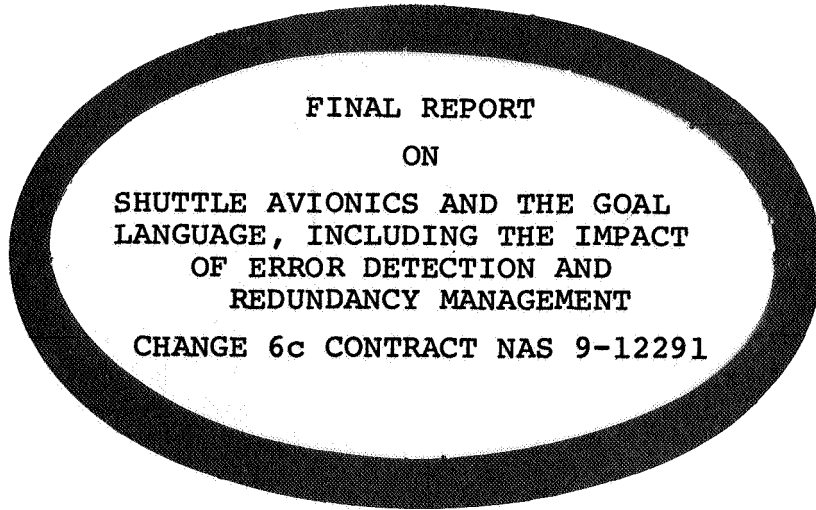
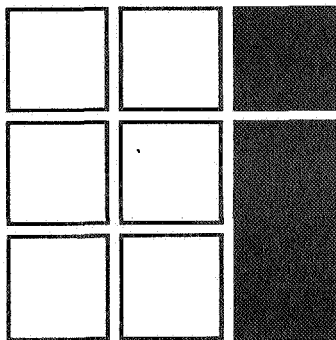


N73-31142



**CASE FILE
COPY**



INTERMETRICS

FINAL REPORT
ON
SHUTTLE AVIONICS AND THE GOAL
LANGUAGE, INCLUDING THE IMPACT
OF ERROR DETECTION AND
REDUNDANCY MANAGEMENT
CHANGE 6c CONTRACT NAS 9-12291

STANDARD TITLE PAGE

1. Report No.		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle FINAL REPORT ON SHUTTLE AVIONICS AND THE GOAL LANGUAGE INCLUDING THE IMPACT OF ERROR DETECTION AND REDUNDANCY MANAGEMENT				5. Report Date June 1973	
				6. Performing Organization Code	
7. Author(s) Flanders, J.H., Helmers, C.T. Stanten, S.F.				8. Performing Organization Report No.	
9. Performing Organization Name and Address INTERMETRICS, INC. 701 Concord Avenue Cambridge, Mass. 02138				10. Work Unit No.	
				11. Contract or Grant No. NAS-9-12291, 6c	
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration Johnson Space Center Houston, Texas 77058				13. Type of Report and Period Covered Final Report on Task 6c	
				14. Sponsoring Agency Code	
15. Supplementary Notes					
16. Abstract <p>This report studies the relationship between the NASA Space Shuttle onboard avionics and the ground test computer language GOAL when used in the onboard computers. The study is aimed at providing system analysis support to the feasibility analysis of a GOAL to HAL translator, where HAL is the language used to program the onboard computers for flight. This report deals with the subject in three aspects. First, the system configuration at checkout, the general checkout and launch sequences, and the inventory of subsystems are described. This material dates from April 1973. Secondly, the hierarchic organization of onboard software and different ways of introducing GOAL-derived software onboard are described. Also the flow of commands and test data during checkout is diagrammed. Finally, possible impact of error detection and redundancy management on the GOAL language is discussed. A companion report is entitled: Final Report on GOAL-to-HAL Translation Study.</p>					
17. KeyWords Test Oriented Language Space Shuttle GOAL HAL				18. Distribution Statement	
19. Security Classif.(of this report) Unclassified		20. Security Classif.(of this page) Unclassified		21. No. of Pages 57	22. Price

NOTICE

This report was prepared as an account of Government-sponsored work. Neither the United States, nor the National Aeronautics and Space Administration (NASA), nor any person acting on behalf of NASA:

- (1) Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately-owned rights; or
- (2) Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, method or process disclosed in this report.

As used above, "person acting on behalf of NASA" includes any employee or contractor of NASA, or employee of such contractor, to the extent that such employee or contractor of NASA or employee of such contractor prepares, disseminates, or provides access to any information pursuant to his employment or contract with NASA, or his employment with such contractor.

FOREWORD

This Report has been generated in order to fulfill a portion of the Statement of Work under Change 6c to NASA Contract NAS 9-12291. The main thrust of the task defined in the statement of work is to determine the feasibility of a translator from the higher order language GOAL to the higher order language HAL. This question is addressed in a parallel report published concurrently and entitled, Final Report on GOAL to HAL Translation.

However, a portion of the study involves considerations introduced by the design features of the Shuttle onboard systems, particularly the avionics. One of these considerations is that of the executive support routines required to support GOAL statements. Compile-time and run-time executive support issues are discussed in the other Report. However, this Report reviews options available in the executive support routine or operating system in the onboard computers. The second consideration is the impact on the GOAL language made by the implementation of error detection and redundancy checking in the onboard systems.

Both of these considerations have been explored and discussed in this Report in the context of the system definition of mid-May 1973. Sufficient design detail was made available to Intermetrics to set forth some options and some recommendations in both areas. Further and more specific results will be possible when the system is more fully defined.

Note: Chapter 3.0 of this Report satisfies Task 1.6 of the Work Plan, dated 4/10/73. Chapter 4.0 similarly satisfied Task 1.7. The whole Report satisfies Task 1.8 of the Work Plan.

TABLE OF CONTENTS

	<u>Page</u>
1. INTRODUCTION	1-1
2. OVERALL SHUTTLE CHECKOUT AND LAUNCH EVALUATION	2-1
2.1 Shuttle Avionics Configuration at Checkout	2-1
2.2 General Sequences	2-3
2.3 Subsystem Inventory	2-6
3. ONBOARD SOFTWARE CHECKOUT MODULES	3-1
3.1 Alternative Implementation Levels	3-1
3.1.1 Flight Computer Software Hierarchy	3-1
3.1.2 Ground-Compiled GOAL Code With a GOAL Executive Onboard	3-5
3.1.3 Ground-Compiled GOAL Code With a Hybrid Executive Onboard	3-7
3.1.4 Onboard HAL Code Derived from GOAL	3-9
3.2 System Configuration and the Operational Relationships in Checkout Software Modules	3-11
3.2.1 Monitoring and Measuring Modules	3-11
3.2.2 Command Control Modules	3-13
4. IMPACT OF ERROR DETECTION AND REDUNDANCY MANAGEMENT ON GOAL	4-1
4.1 Background	4-1
4.2 Signal Selection	4-3

	<u>Page</u>
4.3 Signal Rejection	4-6
4.4 Practical Aspects	4-10
5. CONCLUSIONS	5-1
APPENDIX A	A-1

1. INTRODUCTION

The general approach in this Report has been to relate the checkout software, and in particular, implementation of GOAL checkout statements in the onboard computers, to the system design of the Shuttle. Consequently, Chapter 2.0 sets forth the Shuttle avionics configuration as it is presently expected to exist during checkout and launch. The onboard avionics, especially when all elements of failure detection and redundancy are considered is enormously complex. Therefore, it is important to see certain broad aspects of the configuration without being initially focussed on details.

For example, it is important to recognize that the flight computers from a system point of view possess a multi-level hierarchical organization with the hardwired logical paths on the bottom and the mission application software at the top. Thus, there are several options presented with respect to the installation and operation of GOAL-derived test programs in the onboard computers. These options and some of their implications are discussed in Section 3.1.

It is also vital to recognize that the two Performance Monitoring System (PMS) computers are normally in the feedback paths doing a monitoring function, even though they are physically identical to the three Guidance, Navigation and Control (GN&C) computers which are in the forward or command paths. Furthermore, important distinctions exist with respect to commanding and moding of onboard systems from the ground during checkout.

Some onboard systems can be controlled only through the GN&C computers, others can be reached by discrettes from the ground which are permitted to throw crew switches through parallel contacts, and finally some functions can only be exercised by crew members even during ground test. These matters are discussed in Section 3.2 so that the options are clear as far as command and control statements are concerned.

The concept of testing to determine in-tolerance and failed functional paths is basic to the Shuttle system design. The GOAL language statements have been reviewed for adequacy within the context of the onboard system design as it stood in mid-May 1973 when final design of some in-line error detection and redundancy management elements was still under discussion. An optional new GOAL statement for monitoring such elements is suggested in Section 4. Also, for such elements which are susceptible of being tested by stimuli, another optional statement is suggested.

The topic of Shuttle Avionics and the GOAL language turns out to have many facets. The impact of the avionics system on the language and its implementation is going to be very significant, and much of the significance has yet to emerge because the avionics system design itself is still evolving. Section 5. contains some Conclusions and Recommendations which come out of this study.

2. OVERALL SHUTTLE CHECKOUT AND LAUNCH EVALUATION

2.1 Shuttle Avionics Configuration at Checkout

Reference should be made to Figure 2-1 which shows the onboard Shuttle Systems in a block diagram oriented towards the checkout situation. The systems are divided by command and control considerations.

Those subsystems such as RCS, OMS, ISS, etc. which are substantially under the control of the three GN&C computers form one group. These systems can be commanded by checkout and/or operational software modules located in the onboard GNC, in response to general commands sent uplink from the ground. Response data for such subsystems is widely available in the GN&C computers, in the Performance Monitoring System (PMS) computers, and in the CRT downlink channels.

On the other hand, the remaining subsystems are not controlled by the GNC computers. These are such subsystems as the Environmental Control and Life Support System (ECLSS), the Fuelcell Powerplant System, the Auxiliary Power Unit (APU), etc. Control in this case will be exercised by 1) the available number of commands sent uplink to the command/decoder and 2) the inputs made by test and flight crews at the crew positions. The commands sent uplink through the command/decoder are to go to parallel contacts on Display & Control Switches at the crew stations. The scope of this array of parallel switch contacts is still being developed. Numbers between 210 and 410 have been mentioned.

It can be seen that command and control of these non-GNC functions during test is a key system issue. Test schedules are compressed; concurrent, automated checkout is emphasized, and limitations of time and concurrency mean that test crew inputs at the onboard crew stations must be supplemented.

The non-GNC systems have full support in the data management function. Referring again to Figure 2.1 it can be seen that non-GNC data goes to the Operational Instrumentation Data Acquisition and Format Unit and from there it goes to 1) the ground via the umbilical, 2) to the ground via RF, 3) to onboard recording, and 4) to the Performance Monitoring System (PMS) Computers.

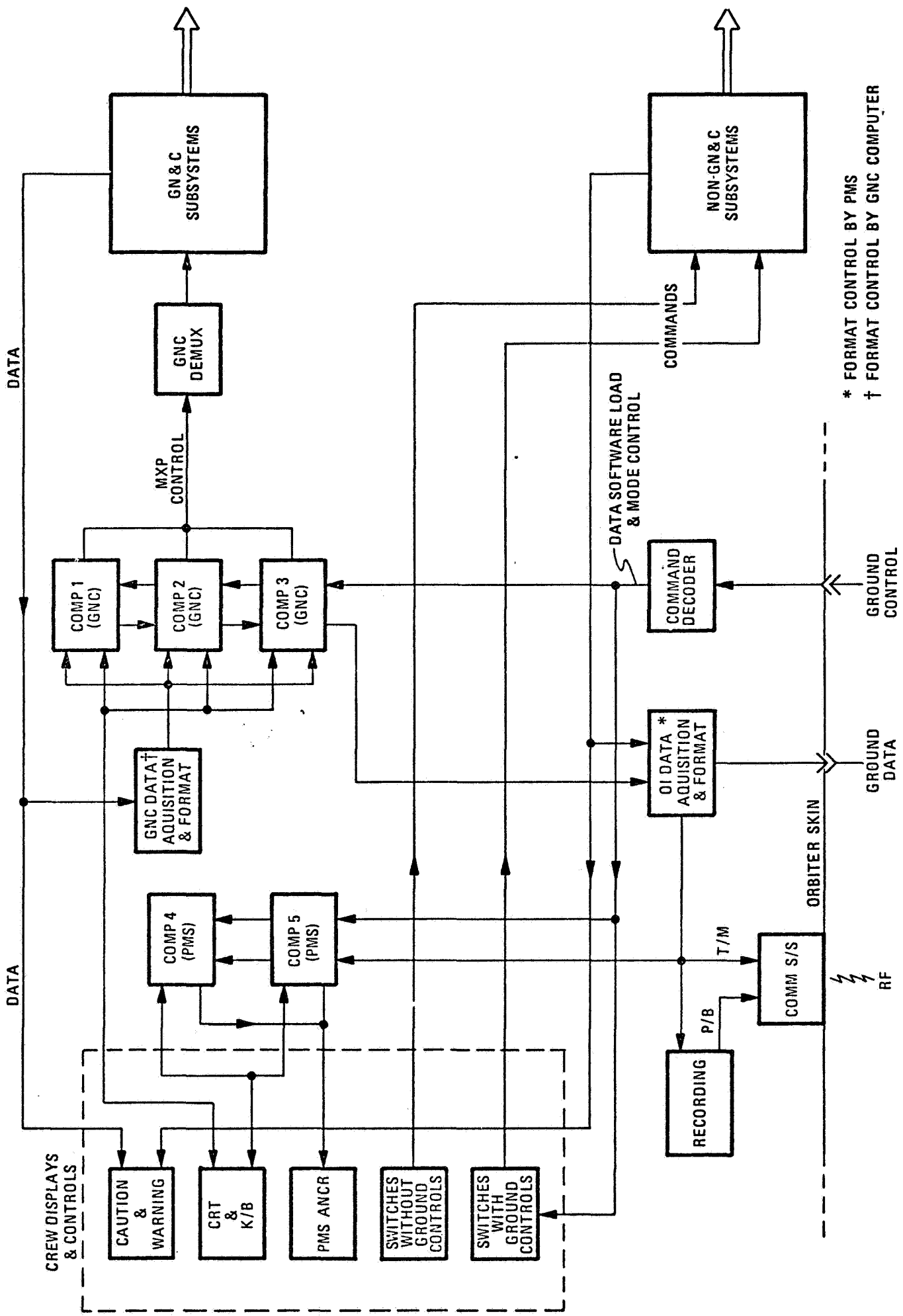


Figure 2-1 Avionics Configuration at Checkout

2.2 General Sequences

In Figure 2-2, a matrix has been constructed of the main developmental and operational test sites in the Shuttle Program combined with an assessment of the subsystems which will be active at each site. In general, each GSE set is expected to have a complete, two-way data transmission capability between the onboard computers and the ground computer system. In addition, a field-set program loader is postulated for use at the HFT site and at alternate and ferry landing sites.

