An Engineering Study of Onboard Checkout Techniques

A GUIDE TO ONBOARD CHECKOUT
VOLUME V: DATA MANAGEMENT

CR 115257

Huntsville

IBM

An Engineering Study of Onboard Checkout Techniques

A GUIDE TO ONBOARD CHECKOUT
VOLUME V: DATA MANAGEMENT

IBM NUMBER: 71W-00312

SEPTEMBER 1971

Prepared for the
National Aeronautics and Space Administration
Manned Spacecraft Center
Houston, Texas 77058

CONTRACT NUMBER NAS9-11189

IBM Federal Systems Division, Electronics Systems Center/Huntsville, Alabama

TABLE OF CONTENTS

Table of Contents (cont)

FOREWORD

This is one of a set of seven reports, each one describing the results, for a particular subsystem, of a study titled "An Engineering Study of Onboard Checkout Techniques." Under the general title of "A Guide to Onboard Checkout," the reports are as follows.

Volume	IBM Number	Subsystem
I	71W-00308	Guidance, Navigation and Control
II	71W-00309	Environmental Control and Life Support
III	71W-00310	Electrical Power
IV	71W-00311	Propulsion
V	71W-00312	Data Management
VI	71W-00313	Structures/Mechanical
VII	71W-00314	R.F. Communications

This set of guides was prepared from the results of a nine month "Engineering Study of Onboard Checkout Techniques" (NAS9-11189) performed under NASA contract by the IBM Federal Systems Division at its Space Systems facility in Huntsville, Alabama, with the support of the McDonnell Douglas Astronautics Company Western Division, Huntington Beach, California.

Technical monitor for the study was Mr. L. Marion Pringle, Jr. of the NASA Manned Spacecraft Center. The guidance and support given to the study by him and by other NASA personnel are gratefully acknowledged.

Section 1

INTRODUCTION

1.1 OBJECTIVE

With the advent of large scale aerospace systems, designers have recognized the importance of specifying and meeting design requirements additional to the classical functional and environmental requirements. These "additional" requirements include producibility, safety, reliability, quality, and maintainability. These criteria have been identified, grown into prominence, and become disciplines in their own right. Presently, it is inconceivable that any aerospace system/equipment design requirements would be formulated without consideration of these criteria.

The complexity, sophistication and duration of future manned space missions demand that still another criterion needs to be considered in the formulation of system/equipment requirements. The concept of "checkoutability" denotes the adaptability of a system, subsystem, or equipment to a controlled checkout process. As with other requirements, it should also apply from the time of early design concept formulation.

The results of "An Engineering Study of Onboard Checkout Techniques" and other studies indicate that for an extended space mission onboard checkout is mandatory and applicable to all subsystems of the space system. In order to use it effectively, "checkoutability" should be incorporated into the design of each subsystem, beginning with initial performance requirements.

Conferences with researchers, system engineers and subsystem specialists in the course of the basic Onboard Checkout Techniques Study revealed an extensive interest in the idea of autonomous onboard checkout. Designers are motivated to incorporate "checkoutability" into their subsystem designs but express a need for information and guidance that will enable them to do so efficiently.

It is the objective of this report to present the results of the basic study as they relate to one space subsystem to serve as a guide, by example, to those who in the future need to implement onboard checkout in a similar subsystem. It is not practicable to formulate a firm set of instructions or recipes, because operational requirements, which vary widely among systems, normally determine the checkout philosophy. It is suggested that the reader study this report as a basis from which to build his own approach to "checkoutability."

1.2 BASIC STUDY SUMMARY

1.2.1 STUDY OBJECTIVE

The basic study was aimed at identification and evaluation of techniques for achieving the following capabilities in the operational Space Station/Base, under control of the Data Management System (DMS), with minimal crew intervention.

- Automated failure prediction and detection
- Automated fault isolation
- Failure correction
- Onboard electronic maintenance

1.2.2 STUDY BASELINE

The study started in July 1970. The system design baseline was established by the Space Station Phase B study results as achieved by the McDonnell-Douglas/ IBM team, modified in accordance with technical direction from NASA-MSC. The overall system configuration was the 33-foot diameter, four-deck, 12-man station. Individual subsystem baseline descriptions are given in their respective "Guide to Onboard Checkout" reports.

1.2.3 STUDY TASKS

The basic study comprised five tasks. Primary emphasis was given to Task 1, Requirements Analysis and Concepts. This task established subsystem baseline descriptions and then analyzed them to determine their reliability/maintainability characteristics (criticality, failure modes and effects, maintenance concepts and line replaceable unit (LRU) definitions), checkout strategies, test definitions, and definitions of stimuli and measurements. After software preliminary designs were available, an analysis of checkout requirements on the DMS was performed.

A software task was performed to determine the software requirements dictated by the results of Task 1.

Task 3 was a study of onboard electronic maintenance requirements and recommendations of concepts to satisfy them. Supporting research and technology tasks leading to an onboard maintenance capability were identified. The study implementation plan and recommendations for implementing results of the study were developed in Task 4. The task final report also summarizes results of the study in all technical tasks.

Reliability, Task 5, was very limited in scope, resulting in an analysis of failure modes and effects in three Space Station subsystems, GN&C, DMS (computer group) and RF communications.

1.2.4 PREVIOUS REPORTS

Results of the basic study were reported by task in the following reports, under the general title of "An Engineering Study of Onboard Checkout Techniques, Final Report."

IBM Number	Title
71W-00111	Task 1: Requirements Analysis and Concepts
71W-00112	Task 2: Software
71W-00113	Task 3: Onboard Maintenance
71W-00114	Task 4: Summary and Recommendations
71W-00115	Task 5: Subsystem Level Failure Modes and Effects

Section 2

BASELINE SUBSYSTEM DESCRIPTIONS

2.1 GENERAL

This section describes the baseline Data Management Subsystem (DMS) which was analyzed to define onboard checkout requirements. In order to assess requirements for onboard checkout, descriptions at the subsystem level and the assembly level are required, as well as the major interfaces between subsystems.

The assembly level description for each of the subsystems (MSFC-DRL-160, Line Item 13) provided the primary working document for subsystem analysis. To reduce documentation, these documents have been incorporated by reference into this report, where applicable. Therefore, where no significant differences exist from the Phase B definition, this report contains a brief subsystem description and an identification of the referenced document containing the assembly level descriptions for that subsystem. Where significant differences do exist, the subsystem level description includes these changes in as much detail as is available. MSFC-DRL-160, Line Item 19, provided the major subsystem interface descriptions for analysis of integrated test requirements.

2.2 SUBSYSTEM LEVEL DESCRIPTION

The DMS consists of the necessary equipment to transfer, store, and process data to and from users and subsystems. As such, it acquires and conditions a wide variety of input data from experiments, vehicle subsystems sensors, uplinked ground communications, and astronaut-activated controls.

Figure 2-1 depicts the DMS baseline configuration. Individual subsystem descriptions are provided because of the differences between the study baseline and the MDAC/IBM Phase B configuration.

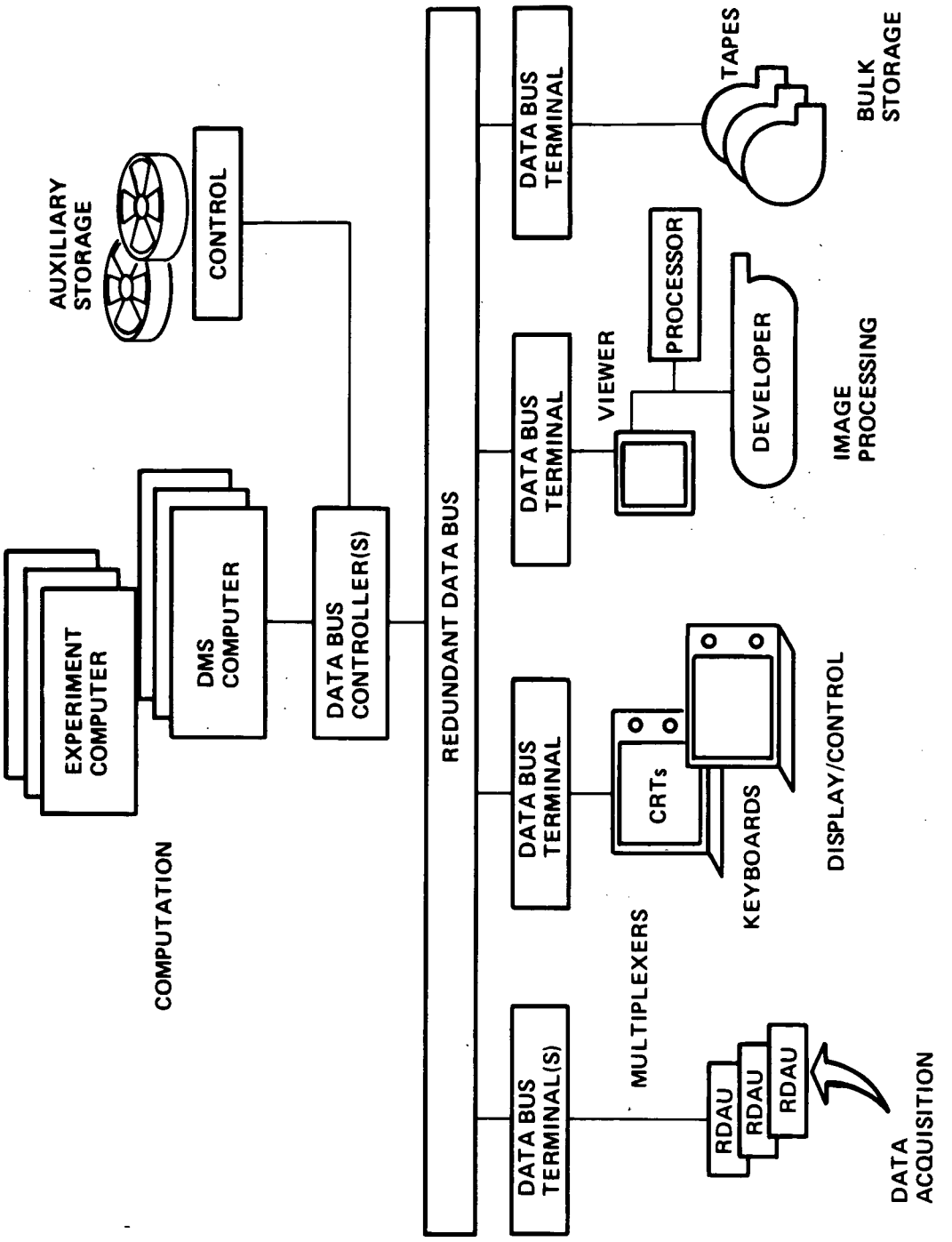


Figure 2-1. Data Management Subsystem Baseline

The DMS Computer Subsystem is comprised of:

- One - Space Station Operations Multiprocessor (3 CPUs)
- One - Space Station Experiment Multiprocessor (3 CPUs)
- Shared Main and Auxiliary Memories
- Bulk Data Storage
- Switching Matrices

Figure 2-2 depicts a functional block diagram for the Computer Subsystem. A lower level functional diagram of the individual Computer Subsystem components is given in Figure 2-3.

The six processors (CPUs) are identical in size and architecture and can provide a backup capability for one another. The main memory (256 K words) and the auxiliary memory (2.5 M words) are shared between all the CPUs and can be individually addressed through the memory switch matrix, by any of the six CPUs. These memories will be primarily used for the storage of subroutines and data that require rapid access from the CPUs. In addition, these memories can be addressed directly from the data bus for direct storage of uplinked program modifications and acquired data. The main memories are high speed monolithic memory units and the auxiliary memories are a combination of high speed magnetic tape, incremental tape, and magnetic disc units.

The bulk data storage uses ultra high density magnetic tape recorders and is configured to meet large data volume storage requirements with a relatively slow access speed. Its use is primarily for recording digital data before onboard processing or before return to earth for ground processing. As such, it will be the last level of memory in the Processing Subsystem and will store infrequently used information not requiring rapid access, such as maintenance procedures, spare parts inventories, or information that may be stored off line. The bulk data storage consists of the following elements:

- Tape Transports
- Tape Transport Controllers
- Digital Buffer and Control Unit
- Record/Reproduce Electronics
- Switching Matrices

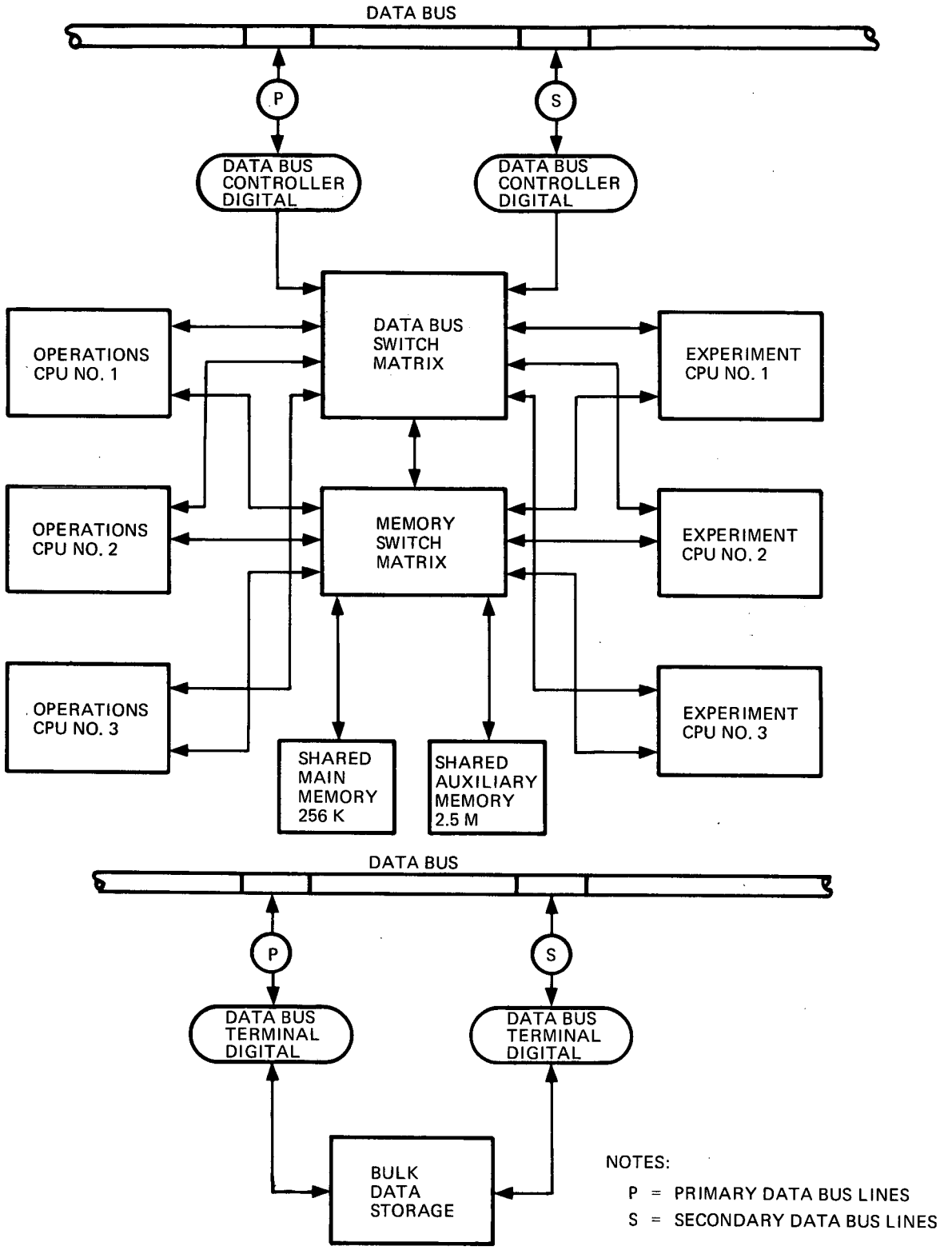


Figure 2-2. DMS Computer Subsystem

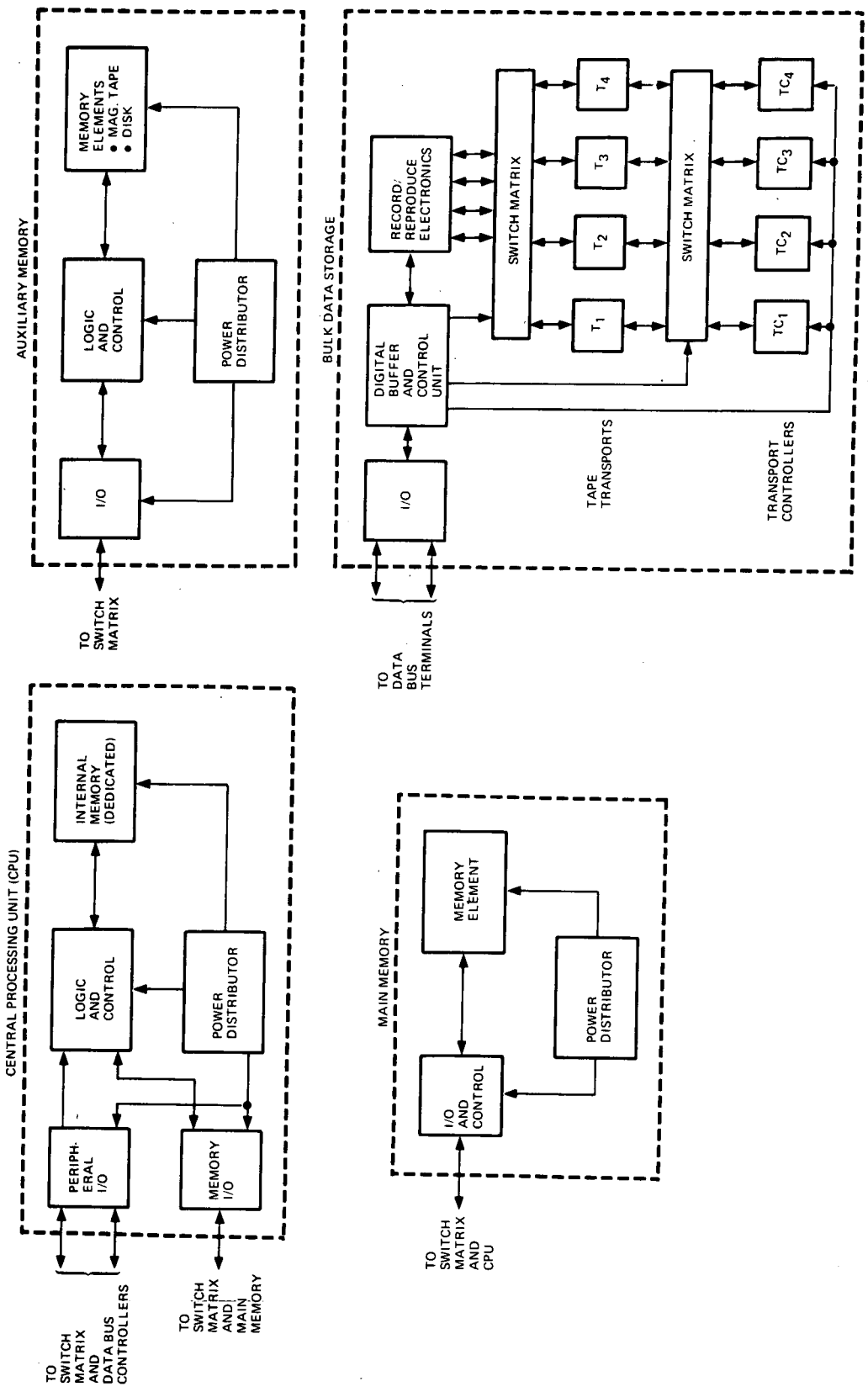


Figure 2-3. Computer Subsystem Components Functional Block Diagrams

The Data Acquisition and Distribution Subsystem is comprised of the following elements:

- Data Bus
- Digital Data Bus Terminals
- Remote Data Acquisition Units
- Local Monitor and Display Units (LMDU)

This subsystem is used by the DMS to distribute all necessary commands and acquire all required data or command responses for Space Station operation, experiment control/monitoring, and for all OCS functions. Additionally, the data bus is used for the distribution of all intercommunication and entertainment audio and video signals.

The data bus consists of redundant coaxial command and response lines (4 total) linking together all primary elements of the DMS. A total data rate greater than 50 megabits per second should be considered for this application. Twisted wire pairs or other suitable transmission lines are used for secondary data distribution common to individual data bus terminals and transmission of warning alarm signals to and from LMDUs.

The digital data bus terminals are configured for modularity and interface commonality. This terminal is designed to handle eight standard four-wire interfaces each with individual bit rates of 1 MHz or less. Each interface is isolated to prevent propagating a data source failure to another interface. A switchable modem is used as the data bus interface. The switching feature permits the modem to interchange its command and response lines such that an off-line data dump to a selected subsystem (i.e., bulk data storage) can be effected with the stated data bus configuration (i.e., separate command and response lines). Clock logic is modular and divides the data bus clock to the frequencies required by the subsystem/experiment interfaces. Buffer storage is also modular and may be provided for any or all inputs individually. This feature allows storage to be tailored to a particular interface data rate. The DMS control would efficiently utilize this storage by (1) sending a control word to cause the terminal to sample its inputs, and at a later time (2) sending a control word to request a data dump. An additional interface is provided to address the stimuli generators and other required discrete signal outputs. The terminal would be used, via a DMS control word, to energize a particular stimuli generator channel, or provide a control function (discrete signal) output. A self-check feature is provided to allow OCS fault isolation to a particular unit.

The Remote Data Acquisition Unit can be considered as a subsystem/experiment preprocessor and is designed to interface directly with the digital data bus terminal. The RDAU performs five functions on analog and digital signals. These are: signal conditioning, multiplexing, A/D conversion (analog only), limit checking, and digitizing to format the data into the standard digital format for transmission to the data bus. Signal conditioning is accomplished through a programmable gain amplifier or both programmable gain amplifier and a preconditioning (ahead of the multiplexer) network. The RDAU inputs may be discrete (on-off) or analog signals, but must be preconditioned to the proper working voltage prior to multiplexing. The A/D converter output is digitally compared with high and low limits extracted from a self-contained read/write memory. If the measured parameter exceeds either limit, the return data is flagged so the DMS processor is aware of any failures or out-of-tolerance conditions. The limits can be changed and adjusted to changing operational conditions by appropriate commands from the DMS/OCS processors.

Operation of the RDAU is under direct control of the DMS processor which transmits control information via the data bus using a standard word format containing the address of the RDAU and the appropriate instruction codes. Three operating modes are provided as described below.

- Compare Mode - The device sequentially scans the input channels and compares the digitized measurements with upper and low limits stored in the device memory. No action is taken unless an out-of-limit condition is detected, in which case an error message is formatted for transmission to the DMS processor. The stored limit values may be changed at any time under processor control. Individual channels may also be inhibited from generating error messages. These capabilities allow the limit check profile of each RDAU to be adjusted to accommodate changing operating modes or conditions of the equipment.

- Sequential Output - The device sequentially scans the input channels and transmits the digitized measurements to the processor. Limit checking is inhibited.

- Single Channel Output - The device selects a single input channel whose address is specified in the control word and transmits the digitized value to the processor. The channel may be sampled once or repetitively. Limit checking is inhibited.

RDAU inputs may be either discrete (on-off) or analog signals, but must be preconditioned to a specified voltage range. The baseline configuration accepts discrete inputs of 0 or 5 Vdc and analog inputs in four ranges of 0-20 mV, 0-50 mV, 0-100 mV, and 0-5V. Other voltage levels may be accommodated if

required, at the expense of additional signal conditioning circuitry in the device. It should be pointed out, however, that the ability to accommodate the development and evolutionary growth expected to occur in the Space Station dictates the necessity to establish standard interface specifications which do not impose unreasonable constraints on either the Data Acquisition System or the data sources. Preconditioning of data at the source satisfies this requirement by providing an easily definable interface which is compatible with established instrumentation practices. The RDAU basic configuration is a device with 32 analog and 32 discrete channels. Other configurations of varied capability are also provided to attain an optimum distribution. The RDAU contains a self-test capability to allow fault isolation to the replaceable unit. A possible self-test concept is to provide calibration voltages, divided from the RDAU power input, into the input of the multiplexer. This would give an indication as to the operational status of the unit.

The LMDU, shown in Figure 2-4, is primarily an RDAU with local critical parameter display capability. It accepts both caution and warning functions and contains the necessary circuitry to: (1) monitor these critical functions continuously for out-of-tolerance conditions, (2) cause immediate activation of self-contained and external alarm indications, and (3) acquire caution and warning function data for normal checkout operations. Limit checking of critical function inputs is performed using the same methods and circuitry employed by the RDAU. Unlike the RDAU, however, the LMDU activates local alarms which are directly wired to the monitor circuitry. Transmission of critical function data to the central caution and warning displays is on the DMS data bus. In contrast to caution parameter limits, which can be changed by remote control, the stored limits for warning parameters are adjustable only by local manual replacement of individual memory modules. Detection of out-of-limit warning function activates audio and visual alarms located within the unit and, under CPU control, those located external to the unit. These include alarms in the Space Station's primary and secondary control centers, and as required in other LMDUs. Once initiated, caution and warning alarms remain active until reset. A capability is provided for selectively inhibiting individual functions to accommodate changing operational conditions. All critical functions are also redundantly monitored via the normal DMS/OCS.

The Space Station caution and warning function is considered a part of the OCS, but is implemented as a separate and redundant system for reliability. Critical measurements are monitored and out-of-tolerance indications are provided primarily through the use of Local Monitor and Display Units. Warning functions are those which, if out of tolerance, could present an immediate threat to crew life. Caution functions are those which, if out of tolerance, could result in major degradation of Space Station performance unless specific crew action is taken.

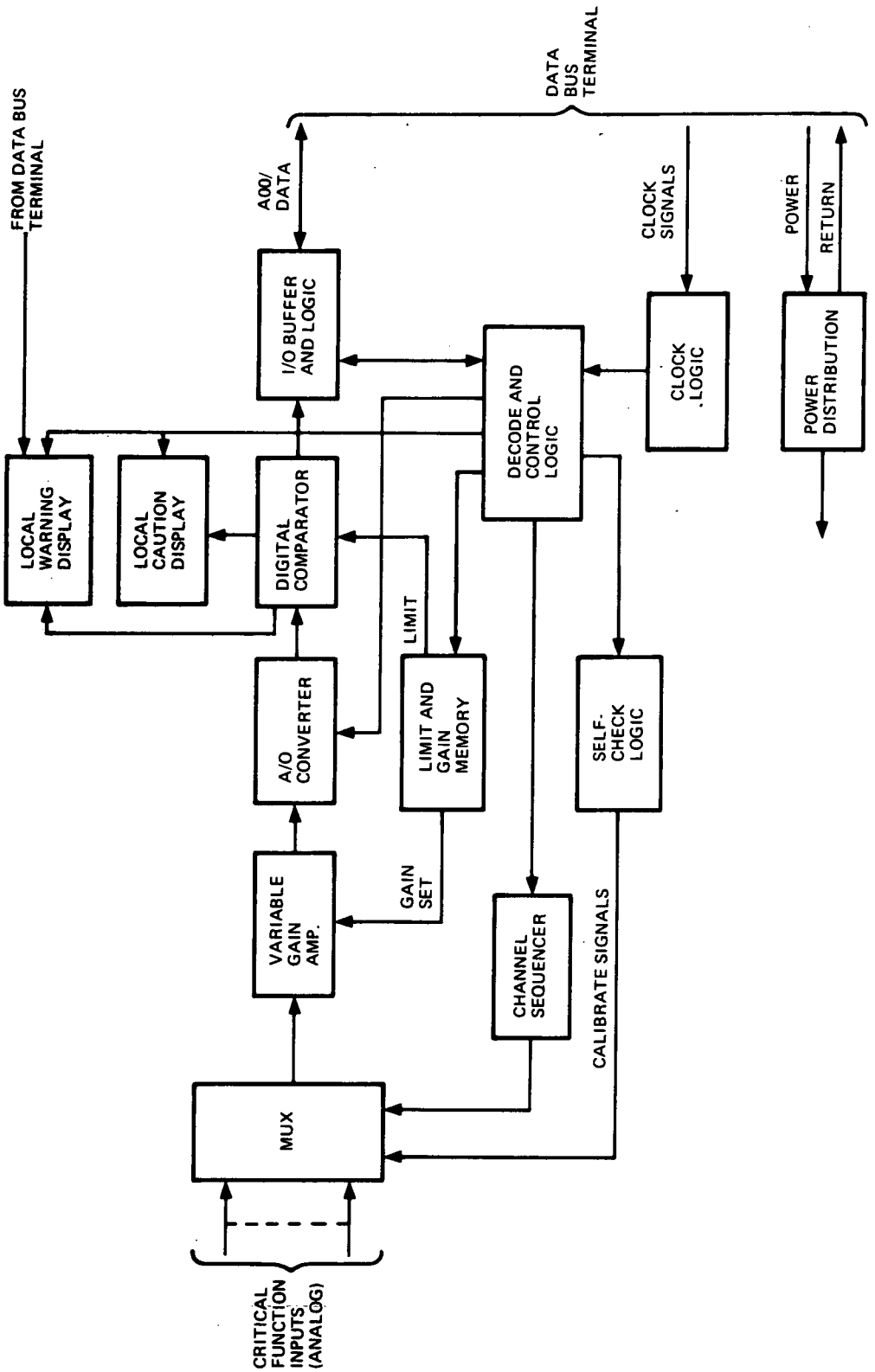


Figure 2-4. LMDU Block Diagram

A functional block diagram of the caution and warning function is shown in Figure 2-5. The redundancy of the monitoring elements can easily be seen from this diagram. Detection of an out-of-tolerance condition causes the activiation of both visual and audible alarms to notify the crew. Annunciator panels and LMDUs with appropriate displays are located in each crew compartment, where required, and on the central command and control consoles. The displays are coded (by color, tone, etc.) to differentiate between the caution and warning levels of alarm. A manual override is provided for the audible alarm.

The Image Processing Subsystem, as shown in Figure 2-6, provides onboard capability to:

- Provide quick look at experiment results
- Calibrate/align experiment instruments
- Monitor and control experiments

The Image Processing Subsystem is configured to process 1923 images per 8 hours, image content 2.5×10^6 bits each. The digital computer associated with this subsystem has tentatively been defined as the DMS Experiment Multiprocessor and is intended to be used for statistical evaluation of image data as well as derivation of annotation information. Requirements for Fourier transformations and convolution processing, in respect to additional special purpose digital processing equipment, are being analyzed.

An experimenter's station is provided which consists of an experimenter's console and display. The console communicates with the experiments it controls and with the computer and analog processor (adjustable multichannel filter). Each station display will have two CRTs for comparing images driven by the working video storage or by the computer.

The central element of the system is the Experimenter's Console which contains displays for film and image information generated in analog form. The functions controlled from the console include:

- Adjustment of viewing instruments
- Annotations and editing functions for stored, processed, and transmitted image information
- Control of processing functions in an interactive manner

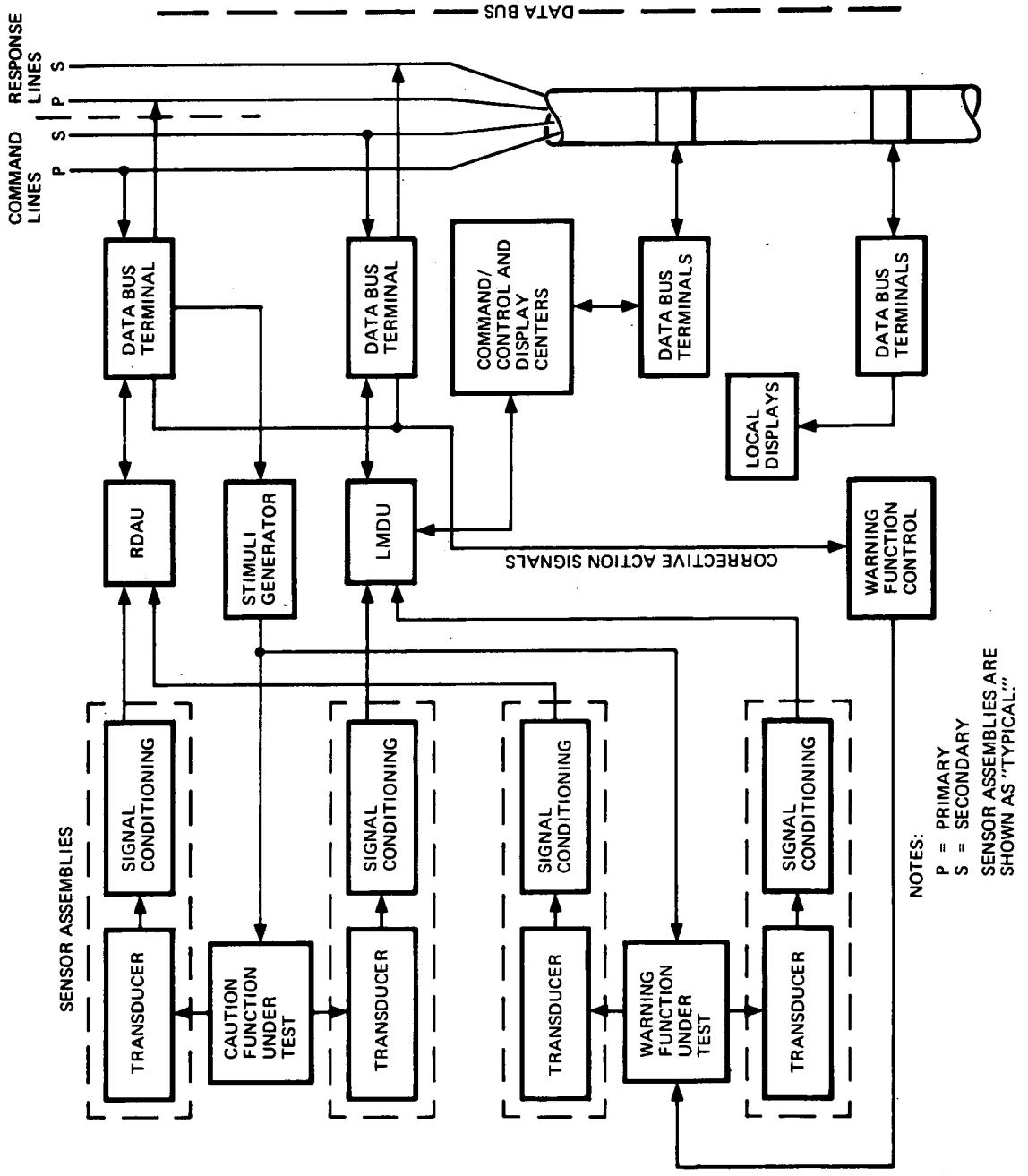


Figure 2-5. DMS/OCS Caution and Warning Functions

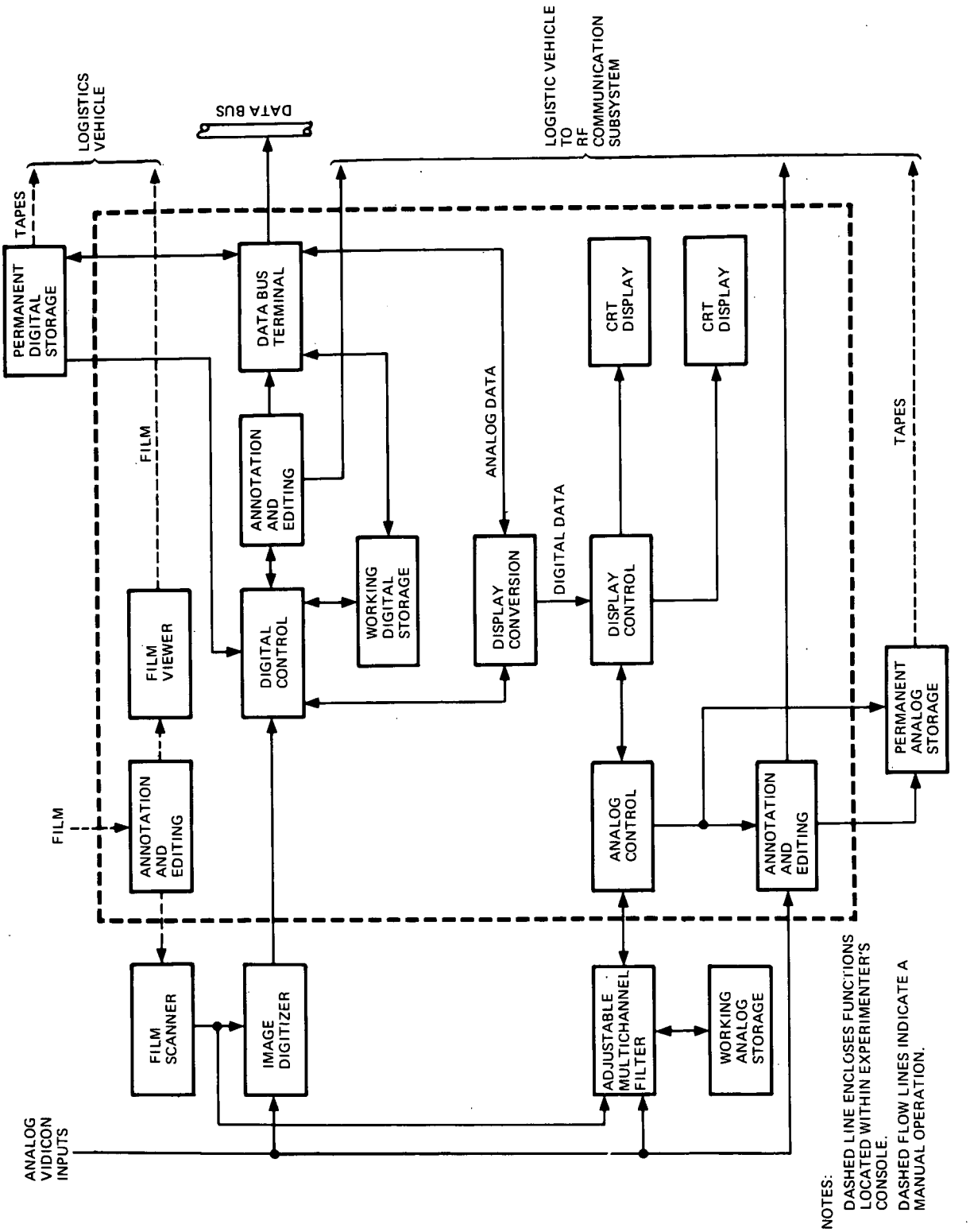


Figure 2-6. Image Processing Subsystem Functional Block Diagram

Film may be directly viewed using the film viewer/reader. This device, which provides for single-and multiple-frame analysis, consists of a screen for viewing or scanning, controls for image magnification and rotation, and a frame counter.

The film scanner is employed to transform film images into an electrical signal. For this purpose, the unit employs a high resolution flying spot scanner which may be programmed to vary the electronic sweeps and scans of the unit in order to reduce nonlinearities or obtain data only on particular areas of interest.

The Command/Control and Display Subsystem (CCDS) is comprised of the following basic elements.

- Operations CCDS Center
- Experiment CCDS Center
- Portable Display and Control Units

These units provide the primary human interface to the DMS/OCS.

The Operations CCDS Center will be the primary central command post for Space Station operations. This station provides monitoring and control capability of all subsystem "housekeeping" activities, mission planning, and personnel/activities scheduling. This station will play a central, active role during all rendezvous and docking phases with other spacecraft and experimental modules and during ground communications for command and data transfer.

The Experiment CCDS Center is a centralized operation center for monitoring and management of the experiment program. In addition, this station is capable of providing emergency/backup vehicle and subsystem control capability in the event the crew is forced to evacuate the Primary Command and Control Center because of a major emergency condition. Because of this, the Experiment CCDS Center is located in an environmentally isolatable compartment.

Displays and controls required at the experiment/Secondary Command and Control Center are basically the same as those required by the primary center, in addition to dedicated experiment displays and controls to permit complete monitoring and control capability over the experiment program.

In addition to the primary and backup control centers, a number of small portable devices are provided which contain alphanumeric displays and input keyboards. These devices may be plugged into the data bus at various locations throughout the Space Station and thereby provide an operator with limited control

and display capability from remote locations. An example of their use would be in certain fault isolation situations where the operator finds it advantageous to operate from a position adjacent to the equipment under test rather than from the center location.

The command/control and display stations, Figure 2-7, contain three multipurpose CRT display devices (one primarily allocated to OCS functions) and two keyboards which provide backup redundancy. This dual design allows onboard checkout to be accomplished from this station by a second crew member on a noninterference basis while sharing common displays, readouts, status lights, etc., if necessary. Some special OCS peculiar displays such as status indicators, as well as special purpose OCS controls such as mode and function switches, are integrated into the console in such a way as to permit access by the OCS operator without interference with other console operations. The prime interface for displays and controls to the Space Station is through the DMS multiprocessor computer via the data bus. The prime control/display devices providing the interface with the computer are mode select switches, computer keyboard unit, and multipurpose CRT displays. The keyboard and associated mode select pushbutton switches provide access to and control of nonprogrammed computer operations and the CRT displays computer-generated alphanumeric/graphic information and stored/processed data. A secondary "hardwire" interface is provided for those functions, such as local controls and dedicated displays, which are wired directly and do not require transmission via the data bus. Intercom and Command Control Television (CCTV) control is provided by the Command/Control and Display Console (CCDC) via analog interface units.

