GENCORP
AEROJET

SUMMARY FINAL REPORT

ALS
ENGINE CONTROLLER SYSTEM

Prepared for:

National Aeronautics and Space Administration
George C. Marshall Space Flight Center
Marshall Space Flight Center, AL 35812

Aerojet Propulsion Division
P.O. Box 13222
Sacramento, CA 95813-6000

November 1993

The Requirement For Use Of International System Of Units Has Been Waived For This Document

November 1993

ALS
ENGINE CONTROLLER SYSTEM

Contract NAS8-38074

SUMMARY FINAL REPORT

Prepared for:

National Aeronautics and Space Administration
George C. Marshall Space Flight Center
Marshall Space Flight Center, AL 35812

Prepared By:

Roger Payne
Senior Engineer

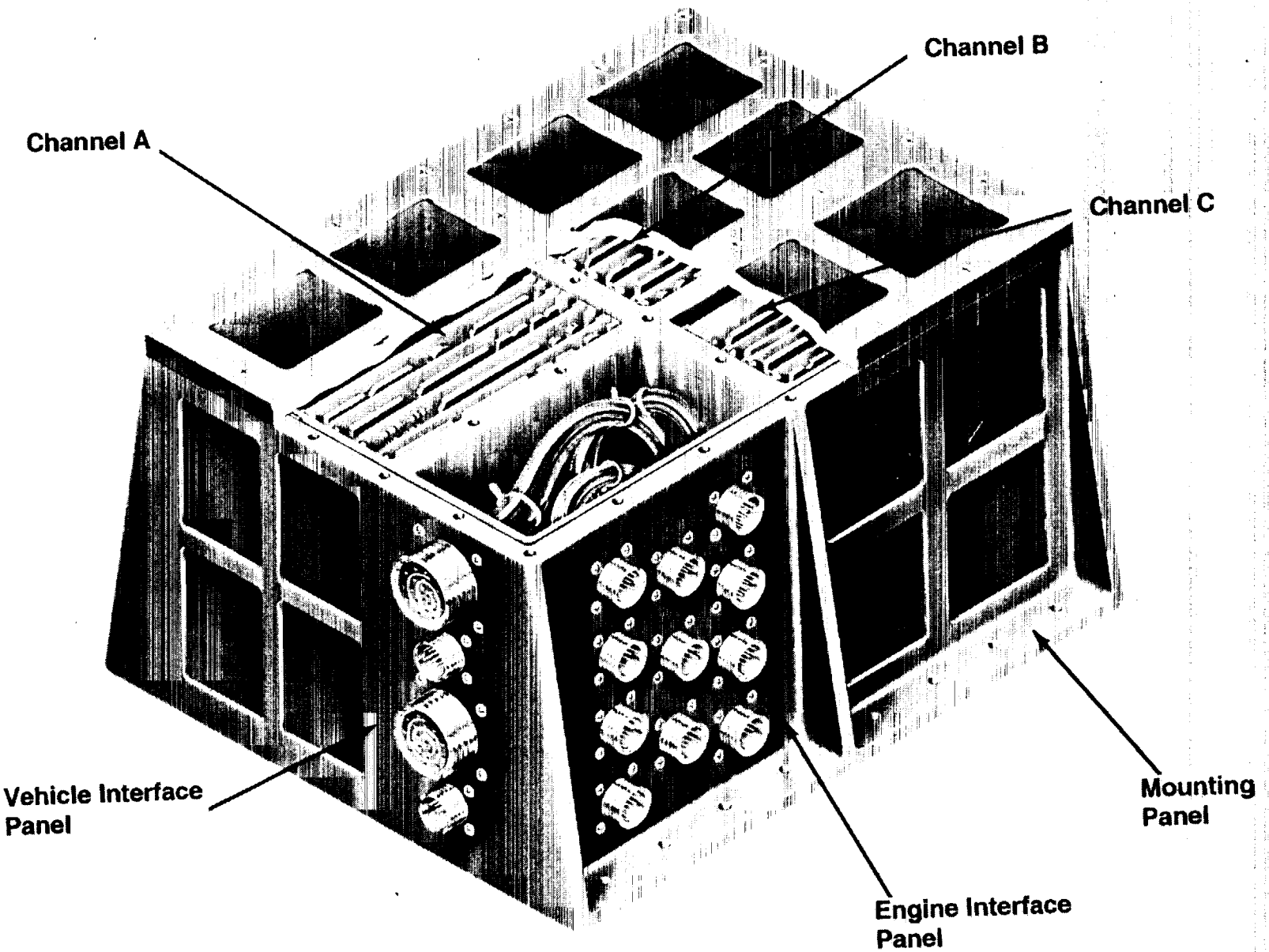
Approved By:

Colin Faulkner
Program Manager

Aerojet Propulsion Division
P.O. Box 13222
Sacramento, CA 95813-6000

The Requirement For Use Of International System Of Units Has Been Waived For This Document

Space Transportation Main Engine
Flight Controller Assembly



FIGURES

TABLES

1.0 INTRODUCTION

This is the Final Summary Report for the Advanced Launch System (ALS) Engine Controller System, Contract NAS8-338074. This program was conducted by Aerojet Propulsion Division (APD) for NASA's Marshall Space Flight Center (MSFC). Authority-to-proceed (ATP) was given on 30 May 1989. APD was directed to descope the program to final reporting and hardware disposition on 6 August 1993.

The objective of the program was to evaluate highly reliable, low cost electronic engine controller systems for the ALS engine. The total effort planned is defined in DR-15, the Technical Implementation Plan. Due to funding constraints, particularly in later stages of the program, and due to premature closeout, the program was not completed as originally planned. However, significant data from hardware and software design activities were obtained.

Funding was limited at program closeout. APD was therefore directed to minimize the final reporting effort. This document does not have the depth normally associated with program final reports but, accepting the limited effort permitted, is designed to enable readers to understand program scope and content, and to lead them to reference material which gives more detailed program data. It gives a top level overview of the program, highlighting results and data pertinent to likely future NASA programs. Recommendations are made for follow-on work which could be performed using data available from this program.

The program as planned consisted of two distinct phases:

Phase 1 - Preliminary Design and Cost Model

Phase 2 - Detailed Design, Fabrication, and Demonstration

Figure 1-1 shows the overall program logic and the interrelationships between tasks. The two phases were originally scheduled to be performed over a total 38 month period, Phase I in 17 months, and Phase II in 21 months.

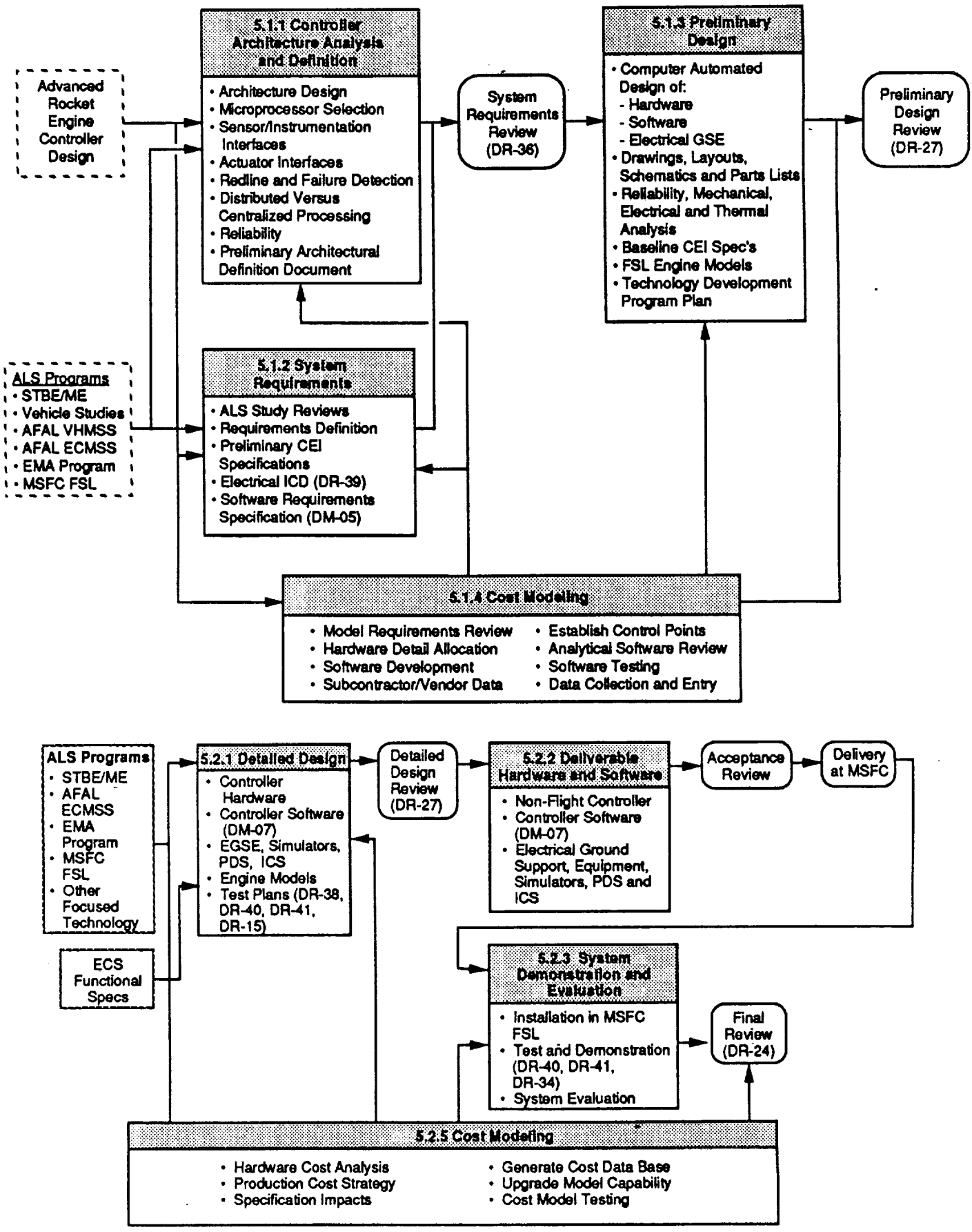


Figure 1-1. Program Logic Chart

The report is structured around the program work breakdown structure (WBS) shown in Figure 1-2. By reporting in this fashion, the reader is informed on the total program plan content as planned, and on actual results achieved prior to program closeout in each specific WBS task.

2.0 KEY ACCOMPLISHMENTS

2.1 Overview

The focus of this program was to develop and demonstrate a brassboard version of a low cost, fault-tolerant engine controller. Activities accomplished included completion of detailed designs of brassboard controller hardware and software and electrical ground support equipment hardware and software. A skeleton structure of the engine controller software code was also generated. Due to programmatic constraints, no further software coding or hardware fabrication was accomplished. More detail on individual tasks performed is given in Section 3.

2.2 Engine Controller Hardware Design

Detailed design of the engine controller hardware was completed. This defined a full triplex-redundant controller configuration with modular expansion capability within each channel. The design included electrical schematics, board layouts and supporting analyses for the controller backplane (multibus II) and each of the following functional modules:

- Digital Computer Unit Module (DCU)
- MIL-STD-1553 Interface Module (1553)
- Interchannel Communications Module (ICC)
- High Speed Input Electronics Module (HSIE)
- Low Speed Input Electronics Module (LSIE)
- Output Electronics Module (OE)