Figure 2-3 gives a concept of the way the 160 working hours of turn-around time are to be used. This flow of refurbishment, maintenance, checkout and launch is very revealing. It is clear that the bulk of time is spent in mechanical and configuration procedures. The systems are powered up for only 27% of the time.

This will place a premium on concurrent testing, on automated testing, and on a careful shaping of each test sequence internal to itself and in relationship to other sequences. Clearly, the higher order language used in checkout can be a key contributor to meeting this challenge.

GSE Station No. Test site	08 Final Assy. & Checkout	09 Orbiter Initial Flight Prep.	16/24 HFT+ALT+ Ferry Landing	19 Orbiter Main. & Repair	20 Shuttle Assy. & Checkout	21 Hypergolic Serv. & Checkout	23 Launch Center & Complex	28 Control and (PAD)
Shuttle Elem.								
Avionics								
Main Engine System								
Orbital Maneuvering System								
Auxiliary Power Unit								
Power Distrib. System								
Env. Control & Life Support Systems								
Air Breathing Propulsion Systems								
Structures & Mech. Systems								
External Tank								
Solid Rocket Booster								
Payload								
GSE								

Figure 2-2. Overall Shuttle Checkout Matrix

Launch Readiness C/O, He
 Pressurization, Precount
 & Clear, Terminal Count

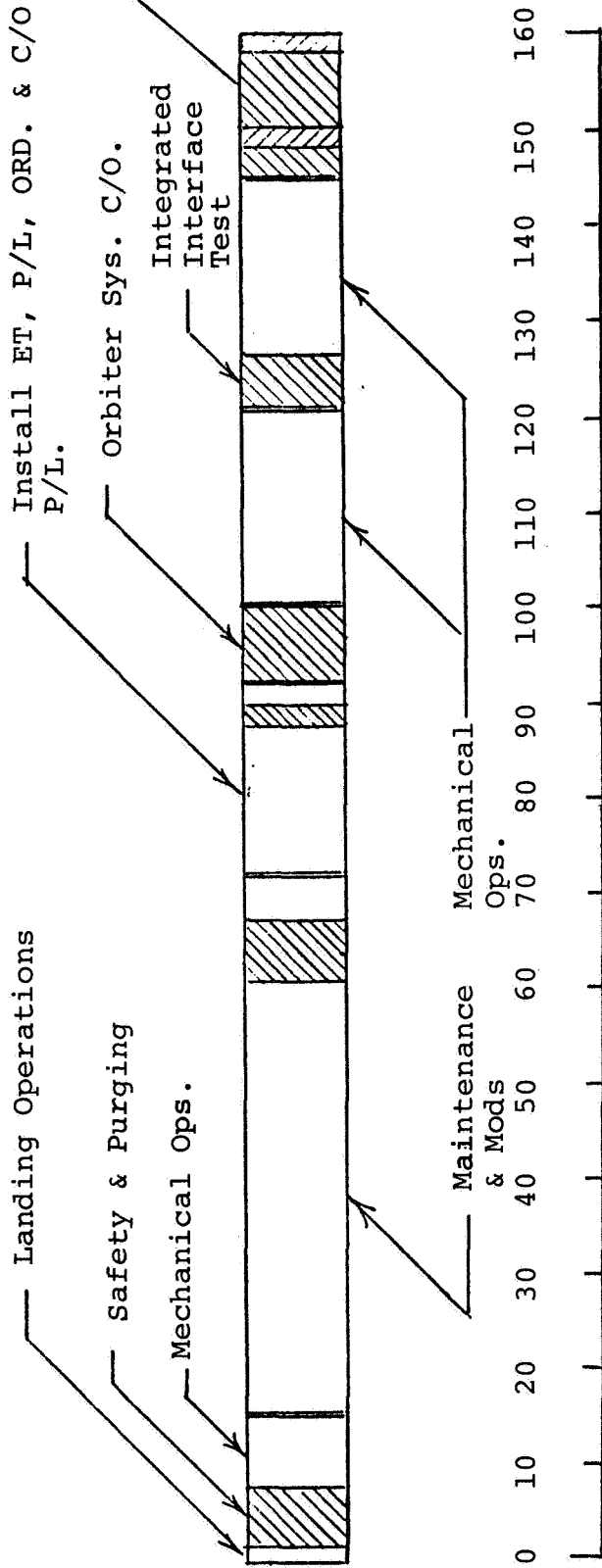


Figure 2-3.
 Shuttle Turnaround Timeline

Note: Shaded blocks indicate power on. 43 hours or 27%.

2.3 Subsystem Inventory

The following pages offer a brief look at the main Shuttle subsystems. Each subsystem is identified, the total parameters in the development flight instrumentation (DFI), the operational flight instrumentation (OFI), and the ground support equipment (GSE) are given, if available, and a brief comment is made about the number of functional paths.

SUBSYSTEM Electrical Power System (EPS)

Consists of 1) Power Generation Subsystem (PGS) including Fuel Cell Powerplants (FCP), heat exchangers, reactant inputs, purge outputs, control elements, and batteries, and 2) Power Reactant Storage and Distribution System (PRSD), consisting of cryogenic supply and distribution network.

GSE: LOX + LH₂


Switch Count:

28 switches per Fuel Cell Power Plant.

14 switches per LH₂ Tank.

18 switches per O₂ Tank.

TOTALS FROM SIGNAL LISTS

<u>DFI</u> 1)	<u>OFI</u> 2)	<u>GSE</u> 3)
32	31	46
		
63		

FUNCTIONAL PATHS.

PRSD (LH₂ + O₂ SUPPLY) - 2

PGS (FCP, etc.) - 3

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Sequential Events Control Subsystem (SECS)

Four elements are located in the Orbiter, the External Tank, and the Right and Left Solid Rocket Boosters, respectively.

TOTALS FROM SIGNAL LISTS

DFI 1)

OFI 2)

GSE 3)

No signal list available.

FUNCTIONAL PATHS.

All Orbiter SECS elements are triply redundant except for D&C panel. SRB sequencer systems are triply redundant. The E/T deorbit functions are dually redundant, as is the propellant dispersal subsystem.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Auxiliary Power Unit (APU)

Helium is used to pressurize mono-propellant hydrazine. There are a pair of helium sphere/hydrazine tank combinations in each of two fuel tank/pressure modules. Four fuel lines pass through regulators, filters, etc. to gas generators from whence gas to drive the APU turbines emerges. Each pair of functional APU paths has a fire detection and extinguisher system.

TOTALS FROM SIGNAL LISTS

DFI 1)

OFI 2)

GSE 3)

72 Analog Inputs
52 Discretes

FUNCTIONAL PATHS.

Four APU's each drive two hydraulic pumps which supply hydraulic power for each of four hydraulic systems. Three of the four APU's provide AC power to three separate AC busses.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Hydraulic System

The hydraulic system receives its power from the APU's. It operates aerosurfaces, landing gear, main engine devices, etc. Hydraulic fluid has a cooling interface with the ECLSS. Operations can be continued with any two out of four systems - Failsafe.

TOTALS FROM SIGNAL LISTS

DFI 1)

OFI 2)

GSE 3)

73 Analog Inputs
45 Event Inputs

FUNCTIONAL PATHS.

Supply: Quadruple.	Main Gear: Line 2
Load: Brakes Line 2 + 4	Aerosurfaces: Lines 1,2,3,&4
Gear Uplock: Lines 2, 3, & 4	Main Engines: Lines 1,2,3,&4
Main Eng. Shield: Lines 2, 3, & 4	

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Communications & Tracking (C&T)

C&T provides Shuttle with internal voice communication, transmitted RF signals (voice, command, and data), television, and RF tracking for all mission phases. C&T provides an RF interface with EVA astronauts, nav aids, STDN and SGLS networks, ATC, and pre-launch checkout facilities.

TOTALS FROM SIGNAL LISTS

DFI 1)

OFI 2)

GSE 3)

58 Analog
35 Event
11 Serial Digital

FUNCTIONAL PATHS.

VHF Simplex from Orbiter to ground stations. Duplex from Orbiter to EVA, detached Payload.

3 Links, non-simultaneous
2 Transceivers (VHF Simplex)
2 Transceivers (VHF Duplex)
4 Antennas

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

S-BAND COMMUNICATIONS

Four S-Band Antennas, fed by TDRS, STDN, SCF/AF-DPL, TV/WB. through dually redundant antenna multiplexers. Each multiplexer has its own SGLS interrogator and transponder as well as USBE transponder. Wide band FM for TV, P/L, etc. and Development Flight Instrumentation can be switched from one antenna multiplexer to the other by a "transfer switch". Multiplexers are selected and antennas are selected by the 2 antenna switches.

SIGNAL PROCESSING

Here are located necessary modulation, demodulation, mixing, routing, and matching of data traffic between the airborne data gathering equipment and the RF equipment. It seems to be SIMPLEX.

RF NAVIGATION AND REDUNDANCY

TACAN - 3
ATC - 2
XPNDER
RADIO ALT, ILS, - 3

ACRONYMS

TDRS - T.D. Relay System
STDN - Space Tracking Data Network (NASA)
SCF/AF-DPL- Secure Comm Facility/Airforce Detached Payload
TV/WB - Television/Wide Band
SGLS - Space Ground Link System (DOD)
TACAN - Tactical Air Navigation
ATC - Air Traffic Control (FAA)
XPNDER - Transponder
ALT - Altimeter
ILS - Instrument Landing System

SUBSYSTEM Environmental Control & Life Support System (ECLSS)

The ECLSS provides a 7 day + 96 hour shirt sleeve environment including N₂O₂ cabin atmosphere, humidity, CO₂, odor, temperature and potable water. Food and waste are managed. Fire protection and EVA, airlock support is also provided.

TOTALS FROM SIGNAL LISTS

<u>DFI</u> 1)	<u>OFI</u> 2)	<u>GSE</u> 3)
0	91	103

FUNCTIONAL PATHS.

1. Water-Freon thermal control system: Primary + Secondary (Dual)
2. Atmospheric Pressure Control System:
N₂ supply, O₂ supply (Dual)
O₂N₂ regulating-mixing: Triple
3. Waste management subsystem

<u>Single</u>	<u>Dual</u>	<u>Triple</u>
Collector	Air Return Urine Dump	Urine Pumps Urine Storage

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Environmental Control and Life Support System (ECLSS)

(Continued)

4. Water Management System

<u>Single</u>	<u>Dual</u>
Dump	Supply from Fuel Cells
Supply to Waste Mgmt.	Potable Water Tank
Supply to Kitchen	Sublimator Subsystem
Supply to Sublimator	

SUBSYSTEM Main Propulsion System

Note: The Main Propulsion System is characterized by a computer subsystem for each engine with self-contained failure detection and redundancy management. The three main engines each have their own dually redundant controller. Each engine has 52 sensors. Vehicle command available to verify redundant circuits and components during ground checkout. Engine is designed to permit a complete Flight Readiness Test during ground checkout. "FRT is included in flight software but is only used on the ground."

TOTALS FROM SIGNAL LISTS

DFI 1)

OFI 2)

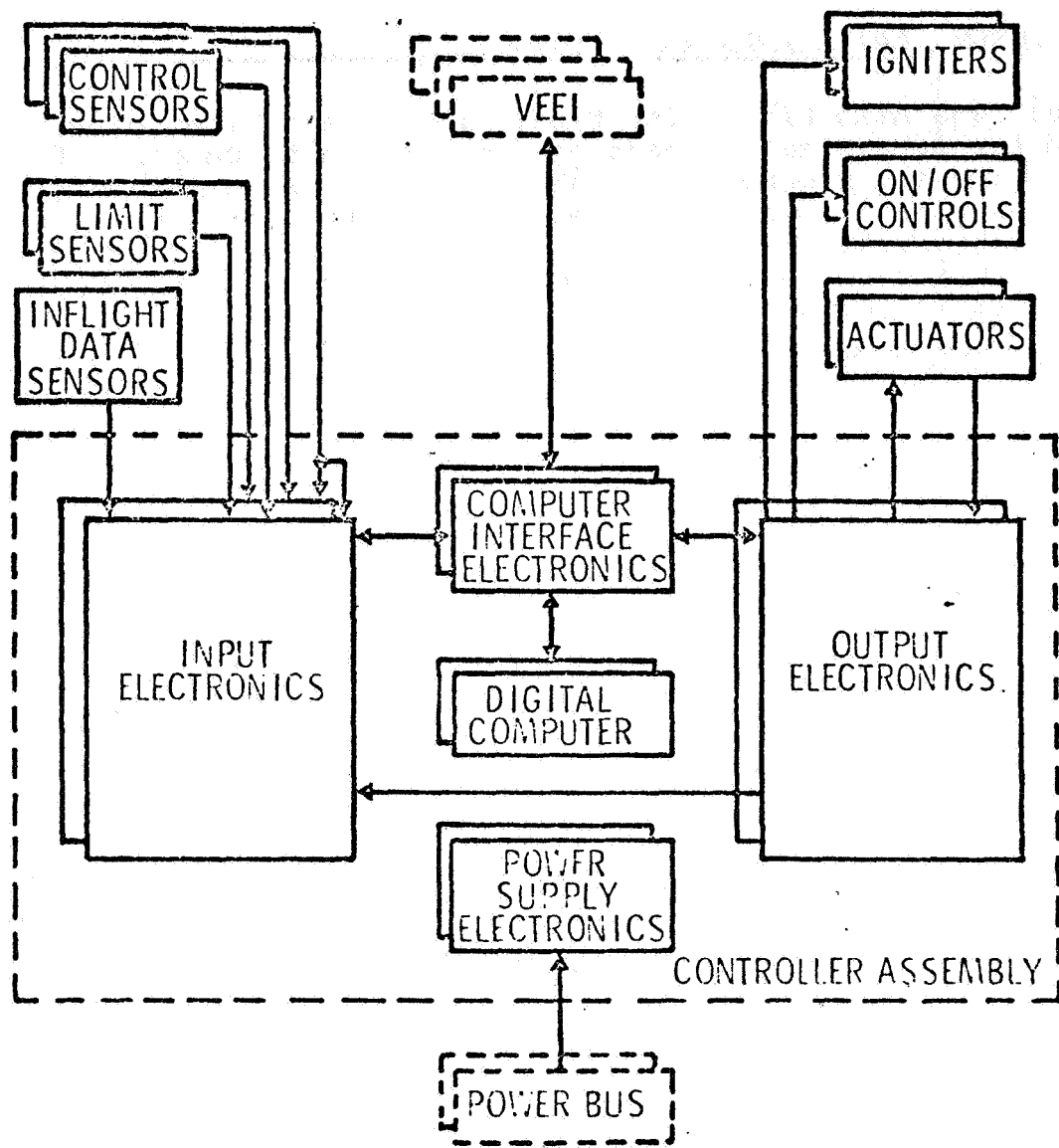
GSE 3)

89 16-bit status/data words.
Words 1,2,3 are ID, ID, and STATUS.
Words 6,7 are failure identifications.