The GN&C preprocessors are included within the DMS only to the extent of their interconnection with the data bus through required data bus terminals. Five preprocessors and associated data bus terminals have been configured for the GN&C Subsystem. These preprocessors provide the capability of operationally interfacing the individual GN&C sensors and controls via required interface electronic assemblies to the operations multiprocessor. In addition, it is anticipated that a significant amount of data formatting and "housekeeping" computations will be accomplished by these preprocessors, thereby relieving the overall operations multiprocessor load. Specific assignments of data formatting and computation to the individual GN&C preprocessors have yet to be determined.

It is assumed that the preprocessors will be simplex, dedicated digital computers with a self-test capability. Specific signal conditioning for inputs and outputs to the GN&C sensors and controls will be accomplished by the interface electronics assemblies, a part of the Guidance, Navigation, and Control System. The preprocessor-to-data-bus interface will be through a standard data bus terminal.

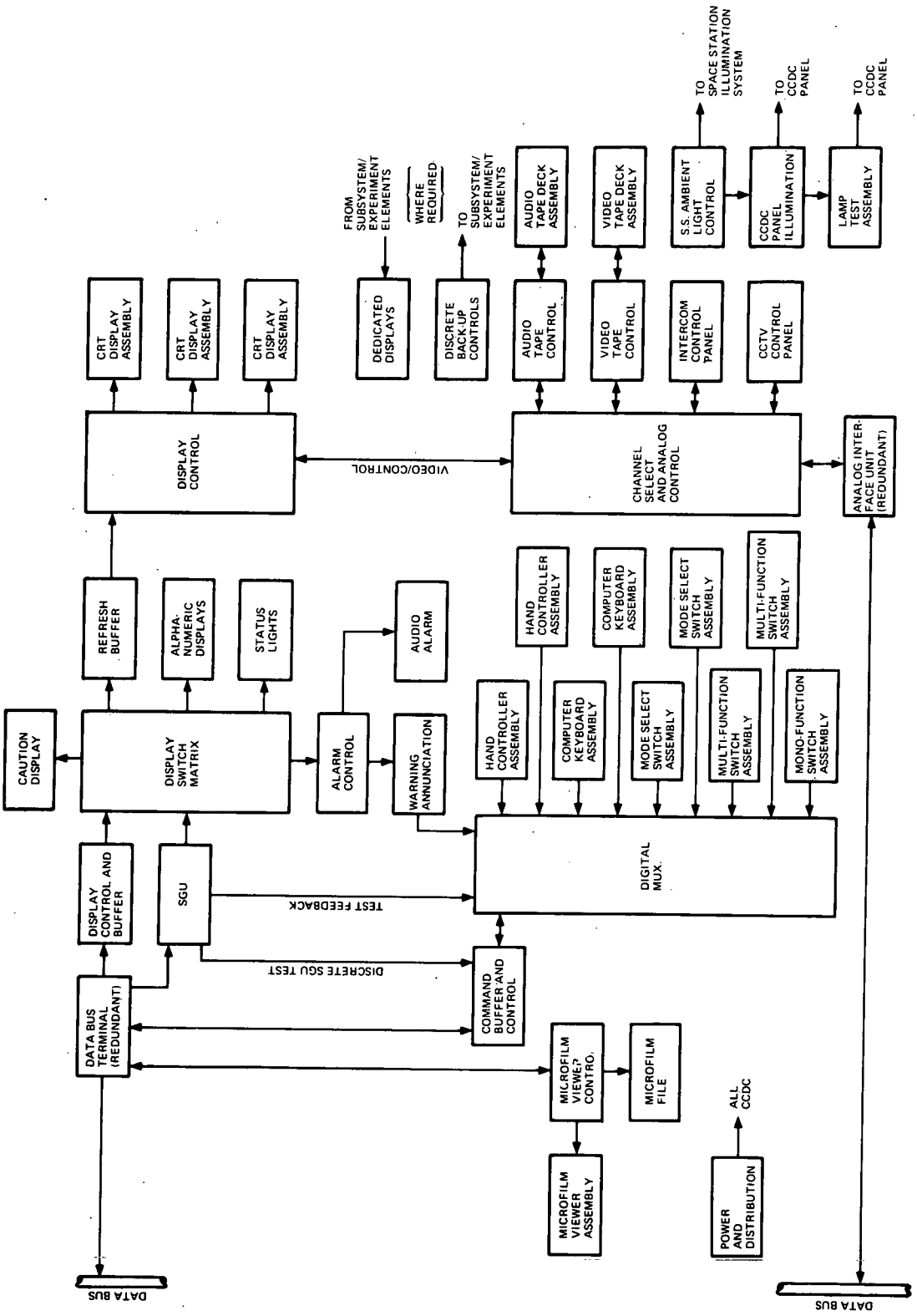


Figure 2-7. Command/Control and Display Console Functional Block Diagram

2.3 ASSEMBLY LEVEL DESCRIPTIONS

Subsystem block diagrams and descriptions of the Data Management Subsystem assemblies not included here are provided in the Space Station MSFC-DRL-160, Line Item 13, Volume I, Book 2, Space Station Electronics. These descriptions include block diagrams, discussion of major subassemblies, physical characteristics, and interface descriptions. DRL 13, Volume I, Book 2, is incorporated by reference into this report as a detailed description of the DMS assemblies and, except where modified by this document, will become the primary working document for further analysis.

Section 3

RELIABILITY AND MAINTAINABILITY ANALYSES

3.1 CRITICALITY ANALYSIS

As a guide to emphasis in subsequent checkout technique studies, an analysis has been made of the overall subsystem and major component criticality (failure probability) of the Space Station subsystems and equipment. As an input to the Checkout Requirements Analysis Task, this data along with the failure mode and effects data will be useful in determining test priorities and test scheduling. Additionally, this data will aid in optimizing checkout system design to ensure that confidence of failure detection is increased in proportion to added system complexity and cost.

3.1.1 CRITICALITY ANALYSIS PROCEDURE

A criticality number (related to failure probability) was generated for each major subsystem component. This number is the product of: (1) the component failure rate (or the reciprocal of mean-time-between-failure), (2) the component's anticipated usage or duty cycle, and (3) an orbital time period of six months, or 4,380 hours. Six months was chosen as the time period of interest to allow one missed resupply on the basis of normal resupply occurring at three-month intervals. The criticality number, then, is the failure expectation for a particular component over any six-month time period.

For visibility, the major components of each subsystem analyzed have been ordered according to the magnitude of their criticality numbers. This number, however, should not be considered as an indication of the real risk involved, since it does not take into account such factors as redundant components, subsystem maintainability, and the alternate operational procedures available.

Overall subsystem criticality has been determined by a computerized optimization process whereby spares and redundancy are considered in terms of a trade-off between increased reliability and weight. This determination, therefore, reflects not only the failure probability of subsystem components, but also the probability that a spare or redundant component may not be available to restore the subsystem to operational status. The methodology used is described in Section 9, Long-Life Assurance Study Results, DRL 13 (Preliminary Subsystem Design Data), Volume III (Supporting Analyses), Book 4 (Safety/Long Life/Test Philosophy) from the MDAC Phase B Space Station Study. Component-level failure mode and criticality data are presented in subsequent paragraphs.

3.1.2 SUBSYSTEM CRITICALITY DATA

The Data Management Subsystem has a six-month reliability of 0.998. This figure is based upon the currently projected potential reliabilities of the components (some of which are in the early development stage), critical failure definitions based upon preliminary DMS functional definitions, and adequate sparing. Criticality numbers for units which are internally redundant cannot be established at this time since the actual values will depend upon detail design. No single failure or credible combination of failures can cause loss of the major DMS functions. Table 3-1 provides the ordered ranking of DMS components.

3.2 FAILURE EFFECTS ANALYSIS (FEA)

The procedure employed in this section is similar to that of the earlier FEA analysis, except that a distinction was made between "single" and "multiple" failures. The term "multiple failures" implies complete loss of the function under consideration. A description of the baseline subsystems is contained in Section 2.

Generally, this FEA, coupled with other results, indicates that no failure modes exist which invalidate the onboard checkout concepts. It is noted that this analysis was conducted at the component level, commensurate with available Space Station subsystem design definition.

Examples of results of the Data Management (DMS) subsystem FEA are given in Table 3-2 (a partial listing).

3.3 MAINTENANCE CONCEPT ANALYSIS

General maintenance concepts and recommendations are summarized in Section 7. The maintenance concepts provide guidelines to definition of Line Replaceable Units.

3.4 LINE REPLACEABLE UNIT ANALYSIS

General guidelines and criteria for the definition of LRUs were established and these along with the maintenance philosophies reported in Section 3-3 were used to determine at what level line maintenance would be performed. For the Space Station Data Management Subsystem, a functional partitioning of the major subsystem components based on the ability to create a viable isolation method to that functional level was performed. The "functional LRUs" were then considered in the light of the standard electronic packaging scheme and actual LRUs were defined and listed. The method employed and the results achieved are discussed for both cases in the following sections.

Table 3-1. DMS Criticality Ranking

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
Experiment Processor	83,870	Not Available	*2/3
Operations Processor	83,870		2/3
Main Memory	8,700		12/14
Auxiliary Memory	354,670		2/4
Digital Terminal	21,660		13/15
Remote Data Acquisition Unit	4,370		
Local Mon/Disp Unit	5,242		
Tape Transport Controller	8,700		2/4
Tape Transports	354,670		2/4
Tape Electronics Unit	21,660		1/2
Switching Matrix	--		Internally redundant

* Information based on two of three units operational.

Table 3-1. DMS Criticality Ranking (Continued)

Component	Single Unit Criticality (10^{-6})	Conditioned Loss Criticality (10^{-6})	Remarks
Film Viewer	83,870	Not Available	
Film Scanner	196,678		
Filter	21,660		
Display/Console	196,678		
Control/Display Console	481,600		1/3
Time Reference Unit	--		Internally redundant
Printer	354,670		1/2
Command Decoder	--		Internally redundant
Remote Command Distributor	8,700		15/16

Table 3-2. Space Station Failure Effect Analysis

SUBSYSTEM: Data Management

Item	Function	Failure Effect On		Space Station
		Failure Type	Subsystem	
Data Management Subsystem	The Data Management Subsystem provides the required computational and storage capability for the Space Station as well as regulating flow of information between the other subsystems and users.			
OPS Processor/ Experiment Processor	Provides computational/ logical manipulation capability for all data processing.	Open/short electronics resulting in erroneous output.	a. Single failures: No effect due to redundancy. b. Multiple failures: Loss of data processing capability.	a. None b. Loss of multiple functions, including attitude control.
Main Memory	Storage of data requiring rapid access time.	Open/short electronics resulting in erroneous output; Head failure Tape drive failure Tape failure.	a. Single failures: No effect due to redundancy. b. Multiple failures: Loss of data processing capability.	a. None b. Loss of multiple functions, including attitude control.

Table 3-2. Space Station Failure Effect Analysis (cont)

SUBSYSTEM: Data Management

Item	Function	Failure Effect On		Space Station
		Failure Type	Subsystem	
Bulk Storage Unit	Provides large volume data storage with relatively slow access time.	Open/short electronics; head failures; tape drive failure. Tape failure.	a. Single failures: No effect due to large capacity available.	a. None
			b. Multiple failures: Reduction in amount of experiment data that can be retained. Inability to store.	b. Degraded experiment capabilities. Possible loss of data.
Memory Switch Matrix	Controls access of processors to memory.	Open/short electronics resulting in erroneous output.	a. Single failures: No effect due to redundancy.	a. None
			b. Multiple failures: Loss of data processing capability.	b. Loss of multiple functions including attitude control.
Data Bus Switch Matrix Bus Controller	Controls interface between processors and data bus.	Open/short electronics resulting in erroneous output.	a. Single failures: No effect due to redundancy.	a. None
			b. Multiple failures: Loss of data processing capability	b. Loss of multiple functions including attitude control.

3.4.1 SPACE STATION SUBSYSTEMS

From the baseline DMS, the LRUs were defined and partitioned from the physical and functional considerations relative to each respective subsystem.

3.4.1.1 Functional Partitioning

Primary selection was generally on the basis of functional fault isolation capabilities. An approach was taken (Section 6.1, Volume II of Final Report, Task 1) whereby automatic (OCS) or semiautomatic (OCS/manual) methods could be employed to diagnose and isolate subsystem faults to a reasonable functional level. This functional level was chosen on the basis of experience and familiarity with the subsystem. The approaches presented in Section 6.1 could be expanded to greater levels of detail, even to the individual piece part level, but the requirements in terms of hardware and software necessary to implement these would increase exponentially. A reasonable rationale for the determination of the level of functional partitioning was defined as that functional level which is required for the intended normal operation of the subsystem without the necessity for considerable built-in test circuitry. Some functional LRUs defined herein include a degree of self-check capability. This was found to be required in terms of implementing the functional diagnostic/isolation approach derived without postulating additional separate "test boxes."

3.4.1.2 Physical Partitioning

Consideration was also given to the physical aspects of LRU definitions, in terms of the standard electronic book module defined in DRL 13, Volume I, Book 2. It appears that such a module, or a basic group of several modules, would be an ideal LRU in respect to replacement, logistics, ease of handling, etc., considerations. Indications are that a majority of the LRUs presented herein could be packaged in one or more "basic" modules. The Remote Data Acquisition Unit (RDAU) and Local Monitor and Display Unit (LMDU) electronics appear to be the smallest defined LRUs and would probably be packaged two to a basic module. These assessments are based on initial unit power estimates and module capabilities in addition to a "subjective" sizing of the circuitry required for a particular function. In the Command/Control and Display Consoles (CCDC), consideration was given to the packaging aspects of the control and display assemblies. These assemblies would be treated as separate LRUs, along with all their associated electronic circuitry. Due to the peculiar nature (keyboards, display lights, etc.) of these assemblies in respect to a "basic" module, they would be packaged as separate removable units. This would greatly enhance the isolation and maintainability of these assemblies.

3.4.1.3 Functional LRU Definition

In order to define a workable fault diagnostic/isolation scheme certain hardware requirements and subsystem functional diagrams were postulated. These requirements and functional diagrams are reasonable, in view of present and future technology, and are in concert with the overall baseline DMS philosophy. A detailed description of certain of these functional elements can be found in Section 3 "Baseline Subsystem Descriptions." The other functional elements are described in DRL 13, Volume I, Book 2, Space Station Electronics.

3.4.1.3.1 Computer Subsystem

The overall Computer Subsystem is comprised of the following functional elements:

- Operations Multiprocessor
- Experiment Multiprocessor
- Shared Memories
- Bulk Data Storage

The multiprocessor elements can be further broken down into the following elements, each of which is considered a functional LRU:

- Data Bus Controller (DBC) - A device, not unlike a data bus terminal, which is used by the DMS/OCS multiprocessors to issue commands to and receive data from the data bus.
- Switch Matrices - These are multiple channel switching circuit complexes which are completely transparent to any coding scheme.
- Input/Output Circuitry - These are multiple channel interface circuits which perform parity checks on all incoming data.
- Logic and Control Circuitry - This is the main arithmetic-control element of the CPU.
- Dedicated Memory - This is a memory which is peculiar to a given CPU. It cannot be addressed directly from any other DMS/OCS element. It is a high speed rapid access element which is used to store the immediate operating and executive routines for that CPU.
- Power Supply and Distribution - This power source provides all required operating power for the I/O, logic and control, and dedicated memory.

The shared memories, main and auxiliary, can be broken down to a lower level of isolation (LRU definition) by supplementing the automatic diagnostics described in Section 6.1 of the Task 1 Final Report with manual procedures.

The following replaceable elements should be considered as actual LRUs.

- Electronics section - Contains I/O, logic, control circuitry, etc.
- Mechanical section (where applicable) - Contains disk drives, tape transports, etc.
- Memory element - Contains solid-state memory, disks, magnetic tape reels, etc.
- Power section - Contains power supplies, distribution, etc.

The bulk data storage elements can be further broken down into the following elements, each of which is considered a functional LRU:

- Digital Buffer and Control (DBC) - This unit provides the input/output and control functions for the bulk data storage facility. It decodes commands from the CPU and sets up the proper write/read channels through the various switch matrices.
- Record/Reproduce Electronics (R/R) - This element is a multichannel, switchable write/read unit. It conditions the data for transferral to and from the magnetic tape storage medium.
- Switch Matrices - These are multiple-channel switching circuit complexes which route signals (data or control) to appropriate hardware elements.
- Tape Transport Controller (TC) - These are the control circuits for the individual tape transports. They provide all the required read/write tape control under command from the DBC.
- Tape Transports (TT) - These are the magnetic tape drives. The tape drive motors and associated electromechanical elements comprise these units.
- Power Supply and Distribution - These units provide all the required power for the bulk data storage facility, with the exception of the DBT.

3.4.1.3.2 Data Acquisition

The Data Acquisition Subsystem is comprised of the following elements, each of which is considered a functional LRU.

It should be noted that the sensor assembly and the function under test are integral parts of the subsystem/experiment group and as such are not considered as data acquisition elements.

- Data Bus Terminal (DBT) - A device used to interface various subsystems and experiments (including RDAU and LMDU) to the data bus.

- Remote Data Acquisition Unit (RDAU) - This unit accepts analog and discrete inputs from various subsystems/experiments, converts these input to digital data, and interfaces directly with a data bus terminal.

- Stimuli Generation Unit (SGU) - This device, upon command from a data bus terminal, provides different calibrated signals (stimuli) to various subsystems/experiments. This is the only unit which is used primarily for diagnostic purposes.

3.4.1.3.3 Command/Control and Display

The Command/Control and Display Console (CCDC) is comprised of the following assemblies:

- Alphanumeric Display Assembly - Display for computer-generated digital data.

- Status Light Assembly - Display for computer-generated digital data. Used to indicate operational conditions.

- Dedicated Displays - Contingency displays hardwired to appropriate subsystems/experiments.

- Command Buffer and Control Unit - Provides control for the digital multiplexer in addition to buffering all the commands from the CCDC control panels. Contains a self-test feature.

- Digital Multiplexer - Combines all the CCDC control commands for inputting to the Command Buffer and Control.

- Hand Controller Assembly - Used for providing continuously variable human input information to the computer. Used in conjunction with the Mode Select Switches.

- Mode Select Switch Assembly - Used to establish the logic that determines the function of the multifunction pushbuttons.

- Multifunction Switch Assembly - Provides for the single selection of a group of commands.

- Monofunction Switch Assembly - Provides for the selection of individual commands.

- Computer Keyboard Assembly - Used for directing computer operations or modifying/correcting existing software routines.

These assemblies can be further broken down into the following elements which are considered as functional LRUs.

- Display Control and Buffer Unit - Provides control for the Display Switch Matrix in addition to buffering all display data to the CCDC.

- Display Switch Matrix - A multichannel switching matrix which routes display data to the appropriate displays.

- Refresh Buffer - Provides the necessary storage capability for the CRT displays.

- Display Control - Provides the primary control of what is being displayed on the CRTs. Can select between digital data or analog information for display. Control of video/Command Control television (CCTV) on the CRT displays is provided by this function.

- CRT Display Assembly - An integral unit containing the CRT and all necessary video control functions.

- Warning Annunciator Assembly - Contains an integral audio alarm along with all required visual displays for critical warning function alarming.

- Caution Display Assembly - Display for all critical caution functions.

- Discrete Controls - Contingency controls hardwired to appropriate subsystems/experiments.

- Microfilm Viewer Assembly - This unit provides the means to view stored microfilms.

- Microfilm Viewer Control - Provides the required control for microfilm retrieval and viewing.

- Microfilm File - Microfilm storage.

- Analog Interface Unit - This unit provides the capability for analog information (CCTV video, intercom audio, etc.) to be transferred to and from the CCDC. It interfaces the data bus with the CCDC circuitry.

- Channel Select and Analog Control - This unit provides the channel selection capability for CCTV and intercom distribution in addition to providing control for all CCDC analog functions.

- CCTV Panel Assembly - Primary setup and control point for all Space Station CCTV distribution.

- Intercom Control Panel - Primary setup and control point for all Space Station intercom distribution.

- Audio Tape Assembly - Audio tape control and deck assembly.

- Video Tape Assembly - Video tape control and deck assembly.

- Illumination Control Assembly - Provides Space Station ambient light control in addition to CCDC panel illumination and lamp test capabilities.

- CCDC Power Supplies - These units provide all the required power for the CCDC. An overall power system rationale has yet to be developed.

The Portable Display and Control Unit (PDCU) is comprised of the following elements all of which are considered functional LRUs.

- Display Assembly - Contains the refresh buffer, CRT display control, and CRT display assembly

- Computer Keyboard Assembly

- Optional Pluggable Features
  - Hand controller assembly
  - Multifunction switch assembly

- Power Supply - Provides all required power for the PDCU

3.4.1.3.4 Image Processing

The Image Processing Subsystem is comprised of the following elements, which are considered functional LRUs.

- Display Control - Provides the primary control of what is being displayed on the CRTs.
- CRT Display Assembly
- Film Viewer - Provides the capability to manually view processed films. Consists of a screen for viewing or scanning, controls, and frame counter.
- Film Scanner - Transforms film images into electrical analog signals.
- Image Digitizer - Converts analog signals from the film scanner and vidicon outputs into digital data.
- Adjustable Multichannel Filter - Provides the analog processing capability. The working analog storage function is an integral part of this unit.
- Permanent Analog Storage - Provides tape recording capability for the storage of analog data.
- Analog Control Assembly - Provides all the required control for the operation of the adjustable multichannel filter, display control, and permanent analog storage in respect to analog image data.
- Digital Control Assembly - Provides all the required control for the various digital components in the subsystem.
- Working Digital Storage - Provides a rapid access storage capability for digital information via the digital control assembly or the Data Bus Terminal.
- Permanent Digital Storage - Provides tape recording capability for the storage of digital data.
- Display Conversion - Used to convert digital data received from the computer into analog signals for viewing on the CRTs.
- Annotation and Editing Assemblies - Provides the capability for annotating and editing processed film, digitized images, or analog information. Specific hardware requirements for these functions have yet to be defined.

3.4.1.3.5 GN&C Preprocessors

A typical functional diagram for the GN&C preprocessors is shown in Figure 3-1. This figure is intended to be representative of the five GN&C preprocessors. These GN&C preprocessor elements are simplex dedicated digital computers with self-test capability, and are considered functional LRUs.

3.4.1.4 LRU Definition

The LRUs defined in this section are listed in Table 3-3 by their respective subsystems and are a result of the degree in which a software/hardware system (OCS) can effectively isolate malfunctioning elements (see Section 5) in addition to the physical considerations of packaging and accessibility within a given equipment complex.

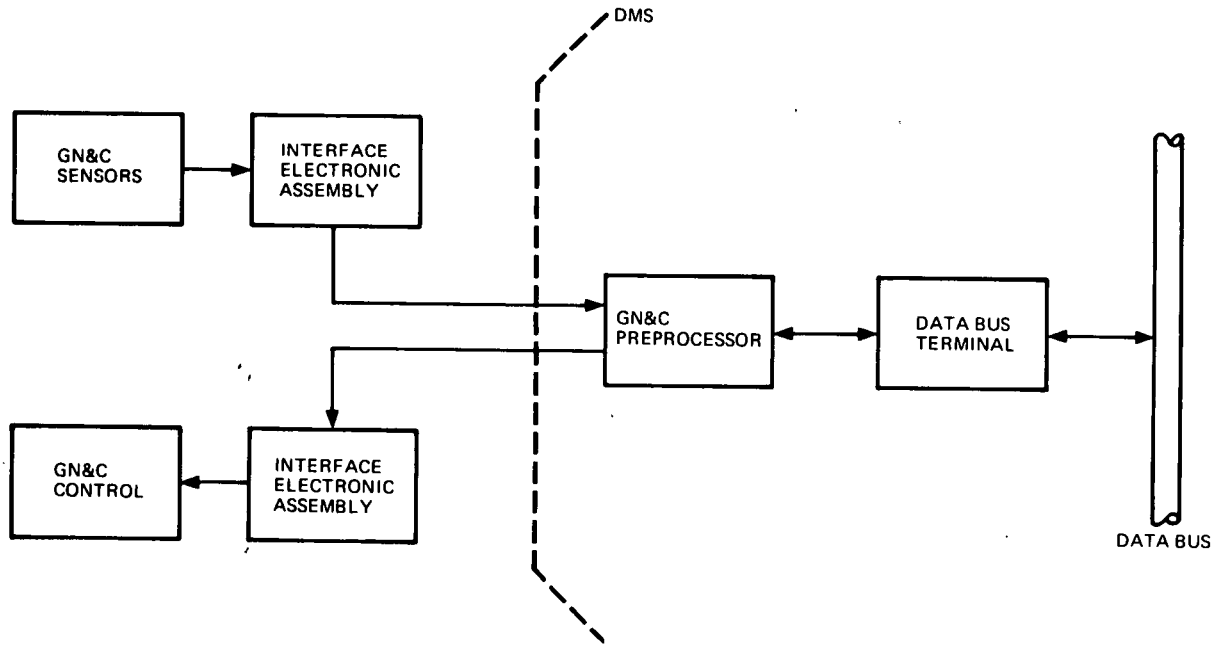


Figure 3-1. GN&C Preprocessor Typical Functional Diagram

Table 3-3. Data Management Subsystem

Item	Quantity
Computer Subsystem	
Data Bus Controller	2
Data Bus Switch Matrix	2
Memory Switch Matrix	2
Data Bus I/O	2
Shared Memory I/O	2
CPU Logic and Control	6
Dedicated Memory	6
CPU Power Supply	6
Shared Memory Electronics Section	2
Shared Memory Mechanical Assembly	2
Memory Elements	16
Shared Memory Power Supply	2
Bulk Data Storage	
Digital Buffer and Control	4
Record/Reproduce Electronics Assembly	4
Transport Switch Matrix	4
Controller Switch Matrix	4
Tape Transports	4
Tape Transport Controllers	4
Bulk Data Storage Power Supply	4
Data Acquisition	
Data Bus Terminal	30
RDAU (or LMDU)	250
Stimuli Generation Unit	40
Command/Controls and Display	
Display Control and Buffer	2
Display Switch Matrix	2
Refresh Buffer	2
Display Control	2
CRT Display Assembly	2
Warning Annunciator Assembly	2
Caution Display Assembly	2
Alphanumeric Display Assembly	2
Status Light Assembly	2
Dedicated Displays	2

Table 3-3. Data Management Subsystem (Continued)

Item	Quantity
Command Buffers and Control	2
Digital Multiplexer	2
Hand Controller Assembly	2
Computer Keyboard Assembly	2
Mode Select Switch Assembly	2
Multifunction Switch Assembly	2
Monofunction Switch Assembly	2
Discrete Controls	2
Microfilm Viewer Assembly	2
Microfilm Viewer Control and File	2
Analog Interface Unit	2
Channel Select and Analog Control	2
CCTV Panel Assembly	2
Intercom Control Panel Assembly	2
Audio Tape Assembly	2
Video Tape Assembly	2
Illumination Control Assembly	2
CCDC Power Supplies	2
Portable Display and Control Units	
Display Assembly	4
Computer Keyboard Assembly	4
Optional Pluggable Functions	4
Power Supply	4
Image Processing	
Display Control	1
CRT Display Assembly	1
Film Scanner	1
Film Viewer	1
Image Digitizer	1
Adjustable Multichannel Filter	1
Permanent Digital Storage	1
Working Digital Storage	1
Permanent Analog Storage	1
Digital Control Assembly	1
Analog Control Assembly	1
Display Conversion	1
Annotation and Editing	1
GN&C Preprocessors	
GN&C Preprocessor	5

Section 4

OCS CHECKOUT STRATEGIES

4.1 SUBSYSTEM CHECKOUT STRATEGY

Prior to any further requirements analysis, it is necessary to develop a checkout strategy for all Space Station subsystems to meet the checkout objectives of the Space Station OCS. The objectives of the Space Station OCS can be summarized as follows:

- To increase crew and equipment safety by providing an immediate indication of out-of-tolerance conditions
- To improve system availability and long-life subsystems assurancy by expediting maintenance tasks and increasing the probability that systems will function when needed
- To provide flexibility to accommodate changes and growth in both hardware and software
- To minimize development and operational risks

Specific mission or vehicle-related objectives which can be imposed upon subsystem level equipment and subsystem responsibilities include the following:

- OCS should be largely autonomous of ground control.
- Crew participation in routine checkout functions should be minimized.
- The design should be modular in both hardware and software to accommodate growth and changes .
- OCS should be integrated with, or have design commonality with, other onboard hardware or software .
- The OCS should use a standard hardware interface with equipment under test to facilitate the transfer of data and to make the system responsive to changes.
- Failures should be isolated to an LRU such that the faulty unit can be quickly removed and replaced with an operational unit.

- A Caution and Warning System should be provided to facilitate crew warning and automatic "safing" where required.

- Provisions must be included to select and transmit any part or all of the OCS test data points to the ground.

To attain these objectives via the use of an Onboard Checkout System which is integrated with the Data Management System, checkout strategies have been developed which are tailored to each Space Station subsystem.

Special emphasis has been applied to a strategy for checkout of redundant elements peculiar to each subsystem. The degree to which each of these functions is integrated into the DMS is also addressed.

4.1.1 SPACE STATION SUBSYSTEMS

Each major Space Station subsystem was examined with respect to the required checkout functions. The checkout functions associated with each subsystem are identified and analyzed as to their impact on the onboard checkout task. The functions considered are those necessary to verify operational status, detect and isolate faults, and to verify proper operation following fault correction. Specific functional requirements considered include stimulus generation, sensing, signal conditioning, limit checking, trend analysis, and fault isolation.

4.1.1.1 Data Management Subsystem (DMS)

The testing of the DMS will involve principally a series of software programs designed to exercise the DMS group in a normal subsystem configuration. If there is a failure in one of the units, the OCS must isolate the failure, reconfigure the DMS Subsystem to restore normal operation, alert the crew of the failure and its location, and record the event. Given that a unit has been replaced, the OCS must maintain knowledge of the operational status of the new unit.

Within the DMS, each functional unit must be tested. This means that there must be at least CPU type tests, main store tests, bulk memory tests, bus controller tests, etc. Since there exists more than one path to perform certain functions in the subsystem configuration, it is important to verify that intercommunications among units also exists. This requirement gives rise to interface tests. Some of the interfaces which exist include CPU-to-CPU, CPU to both main and bulk memories, CPU to primary and secondary bus controllers, bus controllers to terminals, terminals and RDAUs, and RDAUs to individual subsystems. The fact that the many communication paths are possible generates the requirement that a path must be switchable or alterable to restore operation. Determining which path must be altered indicates that a fault isolation capability also must exist. Fault isolation may occur by commanding tests to various equipment in a sequence such that the analysis of the pattern of responses logically leads to a faulty piece of equipment. The maintenance of continuous knowledge of the operational status of the equipment can be translated into the requirement to maintain a subsystem status table (or configuration table) in software. If the operator is to be involved in any actions, interactive crew/display/software tests are required.

4.1.1.1.1 DMS Test Methods

The DMS checkout will consist principally of software diagnostics supplemented with additional temperature, voltage, and logic measurements.

- Central Processing Units - Error detection and isolation in the central processing units depend on diagnostic software. In the multiprocessing configuration, one central processor can be utilized to check another central processor. This can be accomplished through memory or through a direct interface. In addition, parity checking can be implemented between interfaces of the central processor with other units.

- Main Store Units - The main store units can be checked periodically by attempting to address all locations in each unit, performing ripple tests, sum checks, etc. BITE capabilities in the form of parity checking will occur on data read from storage and data presented by the central processors. Parity checking will be the principal means of error detection.

- Data Bus Controller - The data bus controller is the communication path between memory and central processor and the data bus. Verifying operation of the controller can be implemented by software diagnostics. BITE hardware can be incorporated, which upon command from the CPU, inserts a known serial data word (pattern) into the input side of the controller and transmits the word back to the CPU. The CPU can compare the response to the command word.

- Digital Data Terminals - The digital data terminal interfaces the various subsystems/experiments and the data bus. The terminal can be tested much like the bus controllers. A self-check feature in the form of BITE can be added which routes calibrated signals through the unit to the CPU (via the data bus) for verification.

- RDAU - The RDAU can be tested in the same manner as the bus controllers and data terminals. The RDAU contains 32 analog inputs and 32 digital inputs. One input of each type can be reserved to wrap around an analog or digital signal into the input for return to the CPU. The CPU would command the test voltage or signal and examine the response for known conditions.

- Local Monitor and Display Unit (LMDU) - The LMDU electronics will be checked in an identical manner to the RDAU. The displays will require crew participation.

- Command and Display Consoles - The controls and displays associated with the consoles are subjected to a form of continuous test through normal use. For the displays, standard test patterns containing all the symbols and numerics presented to the crew will verify operation of display and symbol generation. The controls are exercised through the normal equipment utilization.

- Image Processing - Tests for the image processing equipment will consist primarily of supply voltage and analog measurements for which an interface via an RDAU should be provided to the DMS computer. Optical equipment is tested through normal use. Integral diagnostics should be included with the special purpose processors such that the diagnostics can be commanded from the DMS computer.

- Bulk Storage - The basic operation of bulk memory can be verified by writing-reading random length records of predefined data patterns and checking the response for correctness. The basic capabilities of writing, sensing, reading forward and backward, I/O test, and control will be verified via this technique. Error detection through parity checking also will be performed throughout the test.

- GN&C Preprocessor - Built-in test equipment is assumed to be applicable. Since the preprocessors are not yet defined, the form of BITE is yet to be determined.

- OCS Measurements - In addition to the software diagnostics and BITE provisions which can be incorporated into the OCS, a series of measurements must be made on certain equipment. Some of the units may be temperature sensitive, which will generate a requirement to monitor the temperature. Most of the units also will contain an integral power supply or converter which must be monitored. There also may be certain logic which must be monitored.

  The measurements which are required fall into three categories. These include:

  a. Analog

  b. Digital/discrete

  c. Visual

The analog measurements will consist primarily of temperature and power supply voltages. The digital or discrete signals will be checked through software analysis of state or patterns. Visual inspections could be a visual analysis of a display, a pulse train or pulse shape - visual inspection may be more appropriate in performing adjustments, but it represents a form of measurement which may be required.

4.1.1.1.2 OCS Computer Program Segments

The operational and maintenance requirements indicate that two levels of testing or test control are required. Depending on the type of test being exercised, different information will be extracted and different actions will result from the testing. Two major sets of computer programs have been identified to perform this testing. Within each program there are several modules required to extract the desired information. The two test levels identified which translate into computer programs include:

- Continuous orbital monitoring (COM)

- Subsystem Fault Isolation (SFI)

The continuous orbital monitoring program is required to maintain cognizance of equipment's operational status at all times and to isolate failures in order to reconfigure the equipment. The continuous monitoring program can be hardware or software. The hardware can consist of Caution and Warning or of a machine check interrupt from parity error or power transients. The software

program would consist of a set of test programs performed iteratively and concurrently with the application programs. The test programs would be interleaved with the application programs, and performed at a rate determined by the executive. The subsystem fault isolation program would be designed to perform more extensive testing than would be performed in the "continuous" program.

4.1.1.1.3 Test Program Modules

Each of the two major program sets will contain several modules to perform specified functions. These are discussed in the following paragraphs.

4.1.1.1.3.1 Continuous Orbital Monitoring Program Modules

The continuous orbital monitoring modules will consist of the DMS test programs (e.g., CPU, memory addressing, I/O operation, etc.), the polling of test points, and a Caution and Warning module.

- Test Program Modules - The test programs are designed to verify operation of individual configurable elements. The rationale for this is to maintain continuous configuration control, necessitating periodic information regarding the operational status of all configurable elements comprising the DMS group. These test modules will be designed to exercise as much of each LRU as possible in the allocated time. The modules will confirm, for example, fundamental operations of the CPUs, main memory, bus control, terminals, etc.

- Test Point Polling - The test point polling module is required to sample voltages, temperatures, and logic patterns for out-of-tolerance conditions or pattern errors. The test points can be handled singly or in blocks.

- Caution and Warning - A Caution and Warning module is required to monitor critical signals on a continuous basis. This module may be implemented through selective parts of the two modules above; i.e., through execution of selective diagnostics or through the polling of selective test points.

4.1.1.1.3.2 Subsystem Fault Isolation Modules

Listed below are candidate program modules which would comprise the Subsystem Fault Isolation program. These change with regard to the number of modules or because of a merging of responsibilities. The list includes:

(1) Failure verification/isolation modules

(2) Failure event analysis module

(3) Reconfiguration module

(4) Subsystem status table

(5) Display/Record/Telemetering Module

(6) Repair verification modules

- Fault Verification/Isolation Modules - Failure verification/isolation modules are designed to resolve failures to the level at which redundancy is applied (for reconfiguration purposes) and to the LRU level to support the on-line remove-and-replace maintenance philosophy. Subsequent to the detection of an error, anomaly, or failure, it may be necessary to verify via an independent path, that an event has occurred or that a particular path is disabled. This may be accomplished by performing a separate routine or by correlating results from other routines. The isolation modules will be executed in whatever sequence is necessary to resolve the failure to a reconfigurable path.

- Failure Event Analysis Module - Failure event analysis modules are designed to evaluate the event in terms of criticality, failure history, active/inactive status, etc. Based on an FMEA, hazards studies, etc., failures can be classified into certain groupings; e.g., critical items, time critical items, items involving crew actions, items automatically switched through internal BITE, etc. When an event occurs, it is necessary to evaluate the source of the event (whether OCS or LRE BITE), the criticality of the function lost and whether the crew must be involved in any subsequent actions, the redundant paths available and their status with regard to power on/off, failure history, etc.

- Reconfiguration Modules - Reconfiguration modules are designed to initiate and execute the sequence of operations necessary to reconfigure the subsystem. Depending on the source of the failure, different procedures may be involved in reconfiguring the equipment. The recon-

figuration can occur in software or it can be a physical switching of redundant paths. These modules will be required to execute the unique actions associated with each LRU, path, function, or subsystem.

- Subsystem Status Table - The subsystem status table is designed to maintain the status of all DMS reconfigurable elements. To prevent the switching or reconfiguring of faulty equipment, it is necessary to maintain a subsystem status table of all equipment. In the event of a failure, the subsystem status table must be analyzed with respect to the failed element to determine if a redundant path is available. Subsequent to the remove-and-replace of the faulty LRU and the successful completion of an LRU test module, the subsystem status table would be updated.

- Display/Record - Display/record is designed to provide interactive display/control with the crew and to provide an event history file. In order to provide prompting information and to provide interactive capabilities between OCS and crew, display formats (or messages) containing such information will be required. In addition, an event history should be maintained for ground processing and analysis (logistics, provisioning, long term trend data, etc). The capability for telemetering any or all test data also will require certain provisions.

- Repair Verification/Adjustment - The repair verification/adjustment is designed to verify proper operation of LRUs subsequent to repair. Special repair verification or adjustment modules may be required to re-verify an LRU or to perform LRU adjustments. These tests may not be as extensive as the failure verification/isolation modules, but could contain certain segments of the diagnostic modules.

4.1.1.1.4 Computer Program Top Level Flow

The Multiprocessor Executive System must provide certain times, on a scheduled basis, during which DMS tests can be performed. The executive may or may not subdivide the DMS tests depending on computer load at the time or on the duration required to perform certain test sequences. Subsequent to DMS tests, the experiment module tests or particular subsystem tests can be performed. At specified intervals, the executive must return to the regular application programs.

If during the DMS tests, a failure is detected, it must be resolved or isolated to an LRU or to a data path that is reconfigurable. The output of the LRU and interface tests is a system reconfiguration, display message to the crew, a recording of the event, and an update of the subsystem status table.

4.1.1.1.5 DMS Redundant Element Checkout Techniques

The control of redundancy within the DMS will be a software function principally and can be implemented through the LRU diagnostics within the Subsystem Fault Isolation Program. The redundancy control function consists of detecting errors or failures and isolation of the failure to a reconfigurable path. The general case of redundancy control is considered initially.

An output from a single function is acquired by one of two RDAUs (one designated as "prime" and the other as "secondary"). The RDAU will perform some processing to the function and feed the information to its respective digital data terminal. From the terminals, the data is fed to the computer via one of two data bus controllers (again, one is designated as "prime" and one "secondary"). Control of redundancy within the computer will depend on diagnostic software. Individual CPU diagnostics can be performed and cross checking of one CPU by the other CPU is possible. Cross checks can be implemented through check words in memory or through a direct control interface. If one CPU is determined to be at fault, the other CPU can assume the load. With regard to memory, each main store unit can be checked periodically by diagnostic software. BITE in the form of parity checking will play a significant role in error detection and isolation on data read from memory to the CPU or to the data bus controller.

