parameters — Control System 7 Dual With Triplex or Dual-Dual Computers and No HMBUC

Component	Unit Cost UC	Weight W	MTBF	PAMH MMH to Access Flu	RIP % Repair in Place	IMH MMH to Repair in Place	COND % Discard at Failure	RMH MMH Remove & Replace	BCMH MMH Fault Isolate	RTS % Flu to Inter	NRTS % Flu to Depot	BMH MMH Inter Repair	DMH MMH Depot Repair	BMC Inter Repair Cost/Unit Cost	DMC Inter Repair Cost/Unit Cost
N2	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
T2	350	0.5	20000	1.0	0	0	50	3.2	1.5	50	—	1.0	—	0.01	—
P3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
WFGG	22000	18.0	17800	1.0	0	0	0	2.4	2.5	80	20	8.0	2.0	0.12	0.08
PLA	1400	2.0	40000	1.0	0	0	100	1.0	3.0	—	—	—	—	—	—
CSVA	5400	21.5	22000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
P2	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P5	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
P13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP3	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
ΔP13	4200	8.0	75000	2.1	0	0	50	3.0	1.5	50	—	1.0	—	0.01	—
N1	700	0.5	15000	1.0	0	0	100	2.0	2.0	—	—	—	—	—	—
T22	350	0.5	20000	1.0	0	0	50	3.2	0.5	50	—	1.0	—	0.01	—
TBT Pyrometer	6000	4.5	10000	1.0	0	0	20	3.0	0.5	80	—	1.0	—	0.01	—
LOD	6000	4.5	17500	1.0	0	0	20	4.0	0.5	80	—	0.8	—	0.01	—
MN	—	—	—	—	—	—	—	—	0.5	—	—	—	—	—	—
WFD(3)	60000	60.0	5950	2.1	0	0	0	3.1	1.0	80	20	16.0	4.0	0.08	0.06
FIGV	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE	11000	26.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJE (Slave)	10000	24.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
AJD	28000	30.0	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
AJD (Slave)	26000	28.0	72500	1.0	0	0	0	7.0	2.5	80	20	8.0	2.0	0.08	0.06
A4	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
A41	5400	21.5	21000	2.1	0	0	0	2.8	2.5	80	20	8.0	2.0	0.2	0.1
Start Bleed	1800	3.0	58820	1.0	0	0	0	2.9	2.5	80	20	8.0	2.0	0.2	0.1
GG Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
B/U Pump	8000	16.0	10000	1.0	0	0	0	6.8	4.8	80	20	10.0	2.5	0.08	0.05
Hyd Pump(2)*	16000	33.0	5000	1.0	0	0	0	6.8	3.5	80	20	10.0	2.5	0.08	0.05
GG Ign(2)	2900	10.0	12739	1.0	0	0	90	0.3	0.8	—	10	5.0	1.0	0.02	0.01
Aug Ign	1500	5.0	12225	0.6	0	0	90	0.8	0.8	—	10	5.0	1.0	0.02	0.01
Computer(3)*	72800	35.9	2500	1.0	0	0	0	0.9	2.5	80	20	20	3.4	0.02	0.005
Alternator	3100	8.0	12820	2.0	0	0	0	6.5	2.5	100	—	8.7	2.0	0.14	0.08
Cables	16000	49.0	5450	2.0	15	1.0	85	6.0	2.5	15	—	6.6	1.6	0.01	0.01
Plumbing	13000	27.0	138889	1.0	15	1.0	85	2.0	0.5	—	—	—	—	—	—

*Cost, weight and MTBF for two hydraulic pumps and three computers.

APPENDIX C

FLEET SIZE MODEL

When investigating the cost-effectiveness of new control system concepts for engines, some analysis should be included which reflects the fleet size required to complete a given mission. This could show some real benefits that a typical life cycle cost for a fixed fleet size may miss. In order to be realistic, both a "peacetime" usage and a "wartime" usage should be considered. A simplified approach is outlined below for tactical systems.