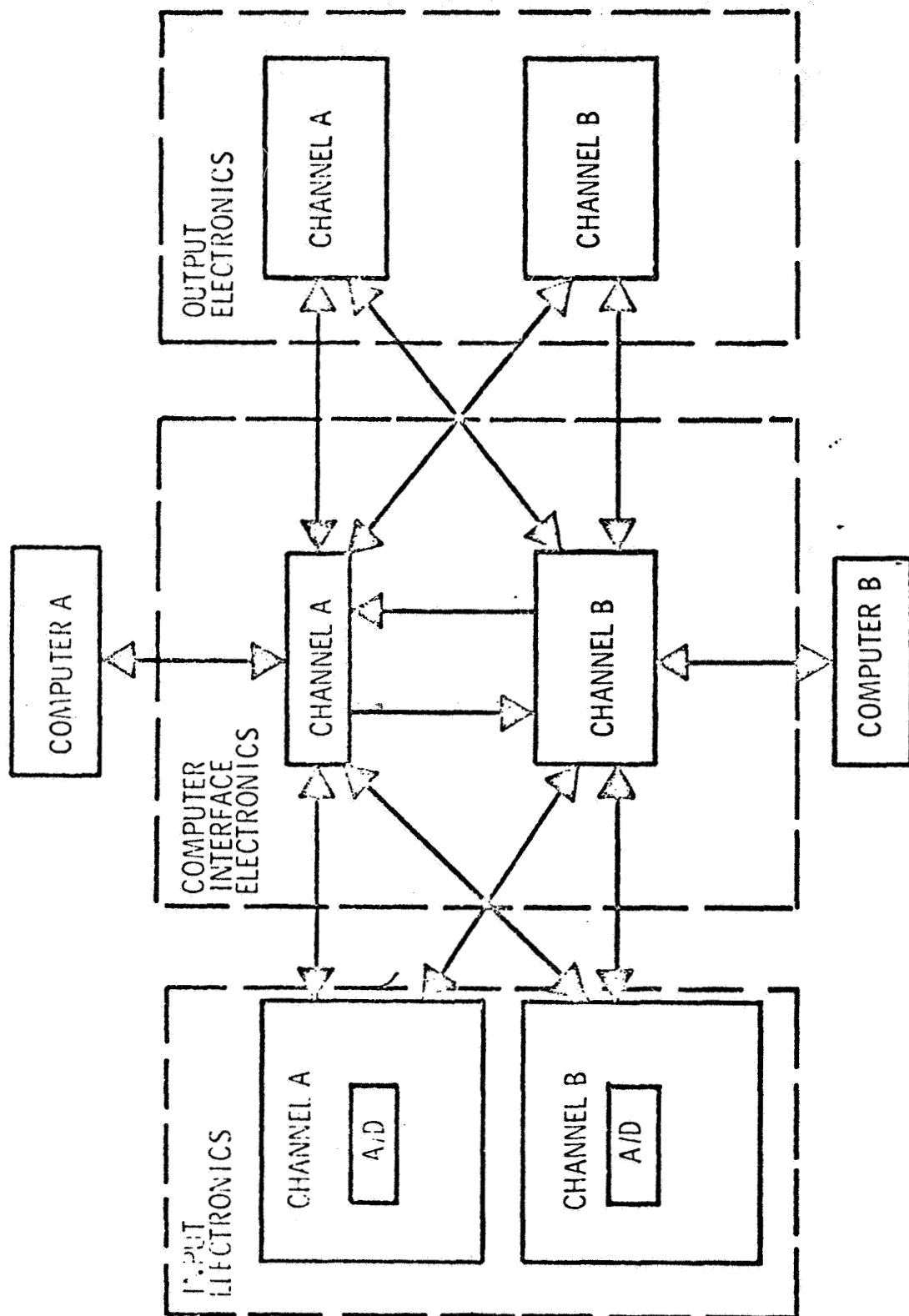
FUNCTIONAL PATHS.

Complex configuration cannot be simply described. (See both ME Controller Diagrams.) Computer A normally controls. If A fails, complete switchover is made to B. If B fails engine shuts down. Controller votes on 2 out of 3 or 2 out of 2 absolute commands and averages variable commands.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment



ME CONTROLLER BLOCK DIAGRAM



ME CONTROLLER SIMPLIFIED REDUNDANCY DIAGRAM

SUBSYSTEM Reaction Control System (RCS)

Three self-contained modules each contain monopropellant hydrazine tankage, helium pressurization, RCS thruster assemblies, and associated feed lines, valves and sensors. After a mission, the three modules are purged, detached from the Orbiter, and serviced separately.

TOTALS FROM SIGNAL LISTS

DFI 1)

OFI 2)

GSE 3)

247 Analog Measurements

48 Events

FUNCTIONAL PATHS. Per Dwg. VL72-000011.

Continued on next page.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Reaction Control System (RCS) - Continued

	<u>Forward RCS</u>	<u>Left/Aft</u>	<u>Right/Aft</u>
Helium Spheres	2	1	1
He Isolation & Req.	3	3	3
N ₂ H ₄ Tanks	3	2	2
Lines to Engines	2	2	2

Note: Crucial hydrazine tank heaters seem to be dual, fed from triple power bus.

SUBSYSTEM Orbital Maneuvering System (OMS)

Two self-contained pods each contain a pressure-fed storable bi-propellant gimbaled rocket engine, propellant and pressurant tanks, feed lines, valves, sensors, and the pod structure. After a mission, the two pods are purged, detached from the Orbiter, and serviced separately. Extra propellant can be provided in cargo bag supply kits.

TOTALS FROM SIGNAL LISTS

<u>DFI</u> 1)	<u>OFI</u> 2)	<u>GSE</u> 3)
Pressure	23	
Temperature	<u>19</u>	
Analog Measurements	42	
Events	126	

FUNCTIONAL PATHS.

Each of two pods is a functional single path with an intersecting cross-feed both ways from the propellant system to the engine. Thus, either tank pair can feed either engine.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

Solid
SUBSYSTEM Rocket Booster(s) (SRB)

The left and right solid rocket booster are each attached to the external tank. Each SRB is equipped with eight thrusters for separation, pilot chute, drogue chute, 3 main chutes, dual redundant reefing cutters, recovery gear, and batteries. The avionics includes electrical power distribution, malfunction detection, and sequencers. SRB ordnance checkout includes initiator simulators and initiator resistance testers.

TOTALS FROM SIGNAL LISTS

<u>DFI</u> 1)	<u>OFI</u> 2)	<u>GSE</u> 3)
23 each (Vib. & Acoustics)	291 each (68 sequencer discretetes) (3x64 GO/NO-GO's for Initiator C/O) (20 temps, 4 press, + TVC parameters)	

FUNCTIONAL PATHS.

All Sequencer Functions are tripled.
Thrust Vector Control commands are tripled.
Actuator Excitation is dual.
Instrumentation Power is single.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM External Tank (E/T)

The external tank consists of structure, LO₂ tank, LH₂ tank, avionics equipment, deorbit rocket motor, umbilical carriers, and attachment/separation hardware between the E/T and the two SRB's and the E/T and the Orbiter. The avionics is divided into the sequencer subsystem which handles the ordnance and the measuring subsystem which provides data to the Orbiter.

TOTALS FROM SIGNAL LISTS

DFI 1)
165

OFI 2)
64

GSE 3)

FUNCTIONAL PATHS.

Main tank and feed line system is non-redundant. E/T sequencer (and other avionics?) is triply redundant.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Guidance, Navigation & Control (GNC)

(from MCR-0164, Orbiter Avionics System Baseline.)

This equipment provides 1) automatic and manual control for all mission phases except docking which is manual only; 2) guidance commands that drive control loops and provide steering displays; and 3) inertial navigation from 3 gimballed IMU's as updated by star trackers (3) and horizon sensors.

TOTALS FROM SIGNAL LISTS

DFI 1)

OFI 2)

GSE 3)

N/A

FUNCTIONAL PATHS.

On Next Page.

-
- 1) Developmental Flight Instrumentation
 - 2) Operational Flight Instrumentation
 - 3) Ground Support Equipment

SUBSYSTEM Guidance, Navigation & Control (GNC) - Continued

<u>Single</u>	<u>Dual</u>	<u>Triple</u>	<u>Quad. or More</u>
NAVBASE	TVC MONITOR	IMU	Horiz. Sensor (6 or 0?)
BACKUP OPTX	SRB/TVC/DRVR	Star Tracker	Aero Suf Drvr
	2/3 AXIS ADI	Alpha Xdcr	APS Drvr/Mntr
		Air Data	Output Demux
		Pilot Head.	N/Lat. Accel (6)
		Air Temp.	Body Rate Gyro (9)
		OMS/TVC/DRVR	
		Sample/Middle/ Select	

3. ONBOARD SOFTWARE CHECKOUT MODULES

The purpose of this section is to examine 1) the appropriate level or levels at which checkout software modules written in GOAL might be introduced into the onboard computers and 2) the operational relationships between the onboard and ground software modules.

3.1 Alternative Implementation Levels

3.1.1 Flight Computer Software Hierarchy

In order to deal with the problem of introducing software checkout modules into the onboard computer, it is necessary to discuss first the hierarchical organization of the processing system. In Figure 3-1, the system is divided into three, general levels as follows:

Level 0: Hardware (Registers, Logic, etc.)

Levels 1 and 2: Flight Computer Operating System (FCOS).

Levels 3 and 4: Applications Software.

The FCOS is represented as having two levels. The Core Executive Functions provide interface and service routines directly to the machine and to the I/O system. Configuration management functions include error fielding, synchronization and moding. Direct control activities of the Core Executive include process management and response to higher level commands, direct interrupts, and direct I/O Sequencing and Control of the I/O Channels. These details are also set forth in Table 3-1.

At a higher level, the FCOS has an array of support software. Functional capabilities at this level will include initial program loading, general loading from tape, error handling, and reconfiguration and restart control. Also at this level are routines designed to interface with and give support to those HAL programming language features which emphasize execution control. Finally, a higher level of I/O servicing routines is a necessity.

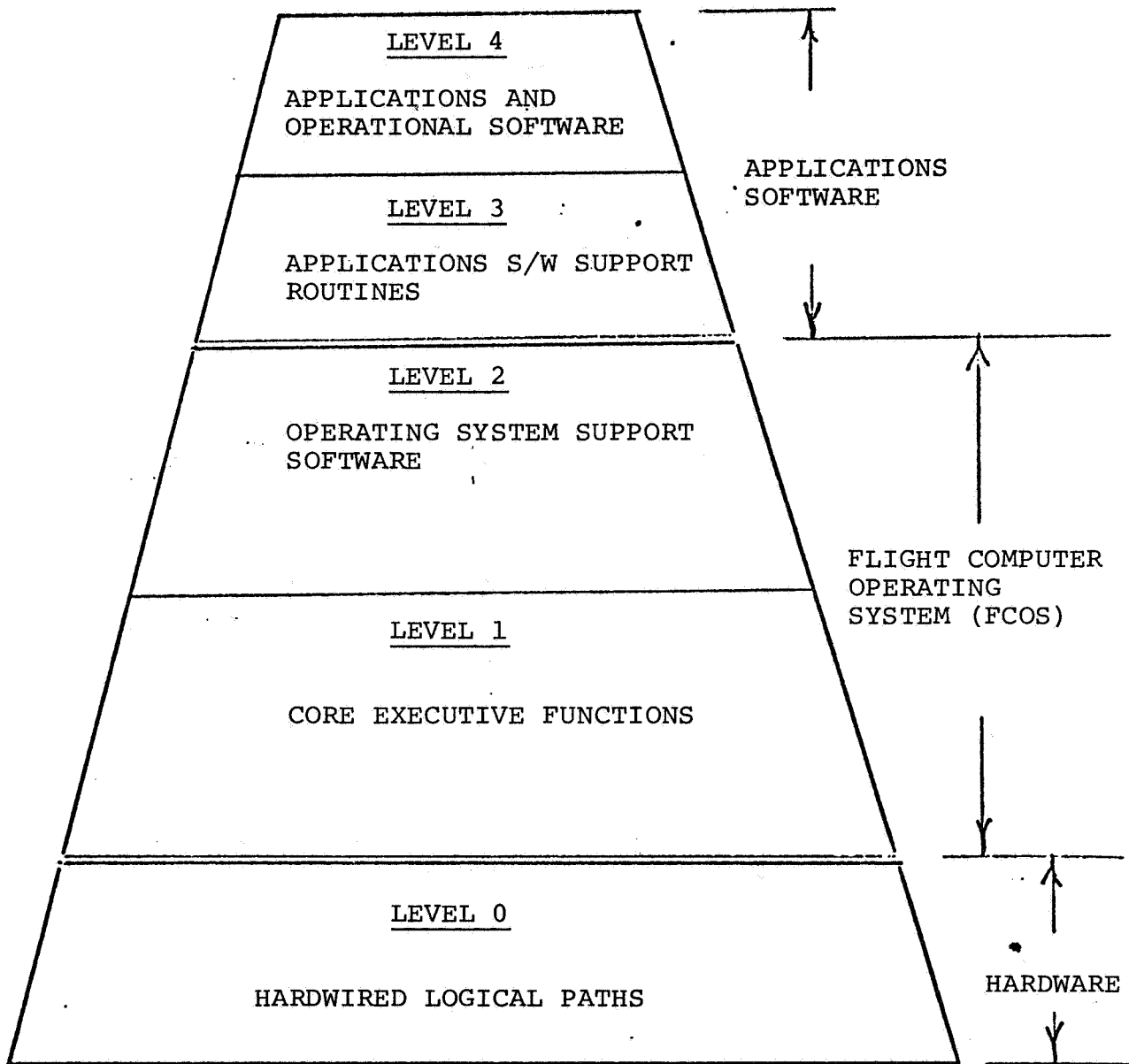


Figure 3-1 A Software Hierarchy Diagram for the Shuttle Computers

LEVEL 3. APPLICATIONS SUPPORT SOFTWARE

AVIONICS EQUIP. SERVICE AND MONITOR.
DISPLAY & CONTROL SERVICE.
TELEMETRY (UPLINK & DOWNLINK) SERVICE.