The control of redundancy in the data acquisition path can be implemented by the incorporation of BITE within data acquisition elements and through software. Figure 4-1 shows a method of isolating and reconfiguring the data acquisition elements. If an out-of-tolerance event or failure indication occurs, it can be true or it can be a false alarm. By performing an RDAU test, the RDAU can be absolved of the responsibility or determined to be the source of the problem. If the RDAU is faulty, the data point has an alternate path through the secondary RDAU. If after performing the RDAU test (which indicated failure) the same indication prevails through the secondary RDAU, the failure is between the RDAU and the CPU. By alternately addressing data acquisition test command between primary and secondary elements, a logical isolation and reconfiguration pattern can be developed (as shown in Figure 4-1). This procedure would isolate to a replaceable unit.

Redundancy at the RDAU/sensor level for the baseline has three configurations. The most critical signals (warning signals) have duplicate sensors and two independent paths to the data bus. The next level signals (caution signals) also have duplicate sensors and two paths to the data bus, but these paths are somewhat different from those for the warning signals. The third level of signals has a single sensor source, but has two separate RDAU paths to the OCS processors. The redundant sensors and redundant paths afford point-to-point correlation of data in the case of anomalies. In the case of warning signals, the data is fed to the CCDC and data bus through an LMDU and to the bus through an RDAU

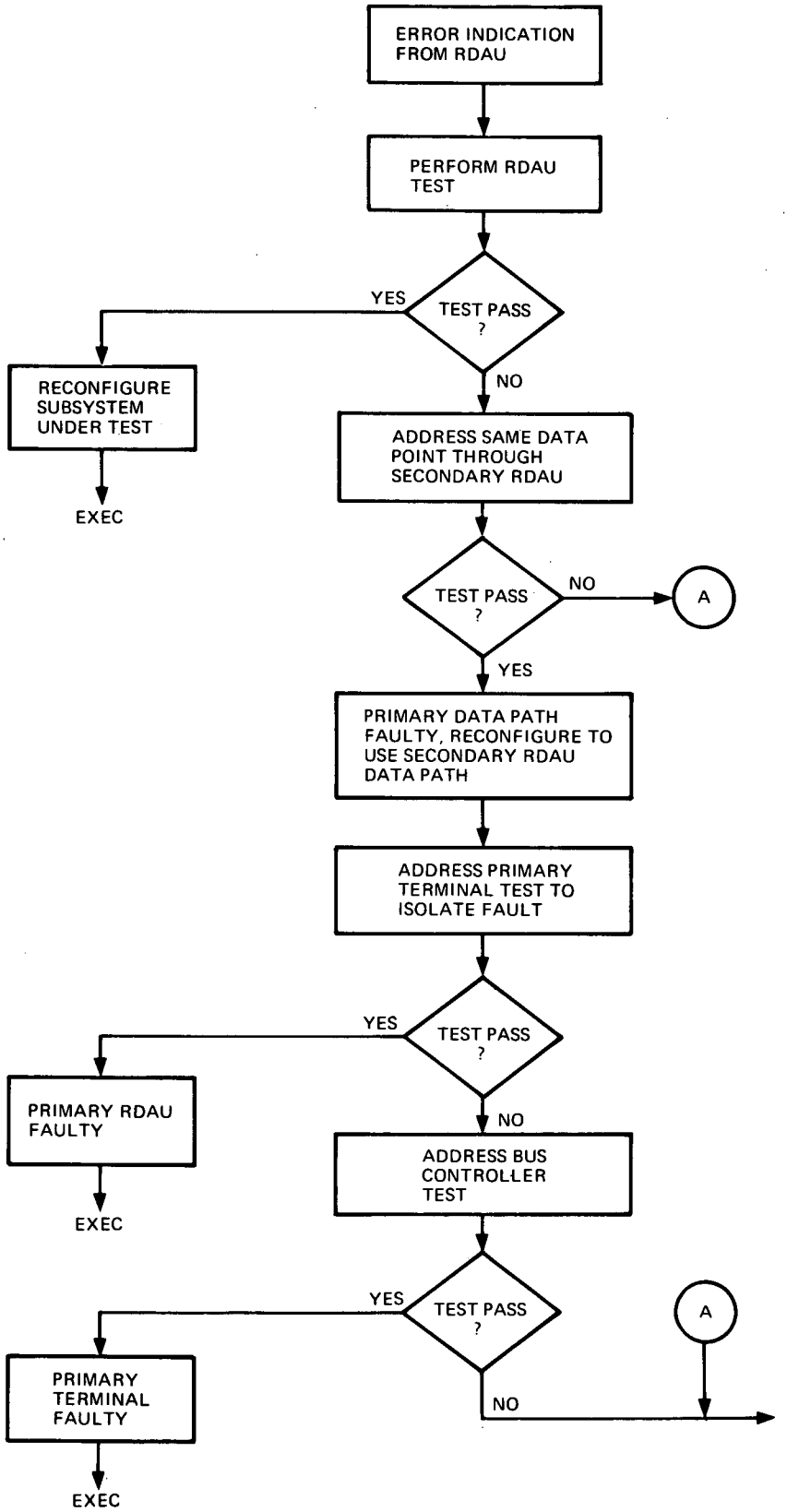


Figure 4-1. Data Acquisition Configuration Control

and terminal. If an out-of-tolerance indication exists, it is possible to address the alternate source and verify the condition. This technique also makes heavy use of software for configuration control.

4.2 INTEGRATED CHECKOUT STRATEGY

This analysis identifies the integrated checkout functions associated with Space Station subsystems during the manned orbital phase of the mission. These functions are depicted in Figure 4-2 and are those required to ensure overall availability of the Space Station. Characteristic of integrated testing is the fact that the test involves subsystem interfaces, and, therefore, test objectives are associated with more than one subsystem.

4.2.1 INTEGRATED STRATEGY

Six checkout functions have been identified:

- Caution and warning
- Fault detection
- Trend analysis
- Operational status
- Periodic checkout
- Fault isolation

These functions represent a checkout strategy of continuous monitoring and periodic testing with eventual fault isolation to a line replaceable unit (LRU). Under this aspect the functions are grouped as -

CONTINUOUS MONITORING	PERIODIC TESTING	FAULT ISOLATION
• Caution and warning	• Automatic tests	• Localize to SS
• Fault detection	• Operational Verification	• Isolate to RLU
• Trend analysis		
• Operational status		

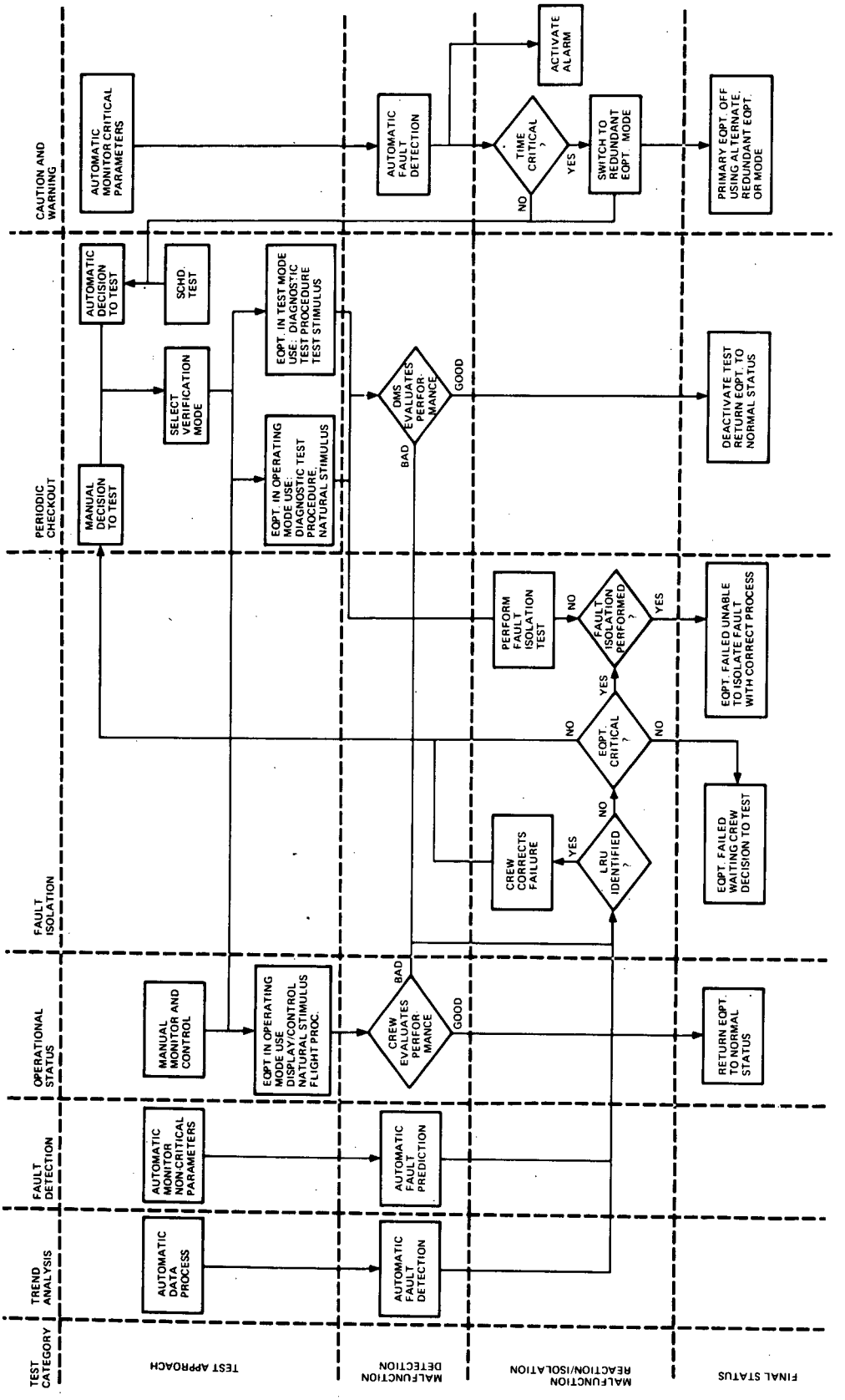


Figure 4-2. Integrated Checkout Functional Flow

General characteristics of these groups are defined below:

4.2.1.1 Continuous Monitoring

Continuous monitoring is not a test per se. It is a concept of continuously sampling and evaluating key subsystem parameters for in/out-of-tolerance conditions. This evaluation does not necessarily confirm that the subsystems have failed or are operating properly. The evaluation is only indicative of the general status of the subsystems. For example, a condition exists where the integrated subsystems are indicating in-limit conditions, but during the next series of attitude control commands, an error in Space Station position is sensed and displayed. Since three subsystems, DMS, GN&C, and P/RCS, are involved in generating and controlling the Space Station attitude, a "positional error" malfunction is not directly related to a subsystem malfunction. The malfunction indication is only indicative of an out-of-tolerance condition of an integrated function. Final resolution of the problem to a subsystem and eventually to LRU will require diagnostic test-procedures that are separate from the continuous monitoring function.

There are situations in which the parameters being monitored are intended to be directly indicative of the condition of a subsystem or an LRU. Examples of these include tank pressures, bearing temperatures, and power source voltages. However, even in these simpler cases when a malfunction is detected, an integrated evaluation will be performed to ascertain that external control functions, transducers, signal conditioning, and the DMS functions of data acquisition, transmission, and computation are performing properly. This evaluation will result in either a substantiation of the malfunction or identification of a problem external to the parameter being monitored.

Figure 4-2 shows the logic associated with each function in the continuous monitoring group, as well as the integrated relationships between these and the total checkout functions. The caution/warning and fault detection functions are alike in their automatic test and malfunction detection approaches, but are different in terms of parameter criticality and malfunction reaction. The caution/warning function monitors parameters that are indicative of conditions critical to crew or equipment safety. Parameters not meeting this criticality criteria are handled as fault detection functions. Figure 4-2 shows that in the event of a critical malfunction, automatic action is initiated to warn the crew and sequence the subsystems to a safe condition. Before this automatic action is taken, the subsystems must be evaluated to ascertain that the failure indication is not a false alarm and that the corrective action can be implemented. After the action is taken, the subsystems must be evaluated to determine that proper crew safety conditions exist. Since automatic failure detection and switching can be integral to subsystem design (self-contained correction) and subsystems can be controlled by the operational software or manual controls, it is imperative that the status of these events be maintained and that the fault detection and correction software be interfaced with the prime controlling software. For malfunctions that are not critical, the crew is notified of their occurrence, but any subsequent action is initiated manually.

The next continuous monitoring function, trend analysis, automatically acquires data and analyzes the historical pattern to determine signal drift and the need for unscheduled calibration. It also predicts faults and indicates the need for diagnostic and fault isolation activities. An example of a parameter in this category is the partial pressure of nitrogen. Nitrogen is used to establish the proper total pressure of the Space Station. Since it is an inert gas, the only make-up requirements are those demanded by leakage or airlock operation. The actual nitrogen flow rate is measured, and calculations are performed which make allowances for normal leakage and operational use. When these calculations indicate a trend toward more than anticipated use, the crew is automatically notified and testing is initiated to isolate the problem to the gas storage and control equipment or to an excessive leak path. The historical data is not only useful in predicting conditions but is also useful in providing trouble-shooting clues. The data might reveal, for example, that the makeup rate increased significantly after the use of an airlock. This could lead directly to verifying excessive seal leakage.

The final continuous monitor function is in operational status. This function is performed by the crew and is nonautomatic with the exception of the DMS computer programs associated with normal Space Station operational control and display functions. The concept of continuous monitoring recognized and takes advantage of the crew's presence and judgment in evaluating Space Station performance. In many instances the crew can discern between acceptable and unacceptable performance, and they can clearly recognize physically-damaged equipment or abnormal conditions.

4.2.1.2 Periodic Testing

As opposed to continuous monitoring, periodic testing is a detailed evaluation of how well the Space Station subsystems are performing. Figure 4-2 shows that periodic testing is not accomplished by any one technique. Rather, a combination of operational and automatic test approaches is employed. The actual operational use of equipment is often the best check of the performance of that equipment. Operation of Space Station equipment and use of the normal operating controls and displays will be used in detecting faults and degradation in the subsystems. This mode of testing is primarily limited to that equipment whose performance characteristics are easily discernible, such as for motors, lighting circuits, and alarm functions.

Automatic testing is performed in two basic modes:

- With the subsystems in an operating mode, the DMS executes a diagnostic test procedure which verifies that integrated Space Station functions

are being properly performed under normal interface conditions in response to natural or designed stimulation. This mode of testing allows the evaluation of Space Station performance without interrupting mission operations.

- For those situations where the integrated performance or interface compatibility between subsystems cannot be determined without known references or control conditions, the DMS will execute a diagnostic procedure in a test mode. In this mode, control, reference, or bias signals will be switched in or superimposed on the subsystems to allow an exact determination of their performance or localization of problem between the interfaces. Since the test mode may temporarily inhibit normal operations, the DMS must interleave the test and operational software to maintain the Space Station in a known and safe configuration.

The scheduled automatic tests are performed to verify availability or proper configuration of "on-line" subsystems, redundant equipment, and alternate modes.

- Periodic Verification of "On-Line" Subsystems - The first checkout requirement is a periodic verification that on-line subsystems are operating within acceptable performance margins. The acceptable criteria for this evaluation is based on subsystem parameter limits and characteristics exhibited during Space Station factory acceptance or pre-flight testing. The rejection criteria and subsequent decision to repair or reconfigure subsystems is based on the criticality of the failure mode. If the subsystems appear to be operating properly, but the test clearly indicates an out-of-tolerance condition, then one of the following alternatives must be implemented:

  - If the failure mode is critical, the crew normally takes immediate action to isolate and clear the problem.

  - If the failure mode is not critical, the crew can take immediate action, schedule the work at a later time, or wait until the condition degrades to an unacceptable level.

- Redundant Equipment Verification - A second checkout requirement is verifying that standby, off-line, or redundant equipment and associated control and switching mechanisms are operable. The acceptable/rejection criteria for these evaluations is identical to those for normally operating equipment. A primary distinction of this function is that equipment may have known failures from previous usage or tests. This situation occurs when the crew has knowledge of a failure but has not elected to perform the necessary corrective action. The checkout

function then becomes one of equipment status accounting and maintenance/repair scheduling. The status information is interlocked with mission procedures and software to preclude activation of failed units while they are being repaired or until proper operation following repair is verified.

- Alternate Mode Verification - The third checkout function is verifying the availability of alternate modes of operation. This function is essentially a confidence check of the compatibility of subsystems' interaction and performance during and after a change in the operating mode. To some extent this function overlaps with redundant equipment verification, but is broader in scope in that it verifies other system-operating characteristics. For example, some modes will involve manual override or control of automatic functions or automatic power-down sequences.

4.2.1.3 Fault Isolation

Fault isolation to an LRU is a Space Station goal. As shown in Figure 4-2, fault isolation testing is initiated when malfunction indications cannot be directly related to a failed LRU. The integrated test functions associated with fault isolation are localizing a malfunction to a subsystem or to an explicit interface between two subsystems and identifying the subroutine test necessary for LRU isolation. In structuring this relationship between integrated subsystem tests for fault localization and subroutine tests for fault isolation, the DMS, in conjunction with the test procedure documentation, must establish an effective man-machine interface so that in the event of an unsolved malfunction the crew will be able to help evaluate the condition and determine other test sequences necessary to isolate the problem. To accomplish this requirement, the DMS must be capable of displaying test parameters and instructions in engineering units and language and be capable of referencing these outputs to applicable documentation or programs that correlate test results to corrective action required by the crew.

Section 5

ONBOARD CHECKOUT TEST DEFINITIONS

5.1 SUBSYSTEM TEST DEFINITIONS

The on-orbit tests required to insure the availability of the Space Station subsystems are defined herein. Also delineated are the measurement and stimulus parameters required to perform these tests. Two discrete levels of testing are defined, i.e., continuous status monitoring tests for fault detection of critical and noncritical parameters, and subsystem fault isolation tests for localization of faults to a specific Line Replaceable Unit. In addition to these two levels, tests are defined for periodic checkout and calibration of certain units, and parameters requiring analysis of trends are defined.

Due to the software module approach to DMS checkout, it was deemed necessary to estimate the CPU time and memory required to implement these modules along with an assessment of the services required from an Executive Software System to control the checkout.

These test descriptions, measurement, and stimulus information provided for each subsystem, and the software sizing information provided for the Data Management System provide the data required to estimate the checkout impact on the DMS software and hardware. Table 5-1 is a summary of the measurement and stimulus requirements for the Space Station.

Prior to defining specific tests, it is necessary to define the operating environment. It is a requirement that testing be performed on-line and that fault isolation to the LRU should be achieved to support a remove-and-replace maintenance philosophy. Operating on-line means that the testing performed must be interleaved with other application programs. Within these constraints, it is necessary to define:

(a) The provisions included to detect errors in data transfer on a continuous basis

(b) The specific actions to be taken when errors occur within individual DMS equipment

(c) The provisions included for verifying equipment operation on a periodic basis

Table 5-1. Measurement/Stimulus Summary

SUBSYSTEM	STIMULUS					RESPONSE			STATUS MONITORING								Remarks
	Analog	Bilevel	Digital	Pulse	RF	Analog	Bilevel	Digital	Total	Non-Critical	Caution	Warning	Periodic Checkout	Calibration	Trend	Fault Isolation	
Guidance, Navigation and Control	20	146	62	6		127	161	70	592	130	16		516	74	74	592	
Propulsion - Low Thrust		134				120	124		378	152	14		378	48	8	378	
Propulsion - High Thrust		126/62				287/117	123/63		536/242	80/28	33/15	14/10	536/242	259/111	117/43	482/222	Art-g/Zero-g periods
Environmental Control/ Life Support	34	111				691	280		1116	139	205	32	1116		135	1116	172 Caution/Warning Signals are for IVA/EVA
RF Communications	37	206	36		77	131	286	28	801	58			576	24	93	801	
Structures	15/16	21/19				60/53	75/66		174/154	7			123/104			174/154	
Electrical Power - TCD	52	1952				292	1292	20(1)	7608	1404	20		724		134	3608	(1) Twelve of these take pulse form
Electrical Power - Solar Array/Battery		1916				4044	928		6780	3704	12		2184		332	6788	
Data Management			53			33	188	83	357	357			62	62	62	357	
Total	151/169	4512/ 4446	151	6	77	5785/ 5628	3457/ 3388	201	14,350/ 14,035	6031/ 5979	300/282	46/42	5110/ 5902	467/ 319	935/ 861	14,266/ 14,016	

(d) The provisions included for reverifying equipment subsequent to a repair

(e) The OCS/crew interface with regard to equipment status information and maintenance

The constraint of operating on-line indicates that overall operation must occur somewhat as indicated in Figure 5-1. Concurrently with the execution of Operations and Experiment programs, the OCS programs will be implemented on a time available basis. During each of the time slots, certain portions of the OCS responsibility must be performed. Test sequencing and control will be performed by an OCS executive while overall time scheduling will be performed by the DMS executive. The execution of the tests will be asynchronous, and the time allocated will depend on the time demands of other programs.

Parity checking of all data transfer will occur during operation of all application programs. This is not sufficient to verify complete operation of the DMS - additional tests are required on functional areas on a scheduled basis during the time slots allocated to OCS. These additional tests must be short enough to be incorporated in the time slots, yet thorough enough to verify operation of the equipment under test. Parity errors, depending on the source, will prompt the running of some of the DMS tests to verify the error (see Figure 5-1). Other subsystems are polled as shown. These tests have been termed "Continuous Orbital Monitoring" tests (COM). The operation described above will be an iterative process - repeating after one complete subsystems test cycle. The tests performed during the COM tests, however, may not be sufficient to isolate an error or failure. It is anticipated that more extensive testing will be required on the DMS to isolate the failure to a reconfigurable element (e.g., the testing of all interfaces after LRU replacement). The second level of testing has been termed "Subsystem Fault Isolation" (SFI) tests.

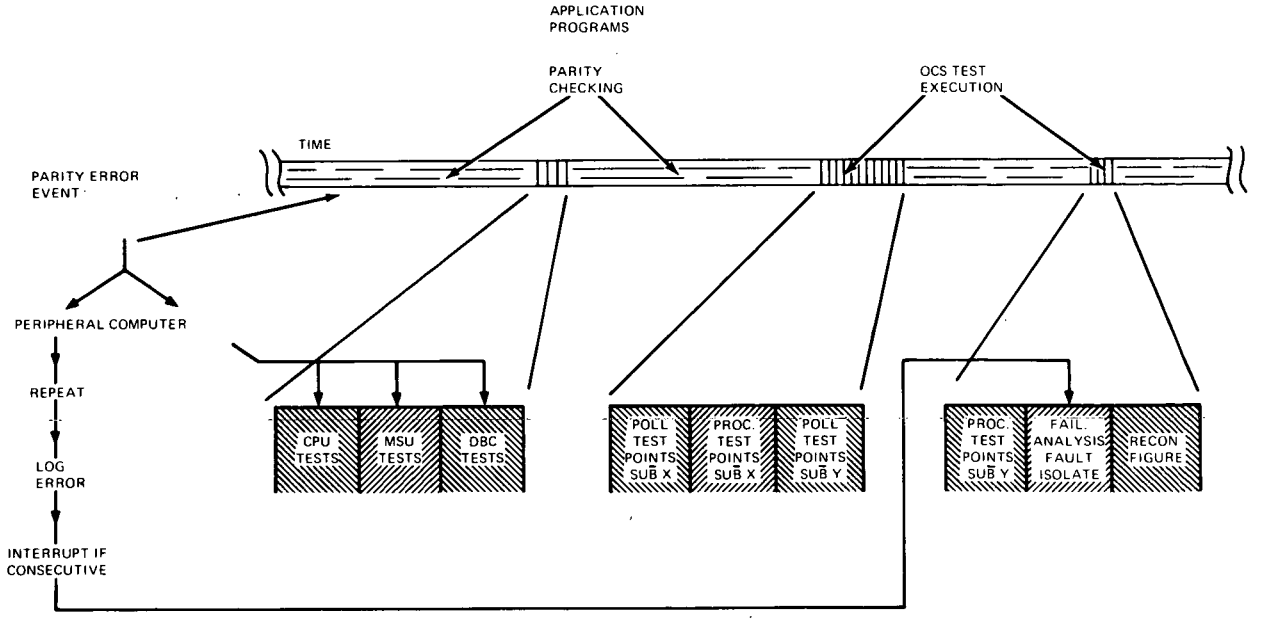


Figure 5-1. OCS Test Program Execution

Within the DMS, errors can be generated from two sources; i.e. from parity errors in any of the data transfer paths or from the COM diagnostics performed on a periodic basis. Central processing unit, main memory, or I/O parity errors will cause the appropriate COM tests to be performed to verify the error. If the error is verified, the SFI tests may be performed to isolate the fault and reconfigure the DMS to restore operation. Errors generated by the COM tests may automatically cause the appropriate SFI tests to be executed or may notify the crew to manually initiate the SFI test.

Bulk memory errors or data acquisition errors may trigger the SFI tests directly. The figure also indicates that crew keyboard entry can initiate the SFI tests. These principally are those tests which may be performed asynchronously, tests performed upon demand, or those tests which may require crew participation.

Other events can be generated by out-of-tolerance conditions emanating from measurements made on subsystem test points. Some additional processing associated with failure analysis may be required for these cases. Figure 5-2 shows a top level flow of a typical failure event analysis. If an out-of-tolerance condition occurs, it should be determined whether or not the event is associated with a critical signal. Subsequent to this, it is important to know the failure history of the function (i.e., whether it is the first or second failure). Other items include determining the source of the event indication. If it is from BITE equipment within a given subsystem, there is no alternative but to believe the indication and execute the predetermined action. If the indication emanates from an RDAU, it is possible to verify the event through an alternate path. Each of these decisions can have two results, and all paths must be analyzed. An OCS test control hierarchy that incorporates the separate responsibilities discussed above is shown in Figure 5-3. The SFI group includes the failure event analysis, fault isolation, equipment reconfiguration sequence, and display/record messages.

5.1.1 CONTINUOUS ORBITAL MONITORING TESTS (COM)

The COM tests associated with the DMS are divided into three groups; i.e., one group contains software diagnostics only; another group includes the acquisition and limit checking of test point data (through RDAUs), and the third group includes the parity checking hardware. Figure 5-4 shows a representative top level flow for the COM tests. These tests will not be performed without interruption as shown, but rather will be performed on a time available basis under executive control.

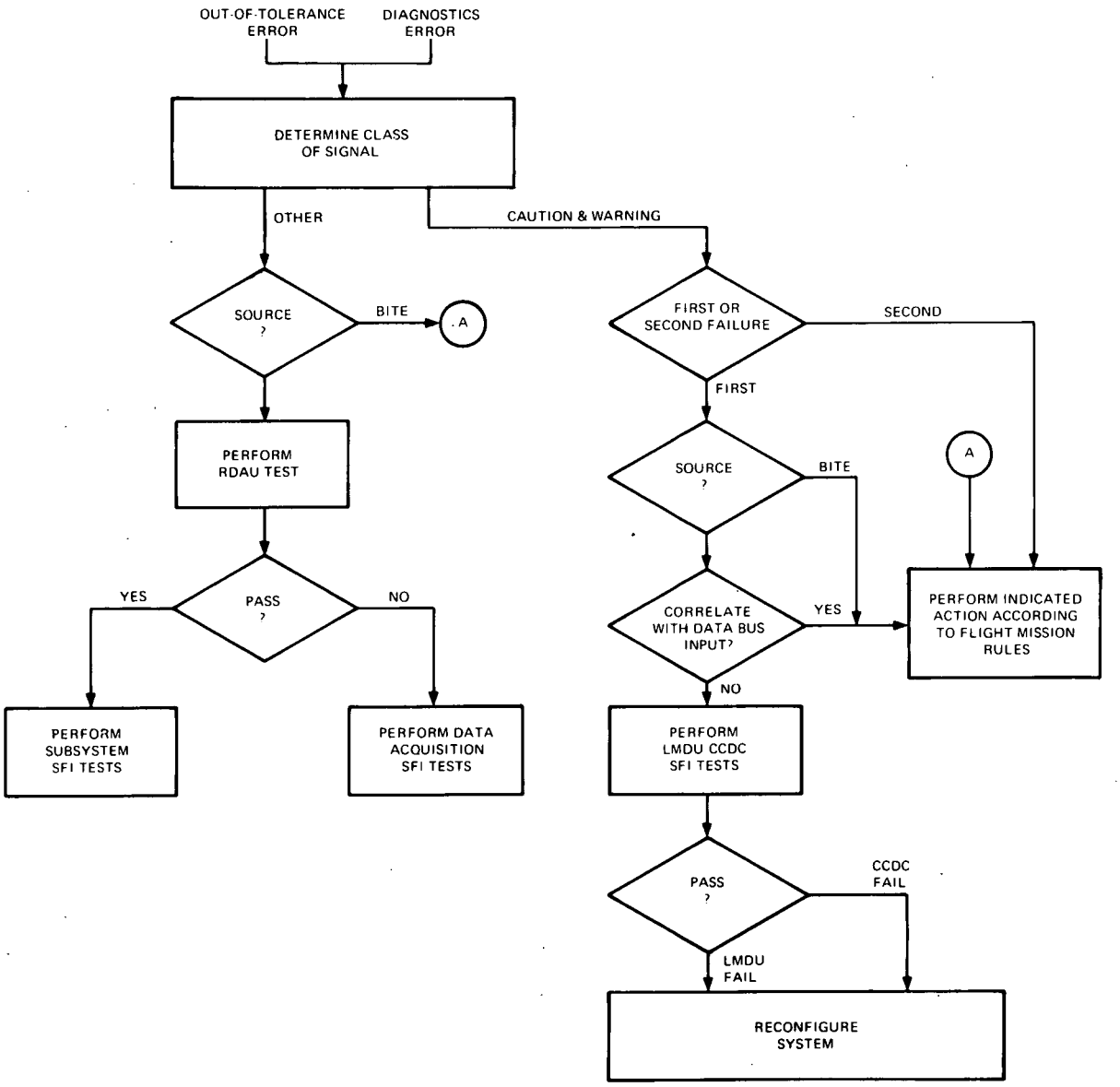


Figure 5-2. Failure Event Analysis

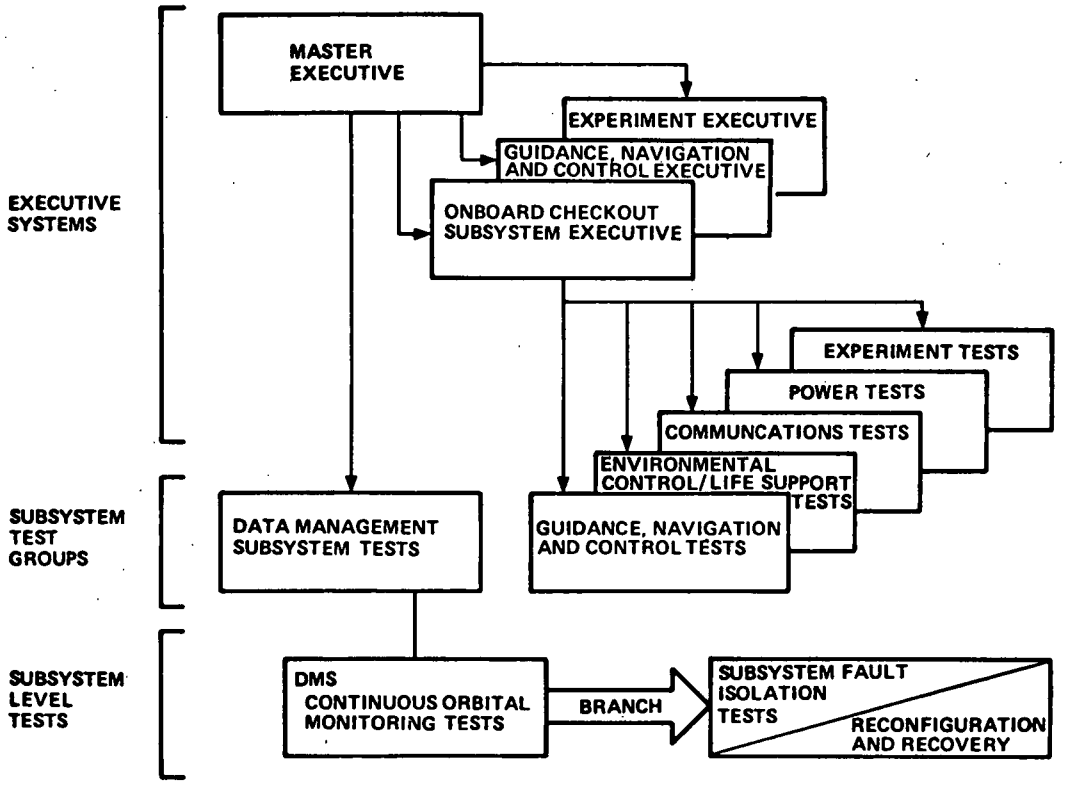


Figure 5-3. Test Control Hierarchy

5.1.1.1 Computer Group

The purpose of the computer COM tests is to exercise periodically as much of the central processing units, main store units, and data bus control units as possible within time constraints and without causing interference to other application programs. The COM tests shall verify capability of the following elements of the computer group:

- CPU instruction operation (i.e., add, subtract, multiply, divide, etc.)
- CPU data flow
- Register, adder, shifter, and mover functions
- Main storage addressing
- Control communication between CPU and data bus controller
- Data flow between data bus controller and main memory
- Power supplies

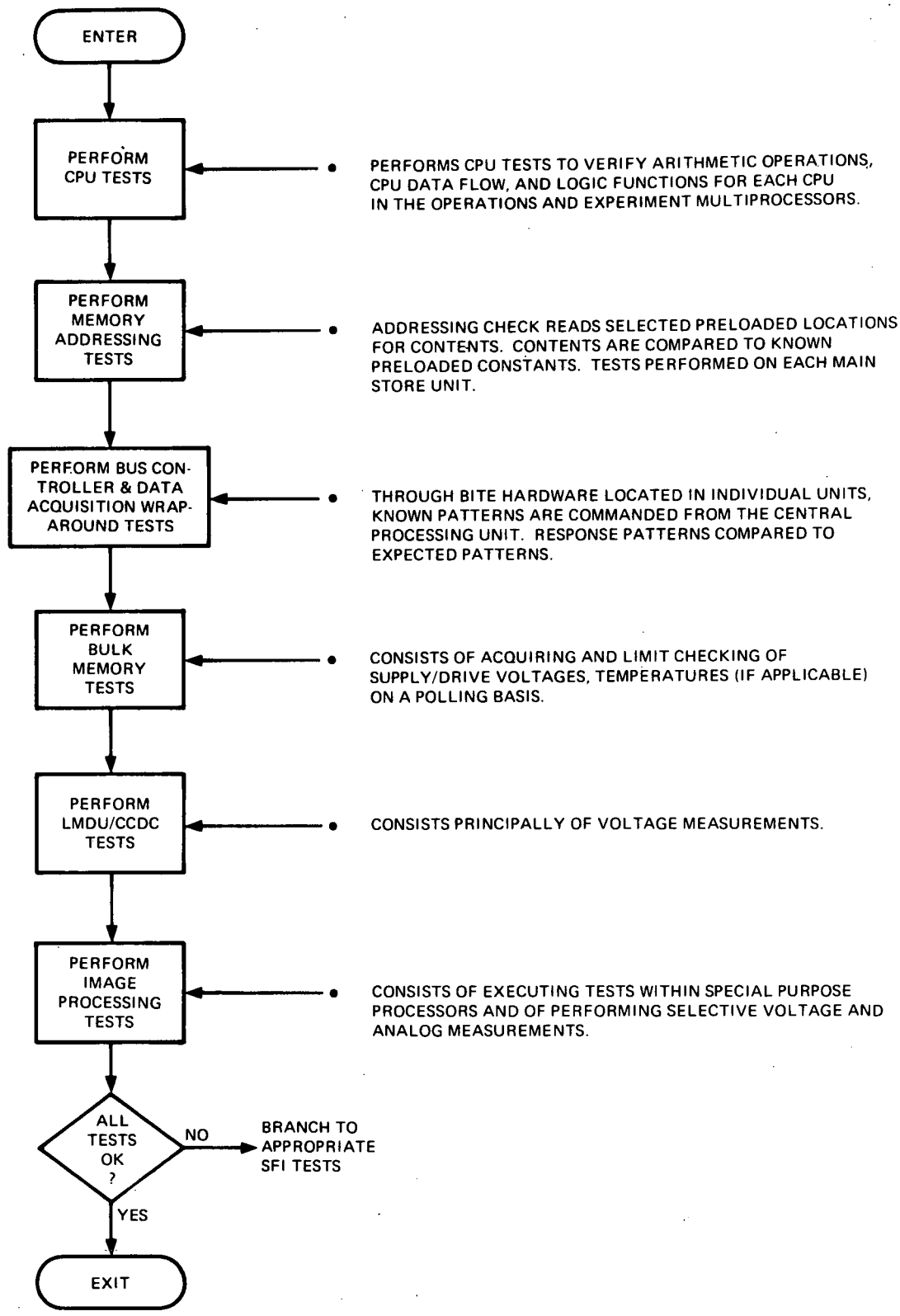


Figure 5-4. COM Top Level Flow

The CPU tests must be designed to test all arithmetic and logic functions of the computer. The basic technique to be employed will be one of performance of an operation and comparison of the actual results with the expected results. These tests must be repeated on a scheduled basis in all six CPUs.

A limited MSU test will be accomplished by main storage addressing. The test shall verify the addressability of individual MSUs by cycling through all MSU addresses on a time available basis. This test need not be repeated for each CPU test.

The COM tests also shall provide a functional check of the data bus controller by a wraparound technique, using BITE hardware. This hardware will effectively connect the bus controller output, address, and control lines to corresponding input lines. The basic technique again is to compare actual results to expected results.

In addition to these tests, power supply voltages and discrete indicators will be polled through RDAUs for comparison or limit checking. As a general rule, two consecutive errors or an out-of-tolerance measurement is caused for a subsystem reconfiguration.

5.1.1.2 Bulk Memory Group

The principal COM tests on bulk memory will be supply voltage measurements. All data which is transferred to or from bulk memory is parity checked, and will be the principal source of error detection. Consecutive errors will initiate Subsystem Fault Isolation Tests.

5.1.1.3 Data Acquisition Group

This group consists of the terminals, RDAUs, and stimulus generation units. The wraparound technique will be utilized on a periodic basis to verify the operability of each terminal, RDAU, and SGU.

5.1.1.4 Command, Control, and Display Group

5.1.1.4.1 Command, Control Display Consoles (CCDC)

The CCDC COM tests will consist primarily of supply voltage measurements. The displays and controls are subjected to testing through normal daily equipment usage. Such items as loss of character generation, display quality, brightness, etc., are self-annunciating, and special tests need not be mechanized. Crew participation is required in most tests of CCDC (see CCDC SFI tests).

5.1.1.4.2 Local Monitor and Display Unit (LMDU)

The COM test for LMDUs should be implemented in a similar manner as the RDAUs; i.e., on a periodic basis, the LMDU should be utilized in a wraparound type test for response generation. The response should be compared to an expected pattern.

The display is subjected to a form of continuous orbital monitoring through crew use and observations. There will be no special COM display tests utilized on a continuous basis.

5.1.1.5 Image Processing Group

The COM tests for the image processing equipment will consist primarily of supply voltage and other analog measurements. Additional integral diagnostics should be included with special purpose processors such that the diagnostics can be commanded from the DMS computers. An interface with an RDAU should be provided to implement communications with the DMS computers.

5.1.2 SUBSYSTEM FAULT ISOLATION TESTS (SFI)

The COM tests performed on a cyclic basis and supplemented with parity checking comprise the fundamental DMS error or failure detection capability. If a failure is detected, it must be isolated to a replaceable unit. The testing capability for isolating to the replaceable unit is called "Subsystem Fault Isolation (SFI).

Since it is incumbent upon the DMS/OCS to be able to isolate failures to the line replaceable unit (LRU), a definition of these elements has been formulated. These are partially a result of the degree in which a software/hardware system can effectively isolate malfunctioning elements in addition to the physical considerations of packaging and accessibility within a given equipment complex.

Several techniques are presently used to provide varying degrees of "self checking" and fault isolation capability within computers. These techniques were investigated with respect to their applicability for the Space Station OCS. In addition to the COM tests, four fundamental techniques will be used in the proposed SFI scheme. The four include:

- Parity checking on all internal data
  - Checks hardware for correct data handling capability.
- Known problem computation
  - Checks hardware for correct data handling and computing capability. Test more conclusive than parity checking.
  - Extract problem routine from memory, work problem, verify answer with correct answer stored in memory.