Regarding "wartime" usage, the measure of merit should be the total number of missions that can be flown in a given length of time. To compute this we start by defining the maximum available sortie rate using the following:

SR = Sortie rate per aircraft
FT = Flight time per sortie
TT = Turnaround time (refuel/rearm)
DT = Average down time (for repair) per engine flight hour
D = Length of combat dug (eg: 12 hr for day fighter, etc.)
EFH = Engine flight hours

Then;

$$SR = \frac{D}{(FT + TT)\ (1 + DT/EFH)}$$

Sortie rate can then be affected by turnaround time or the average down time per engine flight hours. The first could be a function of built-in test, and the second could be a function of both reliability and maintainability. The latter could also be affected by the maintenance concept, including deferred maintenance for redundant systems, since we are talking of system down time. Deferred maintenance tasks could be accomplished simultaneously with other maintenance requirements. Then to find the number of completed sorties per day, we must define the following:

P_m = Probability of mission completion

P_{FO} = Probability of failure on cruise out (including ground operation)

P_{FE} = Probability of failure on engagement

P_{FB} = Probability of failure on cruise back (including ground operation)

SR_e = Effective sortie rate

$$P_m = (1 - P_{FO})\ (1 - P_{FE})$$
$$SR_e = (SR)\ (P_m)$$

If the "peacetime" mission is considered, there are two factors which must be addressed. The first is attrition. This can be treated as follows:

N = Total fleet size
TS = Total sorties per aircraft over fleet life
P_S = Probability of survival
N_A = Number of attrited aircraft

$$N_A = (1 - P_S^{TS})\, N$$

This could be handled in two ways. The fleet could be assumed to be maintained at a constant level by replacing attrited aircraft, or the initial buy may be increased by the attrited number. In the first case, only acquisition cost would change for the life cycle cost analysis. In the second, the attrited aircraft would be maintained until they were lost, and total life cycle cost would be greater than in the first case. While the second may be more realistic, either should be acceptable for preliminary studies. The second factor is the operational readiness rate of aircraft on "alert" status. For this requirement, we have two distinct sets of requirements. Part of the fleet would be required to deliver a given sortie rate per day for training purposes, and the remainder would provide "ready" aircraft, providing a required mission capability. If we make the rash assumption that the attrition rate is negligible (or at least the effects have been accounted for above), then the following defines the first half of our requirement:

SR_e = Effective sortie rate per aircraft

SR_r = Required total daily training sortie rate

N_T = Number of aircraft required for training

$$N_T = \frac{SR_r}{SR_e}$$

The second part of the requirement for the alert aircraft can be defined as follows:
IS = Initial number of completed sorties required from first launch

P_M = Probability of mission completion

N_A = Number of aircraft required for alert status

$$N_A = (IS)\ \ (P_M)$$

In either the peacetime or wartime scenario, fleet size can be defined for a given mission requirement. For a multiple mission aircraft, fleet size may be defined in one of two ways: by weighing the total number of aircraft with the mission mix percentage (which assumes the various missions are being flown simultaneously), or by defining the most critical mission and size of the fleet that might represent a flexible mission defined by combat requirements. Once the fleet size is determined, the life cycle cost of the fleet may be defined for a given utilization.

This assumes that a failure on the cruise back does not affect the mission completion. However, the probability of failure on the cruise out and engagement portions of the mission will affect the ability to complete the mission. The total number of sorties that can be accomplished may now be defined as follows:

CS = Completed sorties
N = Number of aircraft available at start of war
P_s = Probability of survival (Attrition equals 1-P_s)
t = length of war in days

$$CS = N \left[\frac{1 - P_s(SR_e)t}{1 - P_s} \right]$$

The total number of completed sorties is dependent on the sortie rate defined above, and also on the probability of survival. If we look at the probability of survival, we might see a minor effect by looking at the probability of failure during the engagement portion of the mission and assume a failure in that portion would decrease survivability if it resulted in loss of performance. The other alternative for wartime operations might be to look at how long a minimum sortie rate could be supported after an initial requirement for a given number of sorties in a given length of time. This might represent an initial engagement where local air superiority is established; then a fixed air cover is required. The initial calculation would be accomplished, as above, to size the fleet. The following would then be used to define how long the fleet could then provide a fixed sortie rate.