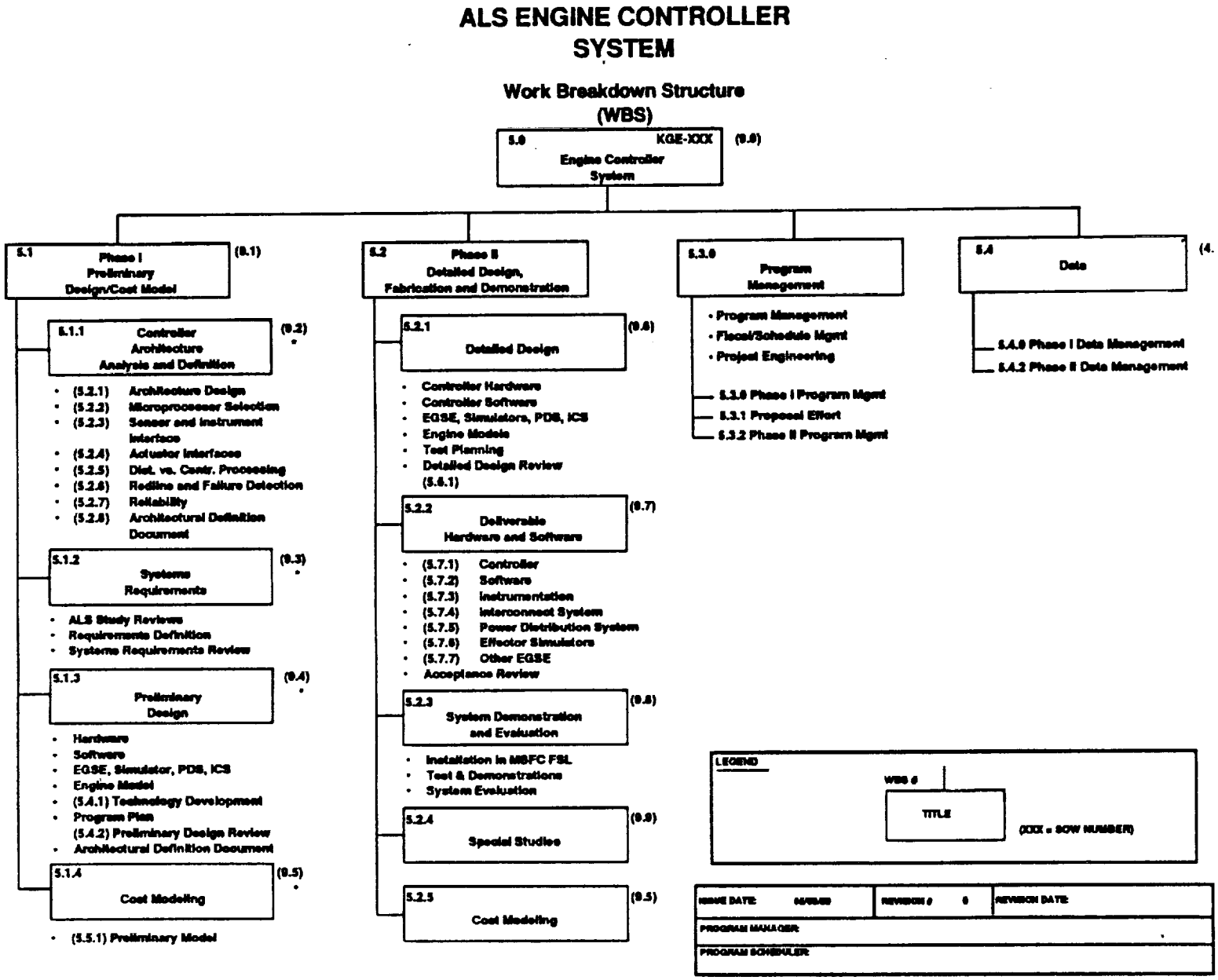


Figure 1-2. Work Breakdown Structure

- Power Conditioning Electronics Module (PCE)

This complement of modules provides all the capability required to control engine operation (e.g. sequence electromechanically actuated valves, solenoid actuated valves and igniter exciters), condition and evaluate standard engine sensor data including pressure, temperature (thermocouple and RTD), turbopump shaft speed, acceleration and shaft displacement, and receive commands from and report status to the vehicle. Full documentation detailing each module was developed and included along with the drawings and electrical schematics as part of the engine controller detailed design review package.

Selection of the Charles Stark Draper Laboratory fault-tolerant architecture was a result of fault tolerance and controller architecture trade studies performed early in the program. Other trade studies conducted which further defined the configuration included:

- Microprocessor selection
- Effector command/data interface configuration
- Vehicle command/data interface configuration
- Sensor interface configuration

Requirements for high speed processing, adaptability to changing and emerging control system requirements, and commonality to vehicle communication protocol lead to the 80960-based design, which features configurable sensor and effector interfaces and a standard MIL-STD-1553B bus for vehicle command/data communication.

Due to budget constraints no detailed design hardware was fabricated or demonstrated. However, a similar core quadraplex fault-tolerant system (DCU, ICC, and 1553 modules) was fabricated and demonstrated in a separate Aerojet-sponsored activity.

2.3 Engine Controller Software Design

A detailed controller software design was also developed as part of this contract. The software is a highly structured, object-oriented design which is segmented into two primary elements; the Application Program (AP), and the Application Program Support Services (APSS). The APSS is a generic set of low level hardware-specific software drivers used to access controller hardware. The AP is a high level program which performs mission-specific tasks. For this effort the AP was designed to perform tasks specific to the operation of the STME, including all checkout, monitoring, and hardware sequencing performed during engine prestart conditioning, engine start, steady state operation, engine shutdown, and unscheduled shutdown (i.e. on-pad abort) conditions. A detailed document describing all software objects, object external interfaces, object calling structures, channel initialization and BIT status parameters was produced and included as part of the engine controller detailed design review package.

In addition to the detailed design, a skeleton structure of the engine controller software code was generated. The code was developed in Ada software language. It contains the structure for all objects defined in the engine controller detailed design including definition of all object functions and procedure definitions, object interface variables, and calling structure logic. A copy of the software code was included as part of the Engine Controller Detailed Design Review and is also available on electronic media.

Due to budget constraints, detailed engine controller software code was not generated or demonstrated. Software code for core quadraplex fault-tolerant system capabilities was generated and demonstrated on the separate Aerojet-sponsored program.

2.4 Electrical Ground Support Equipment

Detailed design of the Electrical Ground Support Equipment (EGSE) was completed. This was designed to provide the intermediate support components necessary to interface the controller with computing facilities at the NASA-MSFC ALS Flight Simulation Laboratory (FSL), and with the software development laboratory facilities at Aerojet for hardware in-the-loop testing and fault injection. The EGSE is capable of providing stand-alone checkout of the

controller including diagnostic support. It also provides capabilities for software development support including software upload/download utilities for code transfer and verification.

The detail design covers both hardware and software aspects of the EGSE. Included in the hardware design are electrical schematics, board layouts, and supporting analyses and equipment lists required for fabrication of the EGSE system and each of its components. Major components include:

- Ground support computer (GSC)
- Solenoid/igniter simulator
- Sensor simulator
- Electromechanical actuator (EMA) simulator
- Interconnect system

Full documentation detailing the EGSE system and each major component was developed and included along with drawings, electrical schematics and design specifications as part of the Engine Controller Detailed Design Review package. Due to programmatic constraints no EGSE hardware was fabricated or demonstrated.

Two major elements of the software design were also completed; the Ground Support Computer Operational Program (GSCOP) and the Electromechanical Actuator Operational Program (EMAOP). GSCOP was designed to upload/download and verify code transfers, initiate operational flight program execution in the controller, and perform controller checkout. EMAOP was designed to provide dynamic emulation of five EMAs, support MIL-STD-1553 communication, transmit EMA status parameters, and respond to fault requests. Full documentation describing software architecture, external interfaces, calling structures, and memory and configuration table management was produced and included as part of the Engine Controller Detailed Design Review package. Due to programmatic constraints no EGSE software code was generated or demonstrated.

2.5 Cost Model

A preliminary cost model was developed which was used to track program progress in meeting design-to-cost goals. This is a comprehensive data base addressing recurring in-house manufactured ("make") and supplier-provided ("buy") parts and recurring operations and support (O&S) costs. The cost model is Microsoft Excel application-based and can be used on either Macintosh or PC desktop computers. The model has applicability to any liquid engine component and will consolidate costs up to the engine level. It gives the model user authority over input costs and manufacturing cost relationships. The model has not been completed or validated but is a potentially useful tool for unit production cost projection and tracking.

3.0 TASK SUMMARIES

3.1 Controller Architecture Analysis and Definitions

3.1.1 Objective

The objective of this task was to analyze and define the controller architecture. The task consisted of several subtasks, with objectives as follows:
Architecture Design: Establish system architecture through trade studies addressing cost and reliabilty requirements and ease of testing.
Microprocessor Selection: Evaluate state-of-the-art processors to determine and rank computational capacity, considering throughput, speed, operational flexibility, program memory and bulk storage memory required, availability of software development tools, and compatibility with Ada programming language.
Sensor and Instrumentation Interfaces: Determine sensor interfaces so as to optimize engine performance, reliability, and recurring cost.
Actuator Interfaces: Determine interfaces with EMAs; consider position, opening and closing rate commands, failure detection, and redundancy management.
Distributed Versus Centralized Processing: Determine whether the overall architecture should be a distributed processing system, variation thereof, or a centralized system.

Redline and Failure Detection: Determine an approach to redline and failure detection, i.e., deterministic, heuristic, or combination.

Reliability: Define controller system to meet allocated reliability figure consistent with overall engine reliability of 0.99 at 90% confidence level; identify component improvements required to meet the allocated figure.

Architectural Definition Document (ADD): Prepare ADD (DR-35) which defines functional requirements of controller system, mission success criteria (i.e., fail-op or fail-safe), redundancy requirements, architecture, allocation of functional and redundancy requirements between hardware and software, hardware elements and allocations of functional and redundancy requirements, external environmental requirements, internal and external hardware and software interfaces.

3.1.2 Activity Overview

Architecture design was driven by requirements for fault tolerance and system reliability, and by controller-defined interfaces derived from vehicle and engine-level requirements specified in the STME CEI and ICD. Fault tolerance was defined as fail operational ("fail op")/fail safe. The fail op/fail safe system maintains full operation when a single failure is experienced; if a second failure occurs, the system safely shuts down the engine. A reliability allocation of 0.99995 was imposed on the basis of the engine reliability requirement. Interfaces were to be consistent with redundancy configurations of the vehicle, engine sensors, engine propellant effectors, and engine purge valve and igniter solenoids and exciters (Figure 3-1).

The architecture was built up from a set of generic controller modules. These included a digital computer unit, an inter-channel interface, a vehicle command interface, input and output electronics, and power conditioning electronics (Figure 3-2).

The architecture incorporated dual redundant MIL-STD-1553B buses for commands and data, and dual isolated power supply buses.