- Hardware pattern generator
  - Checks hardware for correct data handling capability.
  - Generates known data word pattern for checking write/read accuracy of memories.
- Crew interactive/manual tests

5.1.2.1 Computer SFI Tests

For the purpose of deriving a fault isolation scheme, the DMS/OCS computer subset has been modeled as shown in Figure 5-5. This model is comprised of the following elements:

- Data bus controller (DBC)
- Data bus switch matrix (DBSM)
- Data bus input/output (DBI/O)
- Shared memory matrix (SMM)

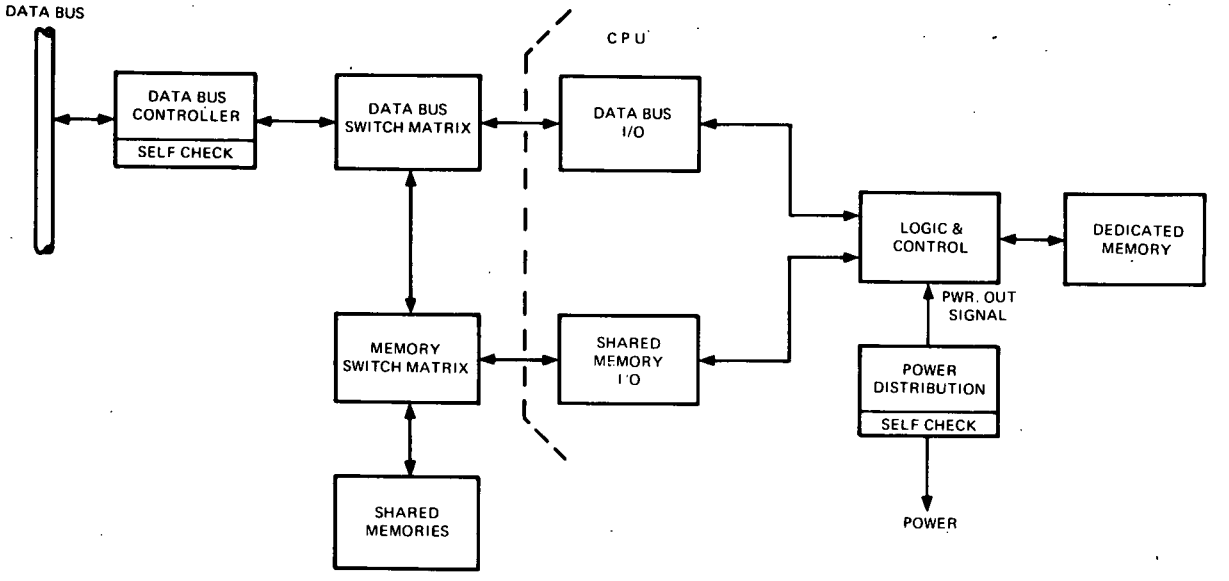


Figure 5-5. Computer Subsystem Diagnostic/Fault Isolation Model

- Shared memory
- Shared memory input/output (SMI/O)
- Logic and control (L & C)
- CPU dedicated memory
- Power supply and distribution

These elements have been described in Section 3.4, Line Replaceable Unit Definition.

Figure 5-6 depicts the proposed computer subsystem fault isolation logic developed for the DMS/OCS. The primary diagnostic conditions utilized in this scheme are:

- Detection of parity errors
- Incorrect (or no) response to a command or pattern check

The "soft power down" activity is noted in Figure 5-6 only to the extent of depicting the isolatable unit involved. By its very nature, it is self-diagnostic and isolating.

The flow diagram indicates a shared memory as an isolatable unit. By employing certain manual procedures supplemented with additional automatic (via OCS) tests, the shared memory units can be further broken down to a lower level of isolation i.e., the LRU level. Figure 5-7 gives a unified fault isolation model for the shared memory unit.

Manual diagnostic/fault isolation procedures for determination of the shared memory LRUs would be dependent upon the type of OCS notification, i.e.,

Type I - Shared memory will not respond to inquiry or command

Type II - Shared memory generating parity errors or incorrect write/read of known pattern

Figure 5-8 depicts the manual diagnostic and fault isolation logic for the shared memories. It is postulated that the mechanical sections will have some type of self-test capability to determine operational status. This self-test capability would be manually actuated in such a manner as to demonstrate the action of various mechanical, and electro mechanical components (motors, solenoids, gears, etc.). A human operator, following a prescribed diagnostic routine, could then reasonably assess the operational status of the mechanical section.

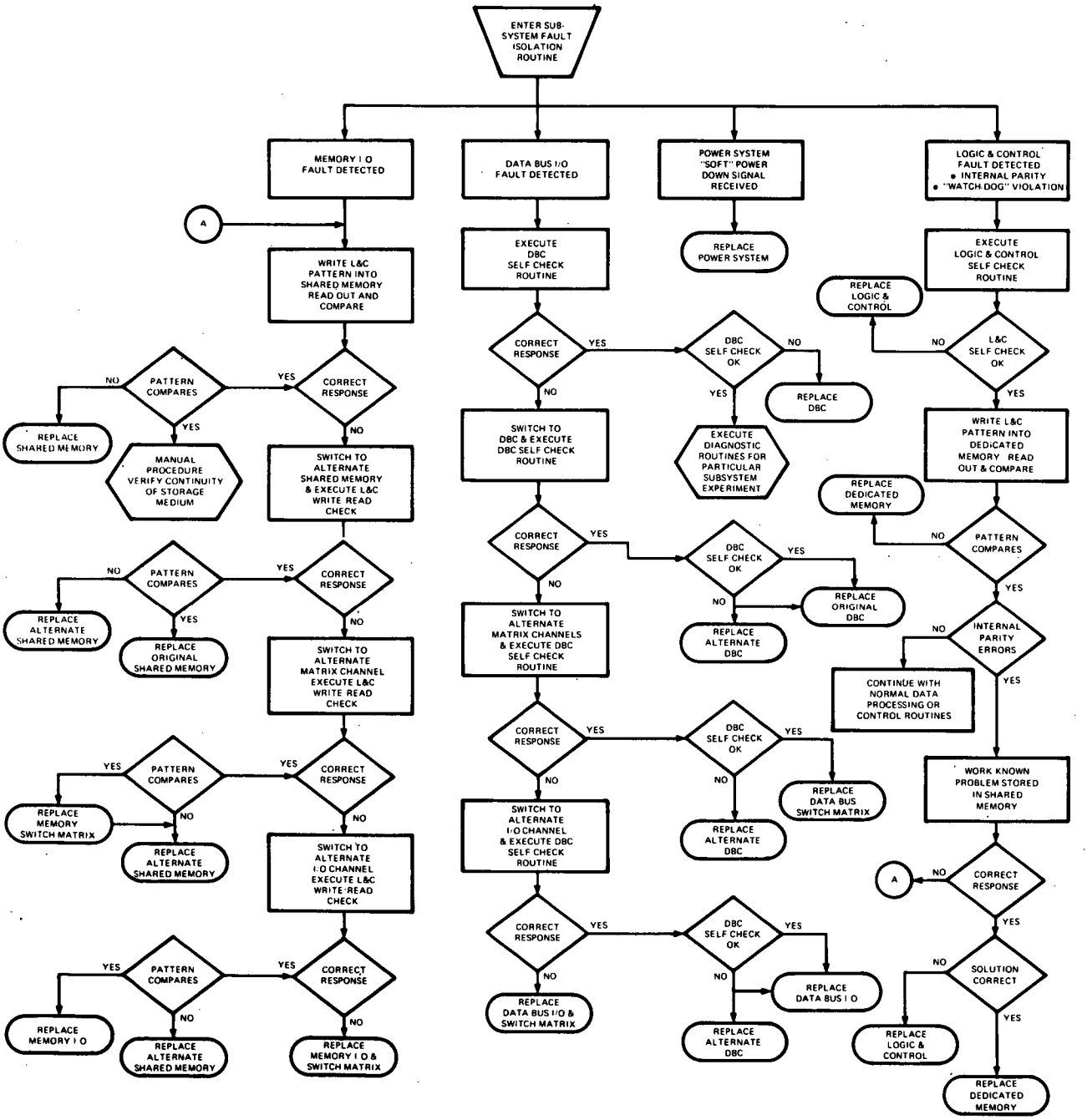


Figure 5-6. Computer Subsystem Fault Isolation Flow Diagram

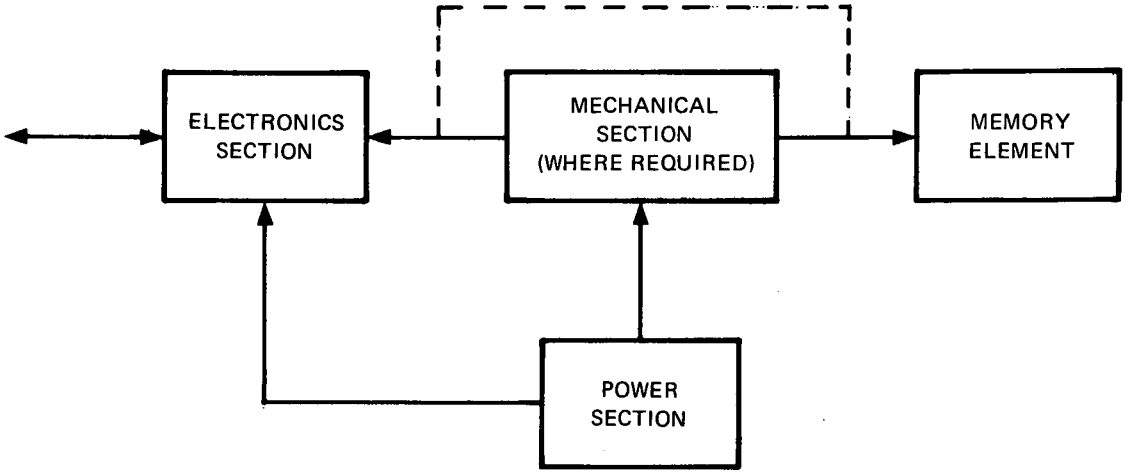


Figure 5-7. Shared Memory Unit Manual Diagnostic/Fault Isolation Model

5.1.2.2 Bulk Data Storage

Figure 5-9 is a diagnostic/fault isolation model for the bulk data storage facility. This model is comprised of the following elements, each of which has been described in Section 3.4, Line Replaceable Unit Definition.

- Digital Buffer and Control Unit
- Record/Reproduce Electronics
- Switch Matrices
- Tape Transport Controller
- Tape Transport
- Power Supply and Distribution Units

Figure 5-10 depicts the proposed bulk data storage fault isolation logic. The primary diagnostic conditions utilized in this scheme are the same as those noted for the computer subsystem fault isolation scheme.

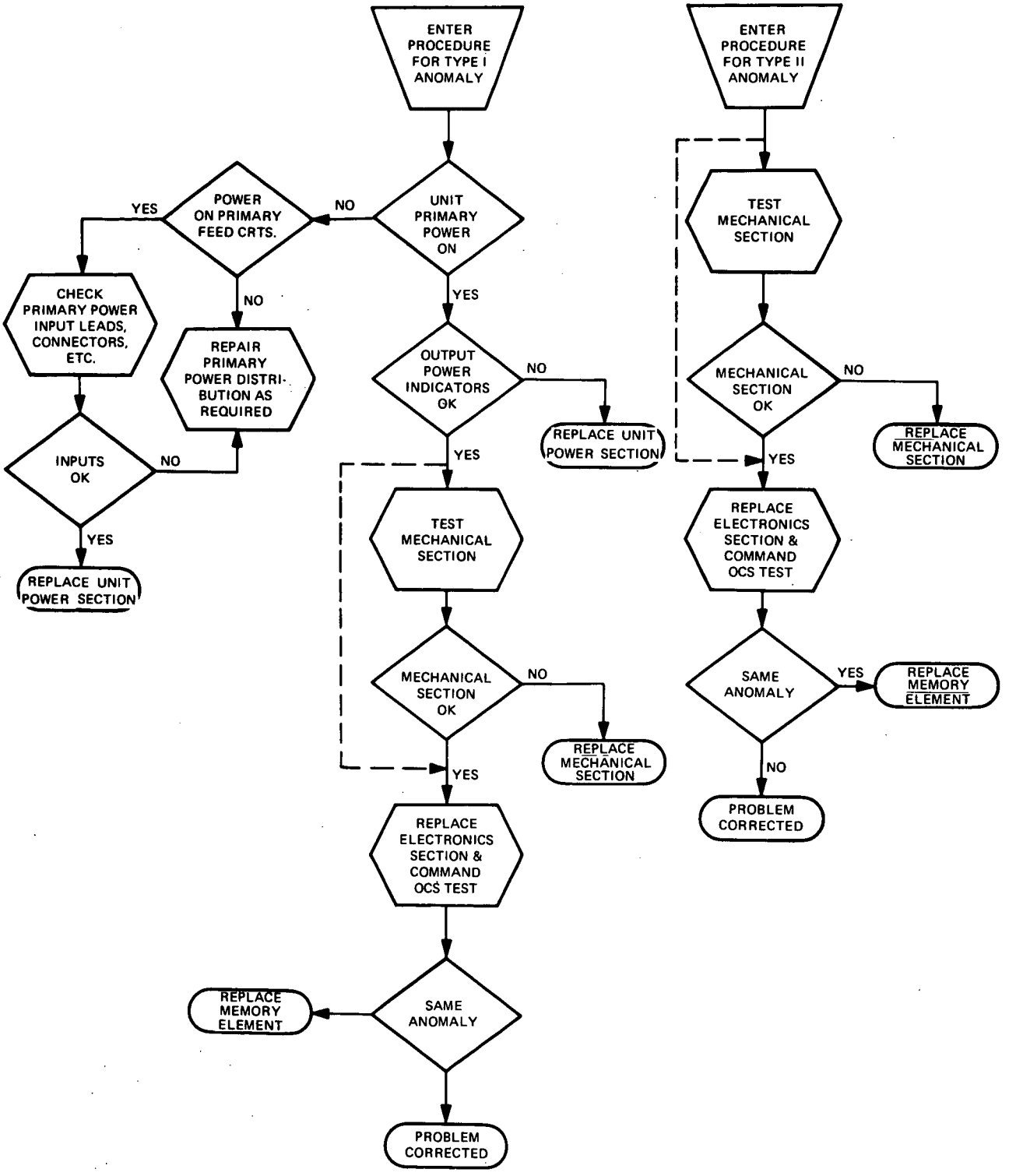


Figure 5-8. Shared Memory Fault Isolation Flow Diagram Manual Procedure

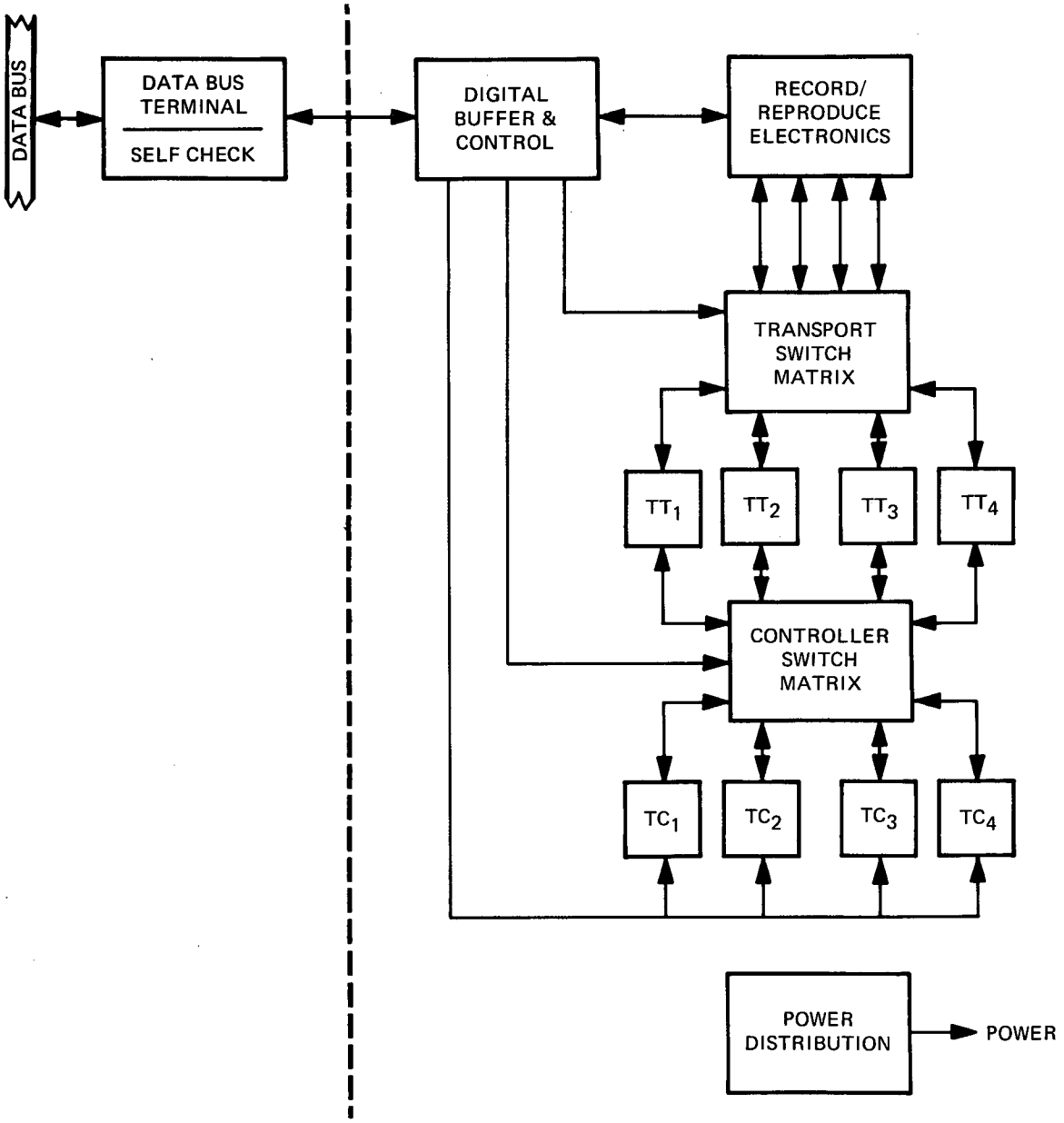


Figure 5-9. Bulk Data Storage Diagnostic/Fault Isolation Model

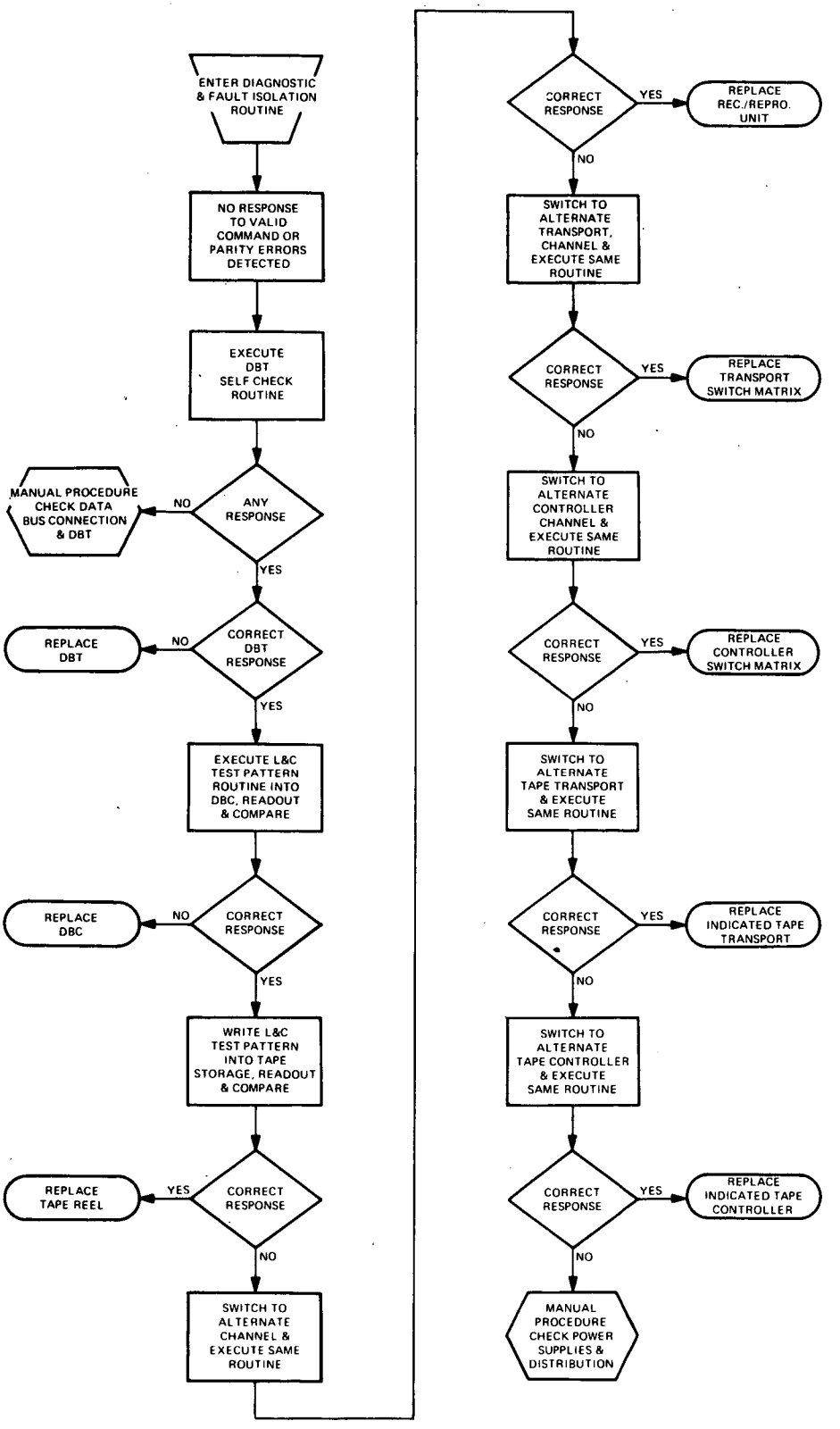


Figure 5-10. Bulk Data Storage Fault Isolation Flow Diagram

5.1.2.3 Data Acquisition Subsystem

A typical Data Acquisition Subsystem element is shown in Figure 5-11. This element is a representative hardware configuration for a majority of the identified data acquisition requirements on the Space Station. It is comprised of the following elements, each of which has been described in Section 3.4, Line Replaceable Unit Definition:

- Data Bus Terminal (DBT)
- Remote Data Acquisition Unit (RDAU)
- Stimuli Generation Unit (SGU)

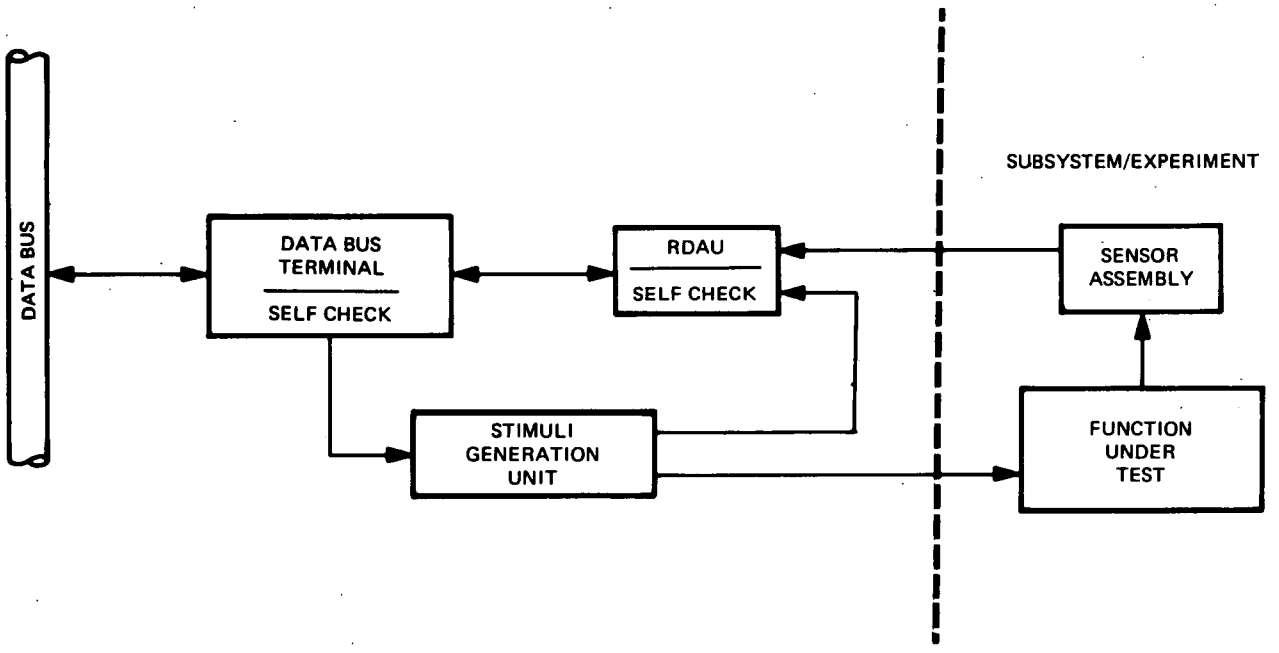


Figure 5-11. Typical Data Acquisition Element

It is incumbent upon the DMS/OCS to be able to identify malfunctioning elements to the lowest replaceable unit (LRU) in the system loop. Each of these units has the ability under DMS/OCS computer control to perform an operational self-check of its circuitry or, in the case of the SGU, to provide a special test output which can be monitored by a known "good" RDAU and thereby provide an indication as to the functional status of the SGU. Using these built-in capabilities, the DMS/OCS can, with proper programming, initiate checkout routines in such a manner as to identify LRUs and other elements which indicate fault operation. The fault isolation logic for the data acquisition elements is given in Figure 5-12.

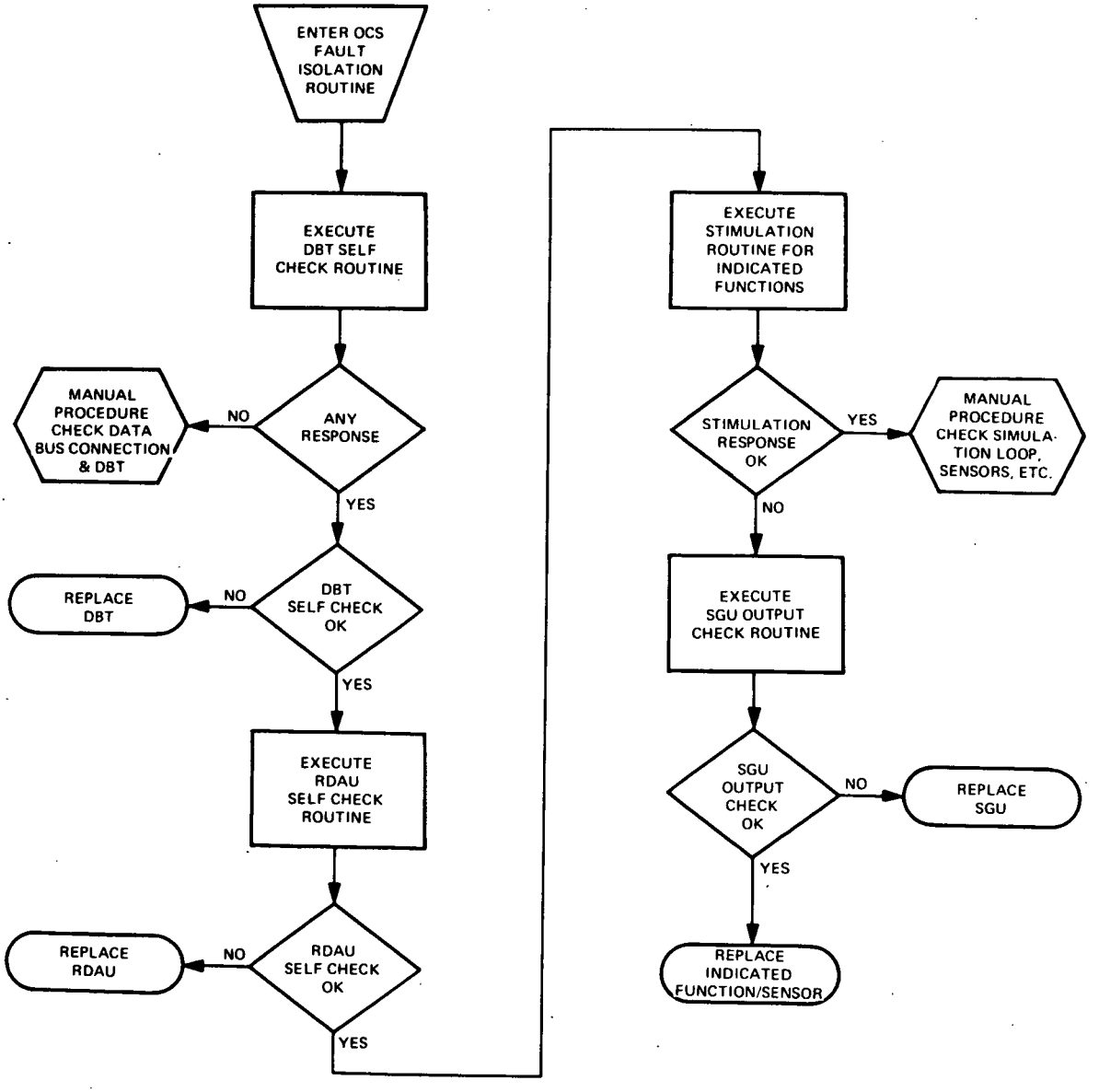


Figure 5-12. Data Acquisition Element Fault Isolation System Flow Diagram

Since the OCS ground rules do not preclude manual fault isolation activities, their use was integrated in the proposed scheme only to the extent necessary to supplement the automatic fault isolation and only in those cases where it would be extremely expensive to implement or would be impossible from a practical standpoint. The flow chart depicts two items which indicate the need for manual troubleshooting.

1. Addressed data terminal does not respond to valid commands. This indicates a possibility of a bad data terminal/data bus connection or a catastrophic data terminal failure. The possibility of a bad data bus can be investigated by checking continuity of data transmission on that particular branch.

2. Bad data is being received but the DBT and RDAU self-checks are satisfactory, and the stimulation responses are correct. This is a situation which would tend to indicate a sensor assembly/function under test which responded correctly to a calibrated input (simulation signal), but not correctly to a measured parameter input. This would, however, be a legitimate indication if the stimulation signal was inserted at points in the system different from the measured parameter input. In this case, it would indicate a fault in the portion of the system not included in the stimulation loop.

This fault isolation scheme would, with the exceptions noted above, automatically indicate which data acquisition LRU would need to be replaced. The actual replacement would then be a manual operation. The "Replace" signals could be used to switch in redundant units for noncritical parameters in addition to providing the display. For critical functions, this scheme would provide a status display only since these functions will be implemented operationally redundant.

5.1.2.4 Command/Control and Display Console SFI Tests

It is postulated that the individual control and display assemblies (status lights, keyboards, pushbuttons, etc.) of the Command/Control and Display Console will be respectively "unitized" and contain their own particular encode/decode electronics. For example: the computer keyboard assembly is comprised of the mechanical key assembly and all required control and encode electronics. This entire keyboard assembly could be removed, as a unit, from the CCDC. Light panels, alphanumeric displays, etc., would be handled in a similar manner. The CRT display assembly would contain the CRT, deflection circuitry, and all required video control circuitry.

Figure 5-13 shows a top level flow for the CCDC SFI tests. The tests include both automatic and manual tests. The automatic tests include those associated with the data bus terminal, command buffer and control unit, and stimulus generation unit. Tests associated with lamps, CRT displays, or viewers are manual tests.

5.1.2.5 Image Processing SFI Tests

As in the CCDC, image processing SFI tests will be largely manual. The automatic tests are concerned with the digital equipment interfacing the computers. Figure 5-14 shows a preliminary top level SFI flow diagram for the image processing equipment.

5.1.3 DMS TEST TIMING

Tests typical of those required for the DMS can be sized for memory and execution time, but the frequency with which the tests must be performed was not specified. In addition, certain units within the DMS probably will be checked more frequently than others. Because the aggregate contribution to computing load by the DMS/OCS depends upon these items, it is necessary to assure the frequency of performing tests and the sequence or order in which the units are checked.

The two principal factors upon which the test iteration rate could be based are the failure rates and mission criticality. Of the two factors, criticality will demand the highest iteration rate. The approach taken has been to examine the mission and to specify a maximum time during which an undetected failure can be tolerated. The cumulative time required for detecting the failure, for isolating the failure, and for recovery must be equal to or less than the total time during which the failure can be tolerated.

A moderate worst case which can be utilized as a basis for affixing the iteration rate is a docking operation. During this operation certain commands and responses are exchanged between the Space Station and the docking vehicle. Some of the considerations involved in this operation are discussed in McDonnell Douglas Space Station Electronics Subsystem Study (DRL 8, Volume 5, Book 5, pages 169-177). The primary docking mode is automatic, but with crew observation having override capability. Failures in the DMS will cause erratic or total loss of data exchange capability with the docking vehicle for a period of time. During docking, range and closing rate are important parameters involved in command maneuvers. Erratic or loss of computational capabilities may be manifested through range errors or closing rate errors. Errors which permit too rapid a closing rate can affect vehicle safety, while errors permitting too slow an approach expend docking vehicle fuel unnecessarily.

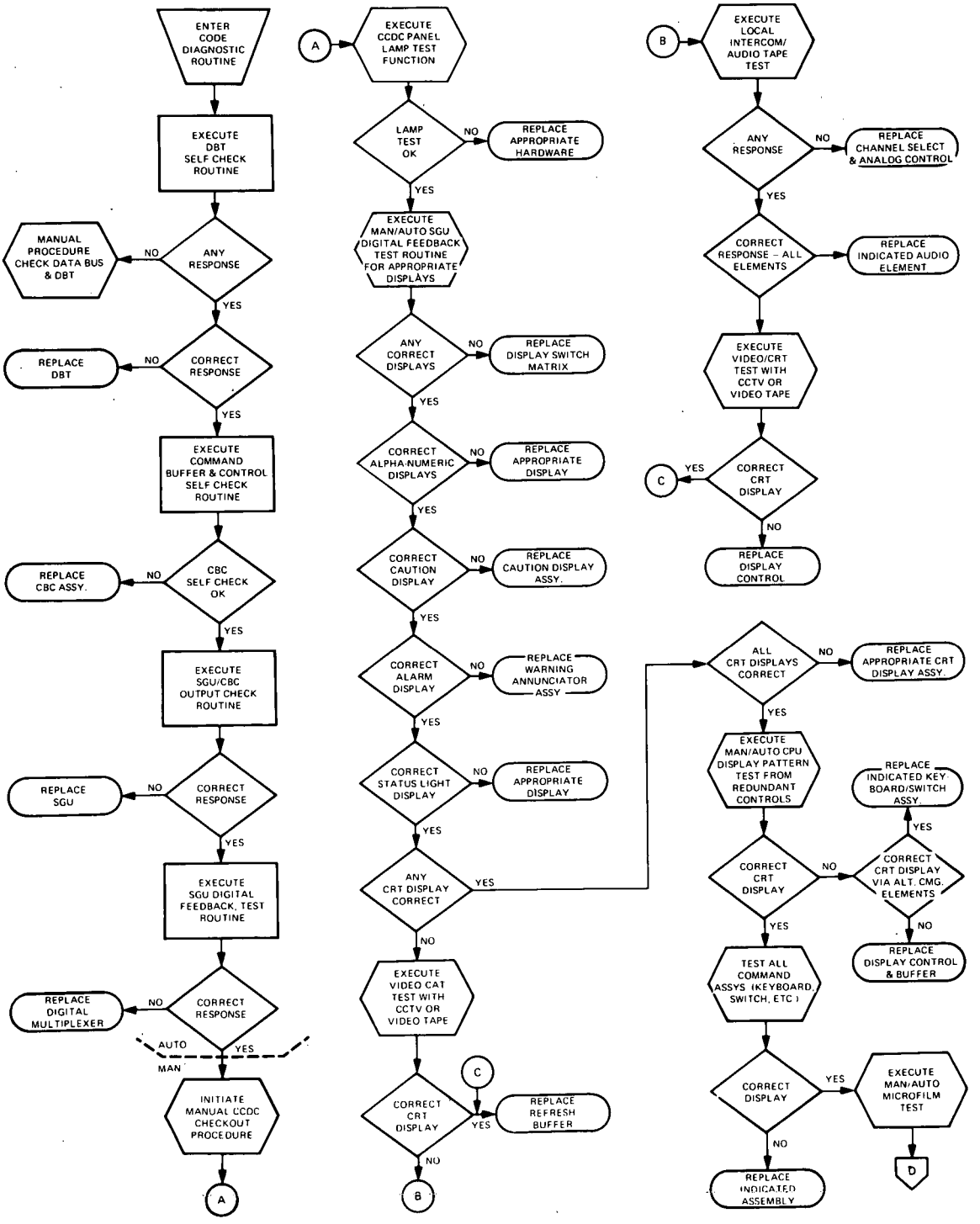


Figure 5-13. Command/Control and Display Console Fault Isolation Flow Diagram

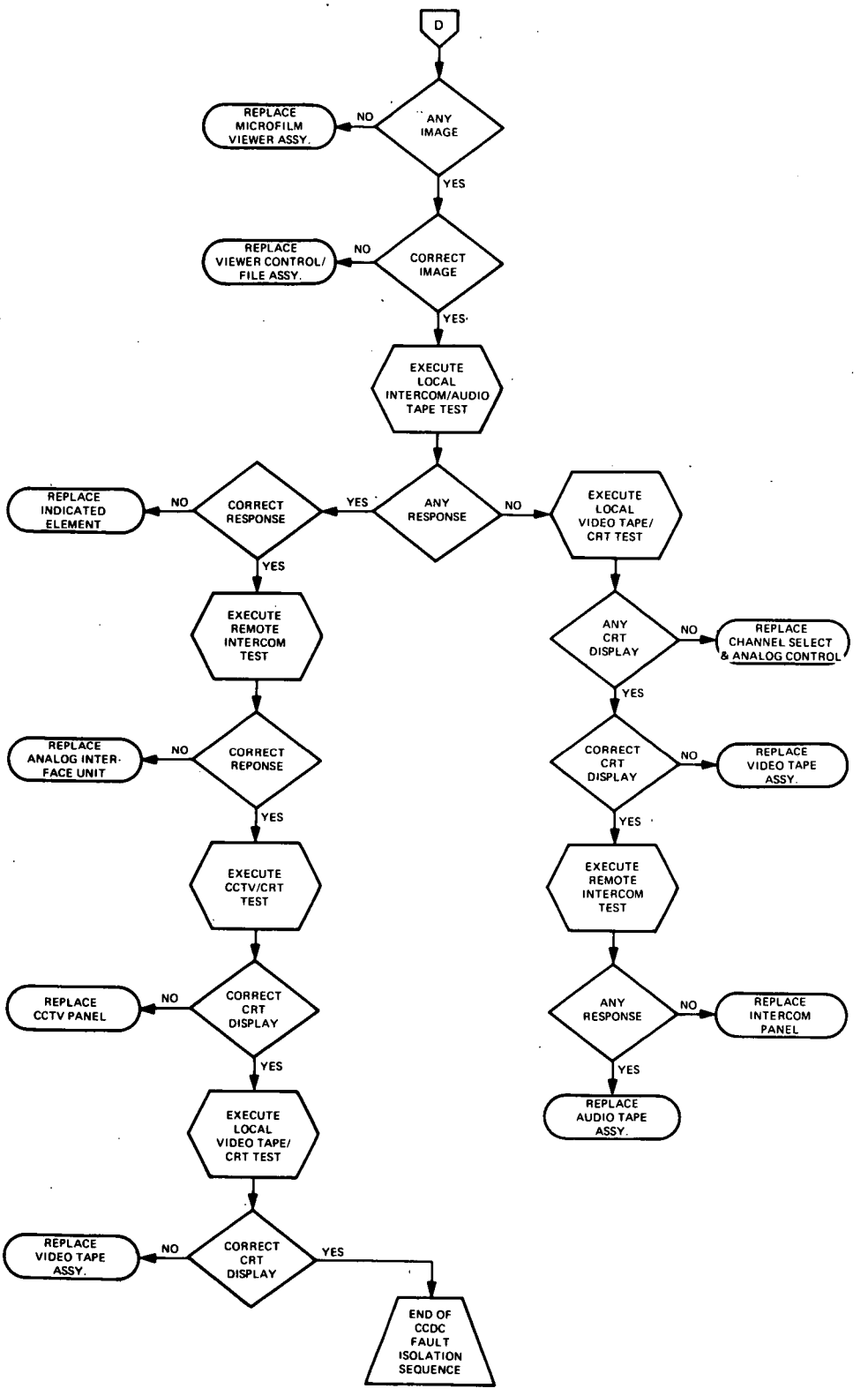


Figure 5-13. Command/Control and Display Console Fault Isolation Flow Diagram (cont)

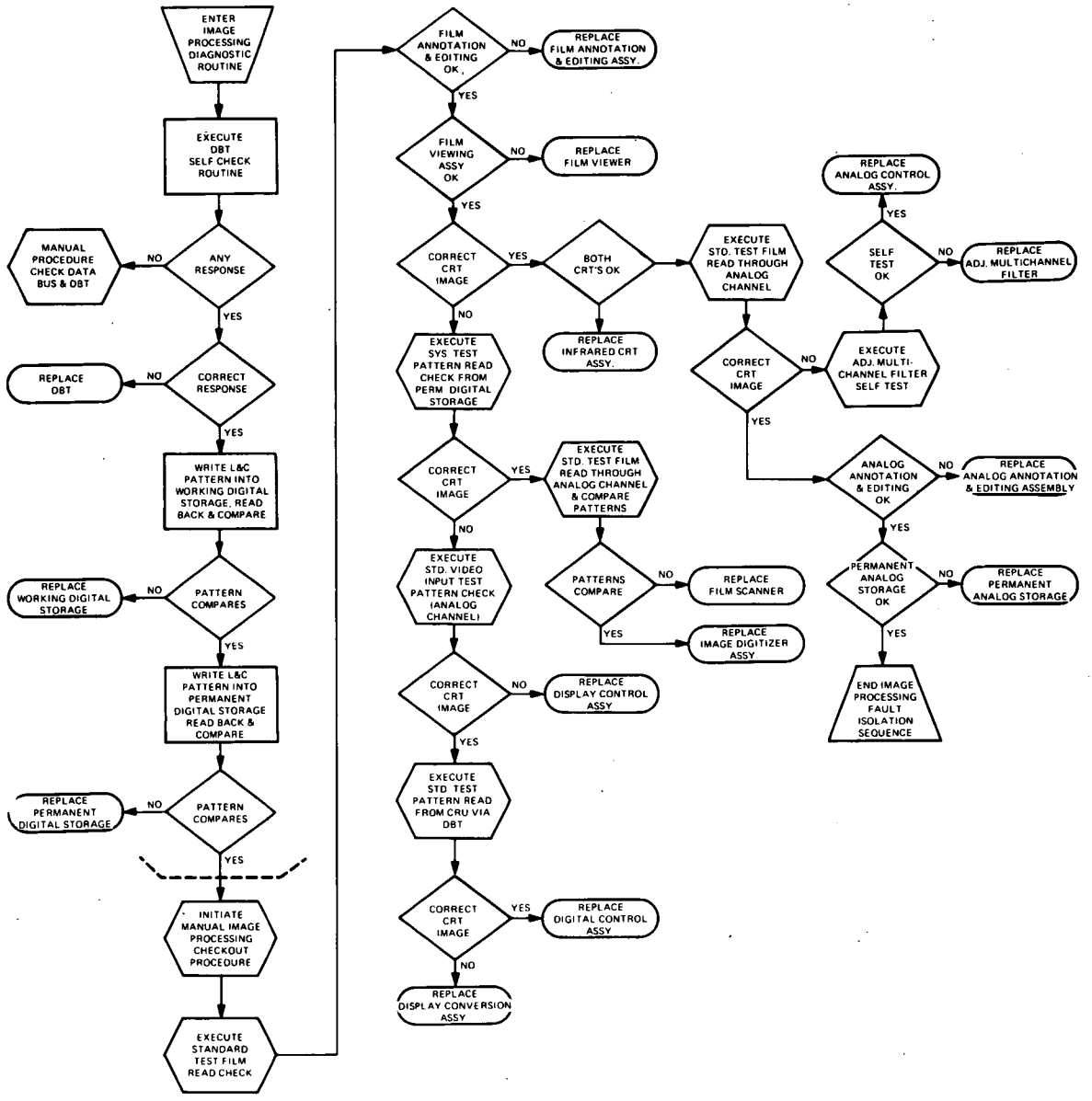


Figure 5-14. Image Processing Fault Isolation Flow Diagram

For analysis purposes, it was assumed that the maximum allowable error build-up in closing rate is 10 percent (i.e., due to DMS failure to deliver or remove some command). At one foot per second in the near vicinity of the Space Station, the maximum allowable error would be 0.1 foot per second. If a 100-pound thruster were left "ON" due to a failure, the time required to produce a 0.1 foot/sec velocity increase towards the Space Station would be (assuming a 40,000 pound vehicle):

$$t = \frac{V}{aac.} = \frac{\frac{0.1}{100}}{40,000} = 40 \text{ seconds}$$

If it is assumed further that any errors imparted to the system must be removed upon recovery, the tests must be performed in one half the time above or 20 seconds. Therefore, an iteration rate of once per twenty seconds was utilized for sizing the software for checkout of that DMS equipment involved in the critical operation.