LEVEL 2. OPERATING SYSTEM SUPPORT SOFTWARE

I/O SERVICES, READ/WRITE SUBROUTINES.
HAL INTERFACES
INITIAL PROGRAM LOADER.
TAPE LOADER.
ERROR (COMPUTER) HANDLING.
RECONFIGURATION & RESTART (COMPUTER) CONTROL

LEVEL 1. CORE EXECUTIVE FUNCTIONS

I/O SEQ. & CONTROL	COMPUTER CONFIGURATION MGMNT. ERROR FIELDING SYNC & MODING	PROCESSOR MGMNT & CONTROL PROCESS TABLES & QUEUE SCHEDULER & DISPATCHER MEMORY CONTROL & ALLOC. EVENTS & TIME SERVICING AND QUEUE TRAPS, CLOCK, ETC.
--------------------	---	--

Table 3-1 Inventory of Support and Operating System Functions

Like the FCOS level, the top level, Applications Software is dual. Second from the top are applications support software routines. Typical necessities at this level include telemetry service, displays and controls service, and avionics equipment service and monitor. This is the level where the error detection and redundancy management capabilities for external subsystems are to be implemented. This is also the level where GN&C computer to Main Engine computer communication will be handled.

Finally, the mission applications software fits into the top of the hierarchy. This software is a matrix of modules encompassing 1) all mission phases, 2) all subsystems, and 3) all modes and interfaces of all subsystems.

The preceding discussion has described the hierarchy proceeding from the bottom up. At each level, the design intent is to provide in all levels below a "virtual machine", such that the programmer at a given level can proceed with concern only for the features in the level below him.

It is now possible to answer some basic questions about how much of the Flight Computer Operating System is needed to support ground testing. The succeeding subsections discuss this question based on 1) a minimum core executive and a complete GOAL executive to support GOAL code (Section 3.2), 2) an overlay GOAL executive which shares the machine with the FCOS and some of the mission software (Section 3.3), and 3) a HAL program translated from GOAL (Section 3.4).

3.1.2 Ground-Compiled GOAL Code With A GOAL Executive Onboard

This Section postulates the existence of a complete and powerful GOAL executive program designed to be loaded into the flight computer(s), with the objective of providing complete compatibility with checkout modules written in GOAL and compiled and (ordinarily) executed on the ground. This approach to ground checkout is presented here for completeness and is depicted in concept in Figure 3-2.

By referring back to Section 3.1.1, it is apparent that the so-called GOAL executive will have to provide all the Operating System Support Software except for the HAL Interface. This Software includes I/O Services, Read/Write Subroutines, Loaders, and Computer Error Procedures.

Referring again to Figure 3-2, the Applications Software is now written in GOAL code. This is straightforward when test programs at Level 4 are being considered. However, there is a crucial requirement to supply GOAL code which will operate the telemetry and display and control services in addition to servicing and monitoring the subsystem avionics. Assuming for the moment that this can be done, it must be pointed out that the system being checked out no longer includes the applications flight support software or the operating system support software which will be used in flight.

The overall assessment of the value of this approach is that it is counterproductive. Savings exist in running GOAL-coded test programs (Level 4) directly on the flight machines but to do so requires significant effort to produce a GOAL executive (Level 2) of considerable scope and a set of GOAL service routines involving display, telemetry, and subsystems (Level 3). Re-writing subsystem service routines in GOAL would be a major and inappropriate effort.

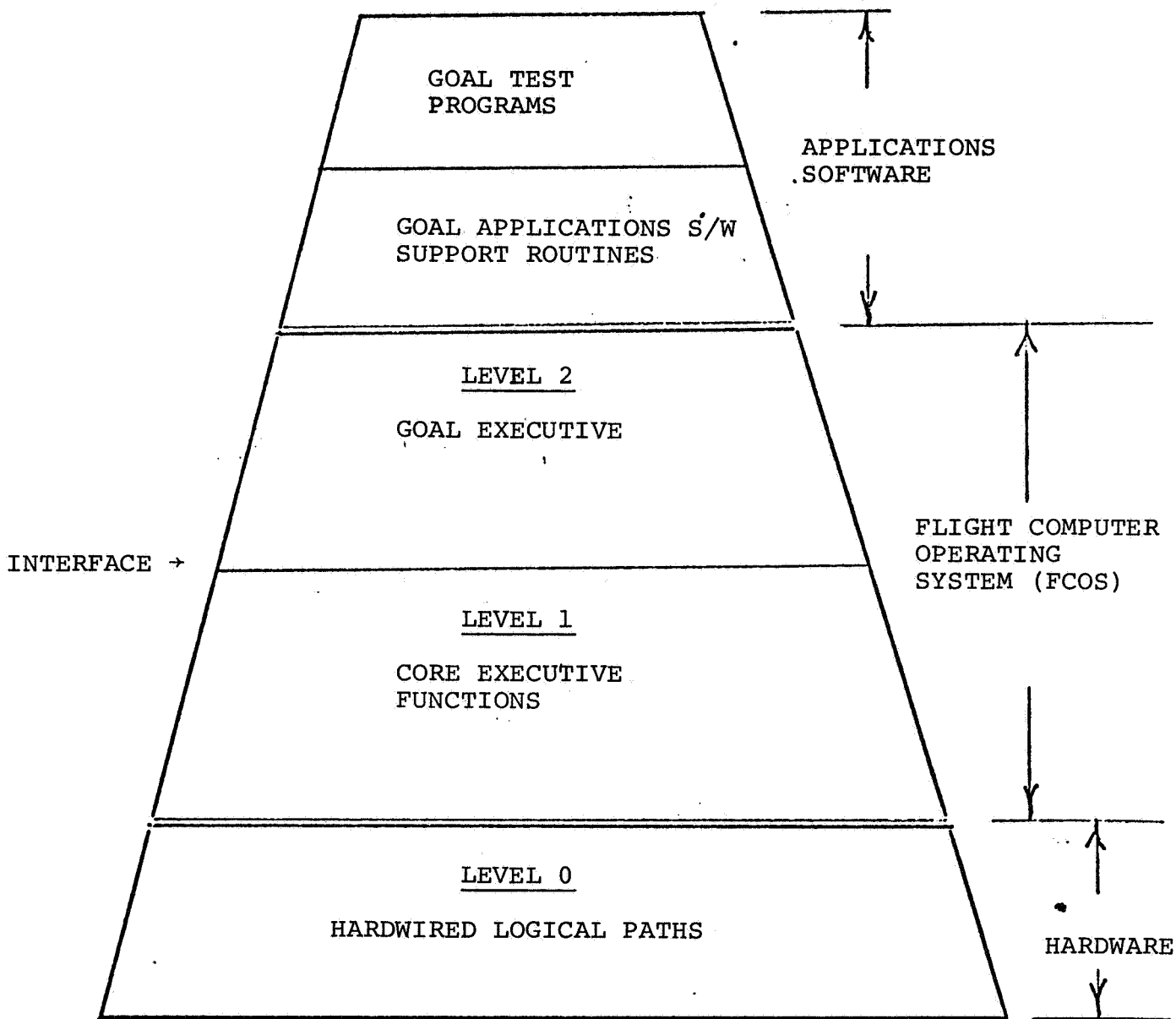


Figure 3-2 A Software Hierarchy Diagram for the Shuttle Computers with a GOAL Executive

3.1.3 Ground-Compiled GOAL Code with a Hybrid Executive Onboard

In attempting to explore all avenues of test software implementation, this section qualitatively describes a hybrid executive (see Figure 3-3). The objective of this approach is to permit the direct, ready use onboard of GOAL code compiled on the ground while preserving intact all the applicable FCOS and applications software necessary to operate the systems. The approach can be expressed once more in terms of implementing a "virtual machine". To accomplish this, it is asserted that the mission software which interfaces with the subsystems is preserved intact as shown by the upper right hand areas of Figure 3-3. In addition, significant portions of the FCOS are also present and in control. Implementation of this approach then requires a module-by-module, function-by-function review of the GOAL interface to the GBOS in comparison with the possible interfaces to the FCOS and necessary portions of the mission applications software. By definition, the GOAL executive and GOAL support software as depicted on the left hand side of Level 3 and Level 4 become interface modules which will make the hybrid approach fully and reliably functional. Inspection of Figure 3-3 will show that this approach involves complex interfaces, and defeats the concept of maintaining a structured software system.

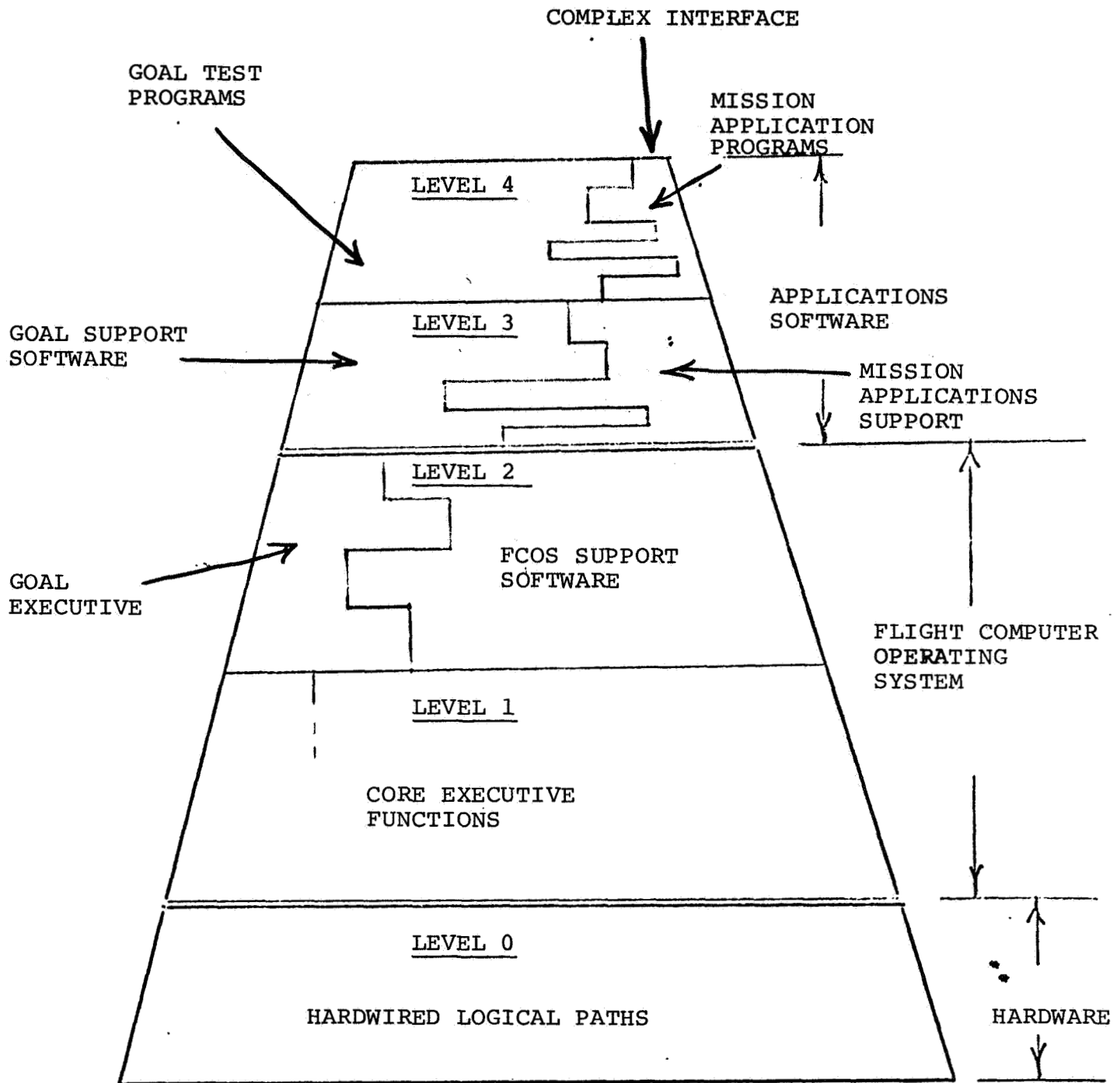


Figure 3-3 A Software Hierarchy Diagram from the Shuttle Computers with a Hybrid Executive

3.1.4 Onboard HAL Code Derived from GOAL

In this subsection, we discuss the case of onboard test routines which are written in GOAL and translated to HAL/S*. This approach is the one which has prompted the GOAL-to-HAL Translation Study. Referring to Figure 3-4, the interface can be seen to have moved to the top of Level 3. This means that the applications software support routines, as qualified for manned spaceflight, are maintained intact and inviolate in the "virtual machine" which consists of Level 3 and all below it.

Using this approach, GOAL programs can be written by test engineers, and translated into HAL code. Following verification, this HAL code can be sent uplink to the flight computer(s), provided that FCOS is implemented with the ability to accept complete HAL applications programs of mission as well as checkout, by the telemetry route. Details in this matter are important, and the FCOS will have to be told what kind of a program it is, where it goes in the directory, and what initial conditions apply. Given these prerequisites, GOAL programs translated to HAL will work.

* HAL/S - HAL dialect for the onboard Shuttle computers.