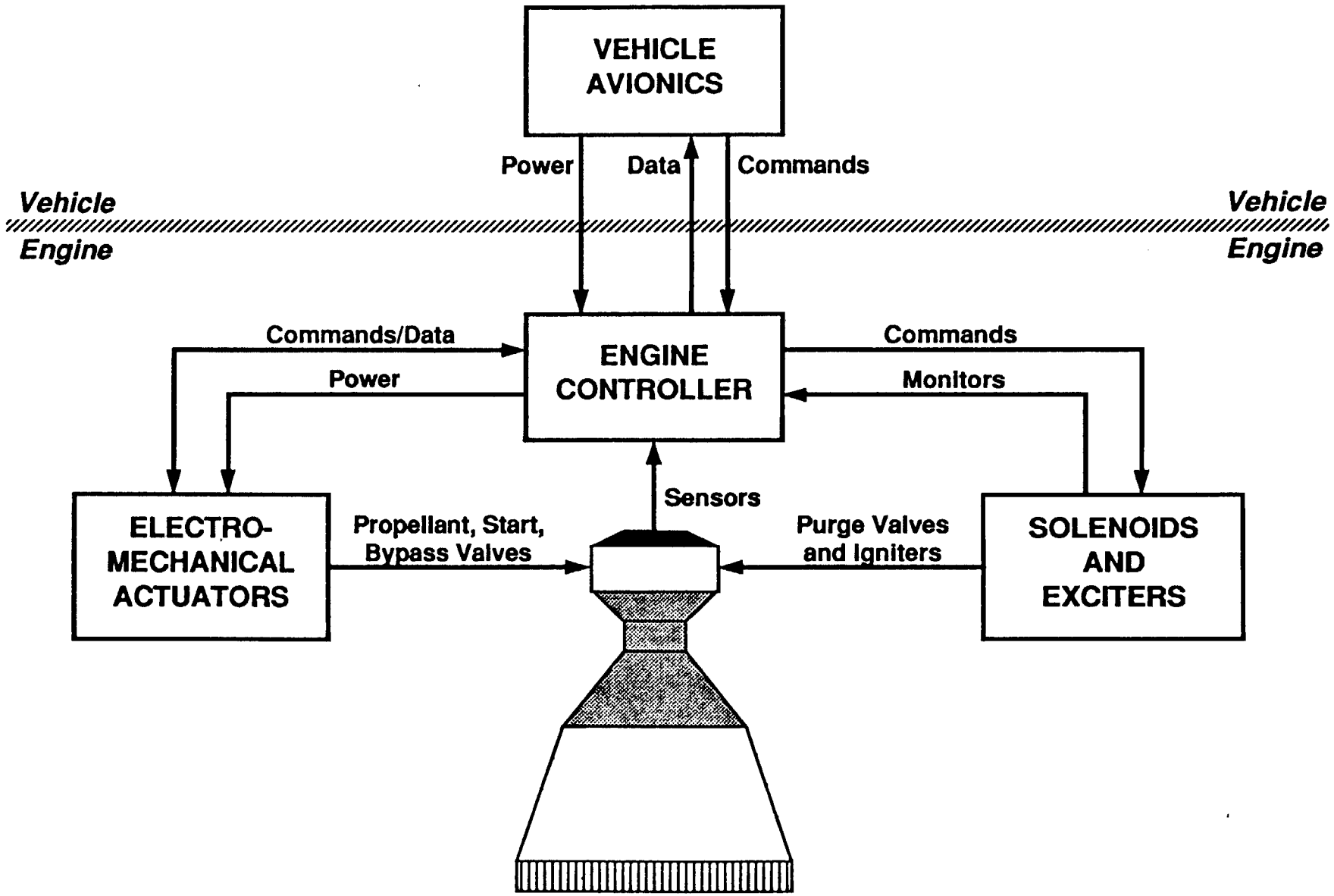


Figure 3-1. Engine Control Architecture Specific To System Requirements

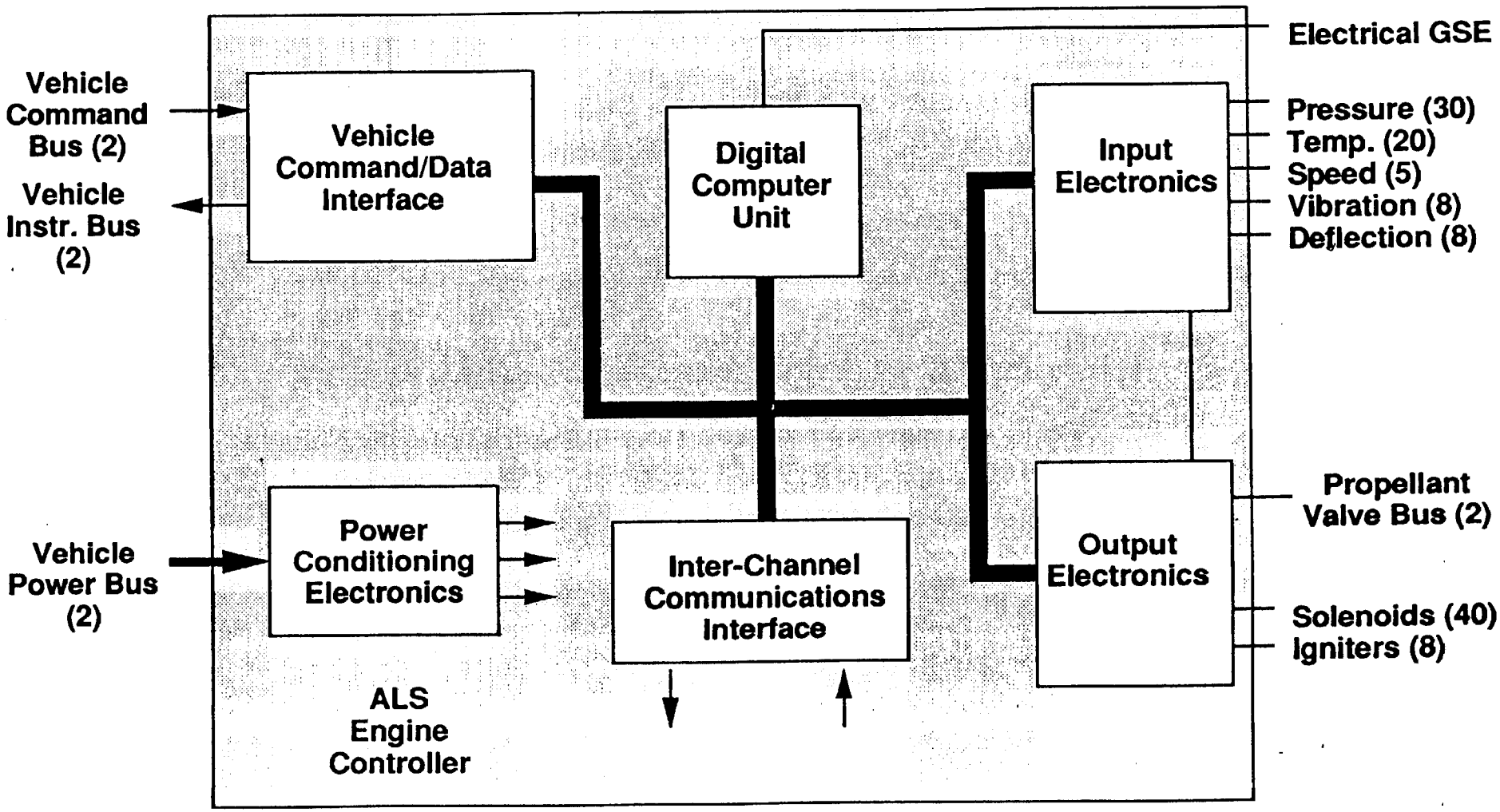


Figure 3-2. Functionally Equivalent Simplex Controller Contains All Major Components

The 32 bit Intel 80960 microprocessor was baselined for the engine controller because it had the required speed and processing power and was designed specifically for embedded system applications. It provides memory management for processor resource protection, floating point numeric capability, and Ada tasking functions. An important additional factor in the selection process was its built-in 50% growth margin.

The baseline engine sensor set consisted of strain gage diaphragm pressure sensors, high temperature thermocouples, low temperature resistance-type devices (RTDs), magnetic speed pickups, piezo-electric accelerometers with integral electronics, and capacitive displacement probes with integral electronics. An itemized list is given in Figure 3-3. Typical input channel schematics are given in Figures 3-4 and 3-5.

Figure 3-6 shows controller-to-Valve EMA command, data, and power interfaces. Dual redundant MIL-STD-1553B buses carry commands and data with command validation required for command input. The system features dual, isolated power supply buses. Controller-to-solenoid command and monitor interfaces are shown in Figure 3-7. Features include use of dual coil solenoids and monitors with feedback monitoring. Figure 3-8 controller-to-igniter interfacing. Dual exciters and dual monitors are used, with igniter electronics providing status data.

Studies covered a range of designs with one to four processors. Capabilities addressed included simplex, duplex, duplex with built-in test (to enhance fault isolation capability), combined triplex and duplex, full triplex, and quadruplex. These candidates were assessed against evaluation criteria. Figure 3-9 summarizes findings regarding fault tolerance, which was one of the key criteria. Having established system reliability, surviving approaches were searched for any excess redundancy on the basis that this would unnecessarily add to control system acquisition and operational costs. The baseline approach was to use output comparison to achieve 100% fault coverage. The architecture selected featured triplex processing and vehicle interfaces with duplex effector outputs (Figure 3-10). For engine control devices, the duplex configured output electronics included built-in-self-test (BIST).

Pressure

1. OXHEX Ox Discharge
2. Purge Supply
3. Ox System Purge
4. Gas Generator Purge
5. GG Injector, Fuel
6. GG Injector, Oxidizer
7. FTPA Pump Discharge
8. FTPA Pump Inlet
9. FTPA Turbine Inlet
10. OTPA IPS Purge (Pri)
11. OTPA IPS Purge (Sec)
12. OTPA IPS Purge (Third)
13. OTPA Pump Discharge
14. OTPA Pump Inlet
15. OTPA Turbine Inlet
16. OTPA Turbine Discharge
17. MCC Injector, Fuel
18. MCC Injector, Oxidizer
19. MCC (Pri)
20. MCC (Sec)
21. MCC (Third)
22. MCC Coolant Discharge
23. Nozzle Coolant Manifold
24. Spare
25. Spare
26. Spare
27. Spare
28. Spare
29. Spare
30. Spare

Temperature (Low)

1. OXHEX Ox Discharge
2. FTPA Pump Discharge
3. FTPA Pump Inlet
4. OTPA Pump Discharge
5. OTPA Pump Inlet
6. MCC Coolant Discharge
7. Spare
8. Spare
9. Spare
10. Spare

Temperature (High)

1. FTPA Turbine Inlet (Pri)
2. FTPA Turbine Inlet (Sec)
3. FTPA Turbine Inlet (Third)
4. OTPA Turbine Inlet
5. Nozzle Coolant Manifold
6. Spare
7. Spare
8. Spare
9. Spare
10. Spare

Speed

1. FTPA Shaft
2. OTPA Shaft
3. Spare
4. Spare
5. Spare

Position

1. Main Fuel Valve
2. Main Oxidizer Valve
3. Gas Generator Valve
4. Oxidizer Turbine Bypass
5. Start Valve

Vibration

1. FTPA Housing
2. FTPA Housing
3. OTPA Housing
4. OTPA Housing
5. Spare
6. Spare
7. Spare
8. Spare

Deflection

1. FTPA Shaft
2. FTPA Shaft
3. OTPA Shaft
4. OTPA Shaft
5. Spare
6. Spare
7. Spare
8. Spare

Figure 3-3. Baseline ADP Sensor Set Derived From RFP And Engine Design With Growth Capacity Added