The DMS equipment appears to fall into four categories with regard to the frequency of testing. The first group is a critical group consisting of the CPUs, main memory units, data bus controllers, critical terminals, and critical RDAUs. This group is tested once per 20 seconds in accordance with the postulated worst case situation. The second group is less critical, and consists primarily of the remaining terminals and RDAUs. The second group should be checked at least once per hour, and will also contain all discrete and analog measurements to be made on DMS equipment (e.g., power supplies).

The third group consists primarily of bulk and mass memories and displays. This group should be checked at least once per 24 hours. The fourth group will be an "on-demand" group associated with image processing, repair verification, calibration, etc. Table 5-2 summarizes the iteration periods.

5.1.4 DMS MEASUREMENTS/STIMULI

In addition to the software programs and BITE provisions, a series of measurements must be made on certain DMS equipment. The measurements will be concerned principally with power supply measurements and temperature measurements.

Each supply contains certain protective circuitry associated with over-voltage, under-voltage, and over-current protection. Each supply should provide a discrete logic output indicating that a limit has been exceeded. The logic output would be monitored via an RDAU.

Table 5-2. Iteration Periods

1/20 sec.	1/hour	1/24 Hours	On-Demand
COM tests		SFI Tests	
1. CPUs	1. All DMS Measurements	1. Bulk and mass memories	1. Image Processing
2. MSUs	2. Noncritical Terminals and RDAUs	2. Standard Display Patterns • CCDC • LMDU	2. Calibration
3. DBCs	3. SGUs		3. SFI Tests
4. Critical DBTs			4. Repair Verification
5. Critical RDAUs			
6. Measurements Associated with above LRUs			

Temperature measurements will be checked on equipment likely to require monitoring. The measurements will be made on the racks through which the coolant will flow. Actual measurement will be performed and limit checked within the RDAUs.

Appendix I-9 of Final Report Task 1 lists the measurements and stimuli required to complete checkout of the DMS.

5.1.5 DMS TEST SOFTWARE SIZING STUDY

The approach taken in the study was to implement the Command SFI tests previously described to estimate the DMS resources required to perform the tests. Flow charts were generated to describe the logic for each test. Accompanying each test flow is an estimate of the memory required, the CPU time required to execute, and the I/O time required if applicable.

Because software sizing is very much involved with the basic organization of the processing equipment, it was necessary to expand considerably the baseline DMS to assume additional architectural features. Many of the assumed features were with regard to:

- Processor interrupt features and instruction capabilities
- How processor-to-processor communications are implemented to convey CPU failure data to other CPUs
- How main memory is organized with regard to addressing, memory contents, table formats, preferential storage areas, etc.
- How the I/O channels are assumed to operate
- The channel command word format
- How information tables are stored with regard to configuration control
- How out-of-tolerance conditions propagate through the data acquisition path

Certain of the features above are key to OCS software sizing of DMS tests while other features may be more important to executive control of OCS and general software design. Most of the features assumed have been utilized in one or more applications for similar purposes (e.g., in the IBM System/4 Pi and IBM System/360 lines).

5.1.5.1 Architectural Assumptions

5.1.5.1.1 Microprogram - The processor can be microprogrammed so that the basic instruction set can be augmented without requiring an engineering change to the processor. The need for such augmentation arises from the requirement to automatically test, isolate, and reconfigure the DMS hardware under software control. An example of this type of instruction is the one used to set the address translation register of a shared memory LRU.

It is also assumed that the processor contains special reconfiguration instructions (e.g., "set configuration control registers"). Configuration control registers within each configurable element will be the principal means of maintaining configuration control.

5.1.5.1.2 Interrupts - An Interrupt System exists to provide a means by which a computer can make rapid response to extra-program circumstances that occur at arbitrary times and perform a maximum amount of useful work while waiting for such circumstances. Parity errors, failures, or out-of-tolerance conditions will result in an "interrupt." The types of interrupts assumed include:

- "Machine Check" interrupt is provided in the event of machine malfunctions (e.g., failures in processors, memories, or data bus controllers).

- "I/O" interrupts are provided as a means whereby a CPU will respond to a request from an external device. Out-of-tolerance conditions as indicated via RDAU limit checking will cause an I/O interrupt.

- "Program" interrupts to denote improper specification or use of instructions and/or data .

- "Supervisor Call" interrupt to implement a high speed request for executive services (e.g., task switching, storage allocation, data logging, configuration control register management, etc.).

- "External" interrupts for miscellaneous purposes (e.g., to enable a response to timers, crew console keys, and processor-to-processor communications).

5.1.5.1.3 Parity - Parity checking will be utilized to provide a continuous checkout of all data transfer to and from the processors. Parity errors in general will result in a machine check interrupt.

5.1.5.1.4 Processor-to-Processor Communications - Processor-to-processor communications exist to permit the asynchronous transfer of data pertinent to reconfiguration to other processors. Actual communication will be implemented through the data bus controllers rather than through a direct interface (avoids the case where each processor must "pass along" information regarding other processor conditions).

5.1.5.1.5 Configuration Control Capability - A "configuration control register" will be maintained in each DMS configurable element to establish the prevailing subsystem structure by specifying to each element its state, the processors from which it accepts configuration changes, and the elements to which it listens in the exchange of data and certain control signals. The operational processors will have the capability of examining and setting all configuration control registers for system configuration data.

5.1.5.1.6 Real-Time Clock - A "real-time" clock is required to keep a copy of the reference clock (reference clock is external to the processor). It is included in the processor to allow high speed reference to real time.

5.1.5.1.7 Interval Timer - A high resolution interval timer is included for storage of the interval remaining until a time dependent event must be initiated. When the interval elapses, an interrupt occurs such that high frequency polling of a clock is not necessary.

5.1.5.1.8 Storage Address Translation Capability - Storage address translation capability exists to facilitate the interchange and reconfiguration of main memory elements.

5.1.5.1.9 Use of Dedicated Memory - The dedicated memory associated with each processor will be used as a buffer which is not addressable by a program, but rather is employed by the processor to contain those portions of main storage currently being used. When the program starts operating on data in a different portion of main storage, the data in that portion is loaded by the processor into the buffer and the data from some other portion removed. This activity takes place without program assistance and is completely transparent to any program instruction.

The main storage organization as seen by each processor is as follows:

- Define Pi, i = 1, 2, 3, . . . as the preferential storage LRU associated with each processor. See Figure 5-15.

- Each processor "sees" the first LRU of addressable memory as the LRU containing its own preferential storage area (PSA).

- Beginning with the highest address expressable in 24 bits (4000 K words) and proceeding downward, each processor has the hardware capability to assess the preferential storage areas of other processors, for fault isolation and reconfiguration purposes. Authorization is under software control.

This arrangement allows for expanding the number of processors and the amount of main storage without disturbing the addressing scheme.

A special instruction is available to set the PSA base address (e.g., as in the IBM/FAA 9020 system) thus allowing the PSA to be in shared, instead of dedicated, memory.

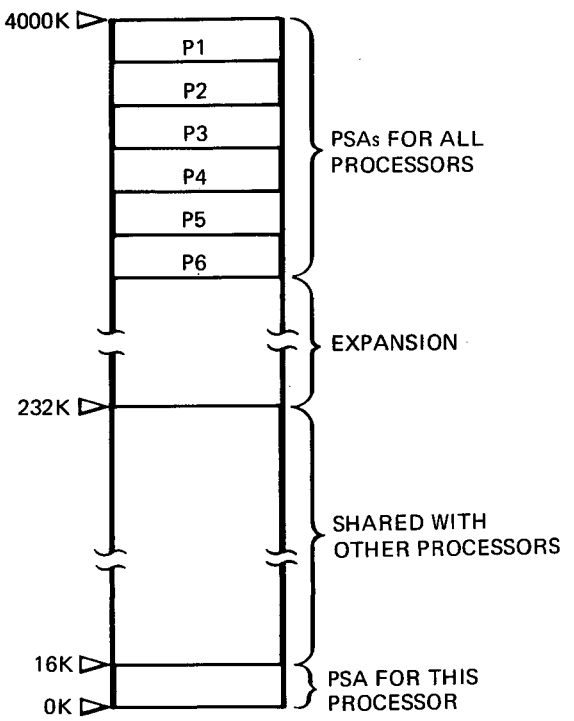


Figure 5-15. Main Storage Organization Seen By Processor

5.1.5.1.10 Processor-to-Memory Communications - It is fundamentally necessary for OCS purposes for any processor to access any other processor PSA because it is in this area that data is stored as a result of a machine check. This data will be used by an OCS processor to perform LRU isolation on other processors.

5.1.5.1.11 Processor Allocation - The processor allocation services of the master executive will effect a partitioning between the Experiment and Operational multiprocessors.

5.1.5.1.12 PSA Access - The Operational processors will be allowed to access a "diagnostic scan out" area within each PSA of other processors for failure detection/isolation purposes.

5.1.5.1.13 Memory Unit Configuration Control - All memory units contain a configuration control register and an address translation register to facilitate real-time changes in configuration.

5.1.5.1.14 Memory Addressing - Units are addressed relative to "zero" to permit logical substitution among memory units. An actual address is formed by a processor, utilizing the sum of the contents of the address translation register and the relative address within the memory. This process is transparent to software.

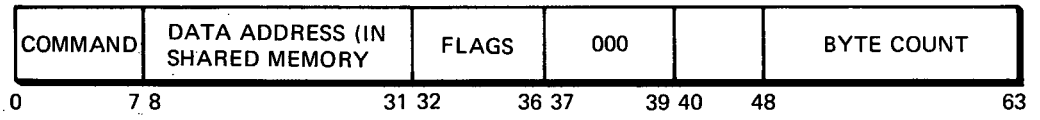
5.1.5.1.15 Duplicate Executive Capability - Duplicate copies of the master executive will be maintained in main memory to avoid loss of configuration control.

5.1.5.1.16 Data Bus Controller (DBC) I/O Operations - It is assumed that the data bus controller can execute I/O operations independent of processor operations by obtaining data bus program from main memory (similar to the channel operation in the IBM System/360). The assumption allows the processor to be devoted to main storage programs leaving the comparatively slow I/O programs to the bus controller.

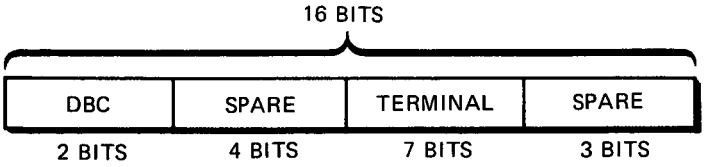
5.1.5.1.17 DBC Configuration Control - The data bus controller contains a configuration control register to facilitate real-time changes in configuration.

5.1.5.1.18 Processor-to-Processor Data Flow - The DBC provides a processor-to-processor data flow path for improved configuration flexibility.

5.1.5.1.19 Data Bus Command Word Format - A sample format for the data bus controller command word is shown below.



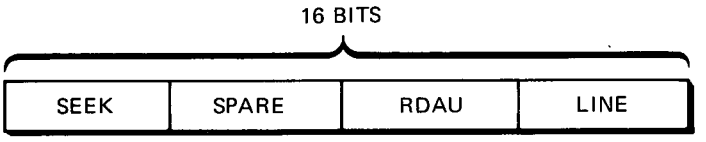
5.1.5.1.20 Data Acquisition I/O Operation - An I/O operation will be initiated by a processor instruction (e.g., Start I/O) containing an operand which addresses down to the data bus terminal level in the data path. The format is shown as follows:



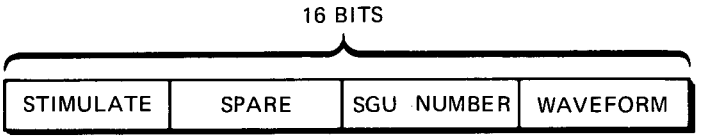
The data bus controller will be commanded by the processor I/O instruction to fetch a data bus command program from main storage. The program will supply the additional addressing and commands to be utilized by the lowest level in the data path (e.g., RDAU or SGU input/output).

5.1.5.1.21 Data Acquisition Command Structure - Typical RDAU commands will include:

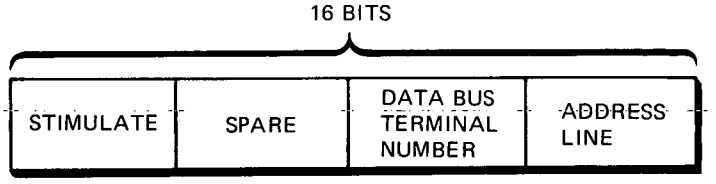
- SEEK (address RDAU/line)
- WRITE RDAU MEMORY (set RDAU limits and mask)
- READ RDAU (sequential read of one or more RDAU channels. Channels addresses "wraparound" from highest to lowest)
- READ RDAU MEMORY (read RDAU limits and mask)



The SGU will be handled as in the case of an RDAU; i.e., a "start I/O" instruction and channel program. The format is as follows:



Discrete command outputs to any subsystem will be handled through the data bus terminal. The format is as shown:



5.1.5.1.22 Controls and Displays - The controls and displays will be treated similarly to the RDAU; i.e., they will respond to a specific set of instructions contained in a data bus command program. The Experiment and Command/Control consoles will be handled the same.

5.1.5.1.23 Polling Technique - The fundamental method of announcing out-of-tolerance conditions (which must generate an unexpected interrupt) is via a hardware polling. Each RDAU, independently of command, limit checks all inputs. Out-of-tolerance conditions will be stored in a register within the RDAU. Each terminal must poll the RDAU continuously and store any out-of-tolerance conditions. The data bus controller will poll the terminals for interrupt conditions. All subsystems which interface with the terminals will announce special status conditions in the same manner, i.e., conditions are announced in the same bit positions. Unused RDAU channels will be masked to avoid generating interrupts. The mask of the secondary RDAU will prevent two separate interrupts from occurring because a single test point signal is out of limits.

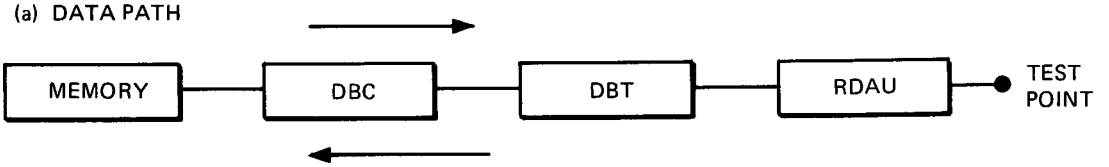
5.1.5.1.24 Functional Levels of Operation - Throughout test descriptions where "reconfiguration" or "configurable element" is used, the subdivisions are as defined in the following hierarchy.

- SUBSYSTEM
- CONFIGURATION
- CONFIGURABLE ELEMENT
- LINE REPLACEABLE UNIT (LRU)

The "Subsystem" level includes the complete DMS equipment. A "Configuration" represents a particular combination of DMS equipment utilized at a given time (e.g., the particular bus controller, bus terminal, and RDAU in use at a given time). A "Configurable Element" is the level at which DMS reconfiguration is performed. A "Configurable Element" can be comprised of one or more LRUs (e.g., the processor contains multiple LRUs). The LRU is the smallest denomination of equipment for which fault isolation is attempted and is the level at which "on-line" remove-and-replace maintenance is performed.

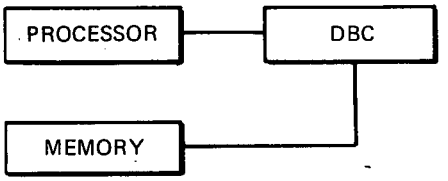
Participation of configurable elements in various DMS operations is shown below:

(a) DATA PATH

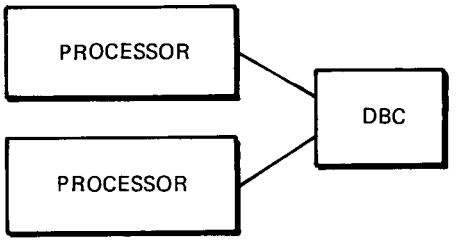


(b) STORED-PROGRAM EXECUTION

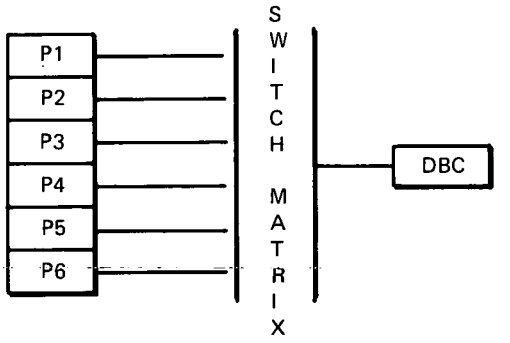
(c) I/O OPERATIONS



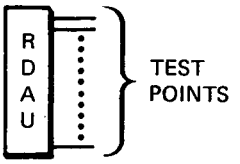
(d) SHOULDER TAP



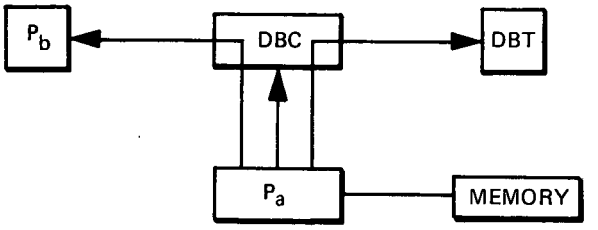
(e) UNEXPECTED INTERRUPT PRESENTATION



(f) TEST POINT POLLING



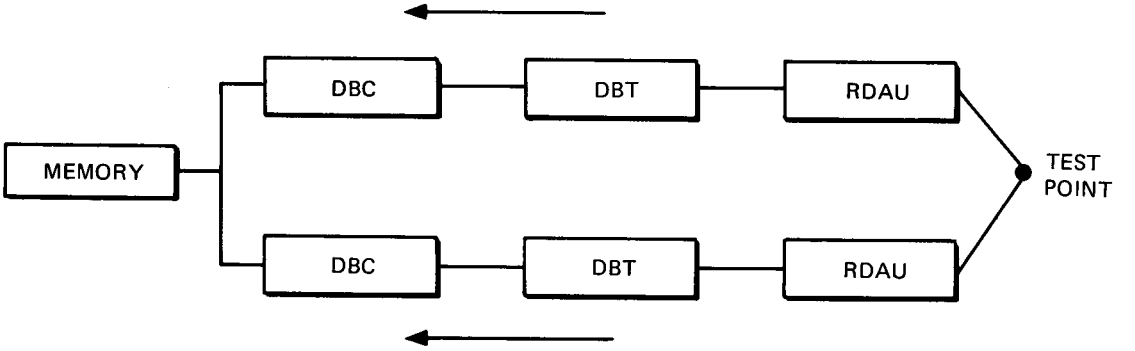
(g) SET CONFIGURATION CONTROL REGISTERS



P_a - OPERATIONS PROCESSOR

P_b - EITHER AN EXPERIMENT OR AN OPERATIONS PROCESSOR

(h) PRIMARY/SECONDARY DATA PATH



NOTE:
A FAILURE AT ANY POINT IN THE DATA PATH FROM THE DBC TO THE RDAU CAN CAUSE A RECONFIGURATION TO THE SECONDARY DATA PATH

5.1.5.2 COM Test Software Sizing

The general organization and descriptions of Continuous Orbital Monitoring tests are shown pictorially in Figure 5-16. Three main groupings occur based on the rate at which each group is performed. Within each group, there is included the item being tested and the name of a test implemented on the item under test. There is another category not shown in Figure 5-16, i.e., an "ON DEMAND" group initiated by the crew. Accompanying each test is an estimate of CPU time, memory required, and the I/O time if applicable. The CPU times are based on a 1 microsecond memory cycle time and instruction timing formulas of the System/4 Pi Model EP computer. Where System/4 Pi timing formulas were used, the times were scaled to take into account the 1 microsecond memory (4 Pi EP memory cycle time is normally 2.5 miscroseconds). Where System/4 Pi EP instructions were not available for the study, appropriate System/360 timing formulas were used.

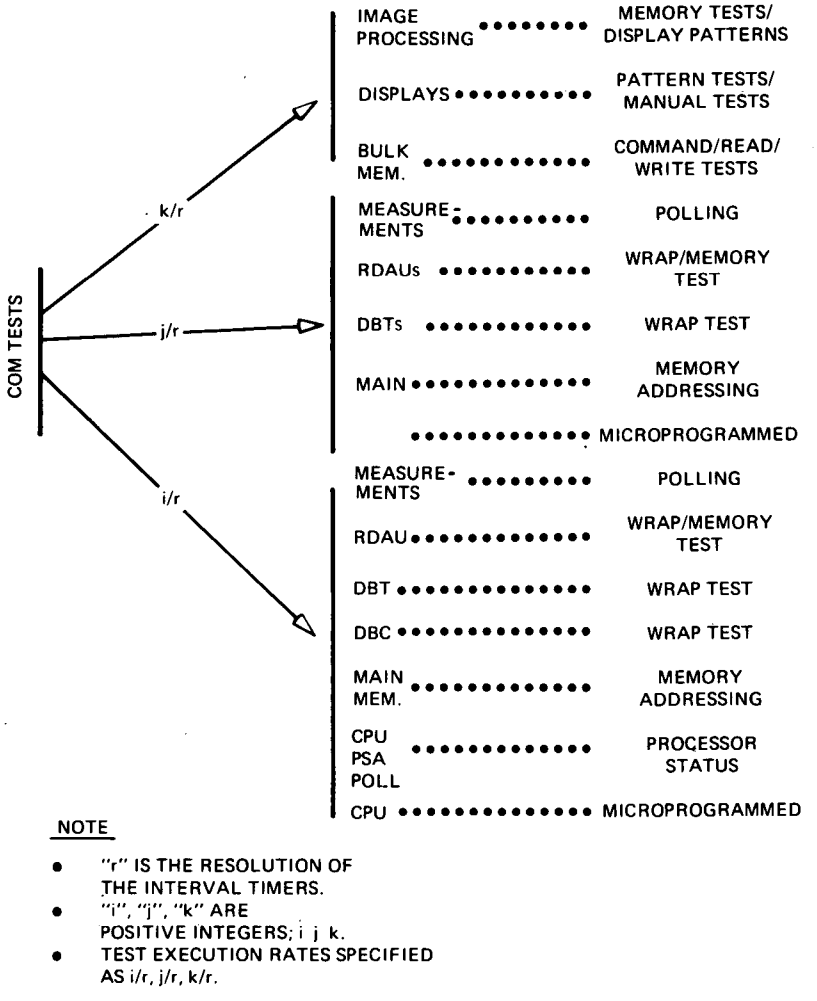


Figure 5-16. COM Test Organization

5.1.5.2.1 CPU COM Test - It is assumed that the CPU test is microprogrammed and initiated with a "DIAGNOSE" instruction. For timing purposes, it is assumed that the test requires 10 milliseconds to execute. The results of the test are read out to a "diagnostic scan out" area of the processor preferential storage in shared main memory. The test results are accessible by other processors for fault detection/isolation purposes. In the assumed implementation there are two methods of indicating that a CPU is in trouble:

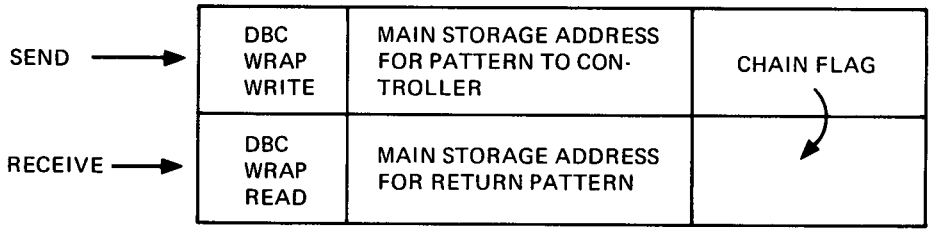
- The processor-to-processor link via the bus controller. This would be a "write direct" to the OCS processor which would generate a machine check interrupt.

- If the above path fails, the OCS processor will poll PSAs to look at the diagnostic scan out area for all processors.

The flow and sizing estimate for the diagnostic scan out area poll are shown in Figure 5-17.

5.1.5.2.2 COM Memory Addressing - The memory addressing test will consist of addressing all main memory locations. A location which cannot be read will cause a parity error. The flow and sizing estimate are shown in Figure 5-18.

5.1.5.2.3 Data Bus Controller COM "Wrap" Test - This test consists of issuing special I/O commands to configure the DBC to a test mode. A hardware feature in the DBC will permit a pattern from main memory to be transferred to the DBC which will "wrap" the pattern to the lines to be relocated in memory. The patterns returned to memory are compared to those sent for failure information. The patterns will be stored on a byte basis and there will be 256 patterns or bytes. The "wrap" test will be performed on all four data bus controllers. The command word format will be as shown below.



The test flow and sizing estimate are shown in Figure 5-19.

5.1.5.2.4 Data Bus Terminal COM "Wrap" Test - This test will be identical to the data bus controller "wrap" test where I/O commands will configure the DBT to a test mode. Patterns will be transferred from memory to the terminal

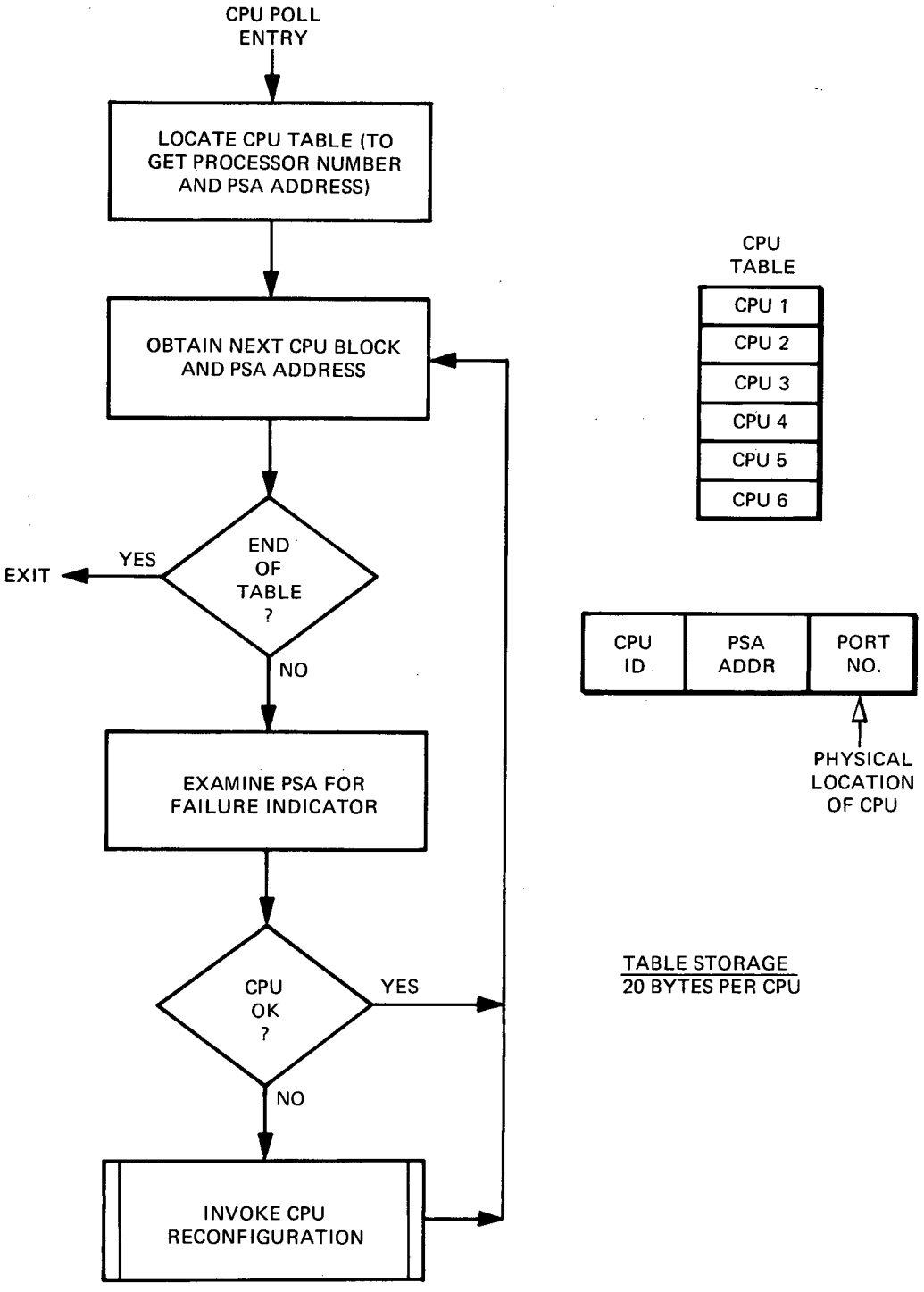


Figure 5-17. CPU Diagnostic Scan Out Area Poll

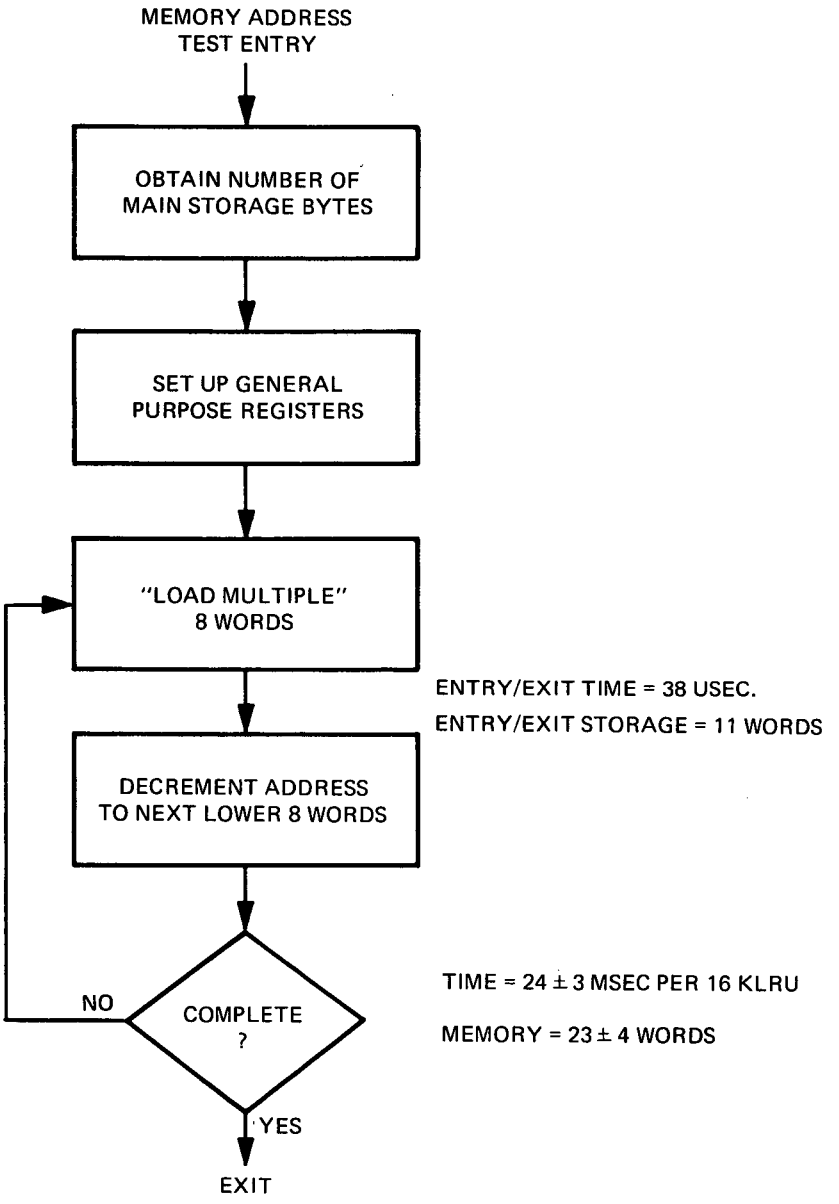


Figure 5-18. Memory Addressing Test Flow

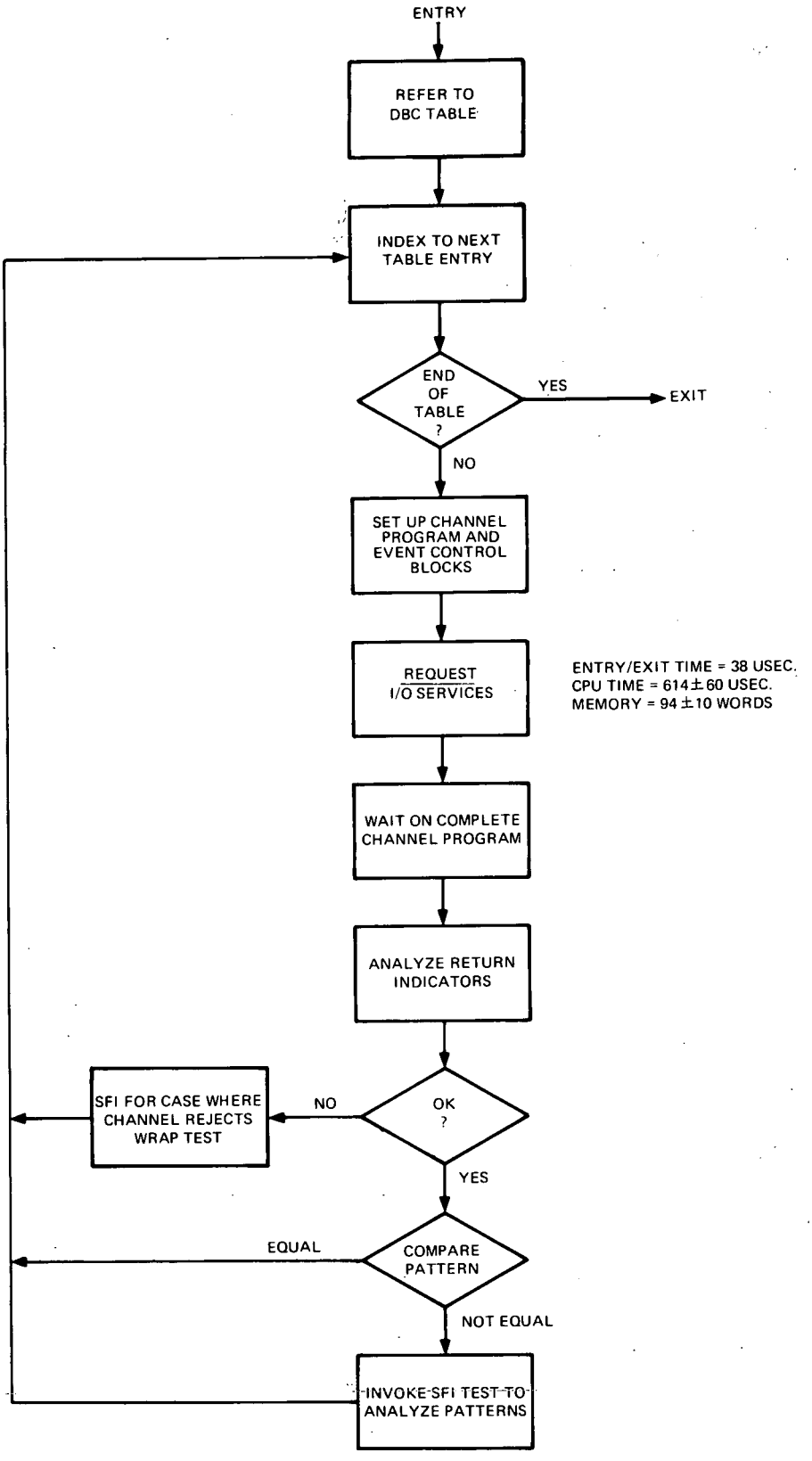
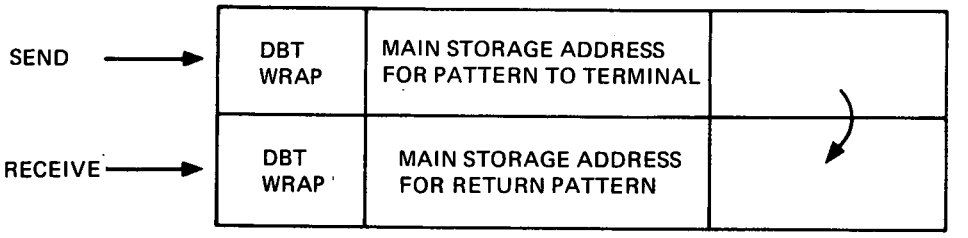


Figure 5-19. DBC COM Wrap Test Flow

and returned to memory for comparison. The patterns are stored on a byte basis, and there will be 256 patterns or bytes. The command word format is as shown below:



There is an additional "time" or delay involved in this test; i.e., there is an I/O time required for the serial transfer of the patterns to the terminal and for the serial return. I/O time is based on a data bus bit rate of one megabit per second.

The flow is essentially the same as for the data bus controller "wrap" test (Figure 5-19). The sizing estimate is as follows:

ENTRY/EXIT TIME = 38 usec

CPU Time/Terminal = 397 $\pm$40 usec

Memory = 98 $\pm$10 words

I/O Time/Terminal = 4096 usec

NOTES:
1. Data bus time is the transfer of 256 bytes at 16 usec per byte. Total I/O time = 200,000 usec for 50 terminals.