SR_r = Required daily sortie rate (total)
t = Length of initial sortie requirement in days
P_s = Probability of survival during initial requirement
P_{sc} = Probability of survival during constant sortie rate requirement
n = Number of days constant sortie rate can be maintained
N = Initial number of aircraft at start of war
N_i = Number of aircraft after initial requirement
N_f = Final number of aircraft required to meet sustained sortie rate
SRa = Average sortie rate per aircraft during sustained requirement

$$N_f = \frac{SRr}{SRe}$$

$$N_i = P_s\,(SR_e)t$$

$$SRa = \frac{\left(\frac{SRr}{N_f} + \frac{SRr}{N_i} \right)}{2}$$

$$P_{sc}^{(SRa)n} N_i = N_f$$

Obviously the measure of merit in this case is the number of days one can sustain the required sortie rate with the fleet defined by the initial total sortie requirement.

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

A4	High pressure turbine inlet area
A41	Low pressure turbine inlet area
AJD	Duct stream exhaust nozzle area
AGRT	Advance group rapid transit
AJE	Core stream exhaust nozzle area
ATAMS	Advanced Tactical Attack Manned Systems
ATDE	Advanced technology demonstrator engine
ATES	Advanced technology engine studies
BCS	Baseline control system
BC	Bus controller
BM	Bus monitor
CC	Computational core
CER's	Cost estimating relationships
CCD	Customer computer deck
CFP	Core fuel pump
CMVT	Constant match variable temperature
CMOS	Complimentary Metal Oxide Semiconductor
CPU	Central Processor Unit
CSVA	Compressor stator vane actuator
DIGBUC	Digital backup control
DMA	Direct memory access
EEC	Electronic Engine Control
EHV	Electrohydraulic valves
EOC	End of conversion
ESS	Electronic switching systems
FAFTEEC	Full authority fault tolerant electronic engine control

FADEC	Fuel Authority Digital Electronic Control
FIGV	Fan inlet guide vane
FMEA	Failure Modes and Effects Analysis
FTMP	Fault tolerant multiprocessor
FN	Net thrust
HMBUC	Hydromechanical backup control
LCC	Life Cycle Cost
LOD	Light-off-detector
LSI	Large scale integration
MBTF	Mean Time Between Failure
MN	Mach number
N1	Low rotor speed
N2	High rotor speed
N2C2	Corrected high rotor speed
N2R	High compressor rotor speed request
P2	Fan inlet total pressure
P13	Duct pressure
P5	Low pressure turbine discharge pressure
PAA	Primary Aircraft Authorization
PLA	Power lever angle
PS3	Compressor discharge pressure
RAEEC	Reliability Advancement for Electronic Engine Controllers
Q101	Ford specifications for vendors
SB	Starting bleed
SMFAN	Fan surge margin
SMHPC	High pressure compressor surge margin
SSI	Small scale integration

T2	Fan inlet total temperature
T13	Duct temperature
T22	Compressor inlet temperature
T3SYN	A synthesized value of compressor discharge temperature
T4	High pressure turbine inlet temperature
T	Temperature
TBT	High pressure turbine blade temperature
TSFC	Thrust specific fuel consumption
VCE	Variable cycle engine
WAR13	A value of corrected duct airflow
WFGG	Gas generator fuel flow
WF/P3	Fuel flow ratio units
WFD	Duct augmentor fuel flow

*U.S.Government Printing Office: 1982 — 559-003/2030


DATE
ILME
8