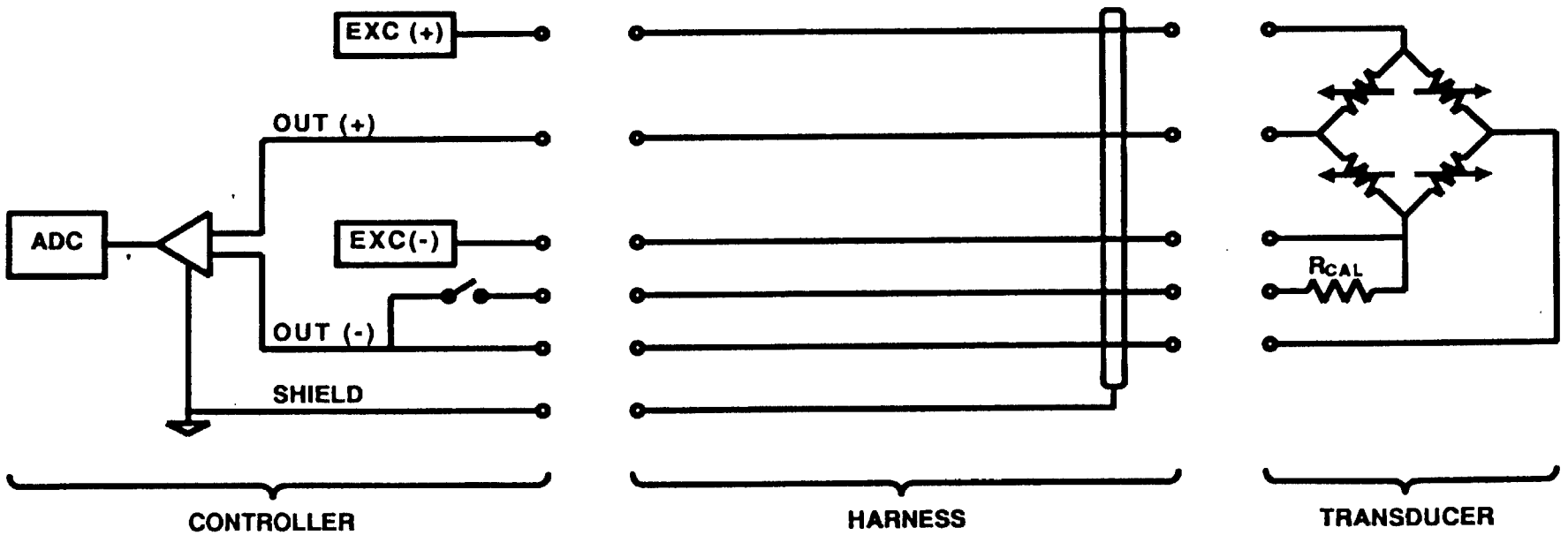


Figure 3-4. Pressure Sensor Input Channel

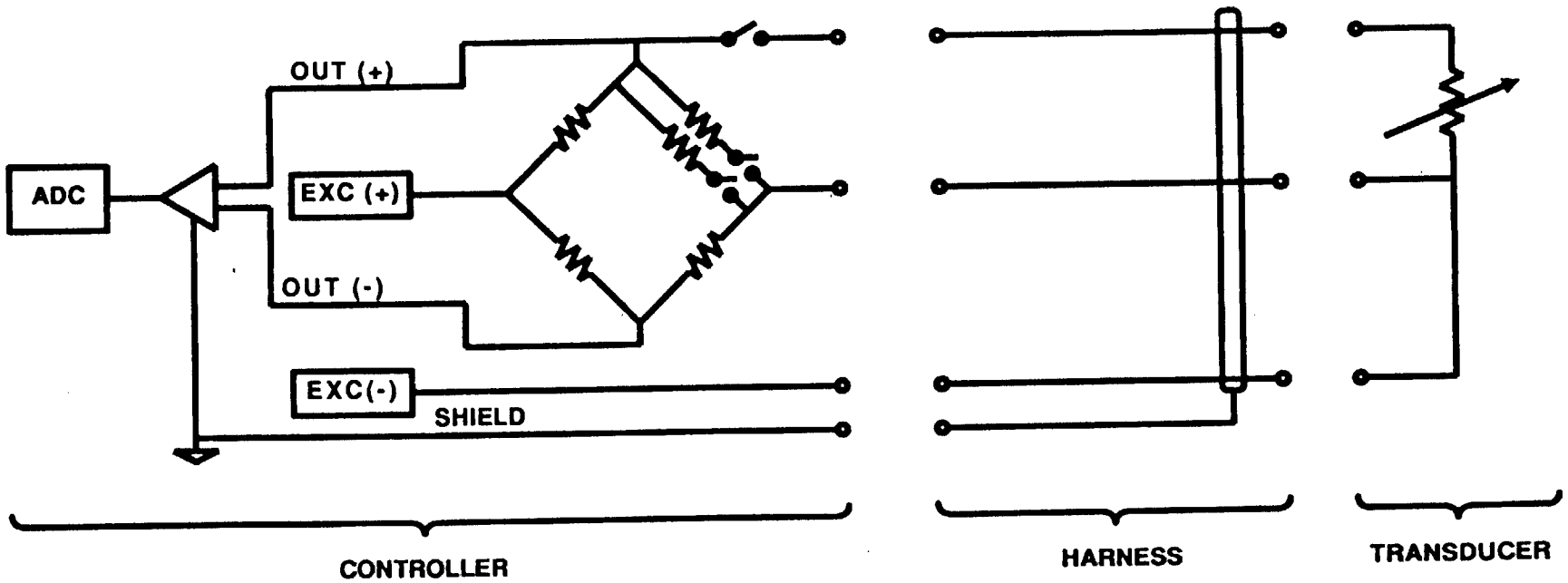
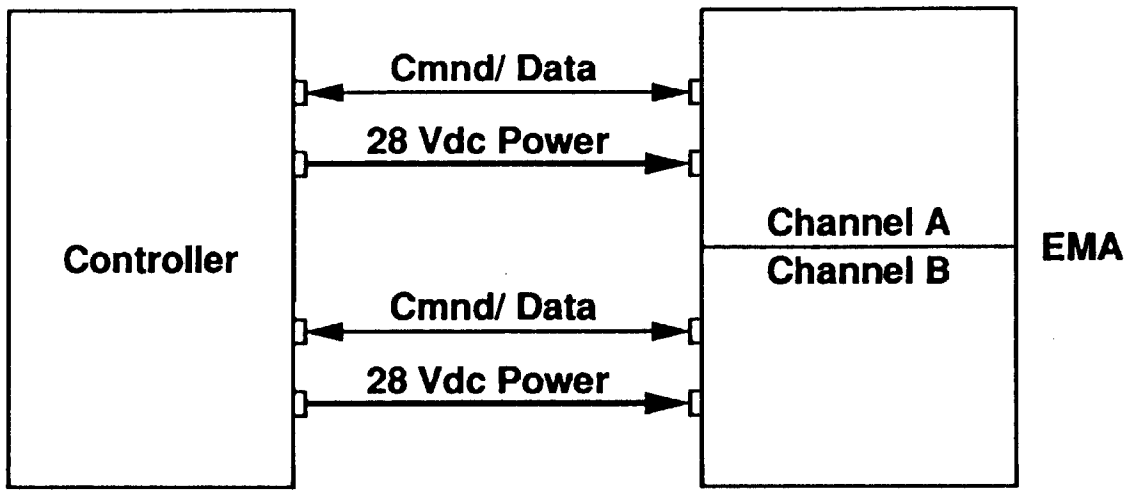
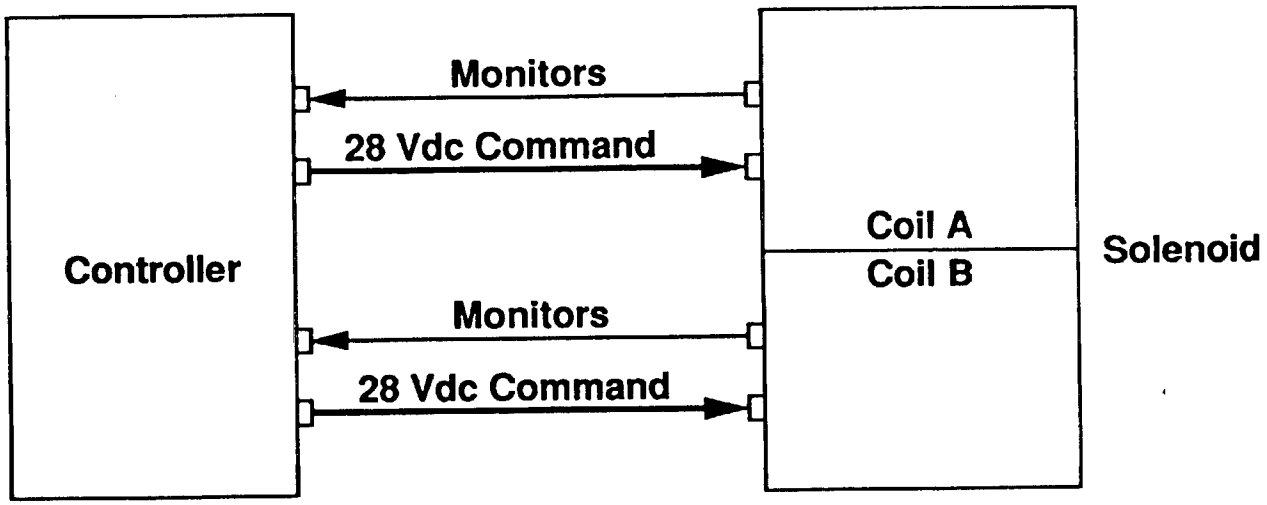


Figure 3-5. RDT Input Channel



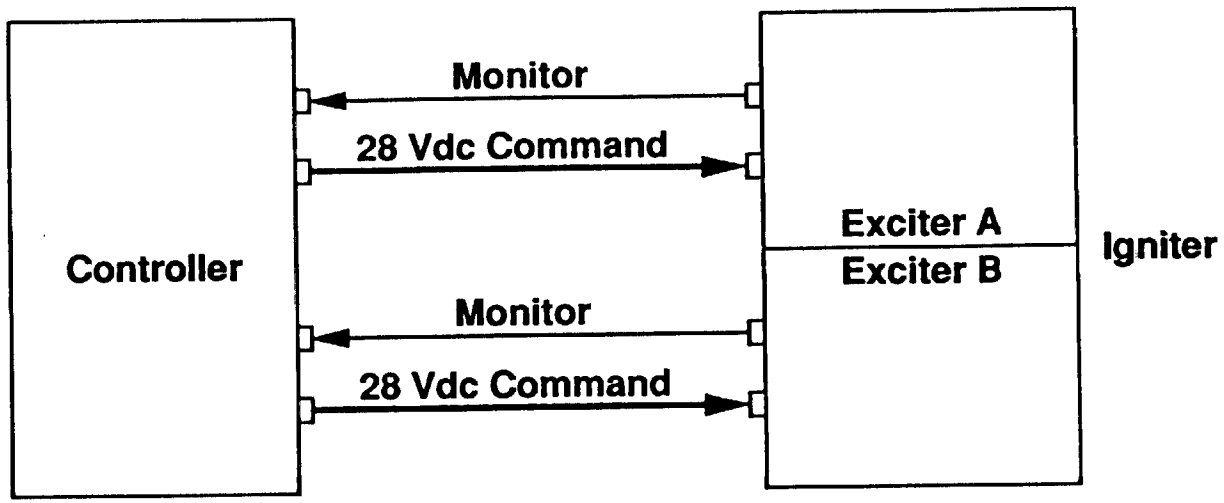
- **Dual Redundant MIL-STD-1553B Busses For Commands And Data**
- **Command Validation Required For Command Input**
- **Dual, Isolated Power Supply Busses**

Figure 3-6. Controller To EMA Valve Command Data And Power Interfaces



- **Dual Coil Solenoids And Monitors**
- **28 Vdc Command, 20 To 50 Ohm Load**
- **Feedback Monitoring Required**
  - **Command Signals**
  - **Current Waveform Monitoring**
  - **Limit Switches At Ends Of Travel**

Figure 3-7. Controller To Solenoid Command And Monitor Interfaces



- **Dual Exciter Igniters And Monitors**
- **28 Vdc Command**
- **Discrete Status Monitor Provided By Igniter Electronics**

Figure 3-8. Controller To Igniter Command And Monitor Interfaces

Redundancy Impacts Fault Tolerance Capability

Redundancy Approach	Fault and Response						Fault Tolerance
	#1		#2		#3		
	(D)	(I)	(D)	(I)	(D)	(I)	
Simplex	No	No	No	No	No	No	None
Duplex	Yes	??	No	No	No	No	FS
Duplex w/ BIST	Yes	Yes	Yes	??	No	No	FO/FS
Tri/Duplex	Yes	Yes	Yes	??	No	No	FO/FS
Triplex	Yes	Yes	Yes	??	No	No	FO/FS
Quadruplex	Yes	Yes	Yes	Yes	Yes	??	FO/FO/FS

(D) = Detect (I) = Isolate (FO) = Fail-Safe (FS) = Fail-Safe

- Simplex, or Duplex, Not Capable of Meeting Fault Tolerance Requirement
- Quadruplex Exceeds the Requirement
- Triplex, or Triplex/Duplex, or Duplex with 100% Fault Coverage, Meets FO/FS Requirement

Figure 3-9. Fault Tolerance Requirement Provides First Screening Of Candidates

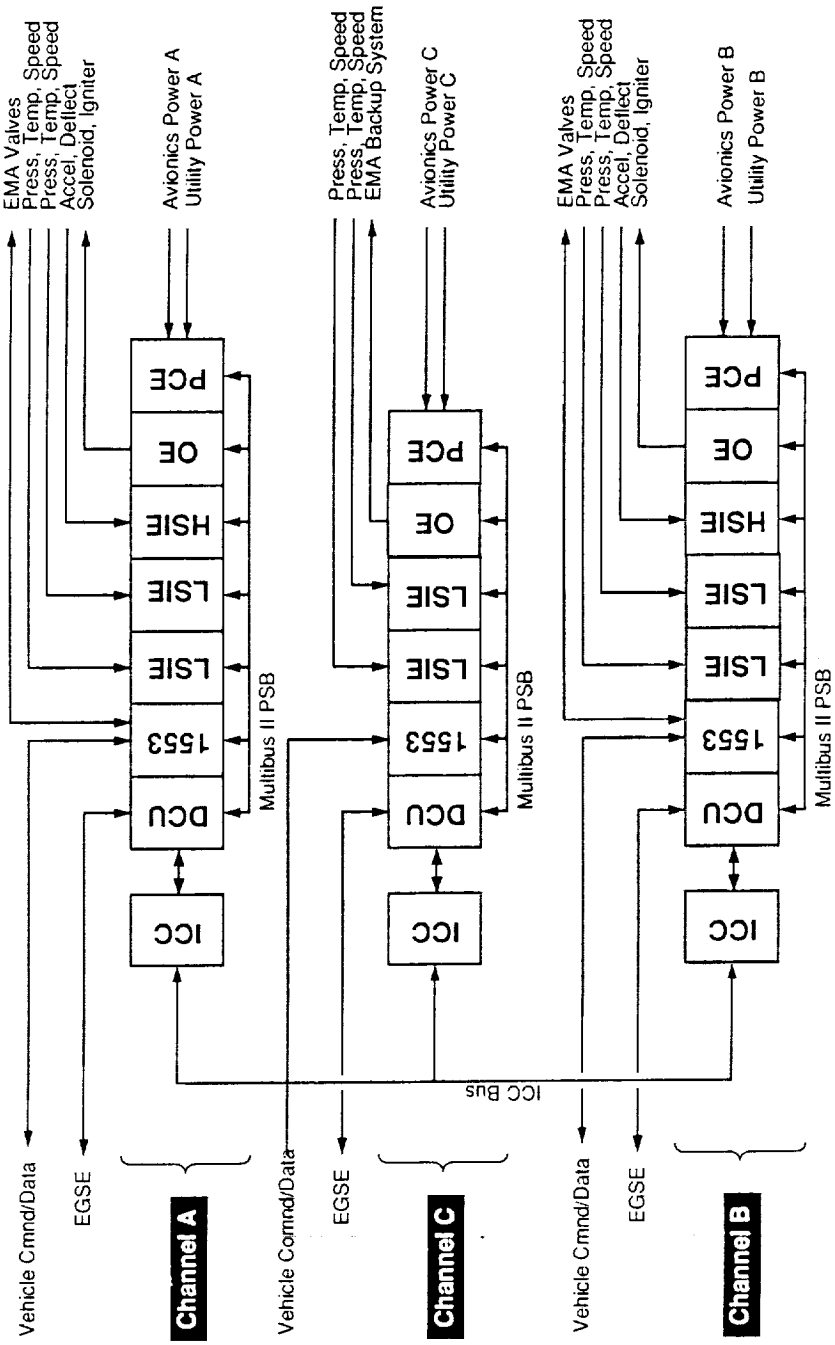


Figure 3-10. Functional Modules Provide Triplex Processing

The architecture included execution of instructions to monitor and control the engine on a 10ms major cycle. The instruction sequence is shown in Figure 3-11. Each cycle begins with an update of sensor values. Sensor managers read their transducers, providing current values to the engine manager. Next, current values of all flight-critical sensors are evaluated by the safety monitor which determines if an instantaneous shutdown respose is appropriate. The redundancy manager then checks the operating status of fault-tolerant components and, if necessary, makes a shutdown recommendation to the vehicle.