2. The CPU time is 46 + 351 n, where "n" is the number of terminals. Total CPU time is 17,600 usec for 50 terminals.

5.1.5.2.5 RDAU COM Tests - There are two tests associated with the RDAUs; i.e., one is similar to the DBC/DBT wrap tests, and the second is a memory/multiplexer test. In the first test, a form of "wrap" test is performed but a pattern is not transferred from main memory. Instead, a DC voltage developed within the RDAU is connected to one channel of the multiplexer. The voltage is converted to digital and transmitted to the CPU for comparison to an expected value. The flow is essentially the same as for the DBC/DBT tests (Figure 5-19) and, for this reason, is not repeated. The sizing estimate is as follows:

ENTRY/EXIT TIME = 38 usec

CPU TIME = 18,750 $\pm$1875 usec (for 133 RDAUs*)

MEMORY = 38 $\pm$4 words

I/O Time = 1400 $\pm$ 1400 usec (105 usec/RDAU)

*Formula for CPU time = 46 + 138 n, where n = number of RDAUs.

The second RDAU test is the memory/multiplexer test. In this test the contents of RDAU memory are read to verify that the contents are as expected, and then a sequential "read" is made to verify all channels of the multiplexer. The approximate RDAU memory assumed is:

LIMITS	64 Bytes
ANALOG MASK	4 Bytes
DISCRETE MASK	4 Bytes
EXPECTED DISCRETE PATTERN	4 Bytes
TOTAL	76 Bytes

The total entry/exit time, CPU time, and I/O time for the tests will be the sum of the times required for the individual tests. The test flow for the memory/multiplexer test and the sizing estimate are shown in Figure 5-20.

5.1.5.2.6 Image Processing COM Tests - An assumption is made that a crew member must manually initiate or commit a device within image processing to actual test performance.

The COM tests cannot interrupt any operation being executed within the experiment group or within bulk memory. It is assumed that a recommended schedule for testing will be relayed to the crew via a CRT display.

In the actual image processing test, the only OCS processor participation is in the check of the permanent and working digital storage and displays (again it is performed only upon authorization or request by a crew member because the test may destroy memory contents). The actual memory tests will consist of transmitting patterns from the OCS to the memories and rereading the memory for pattern comparison. After completion of the memory test, a display pattern is written on the CRTs. The display test pattern will contain all alphanumerics which will be observed by the crew. Successful completion will be entered into a keyboard. The remainder of the image processing group is assumed manually controlled through BITE equipment. These tests will not affect the software sizing. The test flow for the memory test is shown in Figure 5-21.

For the display part of the image processing tests, additional display assumptions were required. These include:

- Operation similar to IBM 2250 Display
- Vector capability
- At least 64 characters

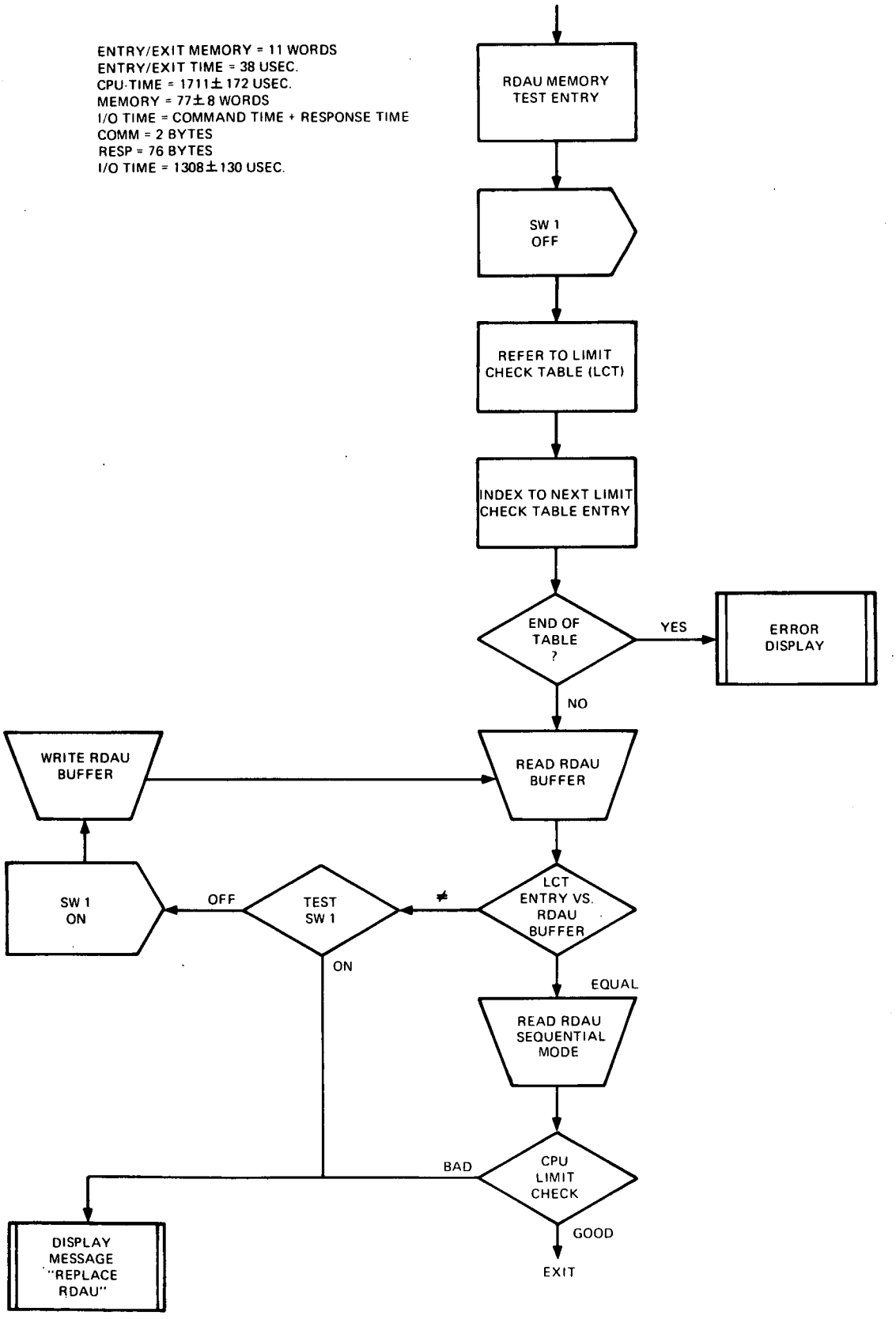


Figure 5-20. RDAU Memory/Multiplexer Test Flow

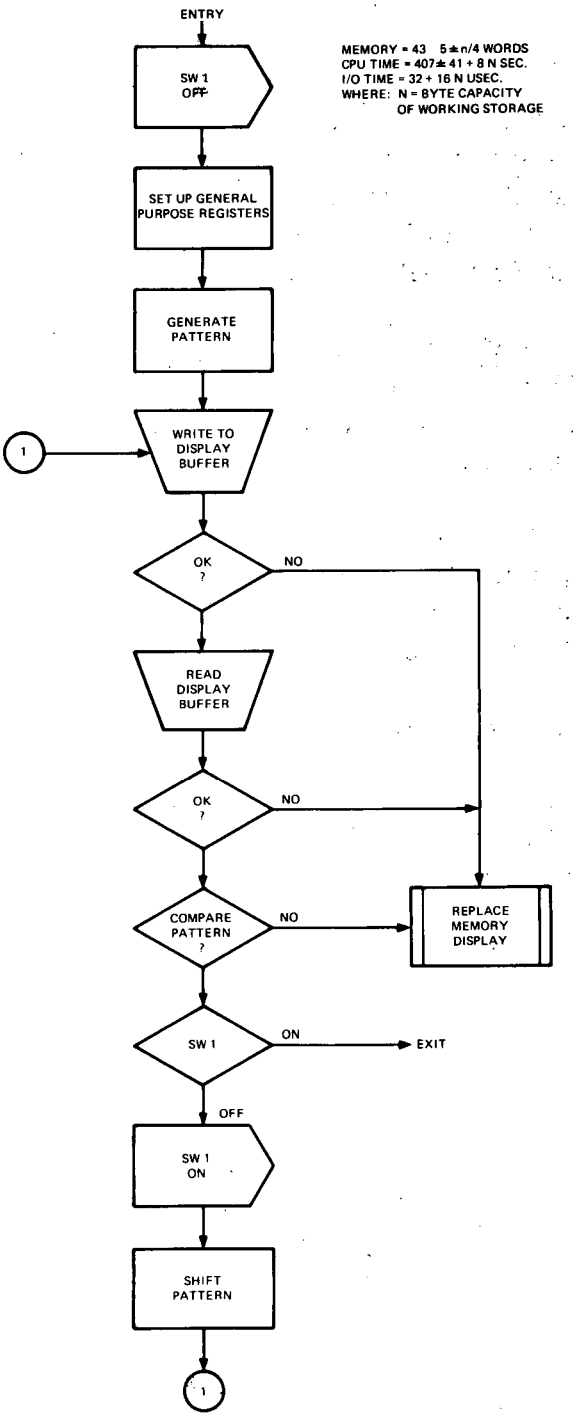


Figure 5-21. Image Processing COM Memory Test Flow

A candidate display pattern which can be sized is shown in Figure 5-22. The display utilizes all symbols, numerics, vectors, etc. The flow for the test pattern is shown in Figure 5-23.

5.1.5.2.7 Bulk Memory COM Tests - The bulk memory tests will be authorized by a crew member as in the image processing tests. In the case of tapes, a crew member must mount a special test tape. The actual tests for peripheral devices are fairly standard and consist of the execution of the various device commands and of writing/reading bit patterns. A top level flow for the bulk memory tests is included in Figure 5-24. Sizing estimates are based on the IBM System/360 On Line Test System (OLTS).

5.1.5.2.8 DMS COM Measurement Limit Checks - In addition to the software programs and BITE provisions, a series of measurements must be made on certain DMS equipment. The measurements will be concerned principally with power supply measurements and temperature measurements.

Since each RDAU independently polls and limit checks measurements, there is no separate program flow as such. If an out-of-tolerance condition occurs, it ultimately causes a program interrupt and the RDAU is checked through a "wrap" and "memory/multiplexer" tests discussed earlier.

5.1.5.2.9 GN&C Preprocessor COM Test - Without explicit details of the preprocessor characteristics, actual test descriptions cannot be evolved. For purposes of sizing the DMS-OCS, it is assumed that the preprocessors have an integral test capability through incorporation of BITE, and that they will respond to test commands from the OCS via the data bus. The response from the

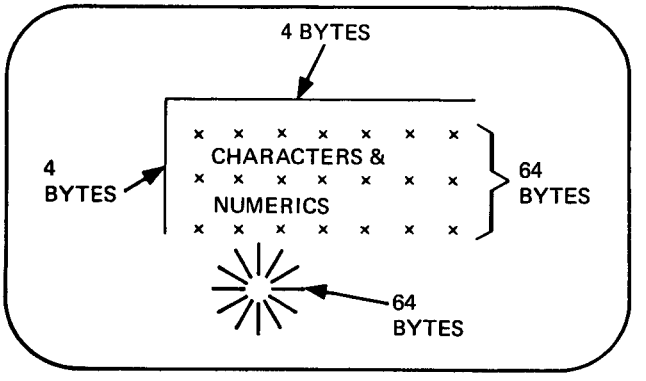


Figure 5-22. Sample Display Test Pattern

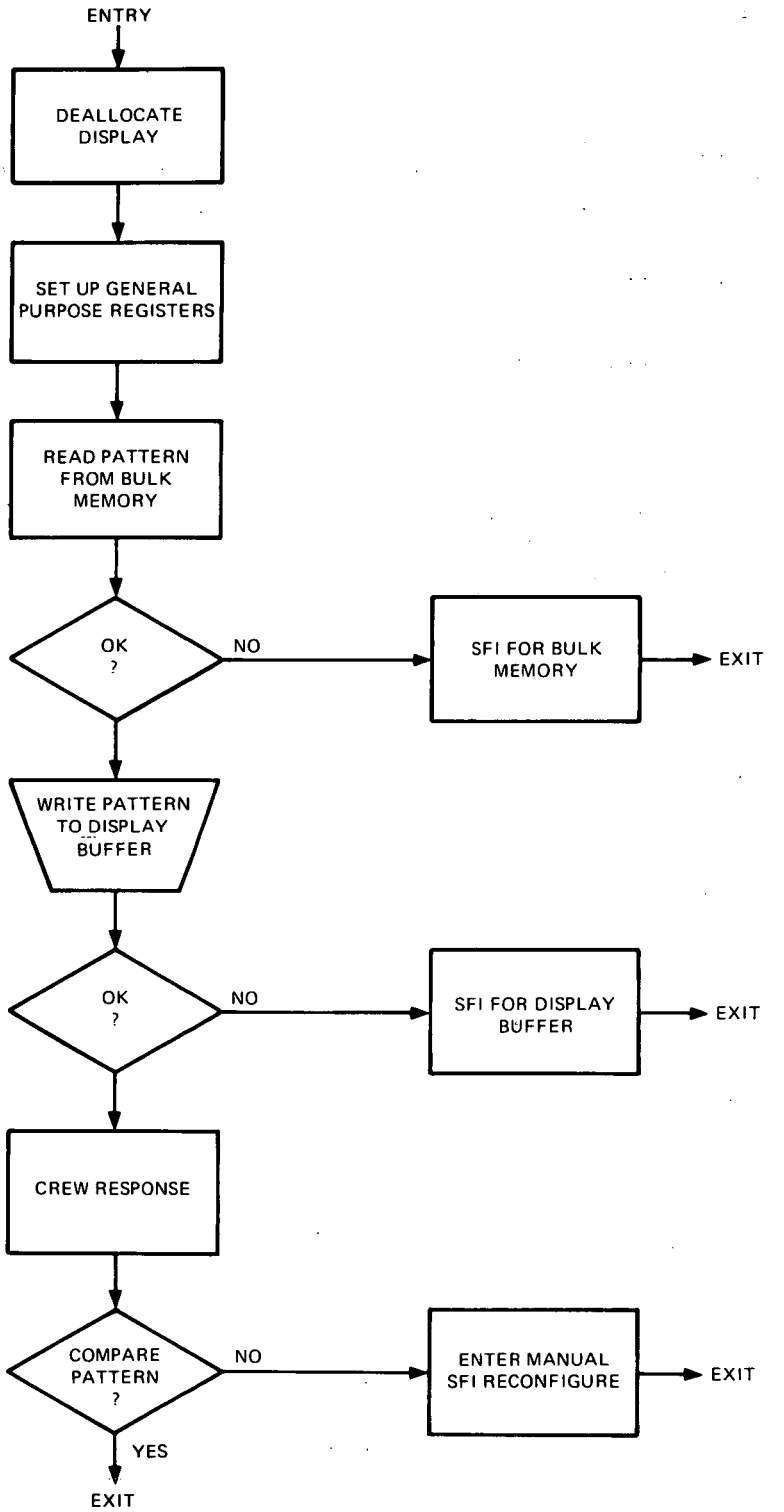


Figure 5-23. Image Processing Display Test Flow

preprocessors is assumed in the form of a GO/NO GO discrete signal. The power supplies for each preprocessor will be monitored and limit checked by RDAUs. The sizing estimate is as follows:

Memory = 100 ±50 words

CPU Time = 40 ±20 usec

I/O Time = 100 ±30 usec/processor

5.1.5.3 Subsystem Fault Isolation Test Software Sizing

In many cases, the performance of the COM tests, through the device addressing, inherently yields fault isolation. Consequently, many of the SFI tests will be common to the COM tests. The capability must exist for performing any of the COM tests (which may be utilized as SFI tests) upon initiation by a crew member. The SFI tests which are common to the COM tests include the CPU tests, data bus controller, data bus terminal, RDAU, displays, bulk memory, and image processing. Unique tests are required in the area of memory units and switch matrices.

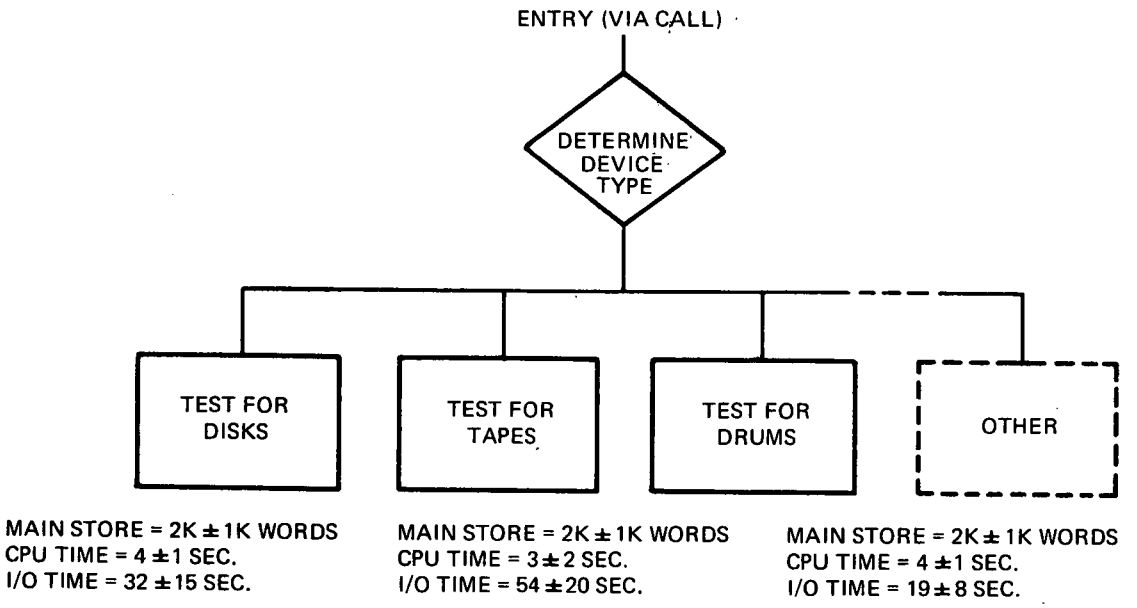


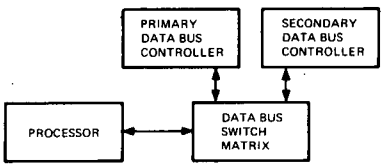
Figure 5-24. Bulk Storage COM Tests

5.1.5.3.1 Shared Main Memory - The COM main memory test checked to determine if each memory location could be addressed. The SFI test consists of generating a pattern in one location in memory, writing the pattern into the memory under test, and re-reading the pattern to compare it to the original pattern. The SFI flow and sizing estimate for the memory test is shown in Figure 5-25.

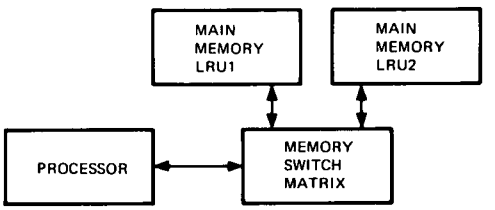
5.1.5.3.2 Switch Matrix - There are two switch matrix units in the baseline; i.e., a data bus controller switch matrix and a memory switch matrix. There will not be an explicit switch matrix test, but rather one of the COM tests may be attempted in different configurations to logically isolate the problem.

Three cases have been considered for problems associated with the switch matrices.

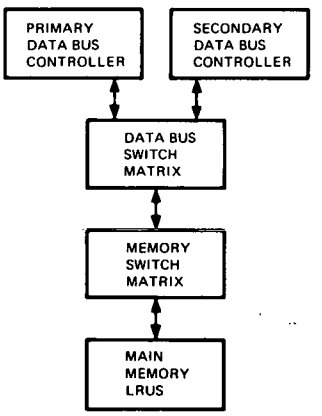
- Case "A" - A problem exists in communication between a processor and a data bus controller as shown below:



- Case "B" - A problem exists in communication between the processor and memory as shown below:



- Case "C" - A communication problem exists between the data bus controllers and main memory as shown below:



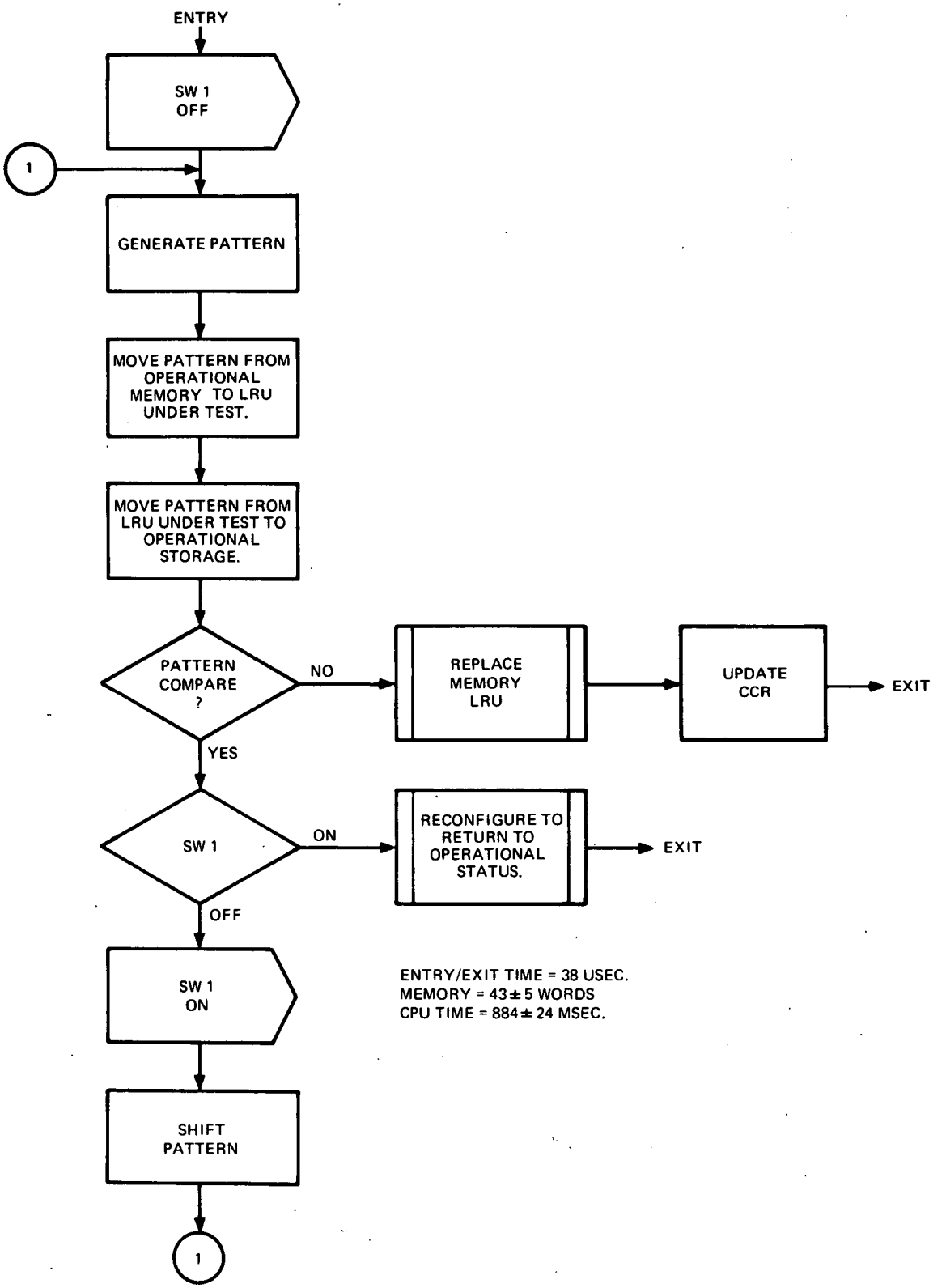


Figure 5-25. Shared Main Memory SFI Flow

Flows for Cases "A," "B," and "C" are shown in Figures 5-26, 5-27, and 5-28.

The aggregate of CPU time and memory required to implement the three cases described is:

CPU time = 200 ±160 usec

Memory = 150 ±100 words

5.1.5.4 DMS Reconfiguration Software Sizing

A set of subsystem elements in which communication and control paths are established constitutes a prevailing "configuration." When elements are added, deleted, or substituted, a new configuration is created; the process of establishing the new configuration is called "reconfiguration." Whenever reconfiguration takes place, the total resources of the subsystem have changed, and appropriate actions are required such that OCS is aware of the conditions. Reconfiguration can be invoked due to failures or due to a resource reallocation, but this report does not consider the latter. Configuration control normally is under program control, i.e., reconfiguration will occur automatically via OCS. Display messages will be sent to the crew for notification of reconfiguration or for cases where manual actions are necessary.

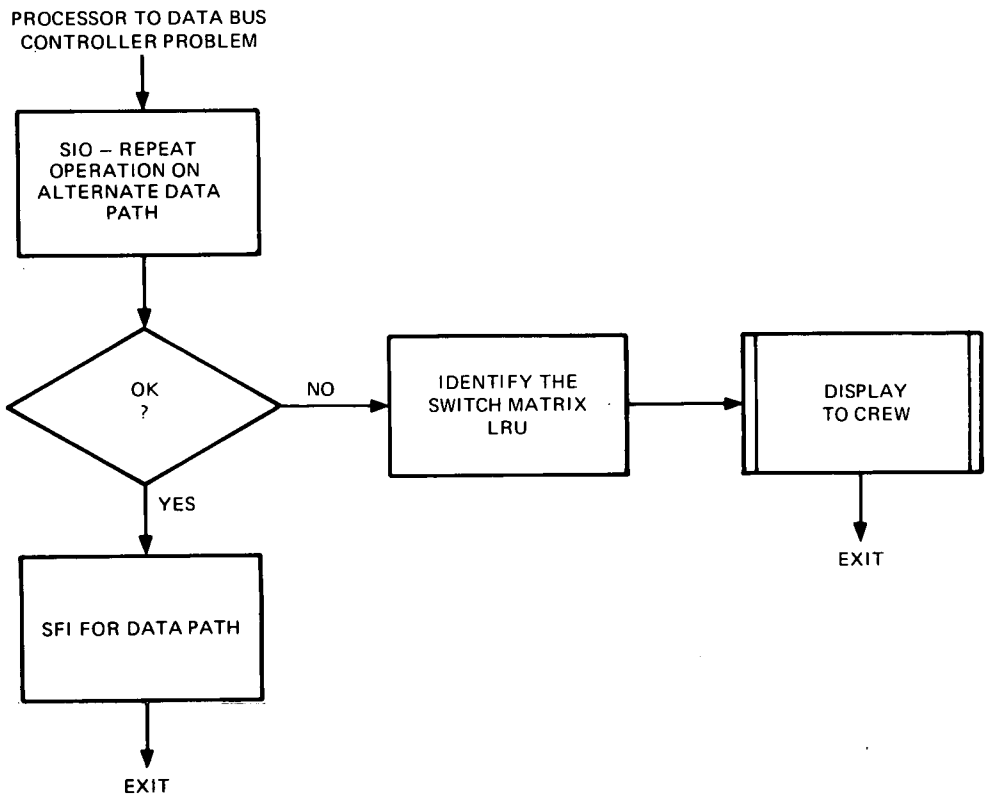


Figure 5-26. Case "A" Flow

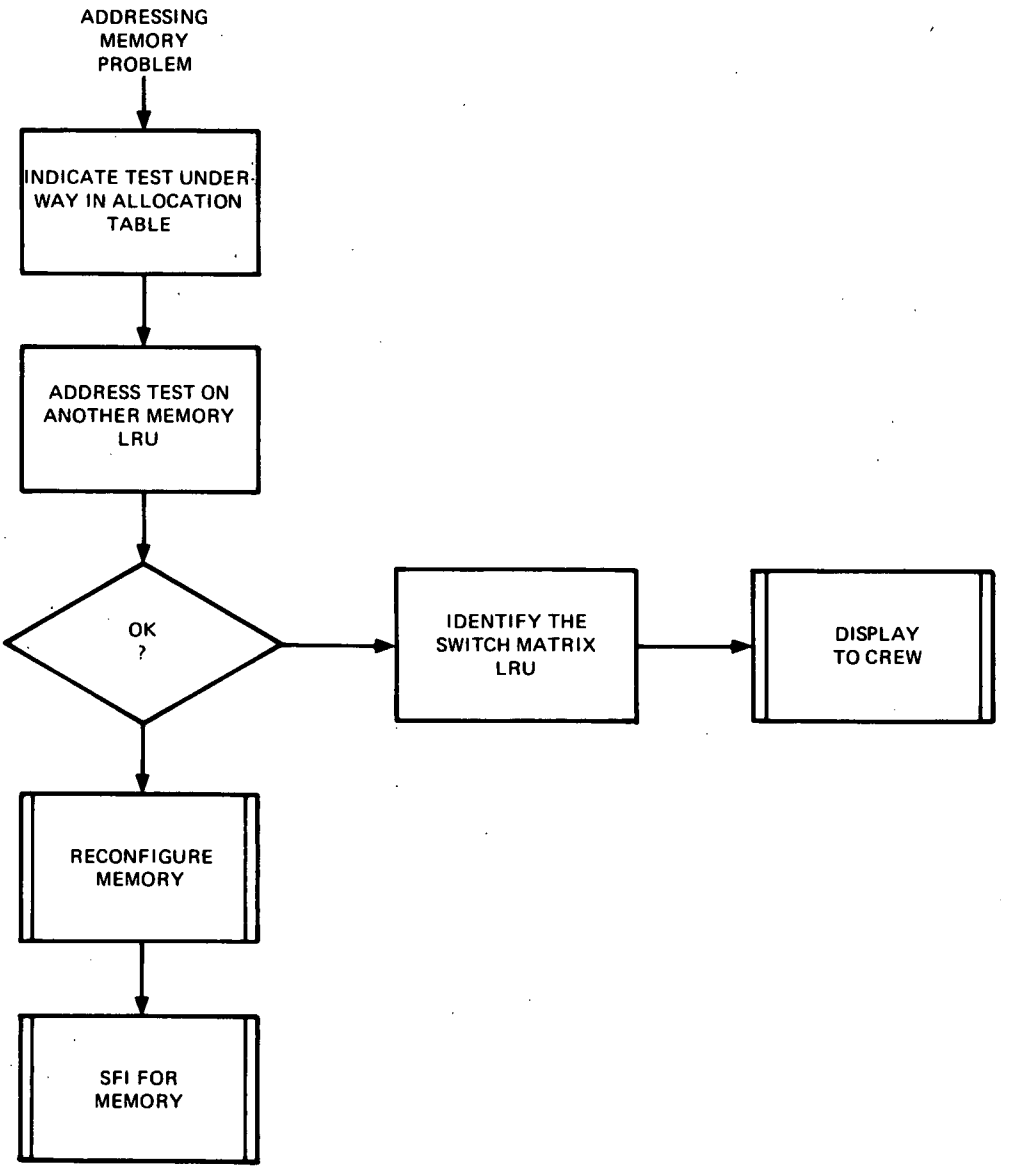


Figure 5-27. Case "B" Flow

Depending on the source of error or malfunction, certain events must occur. In the event of a memory element failure, it must be determined what the contents were, if the contents are recoverable, or if the data is available from other sources, and what program restart steps are necessary. In the case of an I/O failure, configuration control registers and the bus controller table must be updated. If a CPU fails, other CPUs must be notified, and some form of analysis of the intermediate results from that processor may be required. For bulk memory failures, it is necessary to update the bulk memory allocation table. Figures 5-29 through 5-32 show representative flows for the CPU, main memory, the data acquisition path, and bulk memory. CPU time and memory estimated for each are included in the figures.

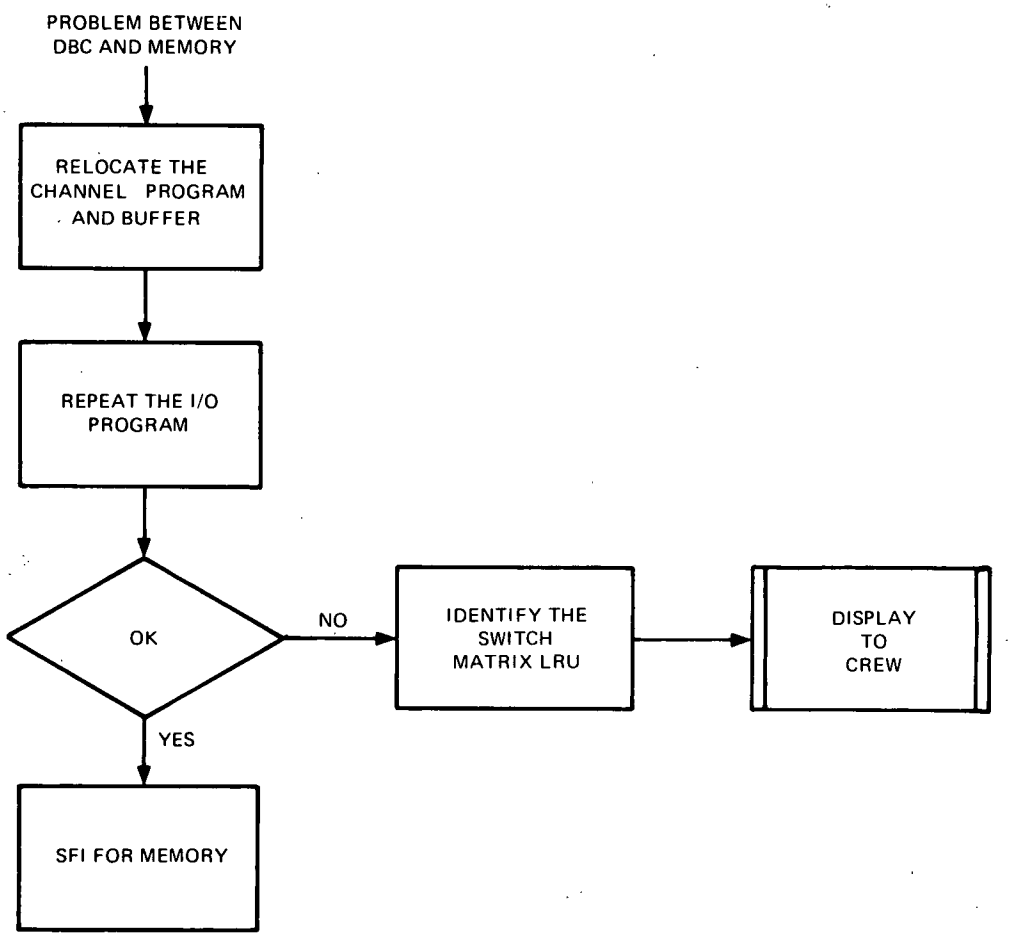


Figure 5-28. Case "C" Flow

5.1.5.5 Program Restart Software Sizing

Subsequent to the steps of detection, isolation, and reconfiguration, it is necessary to resume program operation - ideally with nothing lost in the form of data. Attempting program restart without loss of data necessitates even further definition of the types of data inputs and of the baseline design.

The approach taken has been to define restart categories, assume one category (a worst case) for implementation, assume a technique for restart, define the system, generate the flows, and perform the sizing estimate. The principal reason for assuming one design was that there were seven recovery categories with six failure modes or 42 possible analyses that could be performed. The case assumed was that a real-time data source was being used, that a failure had occurred in working storage, and that a checkpoint/restart technique would be utilized for recovery purposes.

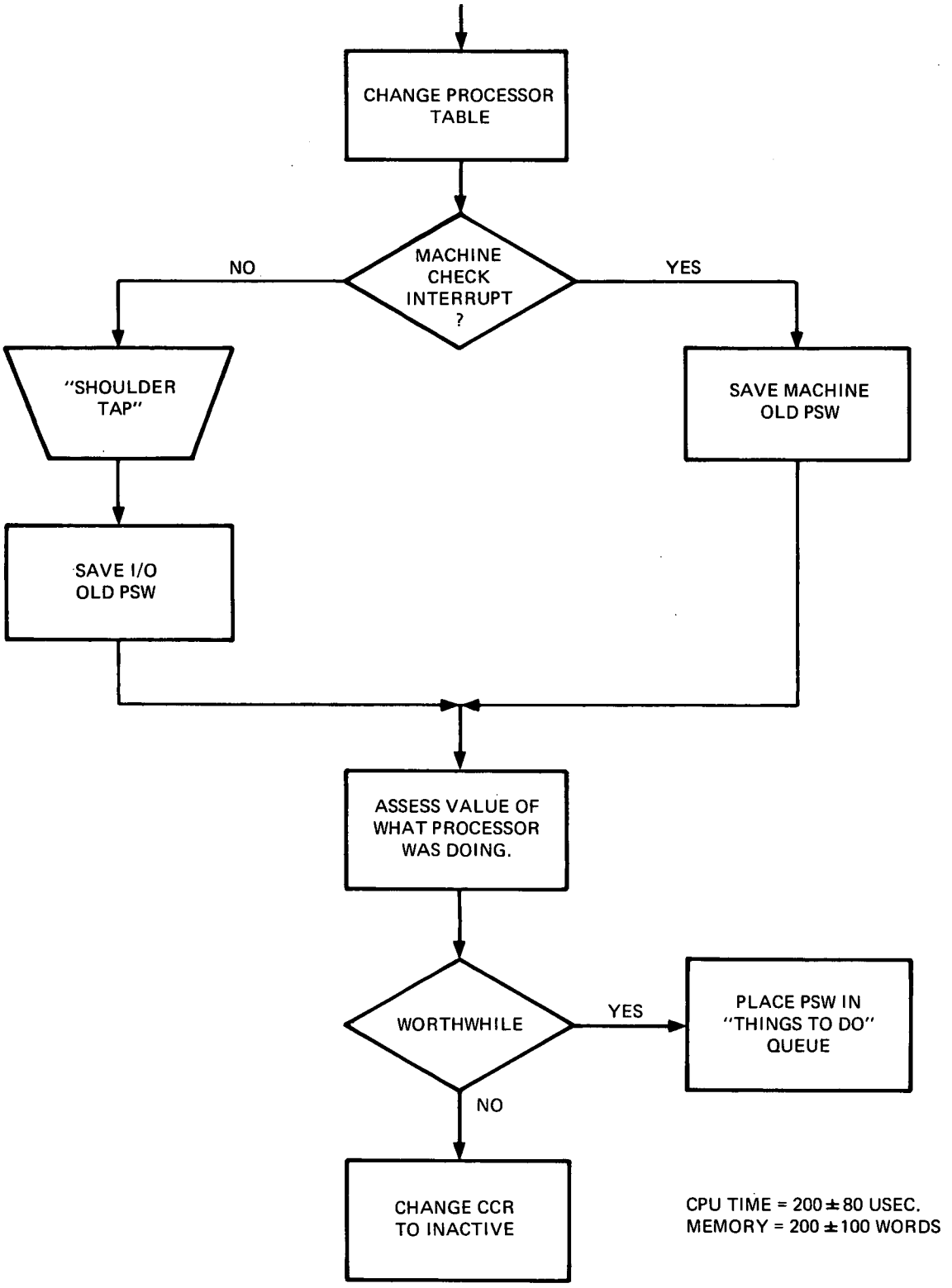


Figure 5-29. CPU Reconfiguration

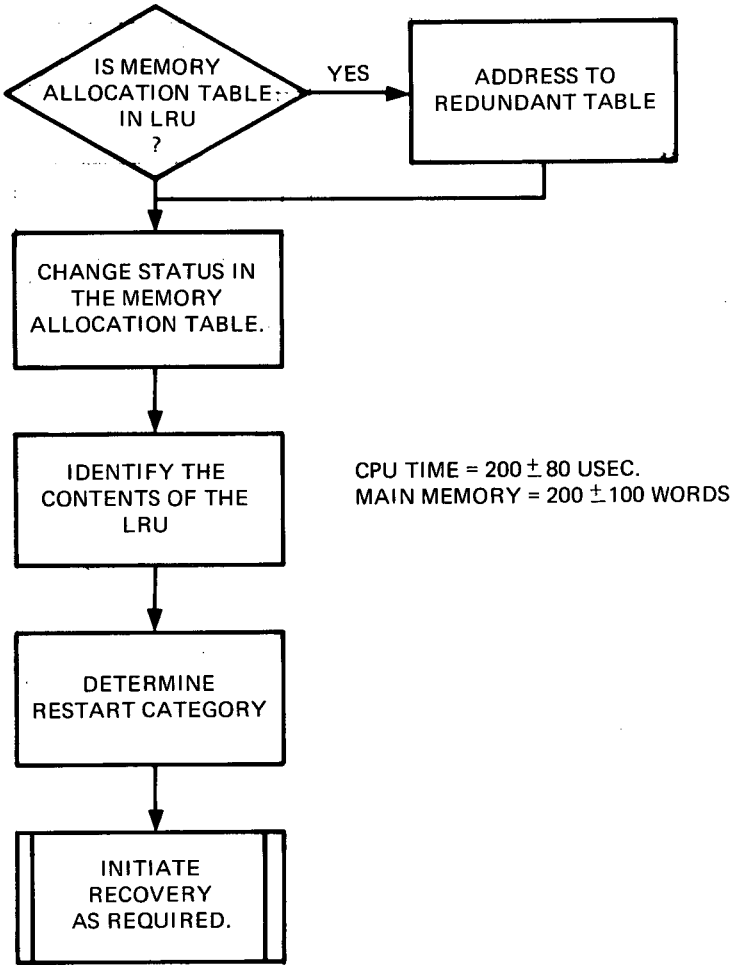


Figure 5-30. Main Memory Reconfiguration

5.1.5.5.1 Program Restart Categories - The various program restart categories arise due to variations in the character of data inputs, whether or not intermediate results are useful and should be utilized in recovery, or whether it is permissible to neglect past data and begin again. Seven restart categories are discussed below.