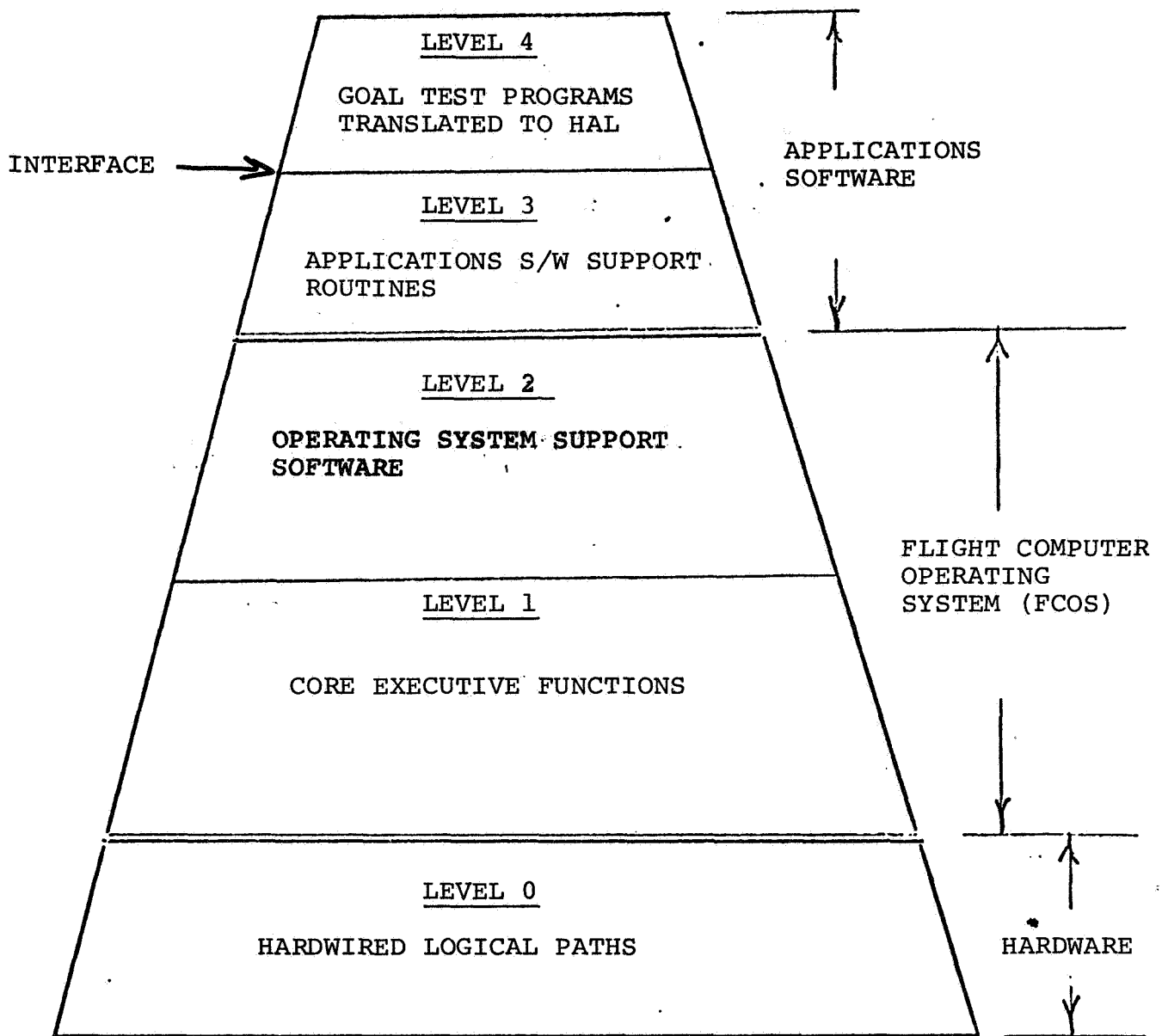


Figure 3-4 A Software Hierarchy Diagram for the Shuttle Computers with GOAL Translated to HAL.

3.2 System Configuration and the Operational Relationships in Checkout Software Modules

3.2.1 Monitoring and Measuring Modules

In Figure 3-5, the role of the GNC and PMS Computer is highlighted in terms of the selection and formatting of data. It is presently planned that there will be four data lists, three fixed and one variable. The list is selected by a command mode from or through the appropriate computer. It appears that control of monitoring and measuring from the ground will be as a result of a simple command sent uplink. Onboard display service programs at Level 3 should be able to reach, format, and transmit every data point included in the DFI, OFI, and GSE lists. The uplink command can be generated, verified, and transmitted by the ground as the result of a GOAL statement. It is thus not clear, with regard to monitoring and measuring, that onboard GOAL translated to HAL will provide any different capabilities than those found in the mission applications software.

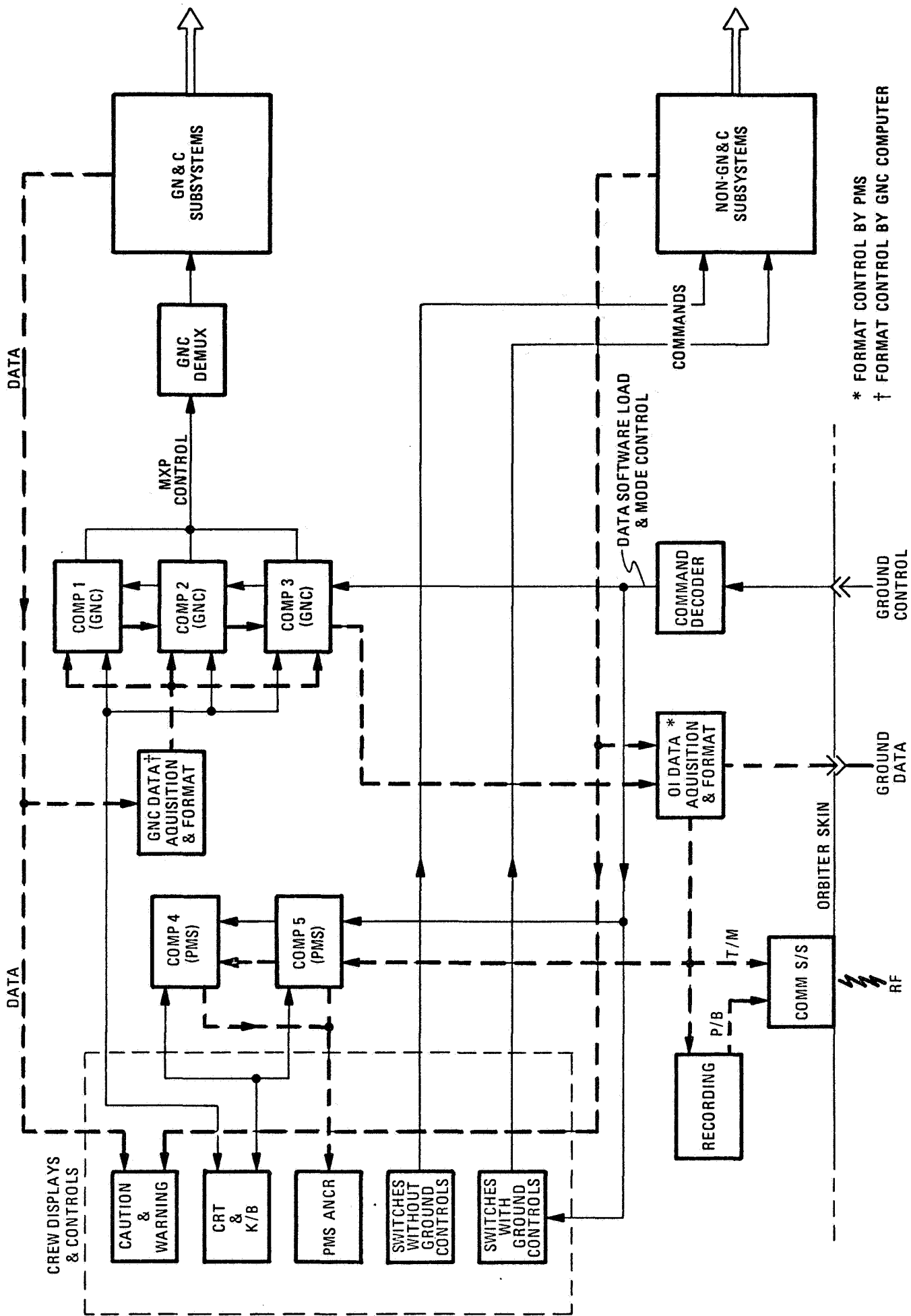


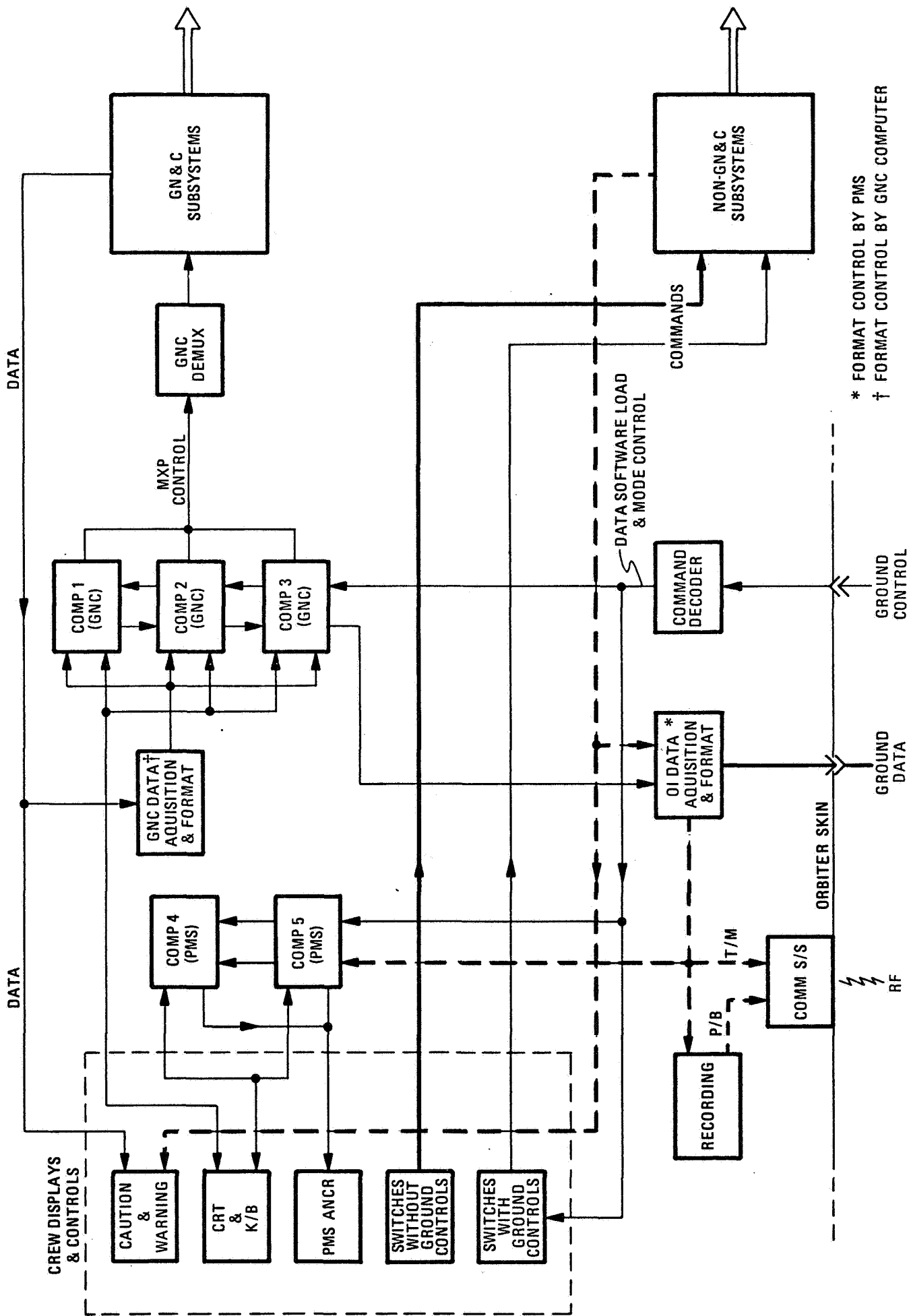
Figure 3-5 Avionics Configuration at Checkout - Data Paths

3.2.2 Command and Control Modules

3.2.2.1 Manual Switch Only. The first category of command and control is for those non-GN&C subsystems that are commanded by switches not equipped with parallel contacts for control from the ground (see Figure 3-6). System commands must originate exclusively from actions of flight or test crew members sitting at the flight stations. These actions can be controlled by Test and Checkout Procedure (TCP) text, by Test Conductors commands over audio channels, or by prompting displays from the computer CRT faces. Only the latter method involves possible software which would stimulate the crew member to start, stop, or alter his actions. Such checkout programs represent a logical application for GOAL programs translated into HAL. The flight station console has to take the place of the ground console because, for the particular functional paths involved, there is no ground control.

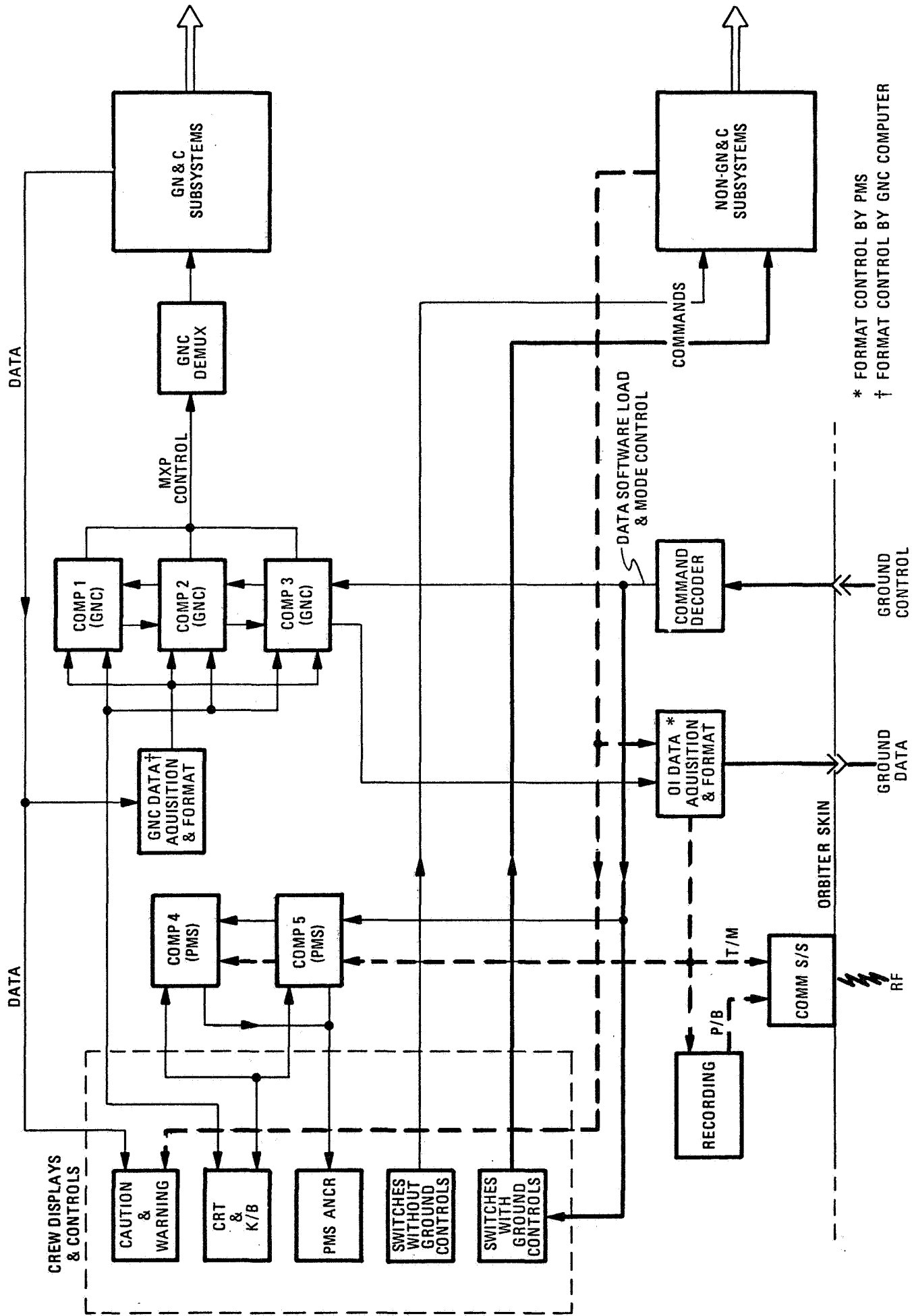
3.2.2.2 Manual Switch with Parallel Contact. Another subset of onboard subsystems is that whose functions and functional paths can be controlled from the ground because the onboard switches have parallel contacts one set of which is wired to the output of the command decoder (see Figure 3-7). Command and control of these subsystems from the ground does not necessarily involve any onboard checkout software modules. GOAL programs on the ground issue commands to the selected onboard subsystems via properly coded bit patterns to the command-decoder. Onboard GOAL or HAL has no mandatory role to play here.