3.1.3 Results

Controller architecture was analyzed, a structured selection process was conducted, and the preferred approach defined. Details were presented at the Preliminary Design Review.

3.2 System Requirements

3.2.1 Objective

The objective of this task was to define system requirements and conduct a System Requirements Review (DR-36) at NASA-MSFC. The review was to include applicable project development requirements, technical requirements and design criteria, and engineering analyses including systems and maintenance considerations applicable to the Contract End Item (CEI) Specification.

3.2.2 Activity Overview

Engine Controller requirements were derived from Advanced Launch System (ALS) Phase I and Phase II studies performed by General Dynamics, Boeing, and the Martin Marietta/McDonnell Douglas team. Engine designs available from the Space Transportation Main Engine (STME) and Space Transportation Booster Engine (STBE) Phase A and STME Phase B activities were also studied. As STME Phase B work progressed in parallel with this effort, the evolving Contract End Item Specification (CEI) and the companion Interface Control Document (ICD) drove controller requirements. In addition, capabilities of the NASA-MSFC Flight Simulation Laboratory were also considered as this facility would eventually be used for system integration and

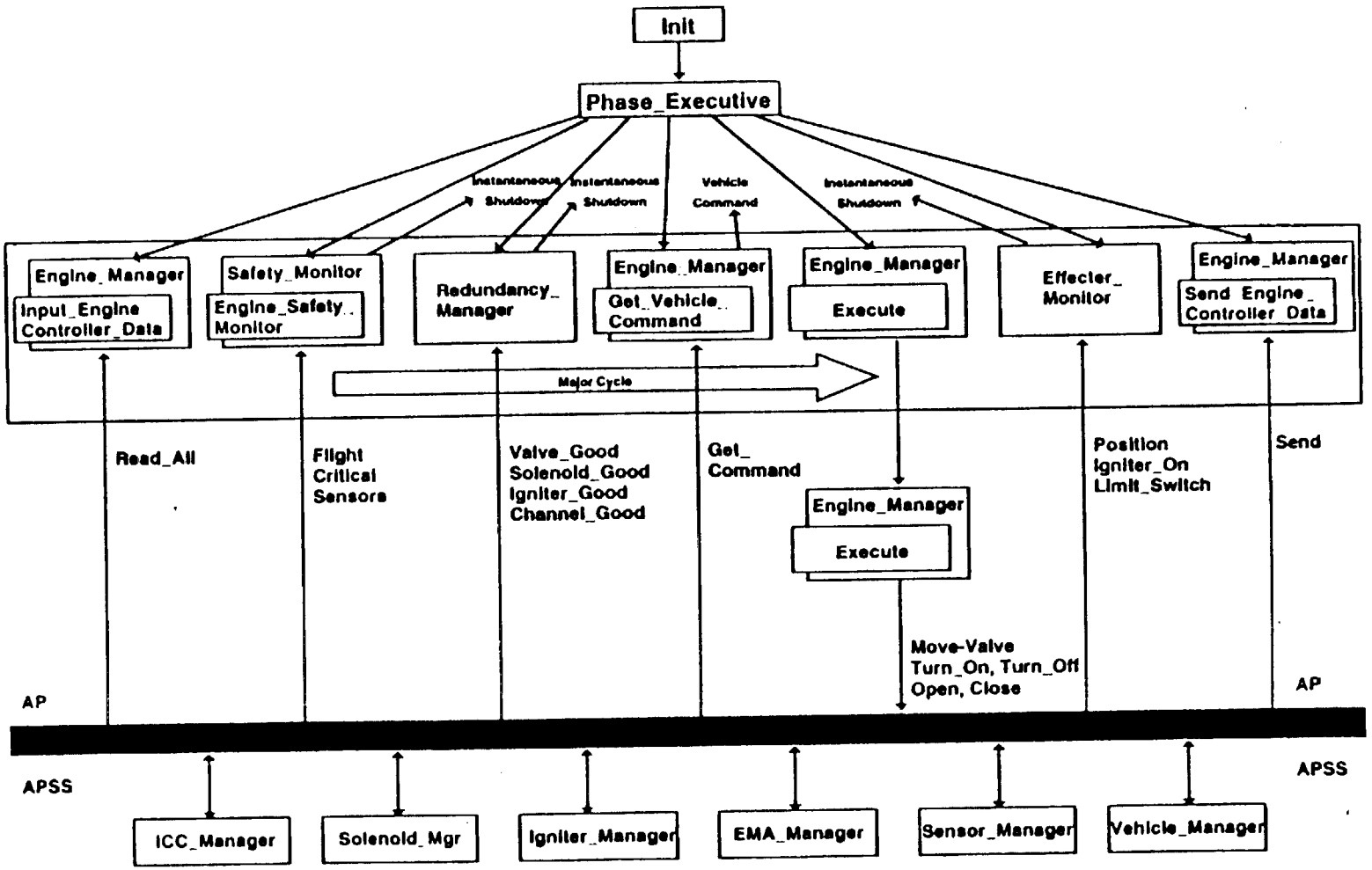


Figure 3-11. The Software Executes A Predefined Set Of Routines For Each Major Cycle

demonstration. Results to date of the Rocket Engine Conditioning Monitoring System (RECMS) study were included in the requirements definition effort, as this provided significant data on the sensor suites (Figure 3-12).

In summary, requirements were developed top-down, from the vehicle to the engine to the controller. A baseline set of intra-engine interfaces was obtained by referring to other STME ADP component programs. At the start of this effort, many interfaces had not been completely firmed up. However, interface variations could usually be accomodated because of the flexibility of the modular system that had been selected.

Software requirements were derived from the engine control system functional requirements. Key software functions were:

- Engine Control - to condition, start mainstage, and shutdown.
- Communication - to transmit data to the vehicle or to another engine channel.
- Command/Sensor/Data Input and Validation - for data validation and conditioning.
- Redundancy Management - to manage use of redundant capabilities.
- Built-In Test - hardware checking and sensor circuitry calibration.
- Fault Detection and Analysis - electronic fault isolation and engine failure detection.

Software Design Standards were also adopted to ensure proper organization, consistency, and maintainability. These included use of the Ada higher order language which is structured and is a highly understandable source code. Structured design techniques included logical partitioning of functions and object-oriented programming. Mission and channel-specific information was to be contained in portable data tables to ensure high software commonality from mission to mission and between redundant controller channels.

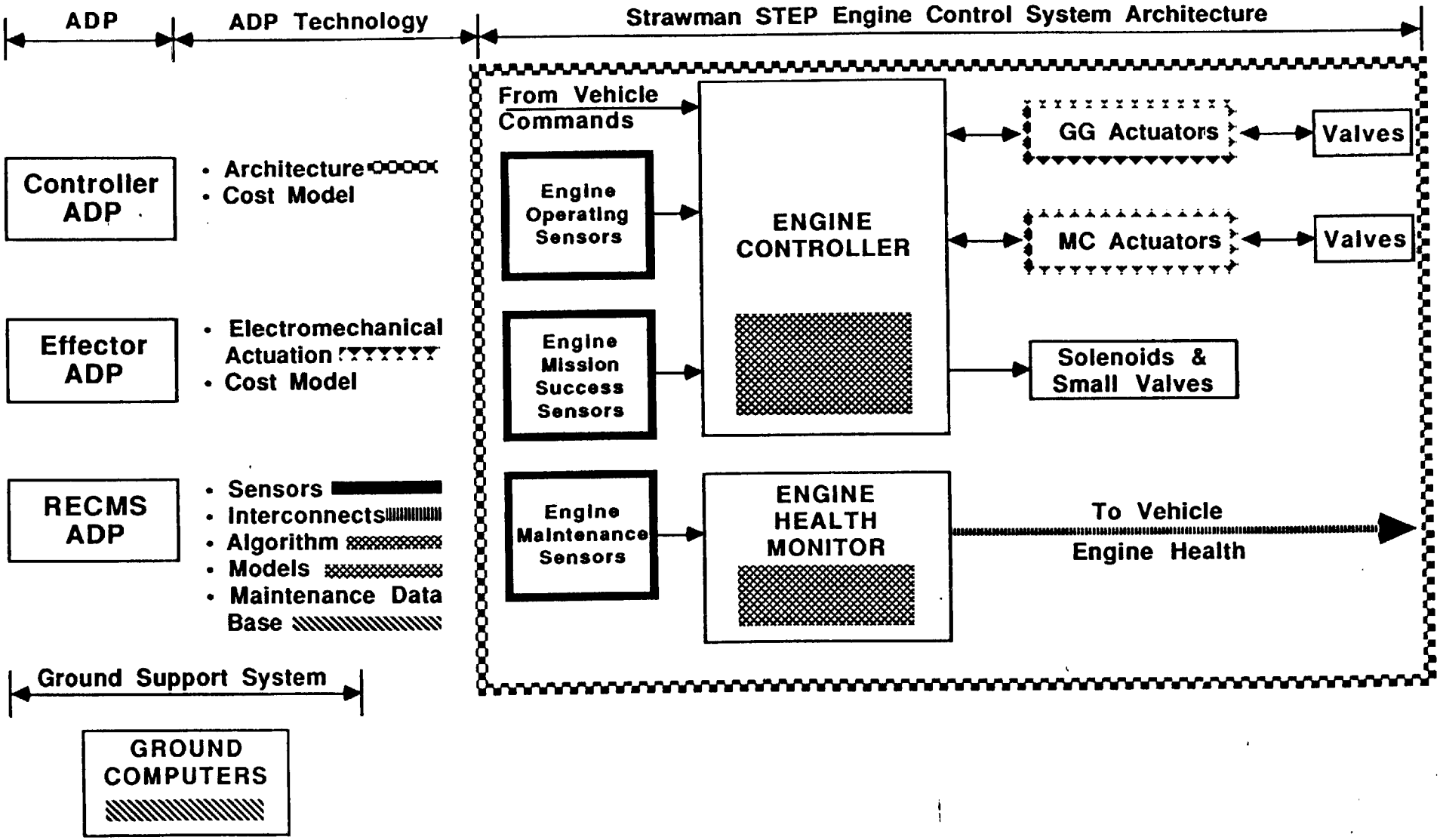


Figure 3-12. Coordinating With RECMS ADP To Define Controller Interface

Figure 3-13 summarizes these requirements which were presented and agreed at the System Requirements Review (SRR).

3.2.3 Results

A consolidated set of controller requirements was assembled using data from vehicle and engine sources, and recognizing system laboratory test and validation capabilities and constraints. These requirements were presented at the System Requirements and Preliminary Design Reviews.

3.3 Preliminary Design

3.3.1 Objective

The objective of this task was to prepare a preliminary design consistent with the requirements defined in Section 3.1 above. Low recurring cost was a major design focus, i.e., both production and operational costs. The design selection was to be supported by trade studies and analyses to identify major cost elements and evaluate options best suited to achieving low cost.

3.3.2 Activity Overview

A preliminary design of the controller was completed and then presented at the Preliminary Design Review (PDR). This review addressed system requirements derived from higher level and/or engine interface sources, and architectural analyses that had been performed. The brassboard design was presented together with an EGSE preliminary design. Testing configurations and interfaces at the MSFC Simulation Laboratory were discussed. The PDR also addressed Phase II plans which included early demonstration of critical modules, benchmarking of representative Ada code, and procurement of long lead parts. Details of the cost modelling effort were also given at the PDR.

ISSUES	ADP SOW	ENGINE CEI	VEHICLE SRD	ADP STATUS
Control	• Prestart • Start • Mainstage • Throttle (60 - 100%) • Shutdown	• Autonomous (Start through Shutdown) • Dual Thrust (MPL = 70%, RPL = 100%)	• Real-Time Fault Management • Engine-Out Capability	• Consistent with all Requirements
Monitoring	• Safety • Condition • Self-Test	• Condition • Checkout • Redundancy Verification • Status	• Integrated Health Monitoring • Support of VHMS	• Consistent with all Requirements
Communications			• Mil-Std-1553B • Separation of Flight-Critical and Non Flight-Critical Buses	• Use of Mil-Std-1553B • Use of Separate Buses
Power	• 28 Vdc		• 270 Vdc	• 28 Vdc
Software	• Ada		• Ada	• Use of Ada
Configuration	• Brassboard	• Engine Mounted	• Propulsion System Controller (Aft Avionics)	• Incremental Progression To Block I Configuration
Reliability	• 0.99995 Allocation	• 0.999 @ Nominal Duty Cycle	• 0.98 for Mission Success	• FMEA for brassboard • Quant Anal for Block

Figure 3-13. ALS Controller Requirements Were Established At SRR

3.3.3 Results

The preliminary design effort was completed and presented at the PDR on 18 September 1990. Results are available in the referenced PDR package. Further data were given at a Technical Interchange Meeting on 25 April 1991.