- In this category, the program is driven by real-time data and inter-arrival time between records, either explicitly or implicitly, forms part of the input. Recovery must make use of the results obtained when the program last ran, the data which caused the latest execution, and the time which has elapsed since the previous cycle.

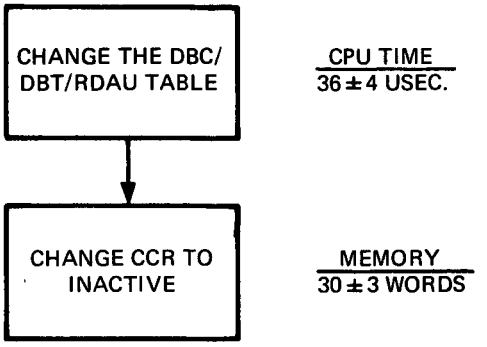


Figure 5-31. Data Acquisition Reconfiguration

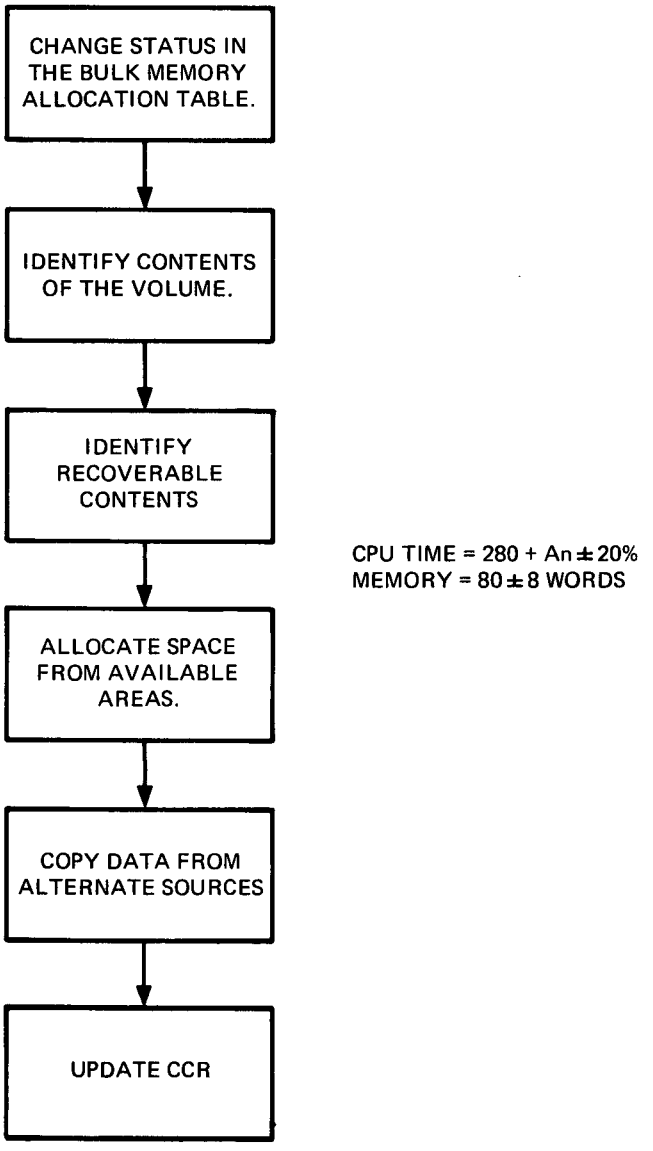


Figure 5-32. Bulk Memory Reconfiguration

- The same as in the previous paragraph except that the inter-arrival time is not a part of the program input.

- The program is driven by real-time data, but the results from previous executions can be ignored for the purposes of restart. Two subsets of this category would be where inter-arrival time is and is not significant as part of the input.

- The program does not process real-time data, but it is advantageous to be able to resume execution at some point other than the beginning of the input stream because of the time required for program execution. In this case, the intermediate results and the relative position in the input stream are checkpointed.

- Program does not process real-time data. Restart consists of repositioning to the beginning of the input stream and rerunning the program.

- The program processes real-time data, but it is not necessary to log the data or to checkpoint the intermediate results. Restart consists of first refreshing the program text and then beginning execution with the first input event which occurs afterward.

- This is a degenerate category for programs which are terminated upon failure of any resource being utilized. Restart is accomplished manually.

NOTES:
1. Whenever real-time data is being processed, it is assumed that either the data rate or the program execution time is such that "catch up" after recovery is possible.

2. It is also assumed that the program is "refreshable"; i.e., program instructions are kept separate from data and intermediate results. It also is assumed that the program instructions are never altered.

5.1.5.5.2 Restart Operation - For analysis purposes the worst case restart category was assumed where real-time data was being processed, past results were required, and inter-arrival time of data is significant. Figure 5-33 shows a diagram indicating overall operation.

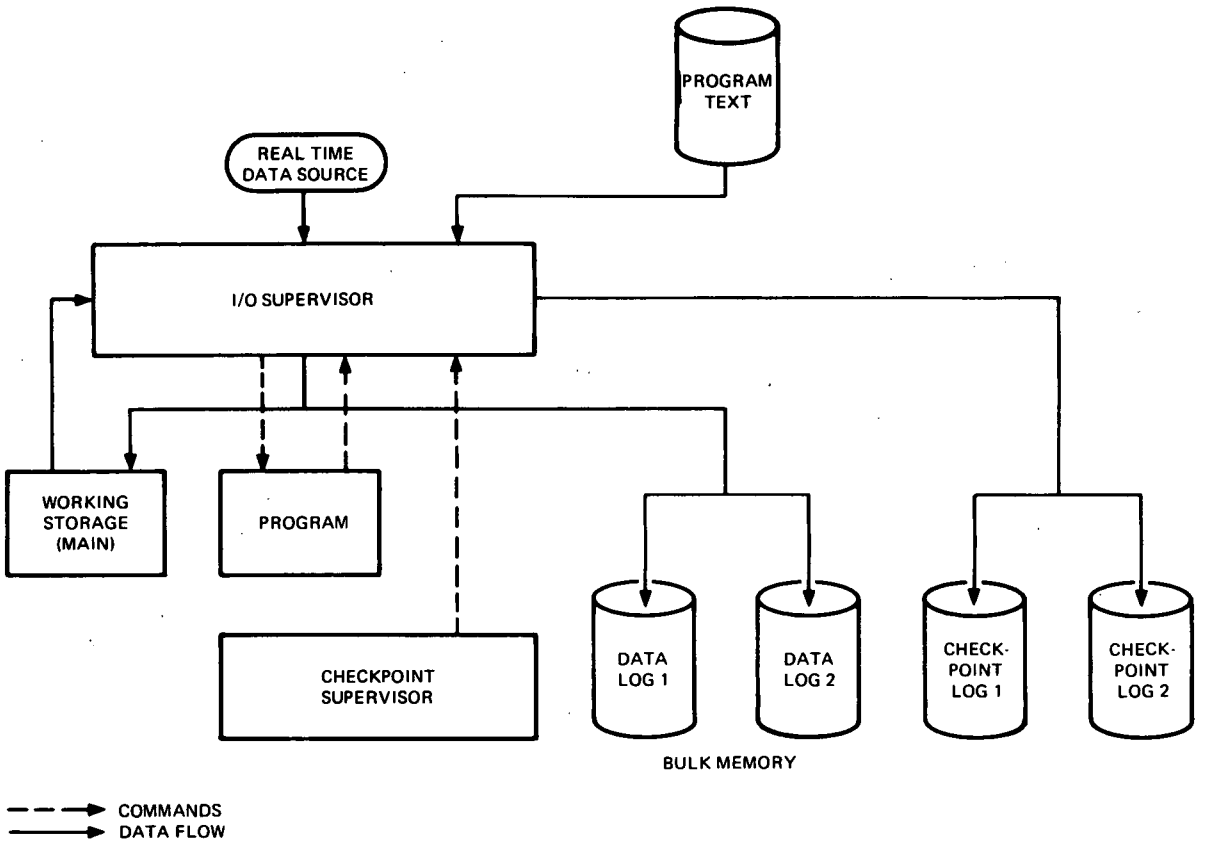


Figure 5-33. Diagram - Program Checkpoint and Data Logging Operation

In Figure 5-33, input data is via the Real-Time Data Source. The actual program executing is redundantly stored in bulk memory. The input data is fed to two places; i.e., to main working storage and to a data log (also in bulk memory). This is a temporary storage area for data between checkpoints (data log also occurs redundantly for recovery purposes). A checkpoint supervisor will cause intermediate results in working storage to be transferred to the redundant checkpoint log, under program control. If a failure occurs in the main program, reconfiguration will occur, the program text will be read into the new memory unit, intermediate results from the last checkpoint are read into working storage, and data from the last checkpoint will be utilized from the data log until the processor "catches up."

The sequence described represents that for a failure in a main storage unit containing an application program. For other failures there will be a somewhat different sequence. The failures which should be considered include:

(a) Main store unit containing program

(b) Main store unit containing working storage

(c) Processor failure

(d) Storage device containing data log

(e) Storage device containing checkpoint log

(f) Storage device containing program text

The actual sizing analysis has considered (a) only, but it is assumed that the other five failure modes will be approximately equivalent to (a) in complexity. Figure 5-34 shows a flow and sizing estimate for the sequence described previously.

Another aspect of program restart is the maintenance of continuity of operational data. This could be a failure external to the computer (e.g., within a bus controller, terminal, RDAU, or within bulk storage itself). Figures 5-35 and 5-36 are flows indicating how the data logs would be utilized during an unexpected interrupt emanating from an RDAU and from an attempt to read a record from a log which has failed.

5.1.5.6 Blocks and Tables

Maintaining configuration control, performing schedules, recovery, and failure verification, etc., imply several tables. There must be a table for device addresses down to the test point level, tables providing information on data paths, tables for scheduling the frequency of performing COM tests, failed item tables, memory allocation tables, a directory table to determine where the other tables are located, etc. The following is a preliminary list and sizing estimate for the blocks and tables assumed in this design. It also has been assumed that all tables must be redundantly stored.

5.1.5.6.1 Device Address Table - A table must be maintained for addresses down to the RDAU channel. The table should indicate (1 bit position) whether the primary or secondary data path should be used.

Memory = 4000 test points x 32 bits address = 8K words

Redundancy = 8K words

Total = 16K words

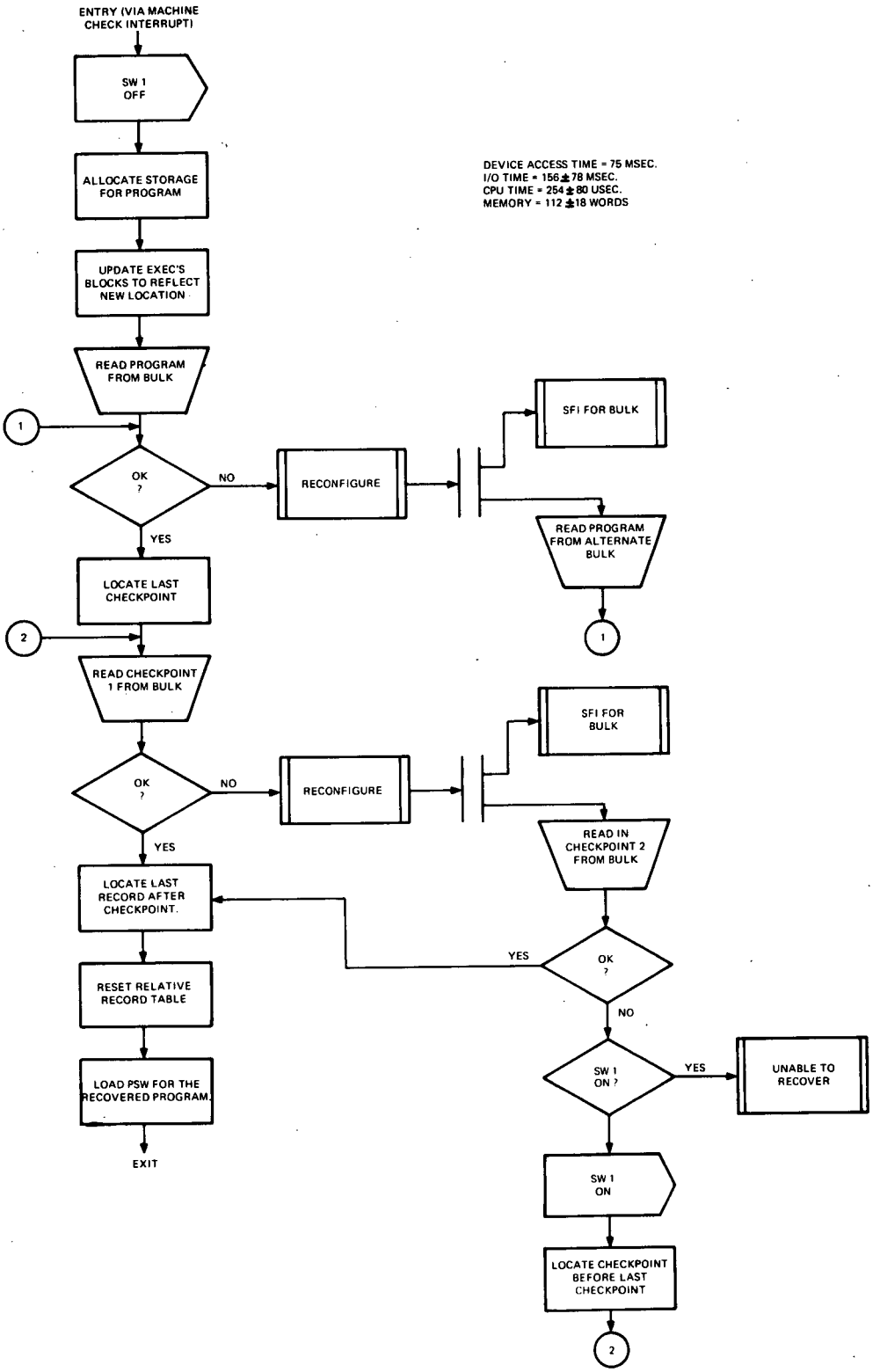


Figure 5-34. Program Restart Flow

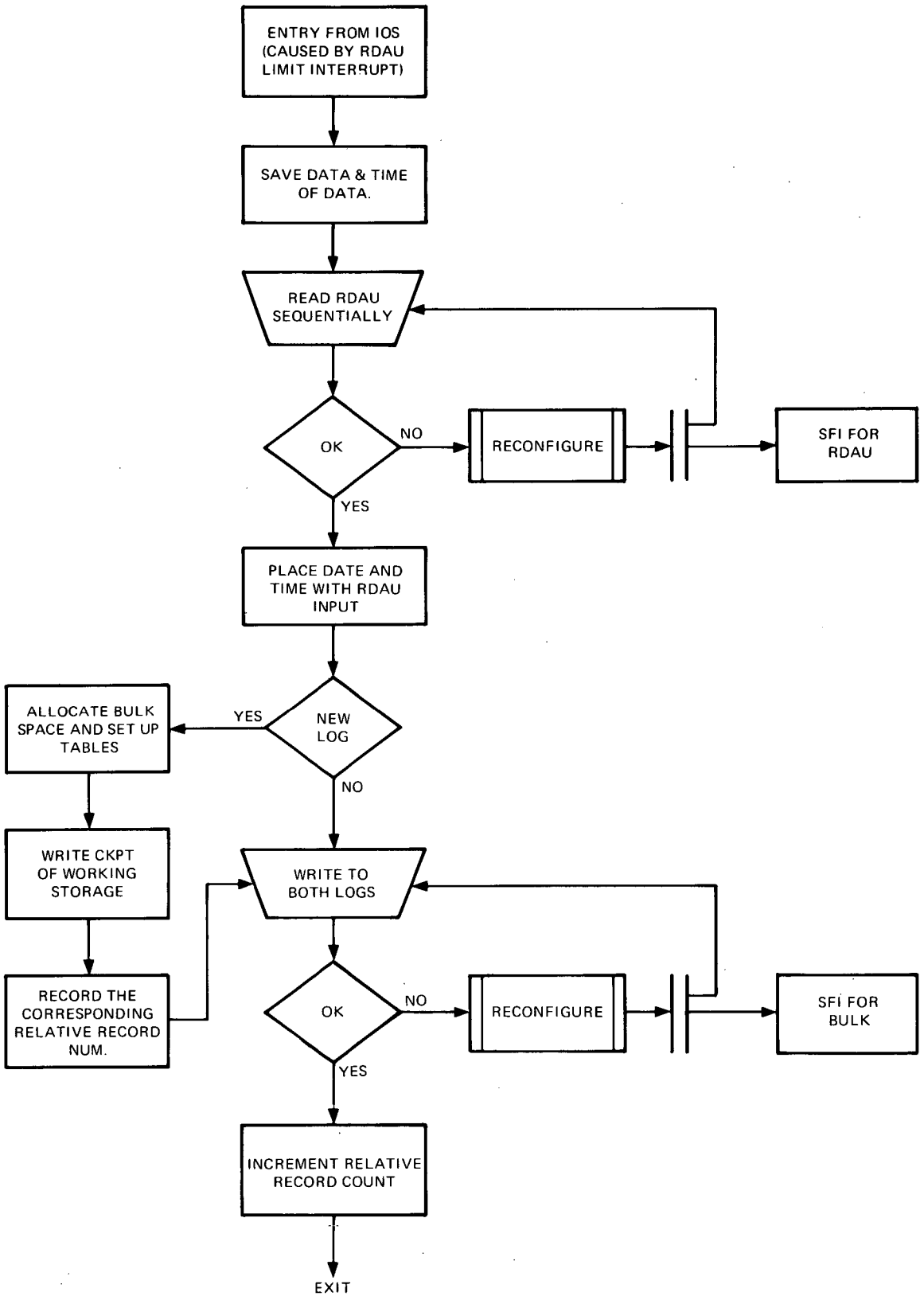


Figure 5-35. Log Supervisor 1

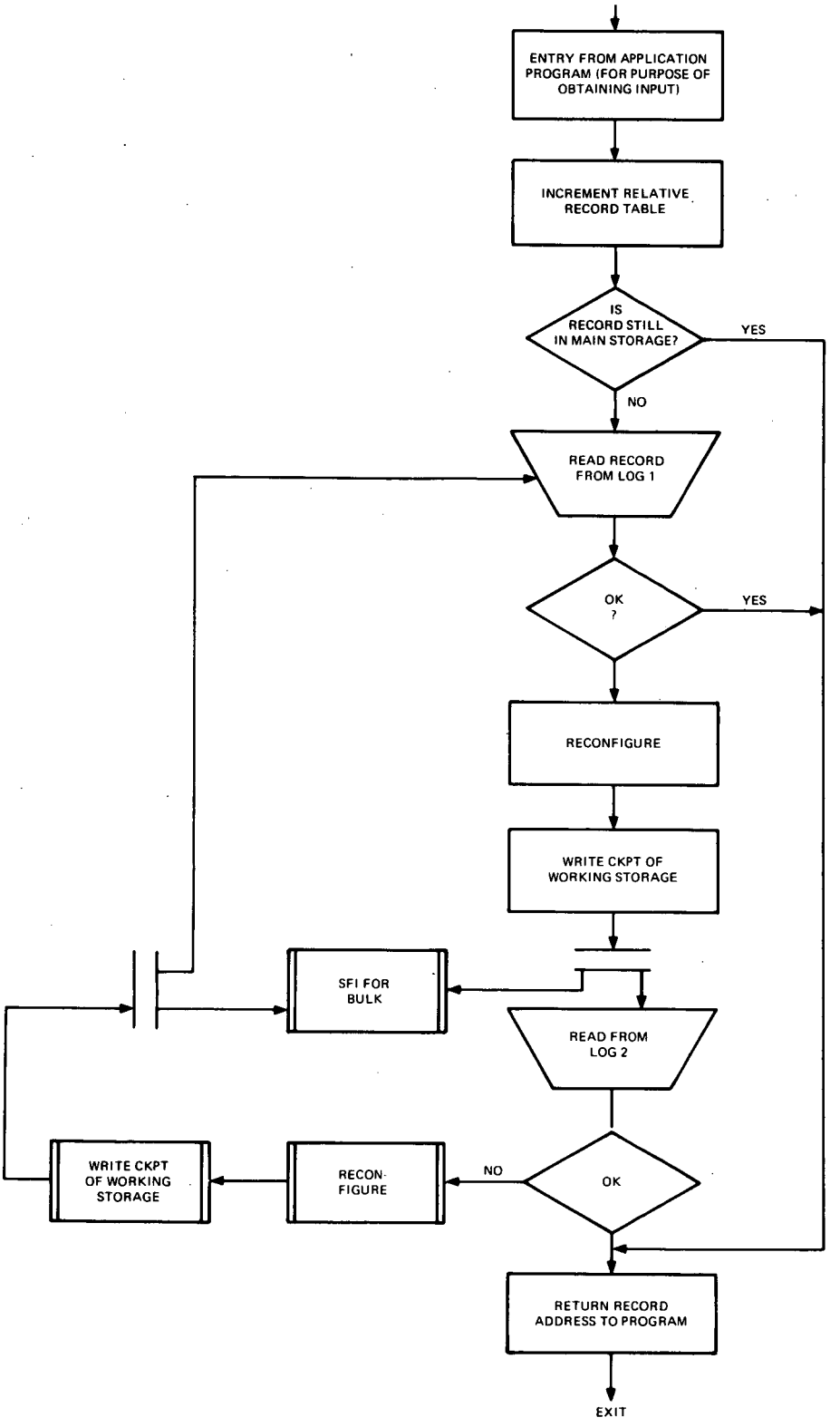


Figure 5-36. Log Supervisor 2

5.1.5.6.2 Data Path Table - This table indicates what bus controller, terminal, and RDAU are "on-line," what their addresses are, and whether they are operational, failed, under test, etc.

DATA PATH BLOCK

RELATIVE TEST POINT ADDRESS	PRIMARY POINTER TO DEVICE TABLE ENTRY	SECONDARY POINTER TO DEVICE TABLE ENTRY	3 WORDS

Memory = 4000 test points x 3 words/block = 12K words

Redundancy = 12K words

Total = 24K words

5.1.5.6.3 Limit Check Table - A copy of each RDAU memory must be maintained for each RDAU "read sequential." Verify the RDAU limit check mode.

RDAU Memory = 76 bytes (19 words)

Memory for 133 RDAUs = 133 x 19 = 2527 words

Redundant storage = 2527 words

Total memory = 5054 words

5.1.5.6.4 Processor Table - This table identifies each processor. It indicates the address of each processor's preferential storage area and the processor's operational status.

Memory = 6 processors x 4 words/proc. = 24 words

Redundancy = 24 words

Total = 48 words

5.1.5.6.5 Switch Matrix LRU Table - This table translates point-to-point switch matrix failures into LRU identification.

Total memory = 600 words (estimate)

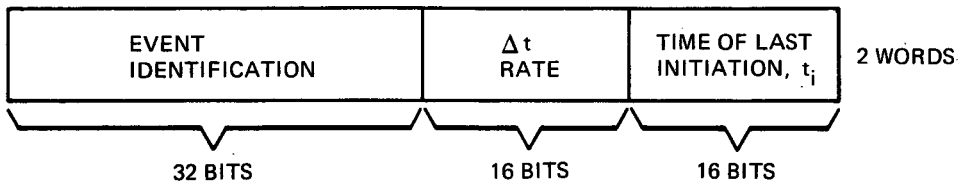
5.1.5.6.6 Memory Allocation Table - This table indicates what main storage LRUs are free, operational, under test, etc.

Memory = 22 LRUs x 4 words/block = 88 words

Redundancy = 88 words

Total = 176 words

5.1.5.6.7 Rate Table - This table is used to initiate events such as the COM tests which may occur at specified frequencies; e.g., once per 20 seconds, once per hour, etc. A priority also must be stored with each event. For sizing purposes, it is assumed that there may be 250 COM test events and 50 OCS executive events and that each event has a 2 word block size.

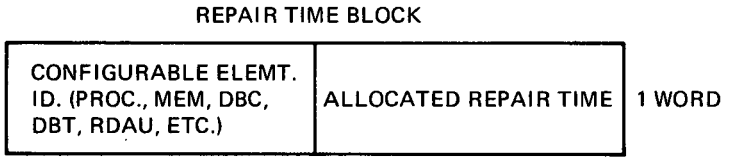


Memory = 300 events x 2 words/block = 600 words

Redundancy = 600 words

Total = 1200 words

5.1.5.6.8 Repair Time Table - This table is utilized to assure (via crew prompting) that the repair rate exceeds the failure rate. It will provide a time in which a failed LRU should be replaced.

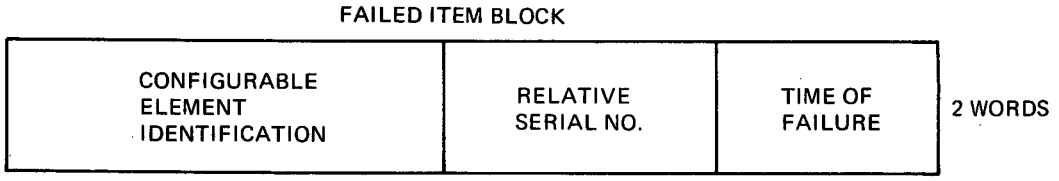


Memory = 1 word/block x 12 blocks for DMS = 12 words

Redundancy = 12 words

Total = 24 words

5.1.5.6.9 Failed Item Table - This table contains the configurable element identification and the time at which the item failed. It is used in conjunction with the repair time table to assure replacement.

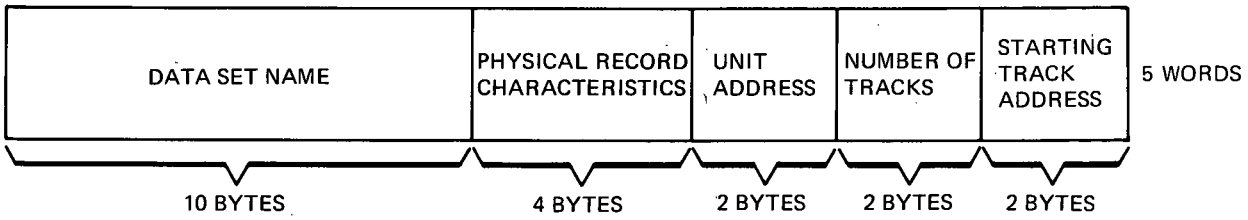


Memory = 2 words/block x 10 failure capacity = 20 words

Redundancy = 20 words

Total = 40 words

5.1.5.6.10 Auxiliary Storage Allocation Table - This table indicates the utilization and availability of auxiliary storage.



Memory = 200 data sets x 5 words/block = 1K words

Redundancy = 1K words

Total = 2K words

5.1.5.6.11 Directory Table - This table contains the locations of all tables. For each table there is a double entry due to the redundant storage.

Total memory = 8K words (estimate)

5.1.5.7 Executive Services

A three-level software hierarchy has been assumed in this design; i.e., there are individual application programs to check the various equipment within the DMS, there is a checkout executive to perform test scheduling, event initiation, and program restart, and there is a master executive to perform interrupt handling, scheduling of I/O services, and overall task scheduling. The executive services of the OCS and Master executives are:

- OCS Executive
  - Provides asynchronous event initiation; i.e., starting a test at a particular time to assure that the prescribed test rate is met.
  - Provides "configuration control register" management for configuration control purposes.
  - Initiation of tests in portions of the DMS which are outside the operational subset (i.e., in the experiment subset).
  - Provides program restart categorization and restart services.

- Master Executive Services

  - Provides I/O services with specific capabilities to start I/O (SIO), test I/O (TIO), halt I/O (HIO), and test channel (TCH).

  - Perform allocation of main storage resources.

  - Perform allocation of auxiliary storage resources.

  - Provide processor-to-processor READ/WRITE direct communication via the data bus controller.

  - Perform dynamic storage allocation for "save" areas, working storage, etc.

  - Perform data logging function.

  - Provide checkpoints for storage of intermediate program results for system recovery purposes.

5.1.5.8 DMS Checkout Sizing Summary

Table 5-3 summarizes the sizing estimates for the various OCS items discussed in previous sections. Some of the items had to be expressed in terms of the number of bytes handled or transferred. To get absolute values for these cases, further assumption would be required.

CPU times were calculated using estimates of the instructions needed to perform each "block" in the flow chart of the program. The time requirements of the instructions were then determined using timing formulas for models of the IBM System/360 and System/4 Pi having similar instruction sets and architecture. These processors had a memory cycle time of 2.5 usec; therefore, the results were scaled by a factor of $1/2.5 = 0.4$ to bring them into line with the baseline processor characteristics, which included a memory cycle time of one microsecond.

5.2 INTEGRATED TEST DEFINITION

The task of ensuring overall Space Station availability is primarily dependent upon the proper structuring of individual subsystem tests. The ability to test the subsystems independent of other subsystems is directly related to the number and types of interfaces. As shown in Figure 5-37, the DMS and Electrical Power Subsystems (EPS) interface with every other Space Station subsystem. In addition, the EC/LS Subsystem provides cooling to most of the electronic packages. This

Table 5-3. DMS Checkout Sizing Summary

Item	Time		Storage		Rate	Comments
	CPU Time	I/O Time	Main	Bulk		
COM TESTS						
1. CPU PSA Poll	106 ±12 usec	--	30 ±6 words	30 ±6 words	Once per 30 sec	
2. Mem. Address	24,000 ±1600 usec	--	13 ±4 words	13 ±4 words	Once per 30 sec	
3. DBC Wrap	614 ±60 usec	--	94 ±10 words	94 ±10 words	---	
4 DBCs	2458 ±240 usec	--	--	--	Once per 20 sec	
4. DBT Wrap	397 ±40 usec	4096 ±410 usec	98 ±10 words	98 ±10 words	---	
2 DBTs	794 ±79 usec	8192 ±820 usec	--	--	Once per 20 sec	Only 2 terminals are assumed checked at this rate.
48 DBTs	19,064 ±1906 usec	156,600 ±15660 usec	--	--	Once per hour	All other terminals checked hourly.
5. RDAU Tests						
Wrap	224 ±22 usec	14,000 ±1400 usec	38 ±4 words	38 ±4 words	---	
Mem MPX	1711 ±172 usec	1308 ±130 usec	77 ±8 words	77 ±8 words	---	
16 RDAUs	29,360 ±2936 usec	244,800 ±2500 usec	--	--	Once per 20 sec	Only 16 RDAUs are assumed checked at this rate.
117 RDAUs	220,200 ±2000 usec	1,790,000 ±200,000 usec	--	--	Once per hour	All other RDAUs checked hourly.
6. Image Proc.						
Memory	407 +8M ±10% usec	32 +16n ±10% usec	43 + n 4	43 + n 4 words	Once per day	1. n = byte capability of memory.
Display	223 ±22 usec	16 + 8n ±10% usec	50 + n 4	50 + n 4 words	Once per day	2. Performed only by authorization of crew.
7. Bulk Memory						
Tapes	3 ±2 sec	54 ±20 sec	2000 ±1000 words	2000 ±1000 words	Once per day	Crew must authorize and initiate.
Disks	4 ±1 sec	32 ±15 sec	2000 ±1000 words	2000 ±1000 words		
Drum	4 ±1 sec	19 ±8 sec	2000 ±1000 words	2000 ±1000 words		
8. GN&C Preproc.	40 ±20 usec	100 ±30 usec	100 ±50 words	100 ±50 words	Once per 20 sec	
SFI TESTS						
1. Main Memory	884 ±240 msec	--	43 ±5 words	43 ±5 words	---	
2. Sw. Matrix	200 ±160 usec	--	150 ±100 words	150 ±100 words	---	

Table 5-3. DMS Checkout Sizing Summary (cont)

Item	Time		Storage		Rate	Comments
	CPU Time	I O Time	Main	Bulk		
RECONFIGURATION						
CPU	200 ±160 usec	--	200 ±100 words	200 ±100 words	---	
Main Mem.	200 ±160 usec	--	200 ±100 words	200 ±100 words	---	
DBC	32 ±4 usec	--	30 ±3 words	30 ±3 words	---	
DBT	32 ±4 usec	100 ±30 usec	30 ±3 words	30 ±3 words	---	
RDAU	32 ±4 usec	200 ±50 usec	30 ±3 words	30 ±3 words	---	
Bulk	280 ±28 usec	200 ±60 usec	80 ±8 words	80 ±8 words	---	
PROGRAM RESTART						
*Recovery	263 ±80 usec	156 ±78 msec	112 ±18 words	112 ±18 words	---	*Access time to disk = 75 msec (not included in I O time). n = number of bytes transferred.
*Log 1	235 ±24 usec	156 ±78 msec	80 ±8 words	80 ±8 words	---	n = number of bytes transferred.
*Log 2	146 ±102 usec	156 ±78 msec	60 ±6 words	60 ±6 words	---	n = number of bytes transferred.
TABLES		--	32,844 words	32,844 words	---	
SFI DISPLAY		--	--	26,000 words	---	13000 words redundantly stored.

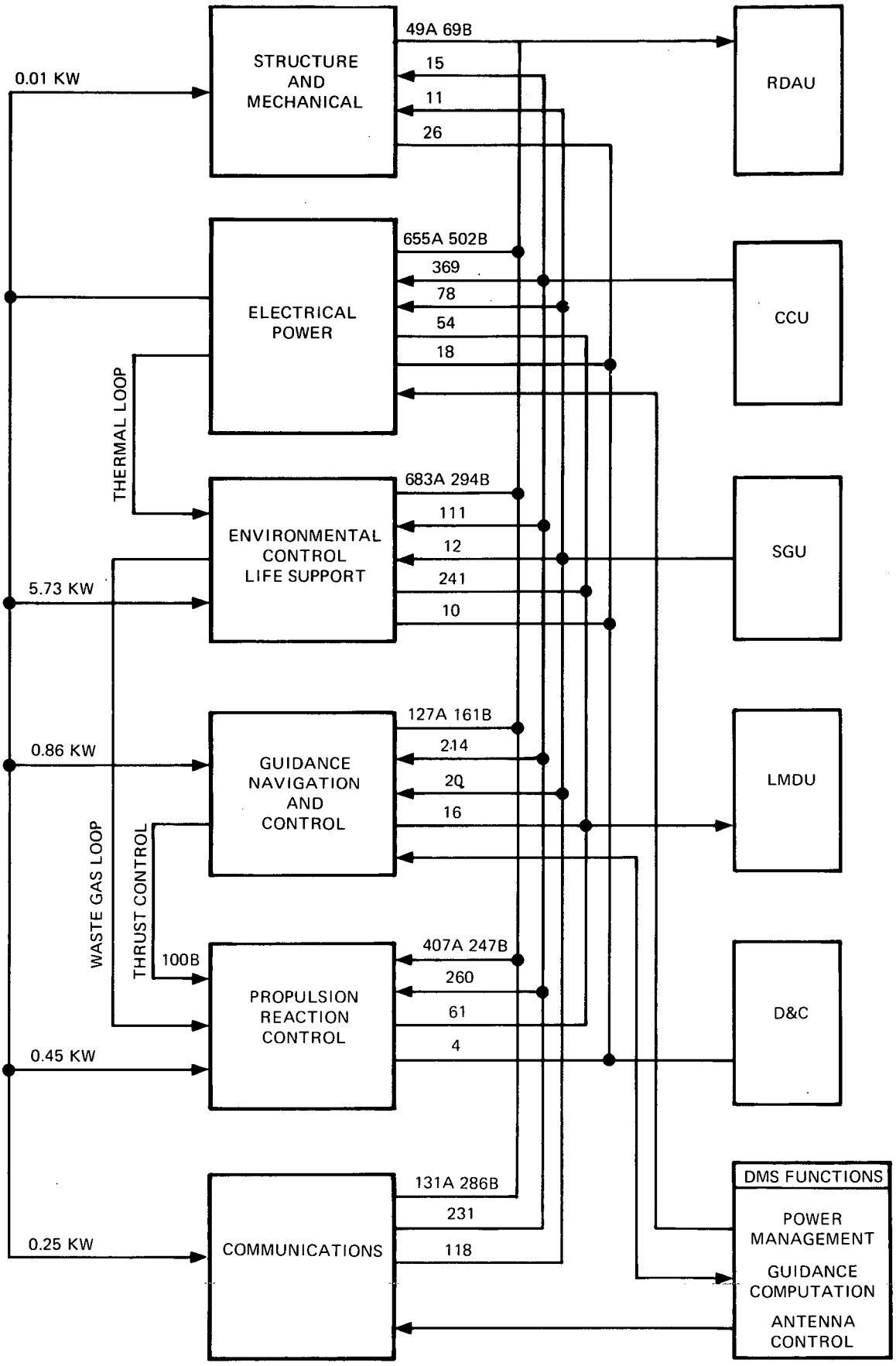


Figure 5-37. Subsystem Interfaces

This situation demands that in constructing the test for a subsystem these interfaces be taken into account so that erroneous or ambiguous test results will not be obtained. In other words, before detailed subsystem fault isolation tests are initiated, a higher level of testing should be performed to verify that all interfaces and Space Station conditions that influence the subsystem are proper. Properly designed, these higher-level tests will (1) indicate what Space Station conditions must be verified, maintained, or changed; (2) localize the malfunction to a single subsystem; and (3) identify the subroutine test necessary for fault isolation.

Since the DMS interfaces with all of the Space Station subsystems and is used as the OCS, it would appear that all of the tests would be integrated. However, this is not a proper interpretation. When the DMS is used to verify the performance of another subsystem, it must first establish itself as a test standard against which the subsystem parameters are compared. Subsequent to this verification, the test is dedicated to the evaluation of the subsystem. This test would be considered as an independent test since the objective of the test was to verify the subsystem and not the DMS. For a test to be considered as an integrated test it must meet one or more of the following conditions:

- Test objectives associated with more than one subsystem
- Test involves subsystem interfaces
- Test requires proper operation of other subsystems

In several cases, the DMS must simultaneously perform the dual role of OCS and functional elements. As an example, the DMS has a functional interface with the GN&C and Prop Subsystems for the computation of guidance equations and the execution of commands to the control actuators. When this functional closed loop is being tested, the DMS must, in addition to performing its normal functions, execute the test routine. For this type of integrated test there must be an intrinsic relationship between the operational and test software. This relationship must be carefully considered in structuring the integrated tests since unstable or intermittent performance may be detected only in the exact operating mode under closed-loop conditions. The number of integrated tests is not extensive due to the approach of minimizing the different types of interfaces between Space Station subsystems. For example, interfaces between the DMS and other subsystems are largely standardized. As a result, relatively common tests can be designed for verification of the multitude of DMS subsystem interfaces or for localization of a fault to one side of a DMS subsystem interface. All special integrated tests that have been identified are discussed in the following paragraphs. The GN&C/DMS/PROP configuration for navigation and attitude control poses the most difficult problem for on-orbit testing so it is presented in significant detail. Other integrated tests are summarized.

5.2.1 GN&C/DMS/PROP

5.2.1.1 Block Diagram

Figure 5-38 shows the block diagram for the GN&C/DMS/PROP Subsystems as configured for the zero g, horizontal mode of operation. The subsystems are shown at the LRU level with all primary functional interfaces. For simplicity, prime power inputs, cold plate interfaces, and mechanical or fluid connections are not shown.

5.2.1.2 Functional Description

The GN&C Subsystem accommodates both the artificial-g and zero-g operations of the Space Station. In the zero-g mode of operation, the GN&C Subsystem provides autonomous navigation, rendezvous command, traffic control, automatic docking, and stabilization and control of the Space Station.

The autonomous navigation scheme utilizes the stellar inertial reference data and the automatic landmark tracker augmented with the drag accelerometer. The navigation is accomplished by automatically tracking known and unknown landmarks several times each orbit. The landmark is similar in operation and mechanization to a gimballed star tracker. The drag accelerometer accounts for anomalies due to Space Station orientation and docked module changes which contribute to navigation errors.

Both ground tracking and onboard subsystems will provide the navigation information for the first year or so of the Space Station Program. The ground-generated data will be transmitted onboard for evaluation of the autonomous navigation system performance. As the confidence in autonomous operation is increased through this parallel operation, the ground tracking is to be phased out.

In all operating modes and orientations, the gyros provide the high-frequency rate and attitude information necessary to supplement the data from the stellar sensors and the horizon sensors.

A more accurate Earth-centered reference is obtained in the horizontal orientation through the use of the strapdown star sensors. The star sensors provide the long-term, drift-free inertial reference data while the gyros provide the short-term, high-frequency attitude and rate information. The passive star sensors are used while the Space Station is maintained in an Earth-centered orientation. The constant rotational rate required of the vehicle to maintain this type of orientation provides the scanning motion for the star sensors, which are completely passive and provide no tracking or scanning capability of their own.