However, it is entirely possible that this particular subset of command and control actions may indeed call for an onboard checkout software module which moves in synchronism with that on the ground. The objective would be for the test crew to follow the step-by-step execution of the test onboard by observing a display of test commands as well as test responses which is identical to that occurring on the ground.



* FORMAT CONTROL BY PMS
 † FORMAT CONTROL BY GNC COMPUTER

Figure 3-6 Avionics Configuration at Checkout — Command and Control by Switches without Parallel Contacts



* FORMAT CONTROL BY PMS
 † FORMAT CONTROL BY GNC COMPUTER

Figure 3-7 Avionics Configuration at Checkout - Command and Control by Parallel Switch Contacts

3.2.2.3 GN&C Directed Subsystems. Finally, the large class of subsystems that are driven from the three GN&C computers must be addressed (see Figure 3-8). All of the "effectors" dealing with controlling the vehicle path are involved:

Aerodynamic Surfaces.

Main Propulsion (Engine Controller).

Orbital Maneuvering System (Pitch and Yaw).

Attitude Propulsion System (RCS Jets).

Left and Right Solid Rocket Boosters (Pitch and Yaw).

GN&C includes many data sensors. Many of these, once turned on, are simply sources of data. The star tracker and inertial measurement unit, however, are quite complex and require mode and position commands from the GN&C computers. All of these subsystems will be supported by Level 3 Applications Software. Level 4 Checkout Software written in GOAL and translated to HAL will have varying degrees of authority. In the case of the APS or reaction control jets, checkout software can exercise the thruster circuitry on a discrete basis. However, to go to the opposite extreme, the main propulsion system with its self-contained controllers gives only limited operational authority to the GN&C computers:

4 Purges	Discrete
1 Start	Discrete
1 Shutdown	Discrete
Thrust Level	Variable
Mixture Ratio	Variable

(In addition to the operational authority, there are multiple discretetes for pre-flight check.)

The IMU's involve high level software support from the GN&C computers, because an IMU without a computer is non-functional. The point to consider is that some of the GN&C systems may require their own Level 4 software in HAL to run concurrently with checkout software modules in GOAL-derived HAL.

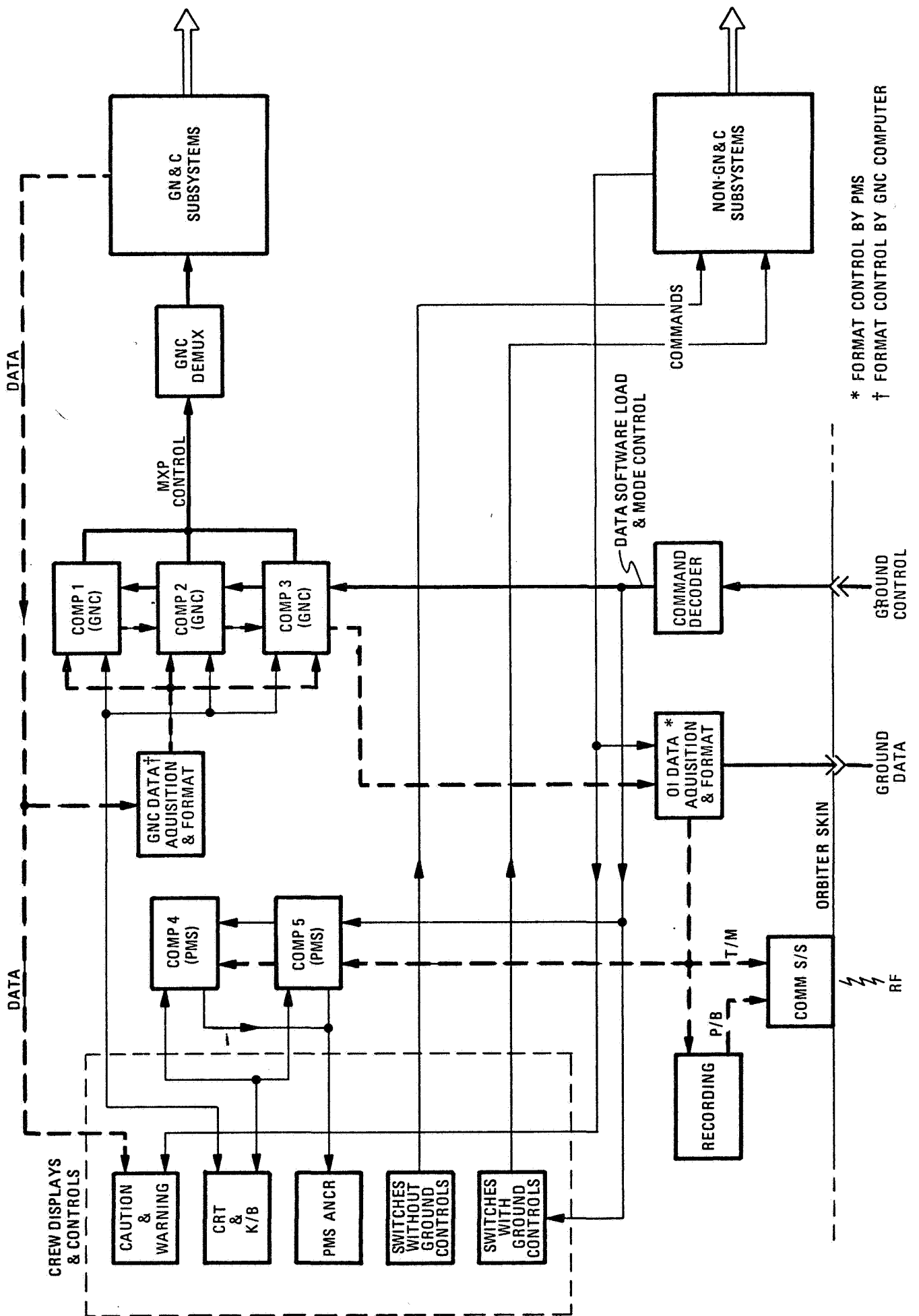


Figure 3-8 Avionics Configuration at Checkout - Command and Control by GNC Computer

4. IMPACT OF ERROR DETECTION AND REDUNDANCY MANAGEMENT ON GOAL

4.1 Background

This topic is of importance because the Shuttle design philosophy incorporates multiply redundant functional paths in most systems. In Figure 4-1 this design philosophy is depicted in a schematic; which, though general, describes many Shuttle subsystems. Alternate functional paths are available from the sensor through the processor to the effector. GOAL has a role to play here in the verification of 1) error detection, 2) the manual or automatic reconfiguration of the functional path, and 3) the health of the functional path itself. Step 3, the verification of the functional path, constitutes the bulk of spacecraft check out and launch testing. Error detection and redundancy management is not new. The Saturn booster family had it and it was tested as part of checkout and launch. Now, however, the extent and variety of multiple redundancy has increased in the Shuttle design.

There are two, three, and four functional paths, or strings, depending on the flight safety and reaction time requirements of the particular subsystem. Reconfiguration is automatic or manual depending in part on the same criteria.

The topic of GOAL statements for use in checkout of error detection and redundancy management can now be addressed. In general, the External Test Action group of GOAL statements (see Section 3.1 of the TR-1228, the GOAL Textbook) is complete in terms of providing the power to stimulate the system under test and to record and distribute the resulting data. Any stimulus that has been provided in hardware can be triggered by GOAL-originated software. Similarly, any data point that has been provided in hardware can be read in software.

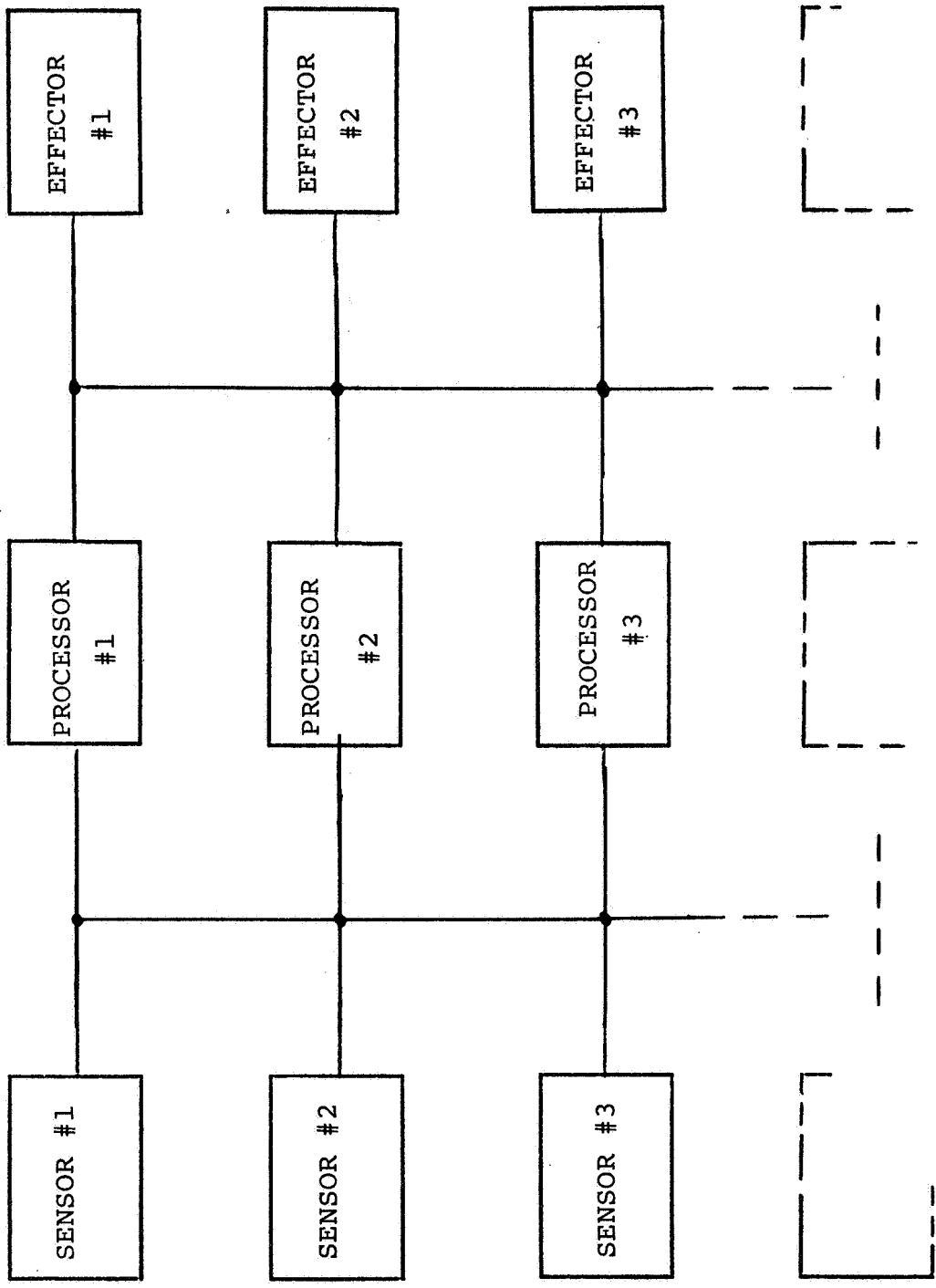


Figure 4-1: GENERAL SCHEMATIC OF MULTIPLE FUNCTIONAL PATHS

4.2 Signal Selection

It does appear, however, that those elements which make a selection of a signal from triple or quadruple candidates could benefit from test statements that will provide a duplicate of the selection logic for the test software and compare the results with the operational system. Figure 4-2 shows such a signal processor using logic for selecting the middle signal from among the three or four which present themselves. It is suggested that the Sample/Middle-Select (S/MS) process be duplicated in the test software with a new GOAL statement. The statement is portrayed in a syntax diagram in Figure 4-3 and a program example is given. An important assumption is that all three input signals and the output signal are available on the signal list.

Alternatively, it might prove more advantageous to perform monitoring of onboard redundant signal selection logic with a PERFORM SUBROUTINE approach. This is fully within the capabilities of GOAL, as now specified and documented. It would be a preferable approach particularly if the onboard redundant signal selection logic changes, either from subsystem to subsystem or for some other reason. An example is given below:

```
PERFORM SUBROUTINE (S/MS CHECK)
<SENSOR #1>,<SENSOR #2>,<SENSOR #3>,
(S/MS OUTPUT);

_____

_____

VERIFY <S/MS OUTPUT> EQUAL TO
(S/MS OUTPUT) ELSE DISPLAY EXCEP-
TION TO <CONSOLE XX>;
```

```
|
|
| _____
|
| BEGIN SUBROUTINE (S/MS CHECK)
| <SENSOR #1>, <SENSOR #2>, <SENSOR #3>,
| (S/MS OUTPUT);
|
| ---S/MS LOGIC FOLLOWS -----
|
| END SUBROUTINE;
|
| _____
|
```

Given the availability of the data points, the monitoring of the S/MS can proceed on a non-interference basis. Of course, if the three sensor (or processor) outputs are indistinguishable within the tolerance of the measuring system then the test is of no value in tracking the S/MS activity. This brings up the possibility of stimuli.