3.4 Cost Model

3.4.1 Cost Model Objective

The overall objective of this task was to construct a cost model capable of predicting recurring costs of a flight controller including production and operations and support (O&S) costs, at production rates of 30 to 100 units per year. The model was to consider the impact of various specification requirements as well as production rate and learning curve effects and to reflect cost estimates made in the design process as well as actual costs of fabricated hardware. The model was intended for use in subsequent evaluations of cost reduction design and manufacturing approaches.

The objective of the Phase I effort was to define general model structure, requirements, underlying assumptions, data sources, and calibration approach, and to create a preliminary cost model.

3.4.2 Activity Overview

During Phase I, various spreadsheet software options were evaluated and Microsoft Excel was selected as the core application. This program permits data transfer between Macintosh and IBM Pcs and has multiple windowing capability with customized menus and dialog boxes. A Supplier Cost Information Form was developed to collect supplier cost data in a consistent manner, with the intent of using this same form in other Aerojet NLS Advanced Development Programs. The Phase I activity culminated in a detailed presentation of program objectives, logic, features and cost model work at the Preliminary Design Review.

The model logic is shown in Figure 3-14. Touch labor and supplier costs for all constituent parts were to be inputted and continually updated as actual costs became available. Using algorithms developed, the model accounts for the variables cited above.

When cost model activities ceased in response to GFY 1990 and 1991 funding reductions, cost model logic had been updated and development of uncertainty algorithms was 90% complete. A data dictionary was also prepared. It included definitions used in model software, as well as all algorithms, and formed the basis of a Preliminary Users Manual. Preliminary software programming was completed but not checked out/validated. Record layouts (monitor screens) were formulated.

3.4.3 Results

Cost model development work defined and partially developed a tool for analyses and tracking of STME engine component costs. Model logic, algorithm formulation, and basic programming were completed. Model operation was demonstrated using preliminary cost data derived from existing Aerojet-produced flight hardware. Model development was discontinued after Phase 1 of the program was completed.

The model, although not fully validated, is a potentially useful tool for similar cost studies in future programs. Since it is based on actual or estimated costs for given manufacturing process flows and specification requirements, rather than on historical data or simple cost estimating relationships, it is suitable for studying new manufacturing approaches or more broadly, new ways of doing business.

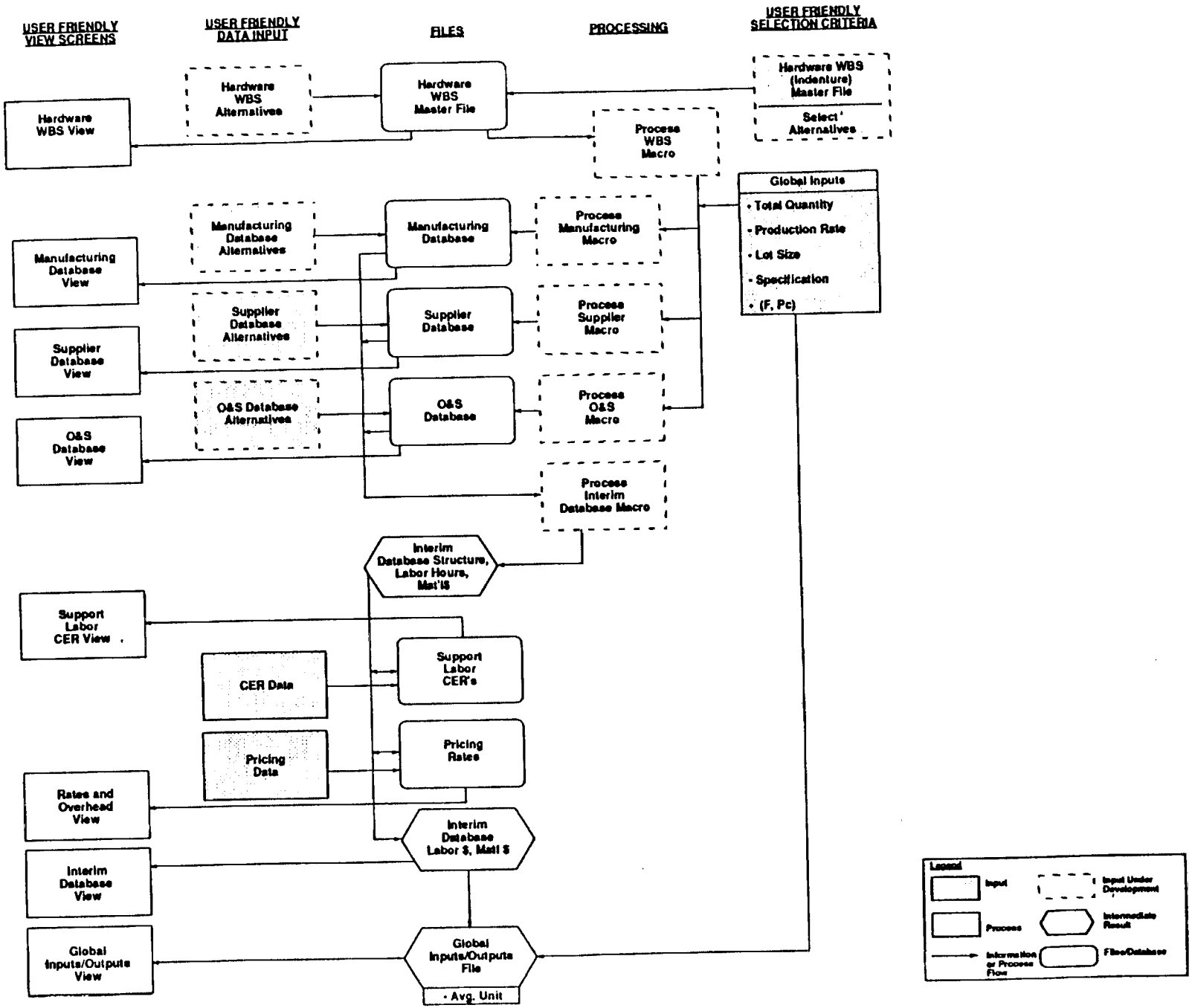


Figure 3-14. Cost Model Logic

Phase II - Detailed Design, Fabrication, and Demonstration Objectives

3.5 Detailed Design

3.5.1 Objective

The objective of this task was to prepare a detailed design and analysis of the controller system, including supporting studies and preparation of manufacturing drawings (DR-29) and parts lists (DR-37). Included in the activity was preparation of an acceptance test plan (DR-38), test program plan (DR-40), and controller test procedure (DR-41). Controller reliability was to be estimated using probabilistic failure analyses of life-critical failure modes and the calculational uncertainties addressed. A Detailed Design Review (DR-27) was to be the culmination of this task effort.

3.5.2 Activity Overview

The detailed design was developed from the preliminary design, requirements definition, and various supporting trade studies noted above. Controller capabilities were designed to be consistent with operational and monitoring functions shown in Figure 3-15, ie. to provide control commands and response monitoring necessary for prestart, start, throttling over 60% to 100% thrust range in 10% increments, shutdown, and post-shutdown events. In addition, the controller was to provide condition monitoring for engine launch commit and unsafe condition determination leading to engine shutdown, self-test and redundancy management, command and condition monitoring for auxiliary devices such as the purge system, and interface with the vehicle avionics system.

A triplex control system was established, with simplex, duplex, or triplex interfaces with sensors, effectors, vehicle command/data, and vehicle power as summarized. in Figure 3-16. The controller block diagram, Figure 3-17, shows the interfacing with specific controller modules.

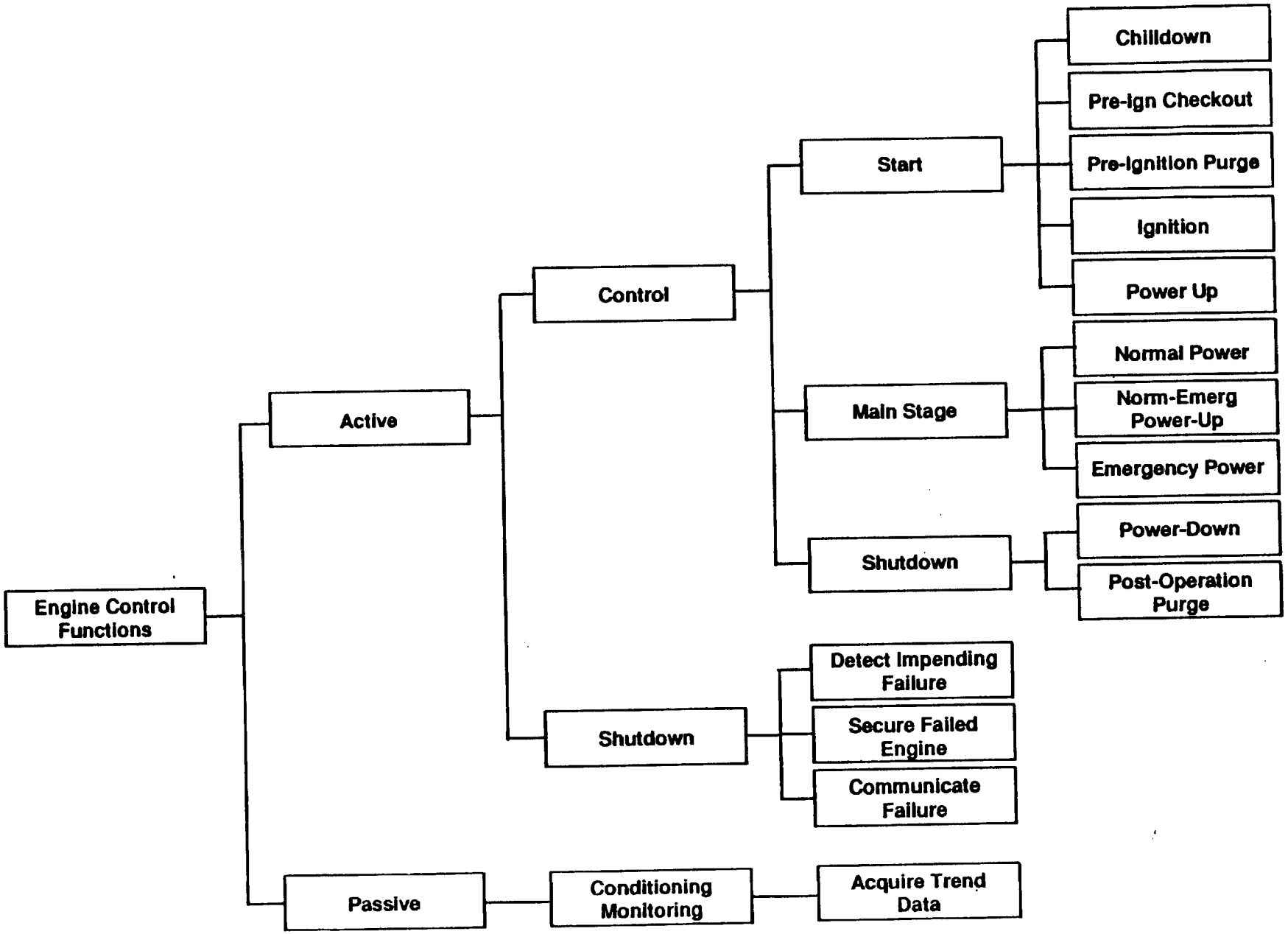


Figure 3-15. Engine Control And Monitoring Functions Supervised By The Controller

	INTERFACE	TYPE	REDUNDANCY	SOURCE
VEHICLE	COMMUNICATION	MIL-STD-1553B	TRIPLEX	VEHICLE ARCHITECTURE
	POWER	28 VDC	TRIPLEX	VEHICLE ARCHITECTURE
EFF TYPES	EMA	MIL-STD-1553B	DUPLEX	EMA PROGRAM
	SOLENOID	28 VDC	DUPLEX	ENGINE DEFINITION
	IGNITER	28 VDC	DUPLEX	TRADE RESULT
EFF MON	EMA	MIL-STD-1553B	DUPLEX	EMA PROGRAM
	SOLENOID	LIMIT SWITCH	DUPLEX	ADP SOW
	IGNITER	STATUS	DUPLEX	ADP SOW
SENSOR TYPES	PRESSURE	0-30 mV	SIMPLEX	TRADE RESULT
	THERMOCOUPLE	0-30 mV	SIMPLEX	TRADE RESULT
	RTD	0-285 mV	SIMPLEX	TRADE RESULT
	SPEED	75 mV -15 V	SIMPLEX	TRADE RESULT
	ACCELEROMETER	0-5 V	SIMPLEX	TRADE RESULT
	DEFLECTOMETER	0-5 V	SIMPLEX	TRADE RESULT