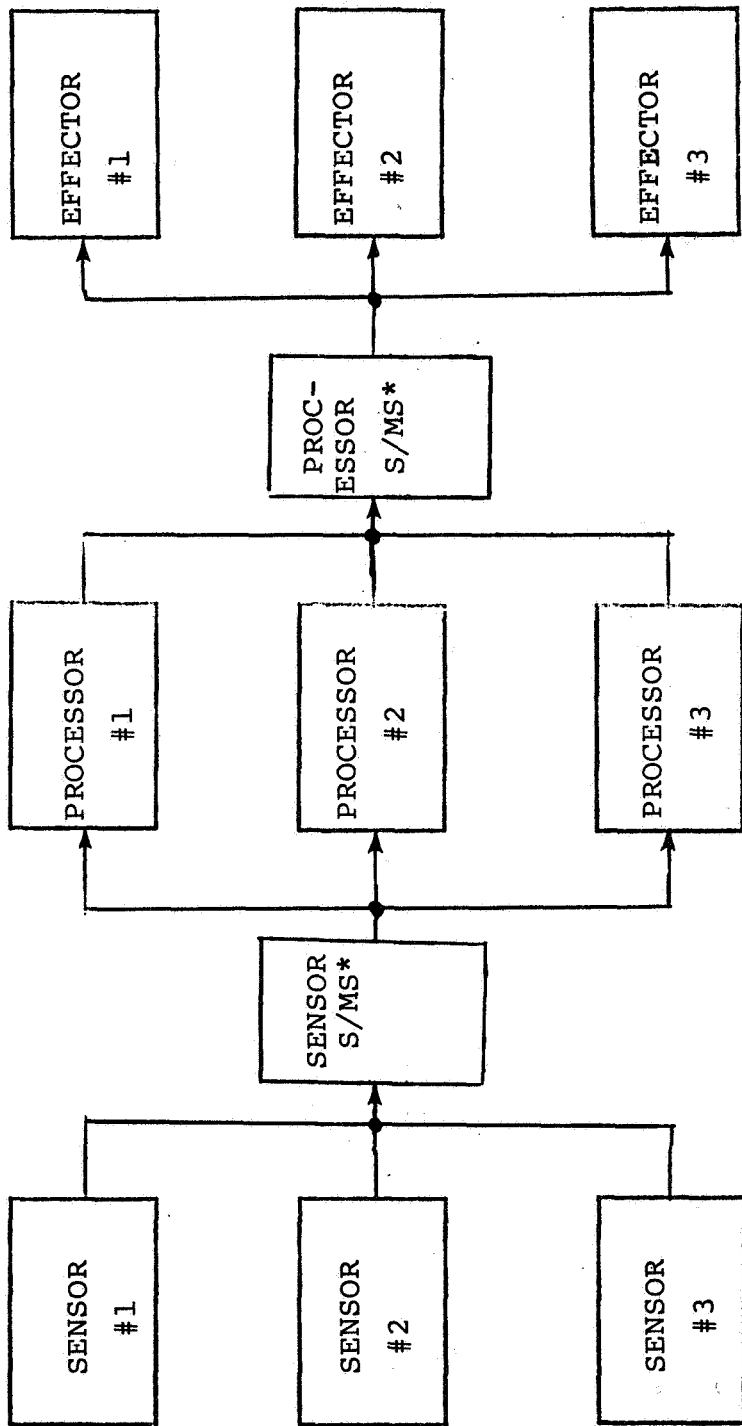
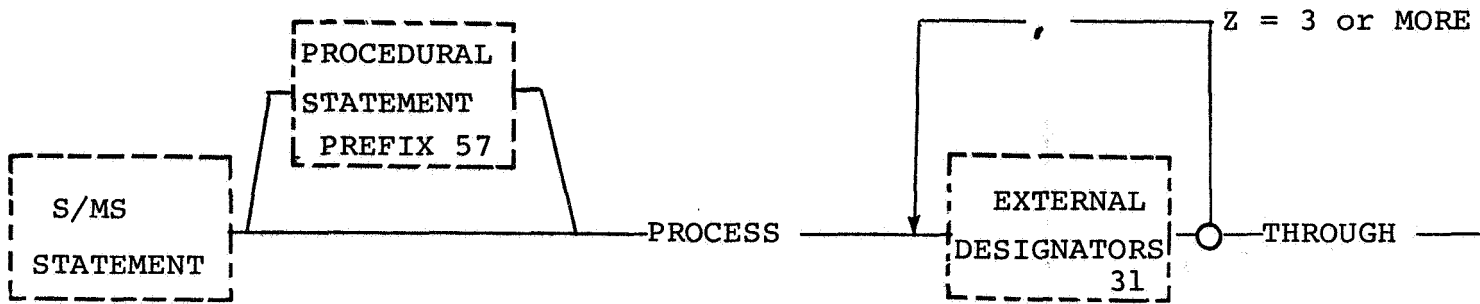


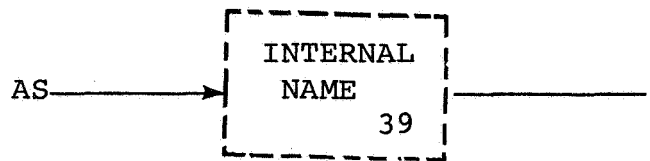
FIGURE 4-2: SCHEMATIC OF VOTING SYSTEM
WITHOUT TEST STIMULI

* S/MS = SAMPLE, THEN MIDDLE-SELECT

SYNTAX:



SAMPLE/MIDDLE-SELECT-LOGIC AND SAVE



(PROGRAM SEGMENT BASED UPON FIG. 4-2).

```
PROCESS <SENSOR #1>, <SENSOR #2>, <SENSOR #3>  
THROUGH SAMPLE/MIDDLE-SELECT LOGIC AND SAVE AS  
(S/MS OUTPUT);
```

```
VERIFY <S/MS OUTPUT> EQUAL TO  
(S/MS OUTPUT) ELSE DISPLAY EXCEPTIONS  
TO <CONSOLE XX>;
```

Figure 4-3: SAMPLE/MIDDLE-SELECT EVALUATION GOAL STATEMENT

4.3 Signal Rejection

Referring to Figure 4-4, there is presented in concept only the capability for exercising the failure detection and redundancy management capabilities of a system in a positive way. In actual fact, software features in the processor can be implemented to produce specified sets of values to the Processor S/MS input. It is less likely that sensors such as the air data sensors, IMU's, or star trackers will be provided with operational test stimuli.

The function these test stimuli could perform is to give unambiguous inputs to the signal selection logic. For this purpose, the GOAL APPLY ANALOG Statement (No. 2) could be used. However, possibilities exist for combining this stimulus command with the evaluation of S/MS logic described in 4.2. This possibility is presented as a syntax diagram in Figure 4-5 with an accompanying example in Figure 4-6. A combined result from the application of these stimuli is that failure detection is exercised by the application of an out-of-limits signal and the voting or selection mechanism is also checked with distinct signal levels. The time duration of each step in the commutative cycle might vary from one S/MS to another because of varying design time constants.

The same alternative exists in this proposed GOAL statement as existed in the Signal Selection statement described in Section 4.2. Again a PERFORM SUBROUTINE call would be made and the S/MS module logic would be defined in a subroutine.