Figure 3-16. Engine Controller Derived Interface Requirements

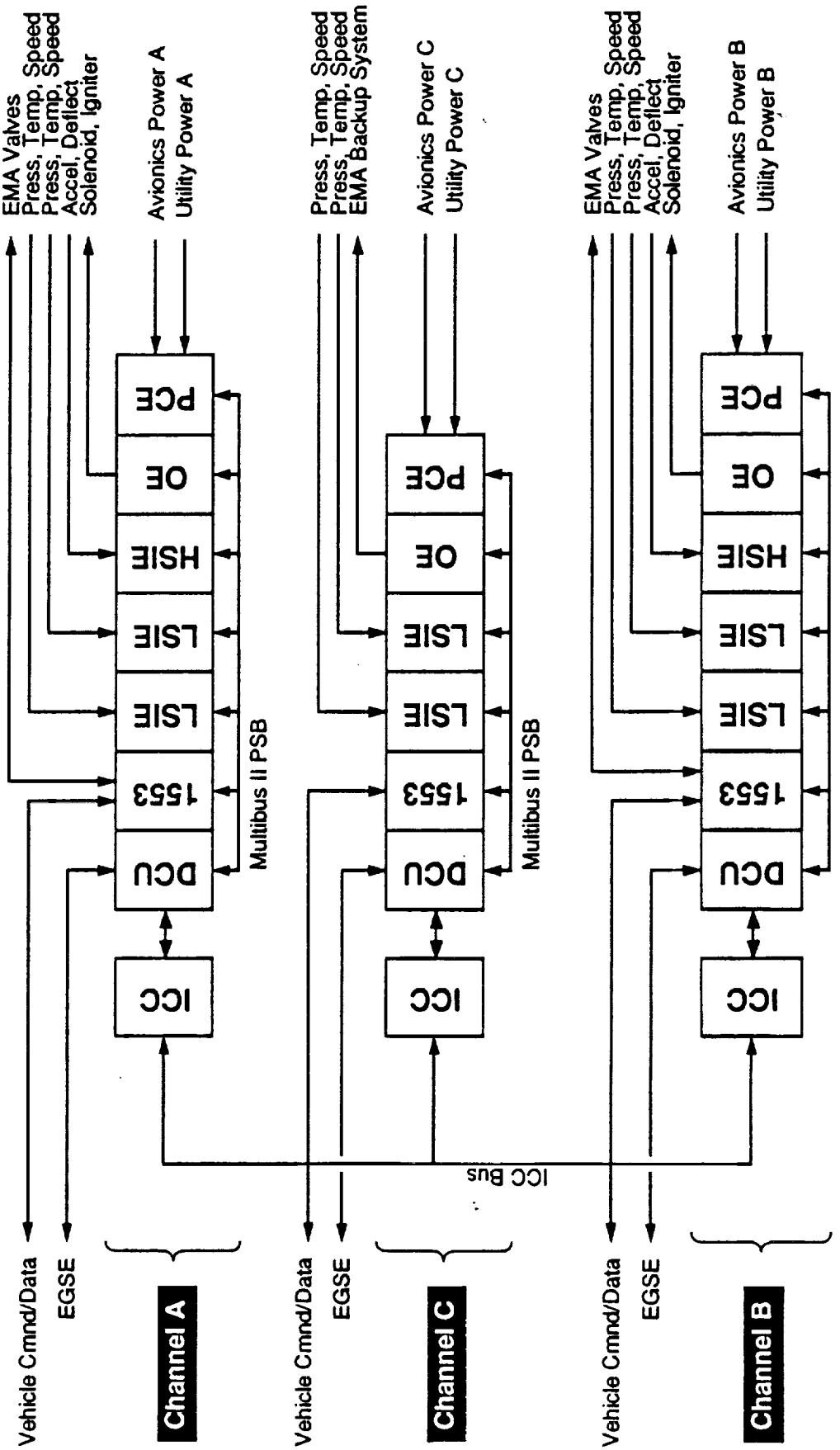


Figure 3-17. Engine Controller Block Diagram

The controller design is based on the triply redundant Draper Fault Tolerant Processor (FTP), an ultra-reliable architecture that combines tightly synchronized hardware and software fault management and reconfigurability to provide extensive fault coverage.

Major elements of the design include the following:

Digital Computer Unit (DCU)

The DCU is the component that provides the processing capability of the FTP. It is composed of five major elements: microprocessor, decode logic, processing resources, Multibus II interface, and the various physical interfaces of the DCU. These five elements relate to each other as shown in the block diagram in Figure 3-10. The microprocessor includes the Intel 80960, a 32 bit RISC type processor. Decode logic includes wait-state generation circuitry. Processing resources include the memory, peripheral devices, and I/O ports which support and offload the 80960. The memory section includes SRAM and EPROM memory. The peripheral devices section includes the interrupt controller, serial controller, and interval timers.

Interchannel Communications Module (ICC)

The ICC links redundant processing units of the FTP and implements FTP redundancy management mechanisms of the by facilitating processor synchronization, fault-tolerant data communication, and asynchronous interrupt servicing.

1553 Module

This module interfaces to the MIL-STD-1553B avionics buses connected to the FTP, which include the communications bus to the vehicle and the command and data bus for the valve EMAs. It receives direction from the DCU module and resonds to incoming commands and data. A single module is capable of managing the interfaces on three separate buses, thus the three modules provide active/active redundant bus interfaces needed to support system level fault tolerance. The module has four major elements: Multibus II interface,

channel status logic, 1553 communications interface circuitry, and the physical interfaces on the board.

High Speed Input Electronics Module (HSIE)

The HSIE module is the component that interfaces with high frequency transducers connected to the FTP, namely the accelerometers and deflectometers. A single HSIE can monitor four accelerometers and four deflectometers. Its six major elements include the Multibus II interface, supplementary decode logic, sensor signal conditioning, power scaling, sampling control, and the physical interfaces on the board.

Low Speed Input Electronics Module (LSIE)

The LSIE module interfaces with the frequency transducers connected to the FTP, i.e., pressure sensors, temperature sensors, and speed probes. A single LSIE module is capable of monitoring eight pressure or temperature transducers and one speed probe. LSIE modules on separate channels monitor redundant measurements of flight-critical parameters to support system-level fault-tolerance. Major elements of the LSIE are the Multibus II interface, supplementary decode logic, pressure/temperature input processing, pressure/temperature multiplexing and digitization, speed probe input processing, and the physical interfaces on the board.

Output Electronics Module (OE)

The OE module is a single string output board that interfaces 28 vdc devices on the control system to the engine controller. It receives direction from the DCU module and connects directly to the external devices via command outputs and monitor feedback signals. A single OE module is capable of driving and monitoring a maximum of 12 such 28 vdc devices. OE modules on separate channels drive the redundant elements of duplex effectors to support system-level fault-tolerance. Major elements of the OE module are the Multibus II interface, supplementary decode logic, command logic, switch input logic, current and power monitoring circuitry, discrete output drivers, and the various physical interfaces of the module.

Power Conditioning Electronics Module (PCE)

The PCE module provides the power regulation and control capability for all the modules in a single channel of the FTP. It supplies the standard +5 vdc voltage for most of the digital logic, the analog voltages used by the input electronics, the digital voltages required by the 1553 bus interfaces and switching of the 28 vdc power to the output electonics. It consists of four major elements: current limiting circuitry, power regulation section, power control circuit, and the various physical interfaces of the PCE module.

Software

The Operational Flight Program (OFP) engine controller system Computer Software Configuration Item (CSCI) consists of four software components: 1) the Application Program (AP) which contains the upper level modules responsible for implementing control and checkout procedures required to operate the engine; 2) the Application Program Support Services (APSS) which provides low level common utility functions used by the AP procedures to access the controller hardware, including both hardware and run time-dependent processing; 3) the EGSE component which includes the Ada run-time kernel and the interface to the RS-232/422 port through which program control and debugging access is provided; 4) the Bootstrap component which provides initial processing that occurs on the application of power to the engine controller and provides the initial facility for loading and executing the remainder of the OFP.

Electrical Ground Support Equipment (EGSE)

The EGSE provides all intermediate support components necessary to interface the controller to the computing facilities of the MSFC Flight Sim Lab (FSL); it also provides configuration checkout and diagnostic capabilities for control system management. The intent was to check out the control system at Aerojet and subsequently perform engine and vehicle simulation testing at the FSL using facility computers. EGSE is composed of six functional elements: ground support computer (GSC), effector simulators, sensor simulator, EMA valve simulator (EMAVS), power distribution system (PDS), and the

interconnect system. Figure 3-18 shows the functional relationships of the controller, EGSE, and FSL computers during simulated operation.

In the physical design, each controller channel is contained in a single 19 inch cardcage, as shown in Figure 3-19, and the three cardcages are then installed in a three tier, 19 inch rack-type cabinet, as shown in Figure 3-20.

A comprehensive documentation package was prepared in conjunction with the Detailed Design Review (DDR). Specific documents are identified in 3.5.3 which follows.

3.5.3 Results

The detailed design effort was completed and presented at the DDR on 9-10 June 1992. Results are available in the DDR Review Package which included:

DR-26	Contract End Item Specification (Rev A)
DR-27h	Test Program Plan
DR-37	EEE Parts List
DR-38	Controller Acceptance Test Plan
DR-39	Electrical Interface Control Document (Rev A)
DR-27	Brassboard System Documentation (vol. 1)
	DCU Module Design Description Document (vol. 2)
	ICC Module Design Description Document (vol. 3)
	1553B Module Design Description Document (vol. 4)
	HSIE Module Design Description Document (vol.5)
	LSIE Module Design Description Document (vol. 6)
	OE Module Design Description Document (vol. 7)
	PCE Module Design Description Document (vol. 8)
	Software Design Documentation (vol. 9)
	EGSE Design Documentation (vol. 10)

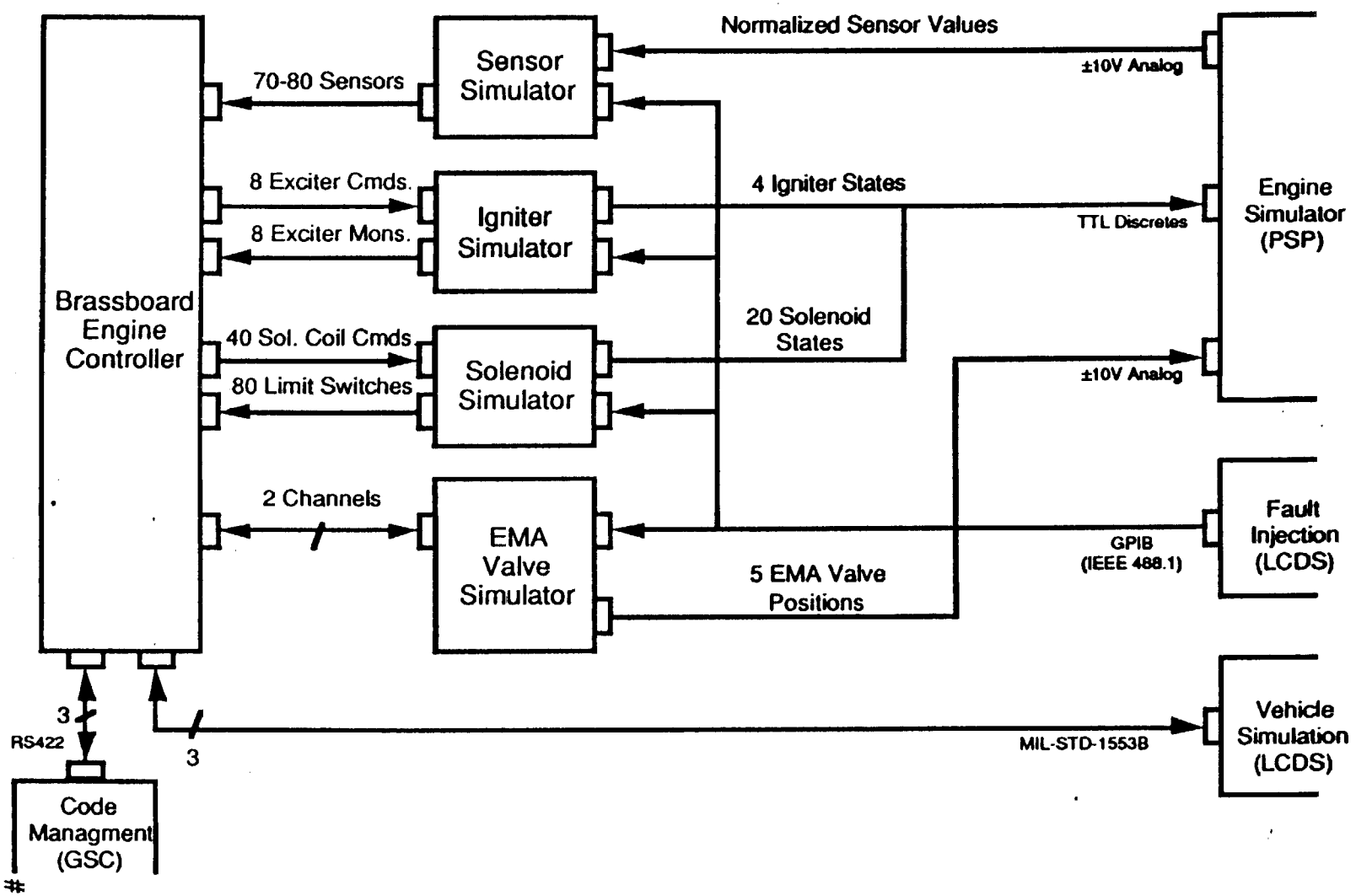


Figure 3-18. EGSE Block Diagram (Operation)

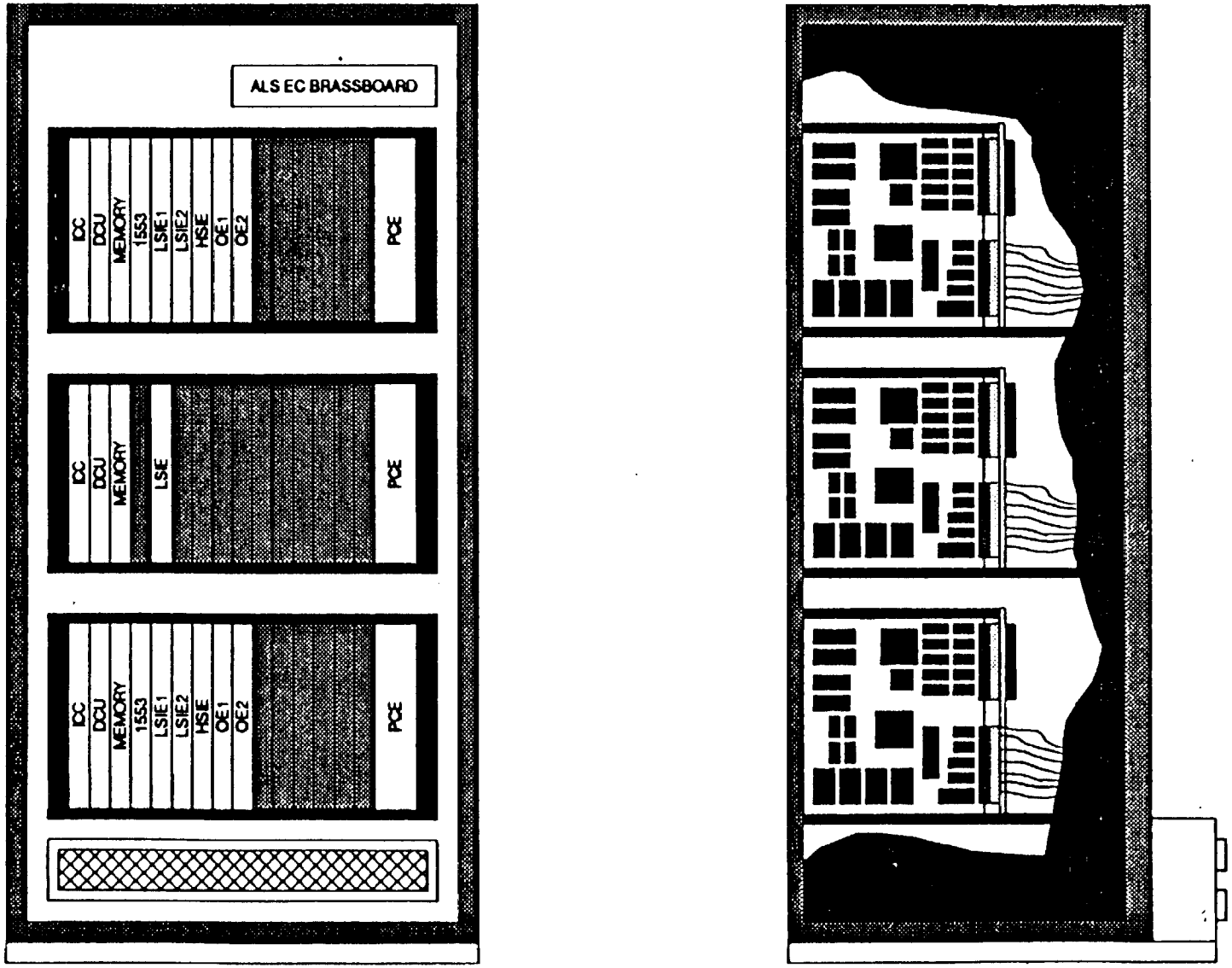


Figure 3-19. ALS Brassboard Modules Installed In Three Tier, 19" Rock-Type Cabinet

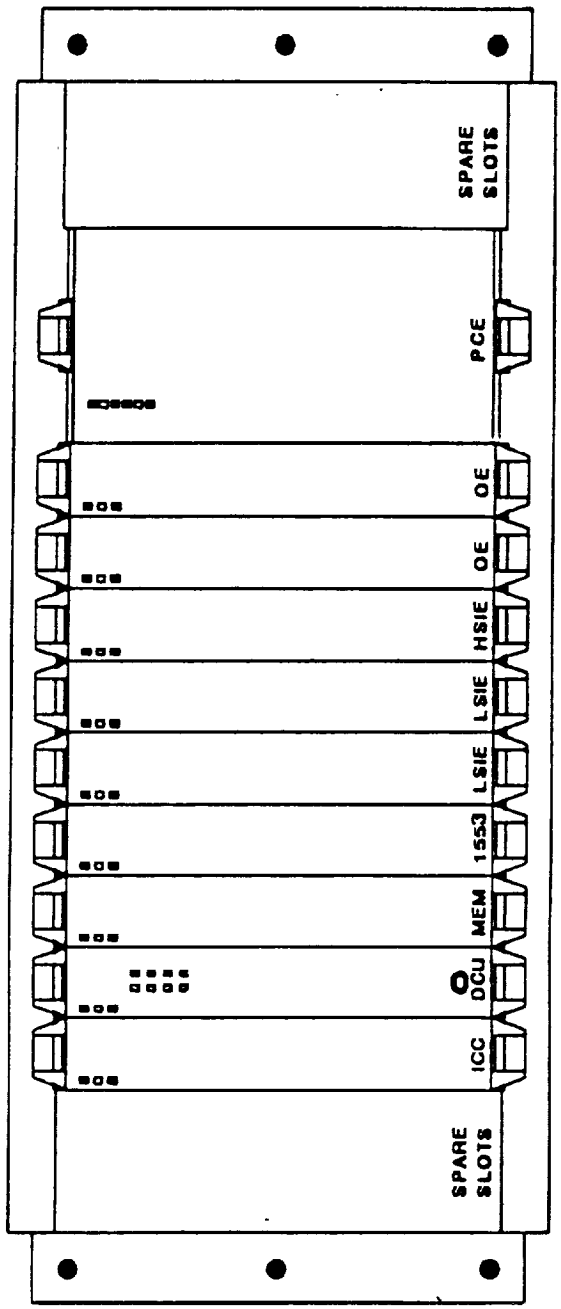


Figure 3-20. Each Channel Contained In Single 19" Cardcage

3.6 Deliverable Hardware and Software

3.6.1 Objective

The objective of this task was to fabricate one complete nonflight controller set plus critical spares, and a nonflight version of the system and application software, as well as: means to dynamically simulate sensor responses; nonflight version of the interconnect system; nonflight version of the supply system delivering power to the EMAs, instrumentation, and EGSE; means to dynamically simulate the characteristics of all control effectors including igniters, solenoids, switches, actuators, regulators, valves, etc.; plus EGSE that emulates all controller interfaces, provides for controller memory load and verification, and provides the capability to test all controller functions.

3.6.2 Activity Overview

Various constituent parts of the controller system were purchased prior to direction to stop work and descope the program. These were not assembled into control system components.

3.6.3 Results

No results were achieved due to descoping of the program.

3.7 System Demonstration and Evaluation

3.7.1 Objective

The objective of this task was to deliver to NASA-MSFC and set up the controller system, perform tests, and evaluate and document test results, so as to demonstrate that design requirements could be achieved in a low cost system.

3.7.2 Activity Overview

This task was not performed due to descoping of the program.

3.7.3 Results

No results were achieved due to descoping of the program.

3.8 Special Studies

3.8.1 Objective

The objective of this task was to provide the NASA-MSFC COTR the resources to have the contractor perform work beyond the requirements of the Statement of Work.

3.8.2 Activity Overview

This task was not performed due to descoping of the program.

3.8.3 Results

No results were achieved due to descoping of the program.

3.9 Cost Model

3.9.1 Objective

The objective of the Phase II cost modeling activity was to prepare a detailed model and to substantiate this model with historical data.

3.9.2 Activity Overview

This task was not performed due to descoping of the program.

3.9.3 Results

No results were achieved due to descoping of the program.

4.0 FUTURE HARDWARE/DATA APPLICABILITY

4.1 Overview

This program has evolved and/or proven a number of innovative approaches to the design, manufacture, and test of liquid rocket engine controller systems. Although these were designed to apply specifically to the Space Transportation Main Engine (STME), the design products of this program should be applicable directly or indirectly to other future NASA engine programs, either for upgrading existing designs or for entirely new engine types.

4.2 Hardware

Unfortunately, this specific program was descoped before any system components could be assembled. However, Aerojet has produced and tested a similar controller under company-sponsored activities. These activities have matured the hardware for a controller design similar to that discussed in this report. The combined results of contract activity and Aerojet-sponsored work mean that controller hardware generally similar to that planned for STME is essentially proven for application to existing or new engines.

4.3 Data/Software

Controller Software: Considerable progress was made in developing a software set for the controller. Detailed Design Review data described all software objects, object external interfaces and calling structures, channel initialization and BIT parameters. A skeleton structure of the controller software code was constructed in Ada language. This defined all object functions and procedure definitions, interface variables, and calling structure logic. Due to program descope, detailed software code was not generated. However, Aerojet has developed and demonstrated similar controller software under the company-sponsored activities. These efforts have matured the controller software design in a manner similar to the hardware maturation noted above. The combined results of this contract activity and Aerojet-sponsored software work means that software generally similar to that planned for STME is essentially available for application to existing or new engines.

Cost Model: Cost model work to date is the foundation of an excellent tool for the estimation, tracking, and control of recurring costs. The model has broad applicability to any component assembly and allows the user authority over input costs and manufacturing cost relationships. Development of a standard tool to be used by NASA and its contractors should be beneficial to all programs.

5.0 RECOMMENDATIONS

It is recommended that the hardware and data/software future application potentials discussed in Section 4 be given consideration by NASA. At the very minimum, data generated on this program are a substantial contribution to the NASA engine controller data base. However, it is considered that the products of this contract effort, particularly when supplemented by the products of Aerojet-sponsored activities, form the foundation for the application of a new generation of electronic controllers to existing and future liquid rocket engines. It is recommended that NASA initiate further controller development efforts aimed at upgrading existing systems and/or supporting a next-generation engine. The effort would leverage from work performed under this contract.

6.0 REFERENCES

All submitted Data Requirements are identified in the reference list, Table 6-1.

Table 6-1 LIST OF REFERENCES

Data Requirements(DRs):

01	533 Monthly Report
02	533 Quarterly Report
03	Monthly Progress Report
04	Facility Plan
05	Equipment List
06	Government-Furnished Property
12	Hazard Analyses Report
15	Technical Implementation Plan
16	Logic Network and Key Milestone Chart
17	Quality Assurance Plan
20	Acceptance Plan
21	Safety Analysis Report
22	Manufacturing Plan
23	Material Control Plan
25	System Safety Plan
26	Contract End Item Specification
27	Package Requirements and Design Reviews
29	Drawings, Lists, Form I, Specifications and Microfilm
35	Architectural Definition Document
36	Controller Systems Requirement Review Package
37	Electrical, Electronics, and Electromechanical Parts List
38	Controller Acceptance Test Plan
39	Electrical Interface Control Document
40	Controller Test Program Plan
41	Controller Test Procedure

DM-01	Software Management Plan
DM-02	Software development Plan
DM-05	Software Requirements Specification (Replaced by SW-02, Software Requirements Specifcation)
DM-07	Detailed Software Design Specification (Replaced by SW-03, Software Design Specification)
DM-15	Software Test Requirements

(Replaced by SW-03, Software Design Specification)

DM-16 Software Test Plan
(Replaced by SW-03, Software Design Specification)

NASA
National Aeronautics and Space Administration

REPORT DOCUMENTATION PAGE

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.

4. Title And Subtitle

ALS Engine Controller System

Summary Final Report

5. Report Date

15 November 1993

6. Performing Organization Code

7. Author(s)

Colin Faulkner - Program Manager

Roger Payne - Senior Engineer

8. Performing Organization Report No.

10. Work Unit No.

9. Performing Organization Name and Address

Aerojet Propulsion Division
P.O. Box 13222
Sacramento, CA 95813-6000

11. Contract or Grant No.

NAS8-38074

13. Type of Report and Period Covered

Summary Final Report

12. Sponsoring Agency Name and Address

National Aeronautics and Space Administration
Washington, DC 20546
NASA, MSFC, Huntsville, AL

14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This report summarizes analysis and design done on the controller system for the ALS main engine.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
Rocket Engine Controller	Unclassified, Unlimited

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of pages	22. Price
Unclassified	Unclassified	45	

NASA FORM 1626 OCT 86