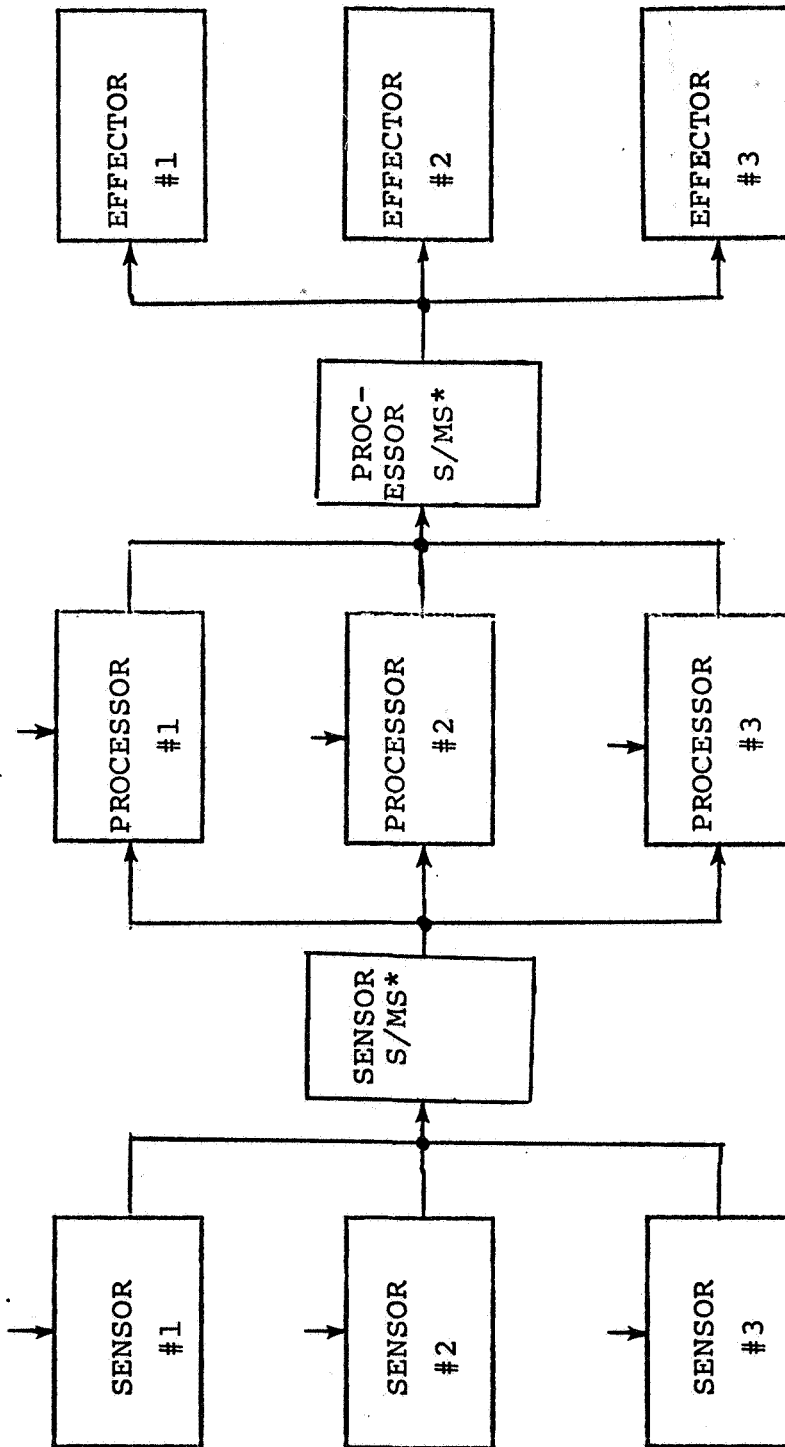


Figure 4-4: SCHEMATIC OF VOTING SYSTEM
WITH TEST STIMULI

* S/MS = SAMPLE, THEN MIDDLE-SELECT

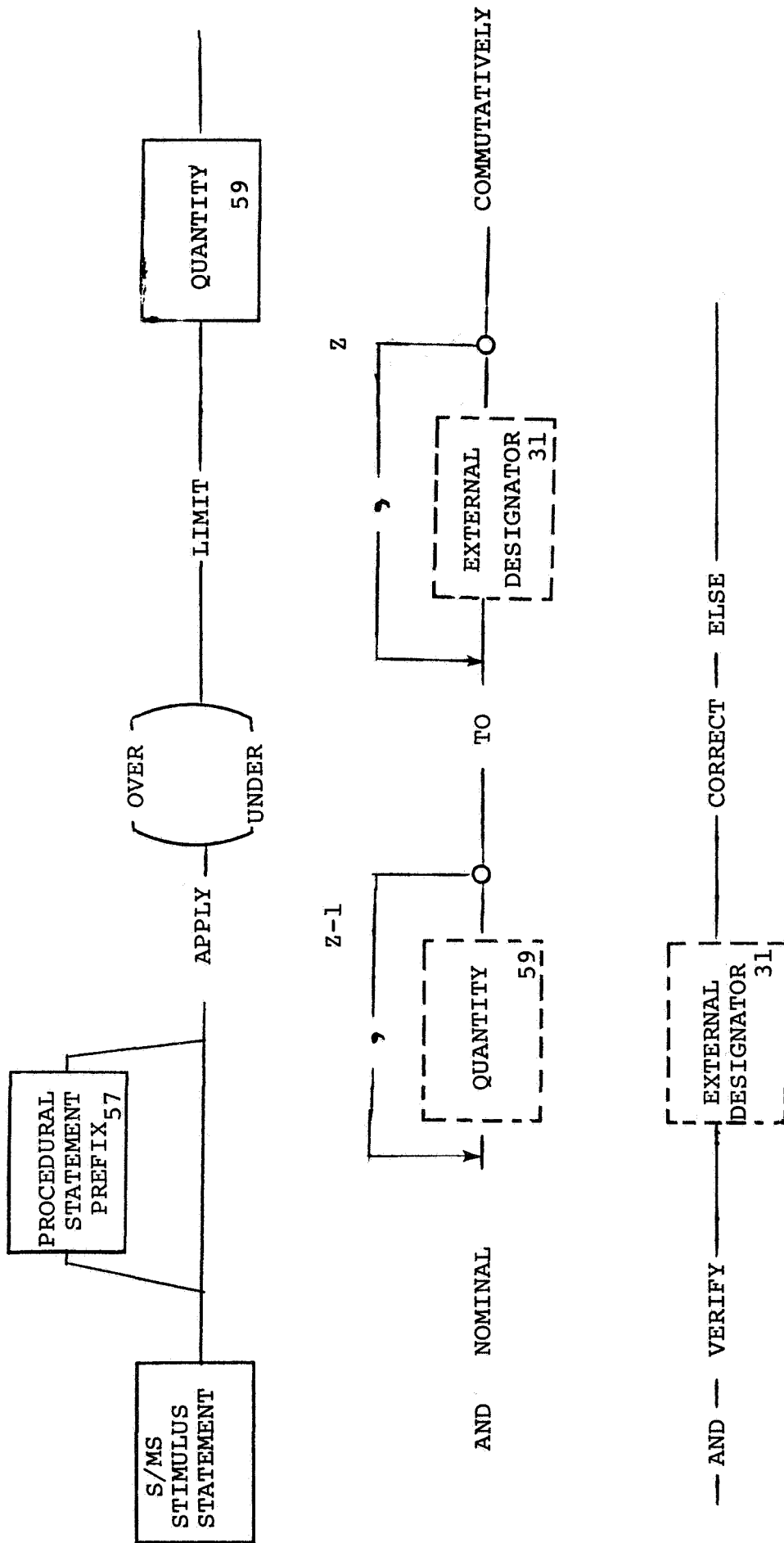
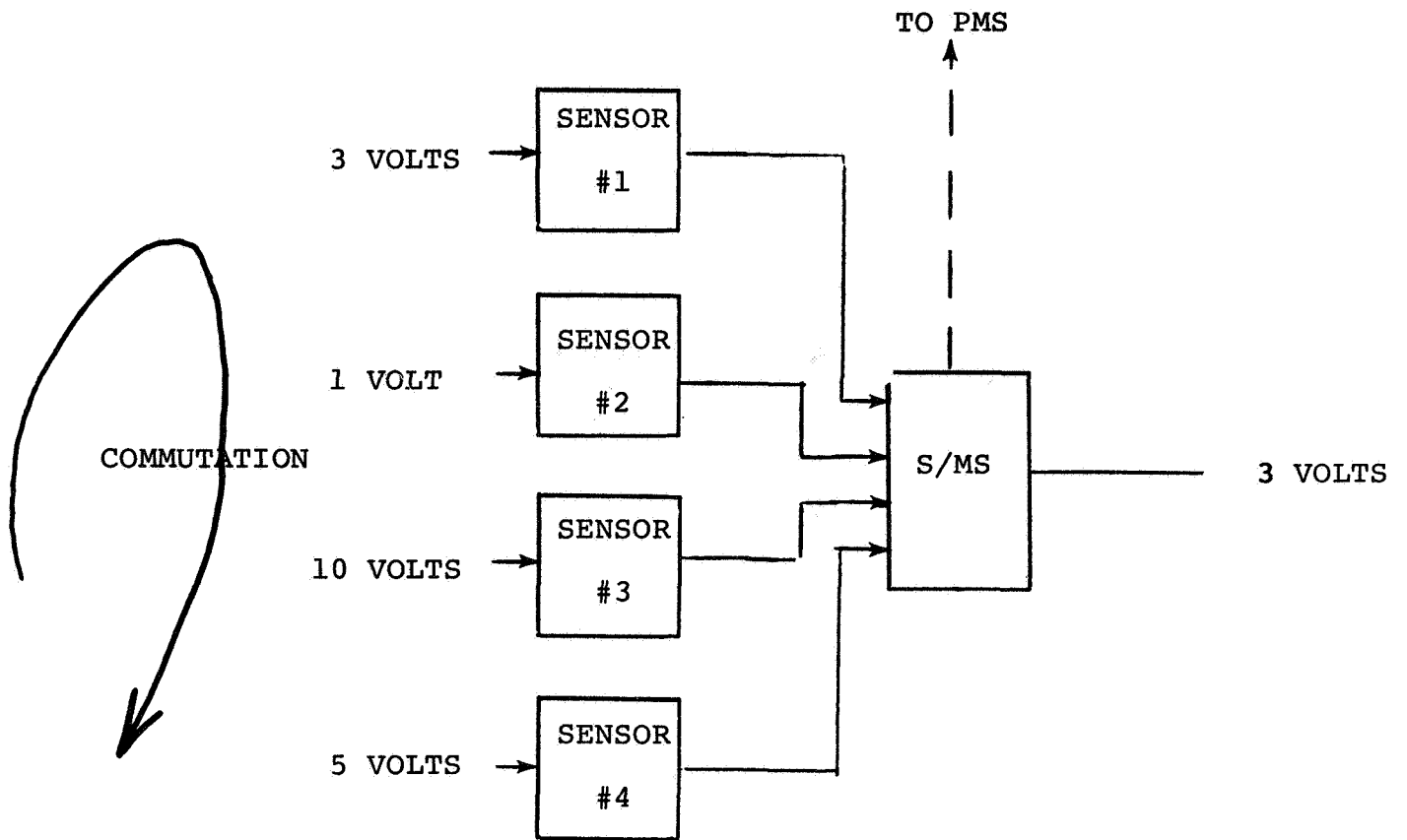


Figure 4-5: SAMPLE/MIDDLE-SELECT STIMULUS GOAL STATEMENT



S100 APPLY OVERLIMIT 10 VOLTS AND NOMINAL
 5 VOLTS, 3 VOLTS, 1 VOLT TO
 <SENSOR #1>, <SENSOR #2>, <SENSOR #3>,
 <SENSOR #4> COMMUTATIVELY AND
 VERIFY <SENSOR S/MS OUTPUT> CORRECT
 ELSE DISPLAY EXCEPTION TO <CONSOLE 1>;

S110 VERIFY <SENSOR #3 FAIL> TRUE;

Figure 4-6: USE OF SAMPLE/MIDDLE-SELECT STIMULUS

4.4 Practical Aspects

The preceding two proposals were based upon the assumptions that 1) the redundant signals going into and the resultant signal out of the redundancy logic elements would be available to the test software in real time, and 2) that stimuli or test voltages could be applied to the redundancy logic elements. The bulk of such redundancy logic elements are in the functional path stretching from the GN&C sensors through the three (or less) GN&C computers to the flight-control effectors (See Figure 4-7). The sum total of signals involved could become very large. It is not known by Intermetrics at this time whether each individual signal will get to the GNC Data Acquisition and Formatting element, and whether it will get to the Developmental and Operational Data Acquisition and Formatting units (See Figure 3-5). Also, as of mid-May 1973, many redundancy management issues and their dependent design decisions are still open. In the thrust vector control (TVC) design area, for example, a choice is to be made between 1) "smart" demultiplexers which also have the voting function between redundant signals and 2) simple demultiplexers feeding into a sample/middle-select element such as is shown in Figure 4-7.

In spite of these unknowns, verification of individual functional paths in the redundant Shuttle signal environment remains a requirement. Furthermore, the sheer number of signals coming into and leaving redundancy points will be extremely large. The use of special GOAL statements aimed at monitoring and evaluating these signal selection logic points seems worthy of careful consideration. However, sufficient system information is not yet available to specify such special statements with absolute certainty.

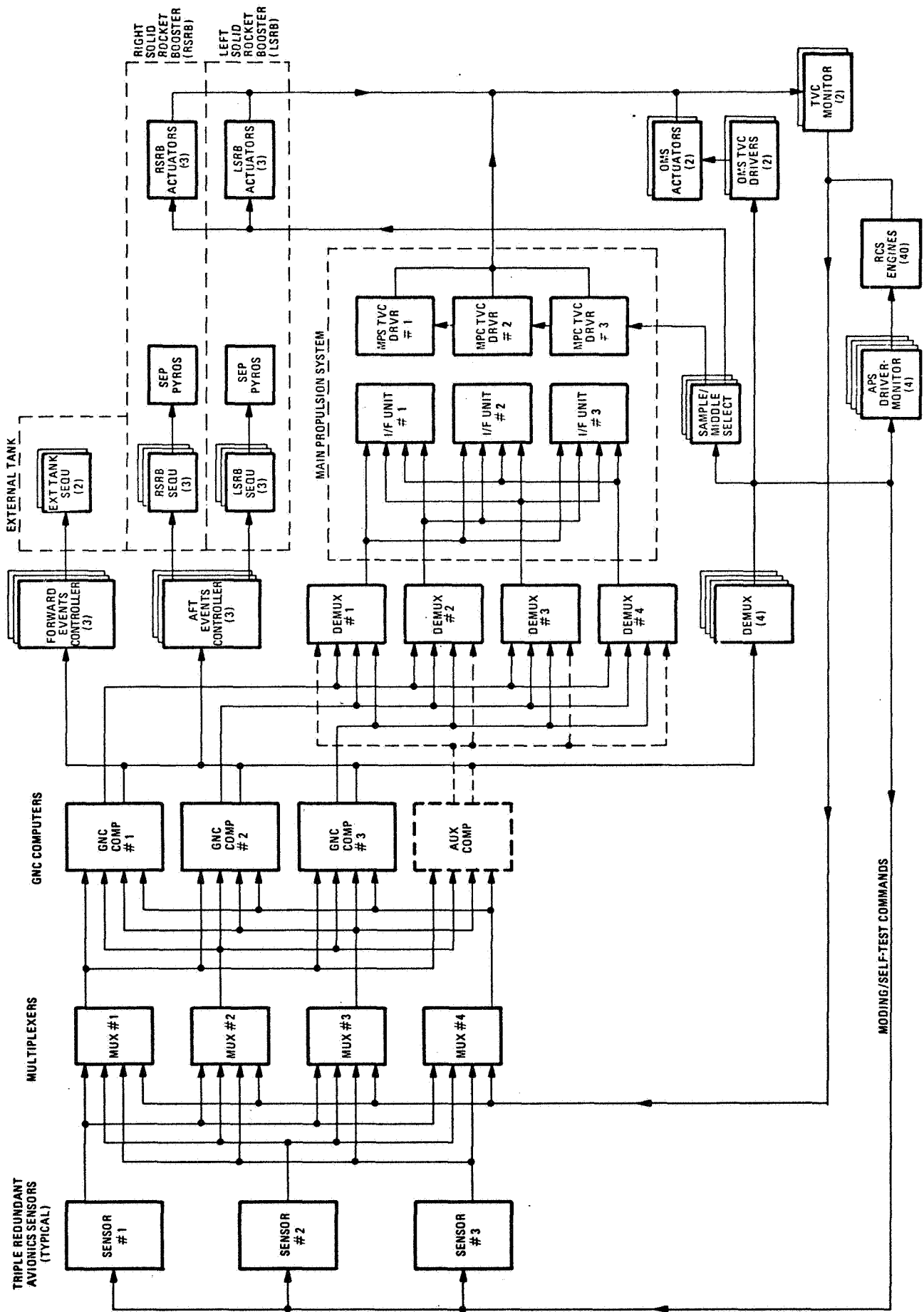


Figure 4-7 Shuttle Avionics Functional Paths (In Part) Derived from Figure 1, Rockwell Master Change Record 0164, Orbiter Avionics System Baseline

5.0 CONCLUSIONS

The brief review of the checkout and launch of Shuttle, as set forth in Section 2.0, indicates that a severe technological and operational challenge exists. The need for concurrent, automated testing under computer control highlights the vital role to be played by GOAL, the high order test language.

In Section 3.0, the proposed software hierarchy for the onboard computers is examined with the objective of determining how best to implement GOAL test statements in the onboard computers. It is clear that these computers are not general purpose machines equipped to compile and run programs written in one or more languages. Instead, these computers are equipped with a multi-level operating system (FCOS) which is designed and dedicated to working with applications programs written in HAL/S. It seems clear that GOAL programs should be implemented by conversion to HAL/S code and executed onboard at the highest level, Level 4 of Figure 3-4.

A review of the three categories of command and control shows that some subsystems can only be accessed through the GN&C computers. For those subsystems, primarily in the avionics area, it will be necessary to have Level 4 HAL/S application programs running simultaneously with the Level 4 GOAL-derived HAL/S checkout programs. Consideration of a GOAL executive onboard does not seem practical.

Finally, Section 4.0 discusses the impact of error detection and redundancy management on GOAL. It is suggested that the onboard signal selection logic used when redundant signals are available can be duplicated in the test software and comparisons can then be made of the signal selection being executed in the system. Special GOAL statements are described. However the exact implementation of the signal selection and configuration management is not available at this writing. The practicality and benefits of special GOAL statements cannot be established at this time. It is recommended that this aspect of GOAL be reviewed again prior to final specification of a translator.

Appendix A

Answers to Specific Questions on Software Checkout Modules

(It is recommended that Section 3.0 be read first).

Question #1: Can different GOAL checkout programs run in different onboard computers (both PMS and GNC) concurrently?

If no computer system errors have been detected, the three GN&C computers form one master and two slave machines or one virtual machine. The two PMS computers may be operated so as to form one virtual machine. Within each virtual machine many checkout programs can run concurrently if they are translated into HAL and if the Levels, 1, 2 and 3 of support software (see Figure 3-1) are available, as long as the standard problems that arise on a multi-computer environment are solved.

Question #2: Will the on-board operating system lend itself to receiving and executing ground checkout software modules?

Yes, if Levels 1, 2 and 3 of support software are loaded in the onboard computers, if the checkout software modules have been translated into HAL code, if the telemetry system is designed to accept software loads uplink, if the FCOS is designed with this in mind, and if the level 3 software and the checkout software have compatible interfaces, initialization parameters, etc.

Question #3: Can KSC send up a GOAL Executive and load it into the onboard machine such that subsequently 'pure GOAL code' can be executed?

This question is interpreted to mean that the GOAL executive is introduced at Level 2 (See Figure 3-2). The answer is a qualified no. The crucial applications support routines that operate the display and controls the telemetry, and most importantly the GN&C subsystems would have to be re-written in GOAL and run through a GOAL Compiler designed for the flight machines. Section 3.3 discusses a hybrid situation.

Question #4: Does the onboard operating system allow individual commands (discretes) to be received and processed?

This question needs to deal with the three types of systems:

Manual Switch only (Figure 3-6) control is by flight crew manual action only.

Manual Switch with Parallel Contact (Figure 3-7). Action is from the onboard computers are involved.

GN&C Computer Directed Subsystems (Figure 3-8). Only those individual commands are processed which are in an approved telemetry uplist and which are recognized by a Level 3 or Level 4 Program, as legitimate words at the time that an interrupt will be processed.

Question #5: Does the onboard Operating System have a trace and dump system that is available to the ground?

The answer is no. (If a sequence of failures is detected a maintenance record is available for playback on the ground. This is not a trace and dump.) Trace and dump is a function of the Software Development Laboratory and simulation facilities.

Question #6: How does the ground change the onboard parameter list?

The GN&C and PMS computer groups each have a Data Acquisition and Formatting unit (See Figure 3-5). Presently, three fixed formats and one variable format have been designated. These formats can be switched from the ground by a signal through the Command Decoder.

Question #7: What method is used to load the GOAL executive for maintenance, checkout, and pre-launch into the onboard computers?

A successful load of any software module uplink through the command decoder to the onboard recorders will require that the Flight Computer Operating System (FCOS) be implemented with the uploading of programs in mind. The FCOS must recognize the program, error, check it, place it in the appropriate directory, and interpret its initialization requirements correctly. Question #3 deals with the practicality of using a GOAL executive onboard.