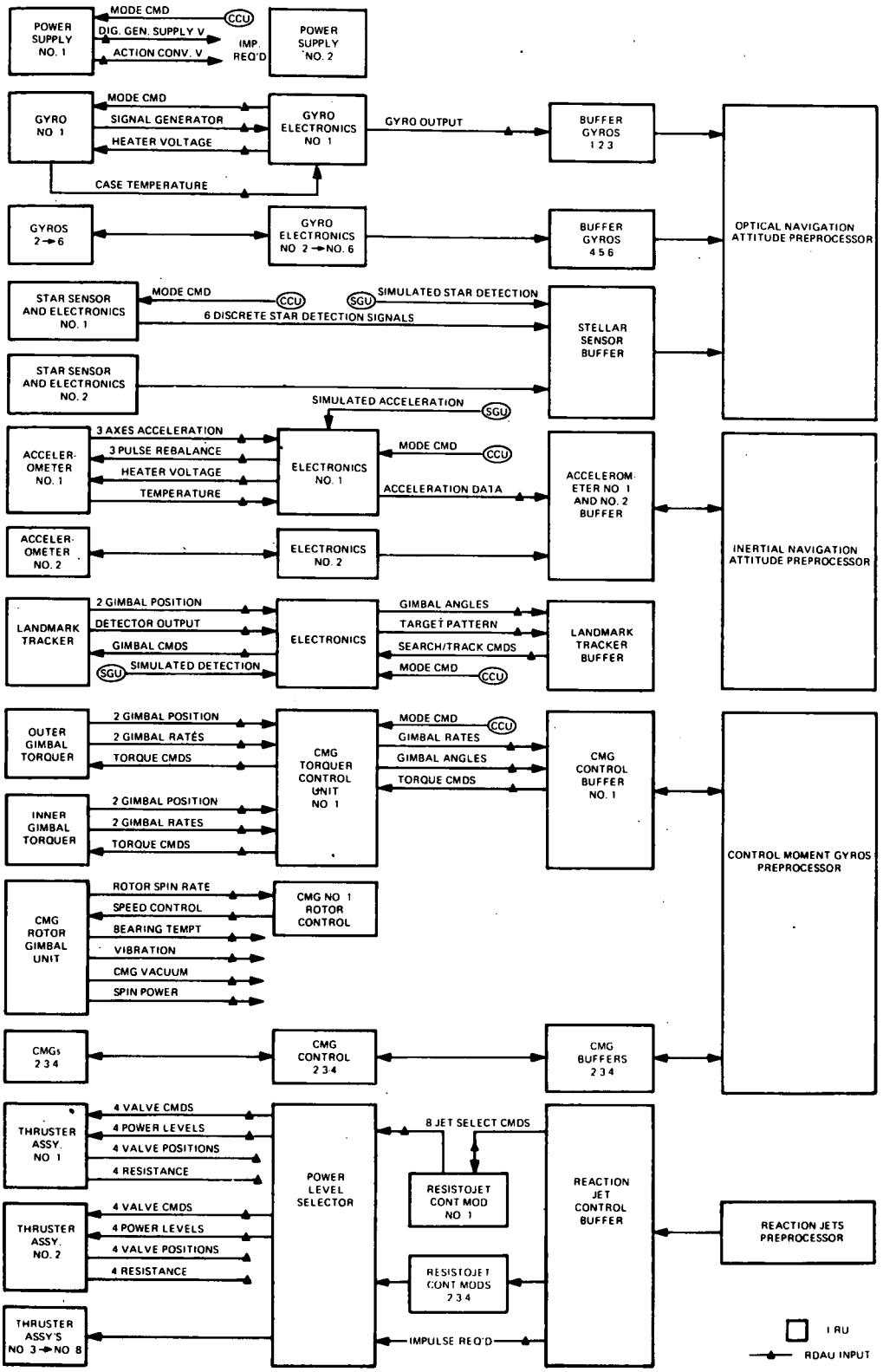


Figure 5-38. GN&C/DMS/PROP Configuration for Zero-G Horizontal Mode

The sensors themselves provide inertial attitude data which is transformed into Earth-centered attitude information by use of the navigation parameters. By this method, both inertial attitude and Earth-centered attitude are derived from the passive star sensors while the vehicle is in the horizontal or other Earth-centered orientation. This Earth-centered orientation is considered to be most responsive to experiment and subsystem requirements.

Primary attitude control actuation is provided by control moment gyros (CMGs). A CMG configuration utilizing four double-gimballed CMGs, each having a momentum capacity of 1,100 ft-lb-sec, was selected for the isotope/Brayton-powered Space Station. Both High and Low-Thrust Propulsion Systems are utilized by the GN&C Subsystem for CMG desaturation and backup attitude control capability. The reaction jet control buffer provides the interface with the Propulsion Subsystem.

The DMS provides the link between the sensors, which are used to determine the vehicle angular position, and the actuators, which are used to maintain or change the vehicle angular position. The use of the DMS provides the flexibility required during both the development and operational phases to accommodate the total Space Station Program objectives. The DMS performs the data processing necessary for all guidance, navigation, and attitude control functions. The interface electronics controls the flow of information from the sensors to the DMS and converts all sensor inputs to a standardized format before the inputs are transferred. The interface electronics performs a similar function for output information from the DMS to the control actuators.

5.2.1.3 Test Flow

The test flow for the GN&C/DMS/PROP configuration is shown in Figure 5-39. The flow demonstrates the technique for malfunction detection, subsystem localization and fault isolation to the LRU. For simplicity some tests associated with prime power, mode commands and cold plate temperatures are omitted. It is assumed that in programming the actual tests these types of measurements will be implemented as standard procedure. In the same vein, detailed tests of the DMS are not shown. Again, it is assumed that the final procedure would contain the necessary self-test, command verification, and other checks to maintain confidence in DMS performance throughout the test.

Many of these test sequences will be repeated for different channels of data or for identical sets of equipment. The test flow does not show the repetition of these tests but indicates the need for them. For example, there are four control moment gyros (CMGs). The flow shows a typical test for one CMG. It should be

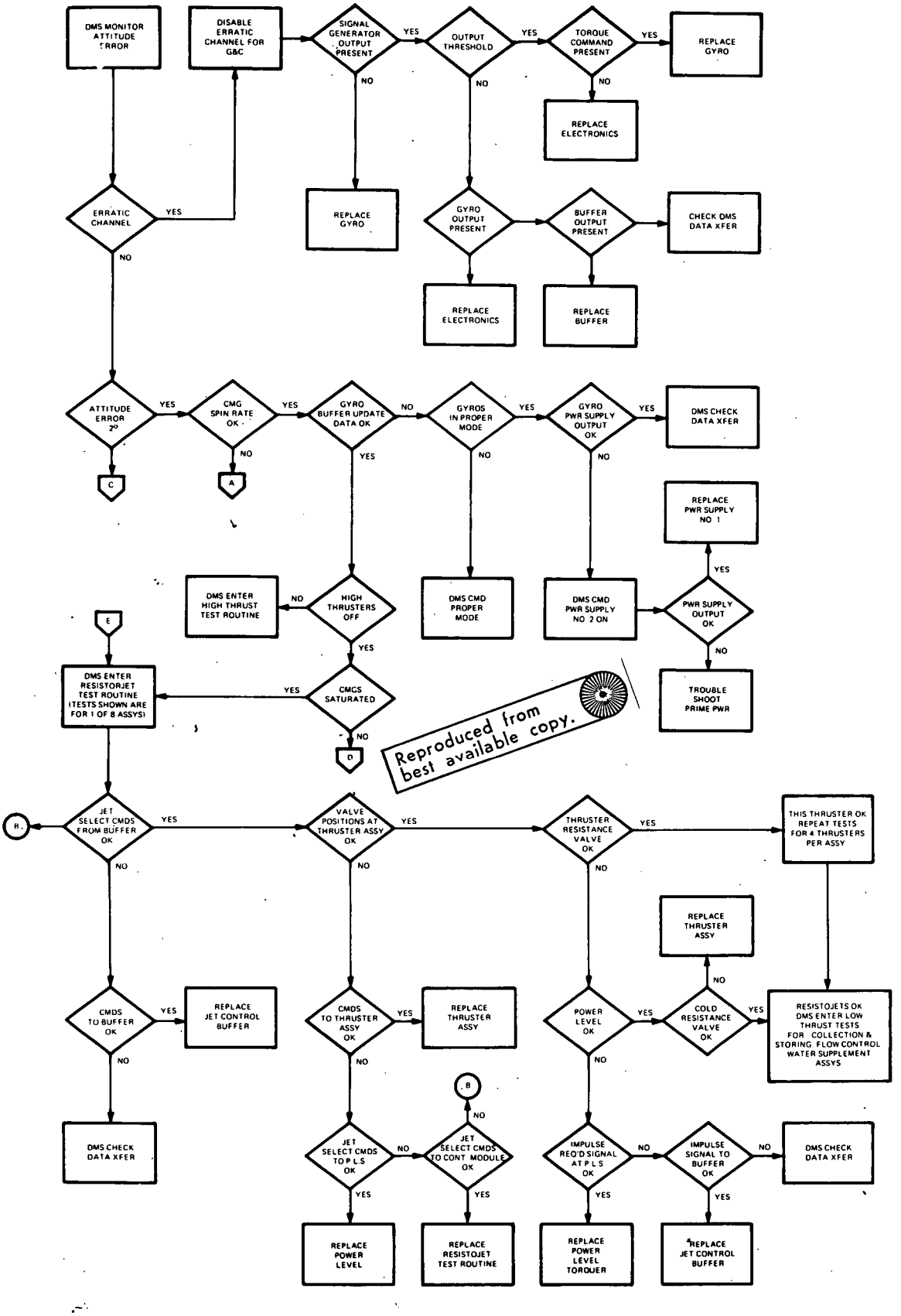


Figure 5-39. GN&C/DMS/PROP Integrated Test Flow (Sheet 1 of 4)

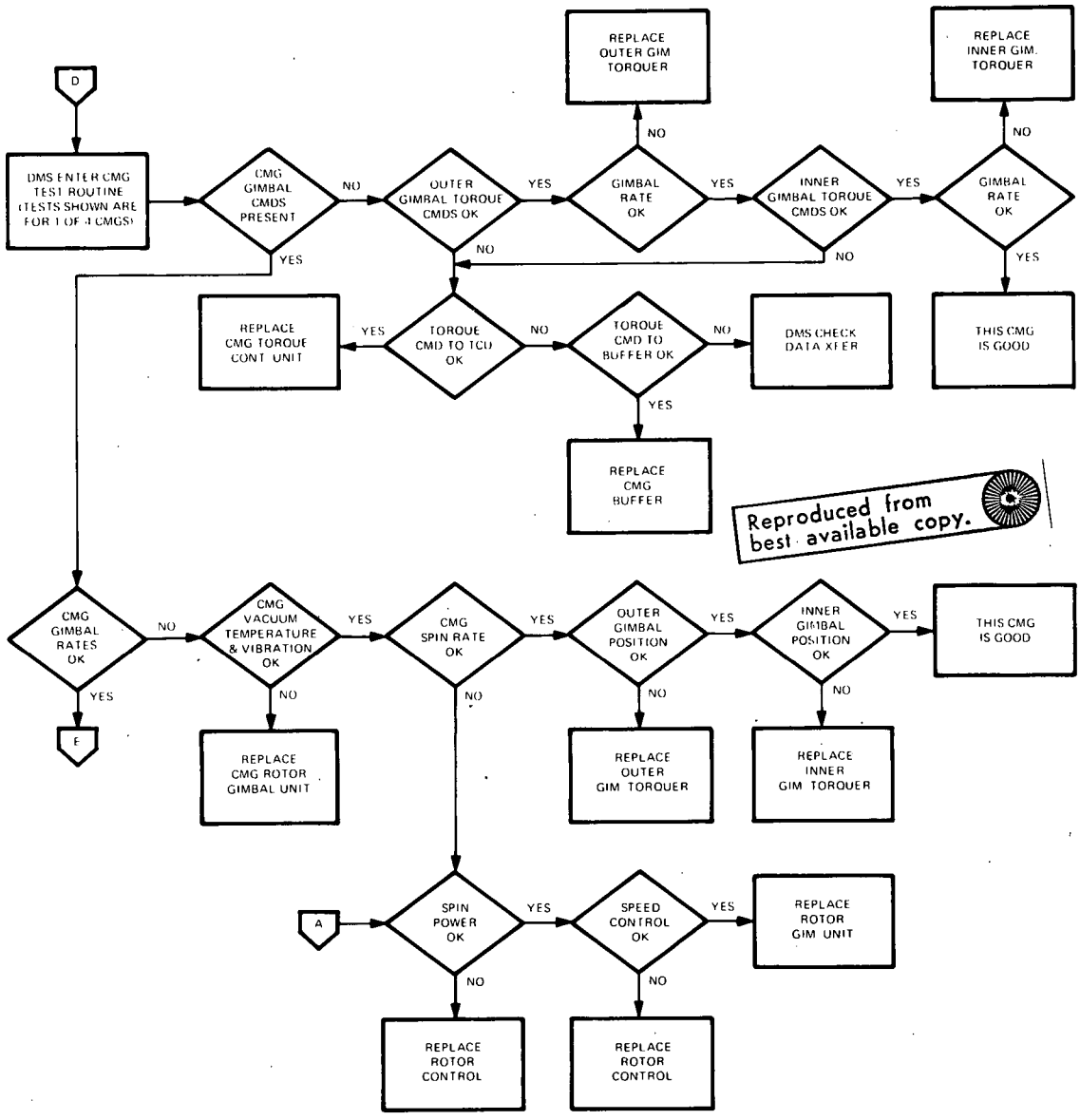


Figure 5-39. GN&C/DMS/PROP Integrated Test Flow (Sheet 2 of 4)

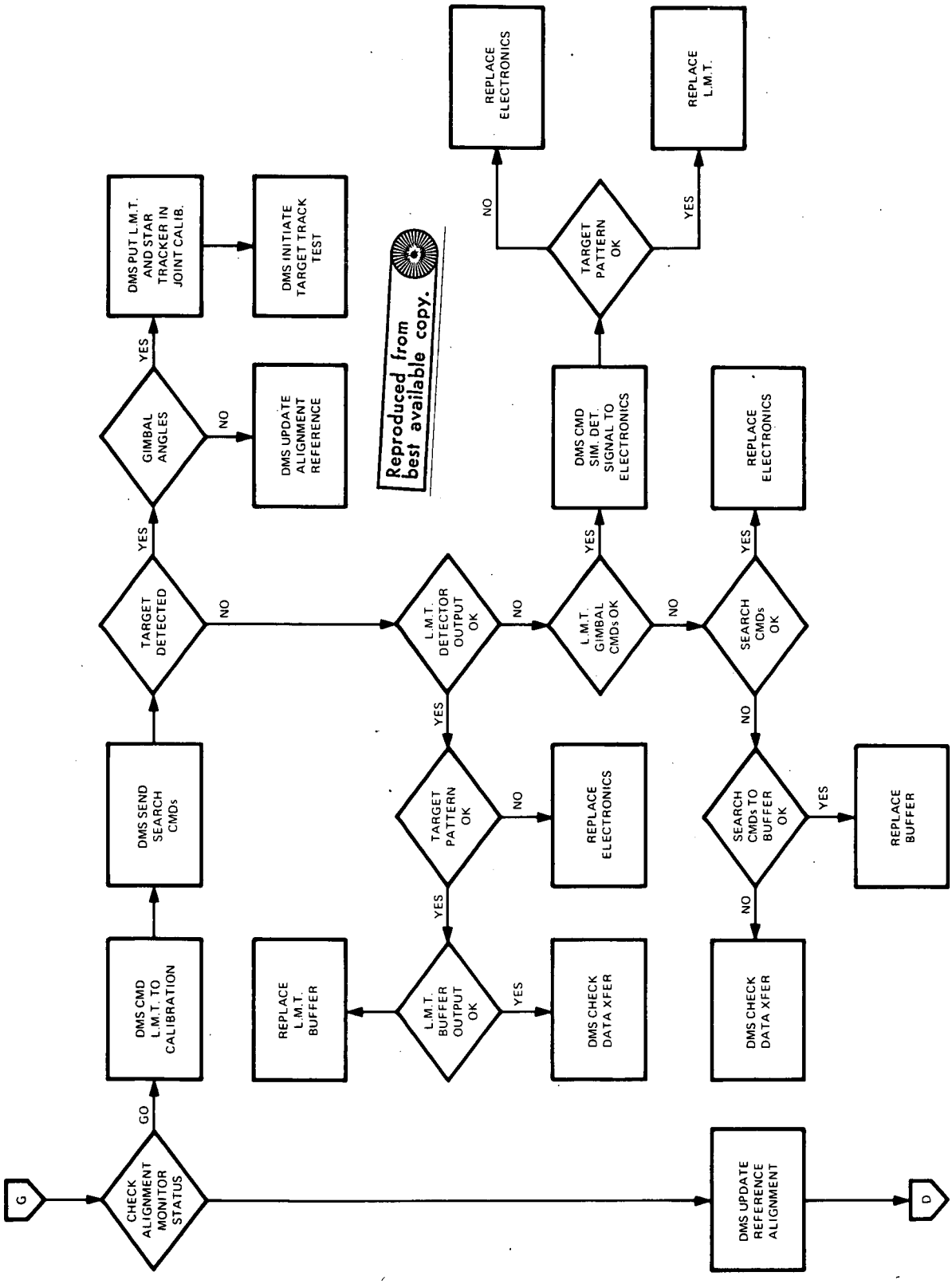


Figure 5-39. GN&C/DMS/PROP Integrated Test Flow (Sheet 3 of 4)

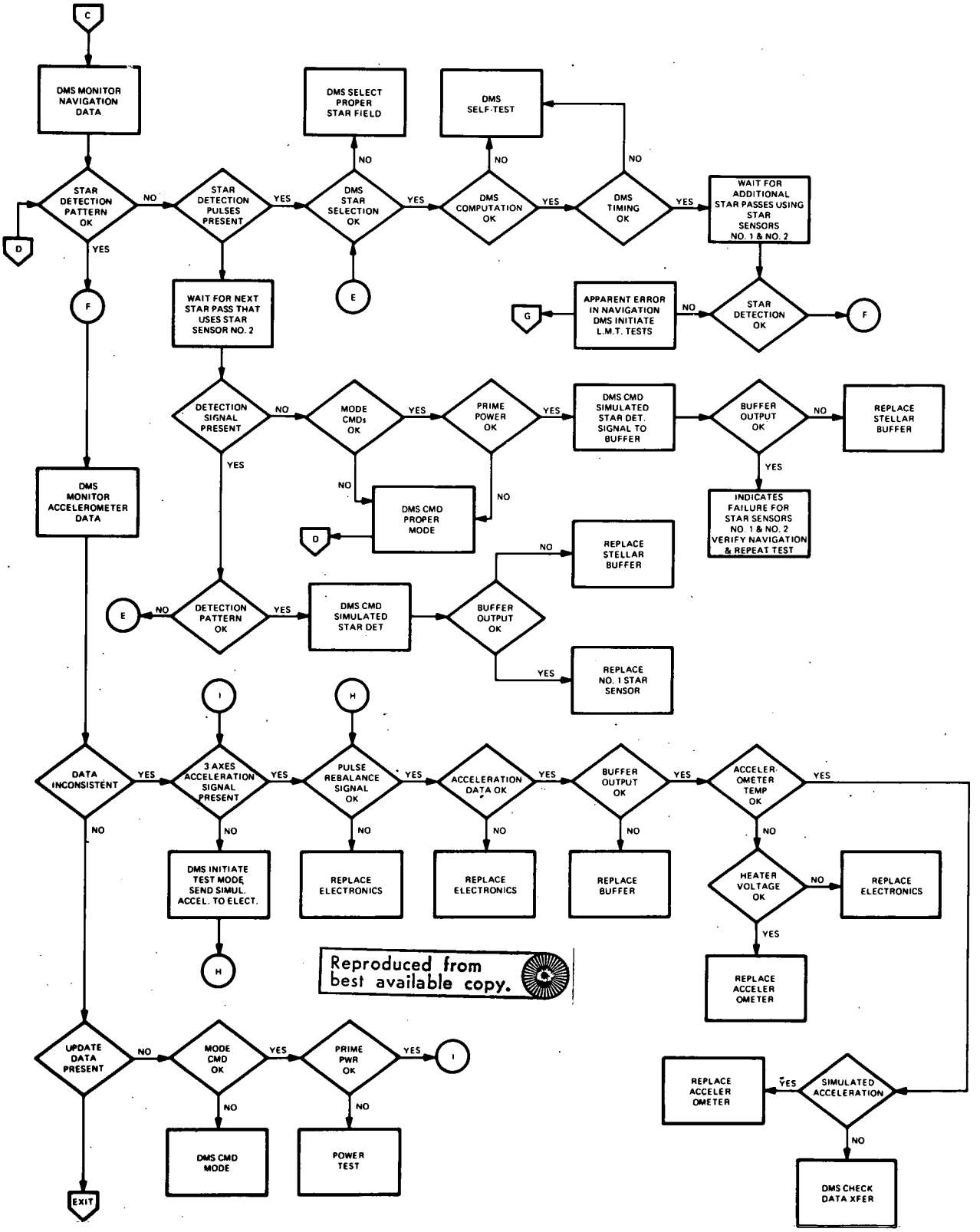


Figure 5-39. GN&C/DMS/PROP Integrated Test Flow (Sheet 4 of 4)

pointed out that although the detail test sequence will be identical for all CMGs, the absolute value of the parameters such as torque commands, gimbal position, gimbal, rates will be different for all CMGs. In some cases, the test flow terminates in an instruction for the DMS to check data transfer. This instruction is intended to include all operations necessary to verify that the DMS is functioning as required to support the operational and test routine.

5.2.2 GN&C/DMS/COMM

The DMS has a functional interface with the GN&C and COMM Subsystems for the pointing and control of antennas. The GN&C sends navigation and attitude information to the DMS which in turn uses it to compute antenna pointing positions and slewing rates. Once computed, the DMS transfers these commands to the antenna actuators in the Communication Subsystem.

Localizing a malfunction to one of the three subsystems will be performed in a manner similar to that described in subsection 6.2.1. The DMS will verify receipt of proper attitude and navigation data from the GN&C Subsystem, check its capability to operate on and transform the data into appropriate antenna commands, and verify the transmission of the control data to the Communication Subsystem. Verification of proper response and operation of Communication Subsystem equipment will be aided by the switching and use of redundant transmitters and receivers.

5.2.3 DMS/EPS

The DMS has a power management interface with the Electrical Power Subsystem. This function primarily includes start-up, control and shutdown of the power conversion equipment, and the control and reconfiguring of the power profile through the distribution buses. Fault isolation is performed by a DMS self-check that verifies proper generation and transmission of control functions to the interface.

The startup, control, and shutdown of the power conversion equipment by the DMS is another example of the integral relationship that must exist between the operational and test software. For example, in starting the Isotope/Brayton System the automatic operational procedure must contain exact instructions for a normal start and an additional set of instructions for aborting or safing an abnormal start. To know the starting sequence (operational software) is not proceeding as planned implies a knowledge of what is wrong (test software). Based upon this knowledge the DMS can execute the appropriate operational controls and identify the malfunctioning element.

Section 6

SOFTWARE

6.1 GENERAL CONSIDERATIONS

The recommended software checkout startegy involves a sequence of detecting faults, isolating faults to a failing LRU or LRUs, and reconfiguring the system to continue operation while the failures are being repaired.

This recommendation was developed by evaluating each subsystem with respect to the three general requirements of fault detection, fault isolation, and reconfiguration.

Fault detection incorporates both the recognition of failure occurrence, and the prediction of when a failure can be expected to occur. The Remote Data Acquisition Units (RDAUs) continually check selected test point measurements against upper and lower limits, and notify the executive on an exception basis when a limit is exceeded. This approach avoids occupying the central multi-processor with the low-information task of verifying that measurements are within limits.

Trend analysis is a fault detection technique recommended for predicting the time frame during which a failure can be anticipated. Data is acquired on a basis of time or utilization, and compared with previous history to determine if a "trend" toward degraded performance or impending failure can be detected.

Another checkout requirement evaluated for each subsystem is periodic testing. This type of test is provided to exercise specific components at extended time intervals or prior to specific events, to assure operational integrity. In the event that a failure is detected, the periodic test will isolate to the failing Line Replaceable Unit (LRU) and accomplish recertification after a repair operation.

Calibration of specific subsystem components will be required periodically, or subsequent to a repair and/or replace operation. The techniques involved are unique to the individual component; and, in some cases, require the acquisition of operational data.

Fault isolation is required when a fault is detected. When a particular fault provides an indication that a life critical failure has occurred, the fault isolation routines are automatically initiated. If the failure does not represent an immediate danger to the vehicle occupants, the crew is notified and they will initiate the fault isolation modules at their convenience.

The basic requirements of the fault isolation function is to analyze the available information relevant to a problem, and identify the LRU which is responsible for the anomaly.

Three basic approaches to meeting this requirement were considered. These are:

- Analyze each fault as an independent problem
- Analyze each fault with a state matrix which defines the possible error states of the subsystem
- Associate each fault with a specific subsystem, and evaluate that subsystem in detail

The third approach was selected on a basis of software commonality and cost effectiveness. The complexity associated with the testing can be reduced by localization of the logic associated with the analysis of the subsystem in a unique package. The software commonality will result in reduced software development and maintenance costs, while increasing the reliability of the software.

The fault isolation software is structured modularly for compatibility with the hardware structure of the subsystem. Checkout modules evaluate the performance of a specific portion of the subsystem. A convenient division for this modular structure is at the assembly level or functional area. A program module which can determine and control the sequence in which these checkout modules are executed is also required for each subsystem.

Subsequent to fault detection, the software associated with the subsystem which is most likely to contain the error will be activated.

The subsystem software will analyze the error indication, and initiate a sequence of checkout modules to isolate the problem. If successful, the crew is notified regarding the Line Replaceable Unit (LRU) to be replaced. If an error cannot be identified, the crew is informed of the situation and has an option to execute the periodic test of the subsystem.

After a fault has been isolated, reconfiguration software restores the functional capability of the subsystem. This is most commonly accomplished by exchanging a redundant element for the failing unit, or by defining an alternate path to accomplish the required function.

The Task 2 Final Report of the basic onboard checkout techniques study provides descriptions of the software requirements, definitions and design in addition to detailed flow charts of specific checkout routines. The Data Management

Subsystem software descriptions given herein focus on language and executive requirements since individual subsystem software requirements are described in the other volumes of this set.

6.2 LANGUAGE AND EXECUTIVE REQUIREMENTS

After analyzing each subsystem in regard to checkout strategy requirements, the area of language requirements was approached. The flowcharts which were developed for selected subsystem components during the development of the checkout strategy were a significant input to this activity. These flowcharts were expanded and analyzed to define the type of operations required to accomplish checkout, and the language elements which could most efficiently meet these requirements.

The baseline elements and associated options were evaluated on a basis of the ease and efficiency with which they could meet the logical, I/O, and arithmetic operations required to accomplish automated on-board checkout, within the constraints established during the preliminary phase of the task. The elements which were selected are summarized and are described in detail in Section 3 of the Task 2 Final Report.

Concurrently with the analysis of language elements for each subsystem, the executive requirements which were associated with each element also received consideration.

6.2.1 PROGRAM SIZING

Each subsystem was also reviewed to provide software sizing estimates for processor time, I/O time, and memory requirements. Table 6-1 refects a summary of the estimates which would be typical to perform a periodic test on each subsystem.

A significant conclusion which can be drawn from this table is that automated on-board checkout with remote limit checking, will require minimal processor time, and that run time of the program will be highly dependent upon the efficiency of the I/O interface.

6.2.2 SUBSYSTEM SOFTWARE DEFINITION

The analysis of each subsystem resulted in the preparation of preliminary design definitions describe the software which would typically be used to accomplish the checkout of each subsystem. Data for each subsystem includes:

- A description of the required software modules
- Interface descriptions

- Language requirements
- Executive requirements
- Program sizing

These documents were developed as the study progressed, and are included in Appendices A through E of the Task 2 Final Report for each subsystem to provide background for the overall conclusions.

Table 6-1. Subsystem Periodic Test Characteristics

Subsystem	Time (Minutes)			Memory (Words)	
	CPU	I/O	TOTAL	Main	Aux.
Propulsion					
Low Thrust	.010	2.649	2.659	6K	8.5K
High Thrust	.015	4.745	4.760	5K	10K
RF Communications	.025	5.024	5.049	13.5K	20K
Guidance Naviagation and Control	.022	3.004	3.026	12K	12K
Electrical Power					
Isotope/Brayton	.021	3.310	3.331	15K	15K
Solar Array	.042	5.302	5.344	15K	15K
EC&LS	.020	4.580	4.600	16K	33K
Structure	.005	2.913	2.918	4.5K	4K

6.3 EXECUTIVE REQUIREMENTS

The incorporation of a multi-level executive, consisting of a Master Executive and an Onboard Checkout Executive, is recommended because of its adaptability to modularization of the required program functions. This concept contributes to the simplification of the definition and control of the program modules.

The significance of program modularization is in its contribution to reducing the logical complexity of the system by providing clear decisions of responsibility. The position of a program module in a hierarchical structure is based upon its functional responsibility and the extent of supervisory influence which it exerts.

Figure 6-1 depicts the major hierarchical levels and associated interfaces in the executive structure recommended by this study.

The determination of Executive System requirements was approached by defining seven general areas of executive functional responsibility, and categorizing each identified requirement. Once the requirements were identified and categorized, it was necessary to determine the hierarchical level at which each specific requirement could best be accomplished on a basis of programming and run time efficiency.

The specific areas of functional responsibility which were established are:

- Scheduling
- Support Services
- System Communication
- Resource Allocation
- Data Handling
- System Recovery
- Interruption Servicing

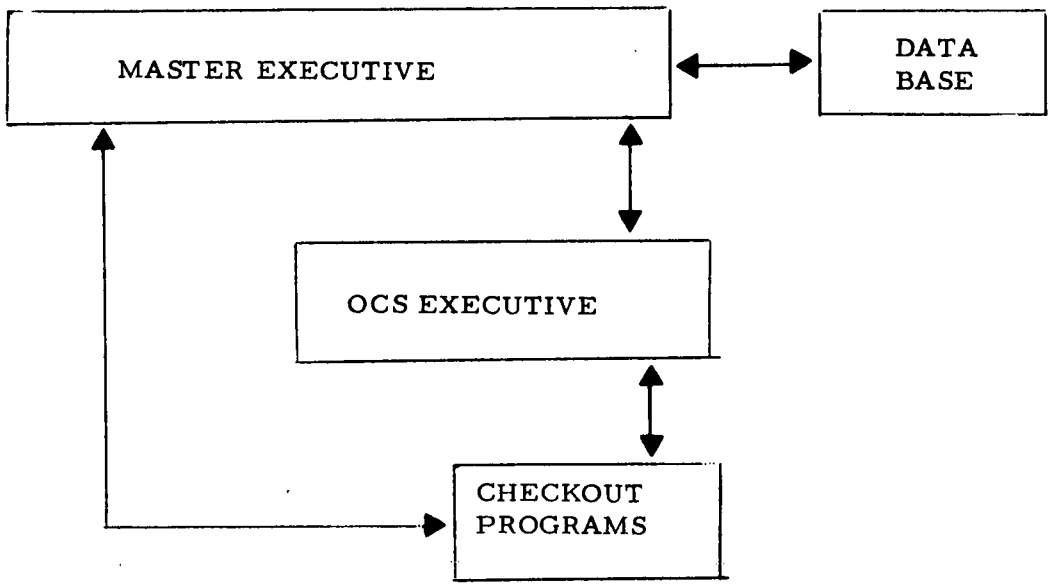


Figure 6-1. Multi-Level Executive Relationships

6.3.1 SCHEDULING

A task is a unit of work for the DMS multiprocessor; and task scheduling is the executive function which controls the flow of work. A multiprogrammed scheduling function is recommended for the space station multiprocessor configuration to permit concurrent execution of two or more tasks. A priority dispatching technique will select the tasks on a basis of their relative importance to the operational objectives of the system.

This strategy utilizes task priority level, memory requirements, and estimated execution time to select tasks, initiate and control task execution, and terminate task execution. This strategy provides the required time and event of oriented scheduling capabilities. The initiation of programs on a time oriented basis is required for the trend analysis and selected periodic check routines. Event oriented scheduling requirements include the initiation of critical fault isolation sequences, and programs which are requested by the crew.

6.3.2 SUPPORT SERVICES

The services of an executive program are primarily concerned with providing the software to meet the requirements for program generation and maintenance. The executive support services required as a minimum to support the recommended high-level language include an interpreter and a compiler.

A compiler program, which will execute in both an on-line and off-line environment, will process the source statements and build the appropriate data list tables. An interpreter program will process the data lists and execute the associated operations.

Another system requirement which is defined in this functional area involves the initialization of the system. The software required to accomplish this must contain the logic required to determine the assignment of the multiprocessor to either the operational or experiment functional areas.

6.3.3 SYSTEM COMMUNICATION

The functional area of system communication is integral to the establishment of an efficient man-machine interface. This application requires an executive program to provide the interface between the operator and computer system through a keyboard/display.

The language used to accomplish this interface with the computer is commonly referred to as job control, or command language. The executive interprets the inputs and initiates the designated activity.

Specific requirements identified relative to the execution of checkout application programs include:

- The capability to provide variable data to a program at both load and execution time.
- The ability to specify options to control the sequence of program operation.
- Permit manual response to a detected error situation.
  - Retest
  - Terminate
- Require operator concurrence prior to issuing specific stimuli.

6.3.4 RESOURCE ALLOCATION

The function of resource allocation is responsible for minimizing interference which can result when concurrent tasks share the same resources. The efficient allocation of memory, external devices, and the data base will reduce the processor time which is lost due to memory contention, and the delays associated with input/output operations.

Memory allocation is responsible for determining the memory currently available for allocation to new tasks, and memory which is already in use. The effects of memory contention can be minimized by a strategy which allocates unique memory modules to concurrent requirements. The memory allocation strategy should also minimize the effect of memory fragmentation by evaluating the total memory which is unavailable due to fragmentation, and reassign memory only when system performance is being impacted.

The function which allocates subsystem resources is particularly important to the On-Board Checkout System. It is essential that interference be eliminated between concurrent requirements. An example of this interference would be an attempt to initiate the periodic test for a subsystem which is currently performing a necessary operational function. These considerations prevent the use of a subsystem or component by a program whose requirements could conflict with the current operation of the subsystem. Executive modules which provide this capability must maintain information relative to the current use of each subsystem component where the possibility of interference exists; and must assure that two conflicting requests are not issued.

This study recommends that the allocation of equipment (displays, printers, and subsystems), be accomplished using a priority queuing technique which would sequence requests to insure that the tasks access the equipment on a non-interference basis, and in consideration of their relative priorities rather than arrival order.

6.3.5 DATA HANDLING

The data handling capabilities of the executive must support the system requirements for acquisition, routing, and retention of information. In a multiprocessor environment, tables will be updated by one processor and used by another. Precautions are required to prevent one processor from accessing a particular table while it is being updated by a second processor. Specific requirements which have been identified to be incorporated into a data base are as follows:

- System Status
- System Configuration
- Redundant elements and paths
- Schedules and procedures
- Inventory control
- Association of symbolic test points with physical addresses
- Program modules

The data base concept which is recommended to meet these extensive and varied requirements involves hierarchical relationships between the specific data which must be retained, with responsibility for operations on the data base vested in an executive function, instead of with application programs. This permits control to be maintained in a central routine, with the result that data base integrity is enhanced.

Techniques are required to handle the exchange of data between programs and between external equipment. The functional capabilities which are required in this area are:

- Exchange of data
- Recognition of the receipt of data and source identification
- Routing of data for subsequent processing or retention

These functions are commonly accomplished by the executive input/output (I/O) routines which provide the interface between the application programs and the external I/O devices. In general, the functional capability which is required in the executive system to assure compatibility with this design concept includes:

- Transfer of data between subsystems and the computer.
- Identification of the specific subsystem.
- Analysis (limit checking, compaction) of the data.
- Presentation of messages on display units.
- Test point measurement.
- Issuance of stimuli to test points.

When errors occur in the equipment they must be analyzed, and the appropriate response taken. This action, dependent upon the problem, includes a subset of the following items:

- Return error analysis information to the program which requested the I/O operation.
- Maintain error statistics.
- Reset the I/O device.
- Retry the operation.
- Notify the operator.
- Initiate recovery procedures

In addition to the above, the inclusion of special processing routines to meet the data retention requirements of trend analysis, data logging, and checkpointing is required for the Space Station application. These requirements will necessitate allocating areas of auxiliary storage to hold the data, and periodically deleting data which is no longer required.

6.3.6 SYSTEM RECOVERY

The functional area of system recovery relates to the capability of the space station subsystems to remain operative in the presence of failures. The primary

responsibility in this area involves the analysis of a failure, and reconfiguring the system to reduce the impact of the problem. Specific requirements related to this area include configuration management, redundancy control, and the interface to assure that the checkpointing of data is accomplished.

Redundancy control refers to DMS control and accountability of system elements which are redundant. It is essential that the DMS have the ability to alternate redundant elements between primary and secondary status, in order to assure operational readiness.

Configuration management routines establish and maintain the information which provides the current system organization description required for redundancy control.

The functional area of system recovery is also responsible for assuring that timely checkpointing of the appropriate data is occurring.

System recovery is also responsible for coordination of program termination when required, prior to successful completion of an application program. This function must assure that any subsystem elements which may have been affected by the program are restored to a proper configuration prior to continuation of other system operations.

6.3.7 INTERRUPTION SERVICING

The real time response requirements of the space station environment are particularly adaptable to interruption servicing. The interruption servicing routine performs the following functions:

- Save machine status (i.e., processor status, register contents) at the point of interruption.
- Identify the interruption source and type.
- Select and execute the appropriate program module.
- Restore machine status and return to the interrupted program.

Specific requirements identified by this study relative to on-board checkout relate primarily to responses to out-of-tolerance indications which are received from the RDAU's. Special emphasis is required to analyze multiple failure indications. The study focuses attention on the problems encountered as the result of an error whose effect will impact other areas. When this situation occurs, measurements associated with downstream components will exceed tolerance limits. These

measurements must be evaluated to determine if they are within the scope of the original problem, or represent a unique problem.

The approach which is currently considered appropriate is to disable the RDAU limit check capability, thus eliminating repetitive interruptions. The RDAU scan of those test points which could normally be expected to exceed limits in view of the detected error, is also disabled. When the fault isolation sequences have successfully isolated the problem and repair has been accomplished, limit checking is reinitiated.

6.4 EXECUTIVE FUNCTIONS

The Space Station Executive is a program which supports the on-board checkout functions of status monitoring, fault isolation, reconfiguration, periodic check, calibration, and trend analysis. The requirements of the Master Executive are to service interruptions, provide an interface between hardware and other programs, allocate the processor resource of DMS to tasks on a priority basis, and serve as a repository for routines which have common usage among higher-level executives such as the OCS Executive and the Experiment Executive.

6.4.1 MULTI-LEVEL APPROACH

The executive design is a multi-level one in that functions are stratified with regard to their scope of use. At the lowest level are functions which provide the interface with hardware devices such as the data bus controller. All on-board programs being executed by the multiprocessor make use of the low-level functions, regardless of whether they are checkout oriented or not. Low-level executive services are normally used by the higher level functions, rather than directly by the application programs.

The lower levels of the executive are referred to as the Master Executive because of the central control and interface with the DMS hardware which they provide. The upper levels of the executive are oriented toward individual system of the Space Station; therefore the OCS Executive functions are generally found in the upper levels of the hierarchy.

Portions of the OCS Executive reside in main storage, and are closely aligned with the Master Executive routines because of their frequency of use. From the standpoint of how processor control is given to certain OCS routines, these routines are indistinguishable from some of the Master Executive routines; however, they are categorized as OCS routines because their function has no wider application than on-board checkout.

6.4.2 CENTRALIZATION VS. DECENTRALIZATION

In order to perform detection, isolation, and reconfiguration in an integrated and autonomous checkout system, a centralized data base is required to achieve coordination. There appears to be no trade involved in the area of whether to centralize or decentralize that portion of the DMS which fulfills the coordination function.

If it was desirable to disperse DMS functions as much as possible, the minimum which would require centralization would be a configuration table reflecting the logical relationships among assemblies of the Space Station. Shared auxiliary storage could be used to contain the configuration table. However, by centralizing, definite advantages relating to equipment utilization and operational capability can be realized.

From the standpoint of equipment utilization, more efficient use of equipment can be achieved in a centralized configuration because other functions can be performed during those intervals when a decentralized arrangement would produce idle time.

From the standpoint of retaining operational capability when a failure occurs, a centralized arrangement can be reconfigured to supply redundant idle components to serve in place of the failed item; and, the switch can be made automatically.

Preprocessors in the GNC Subsystem provide an example of the effect of decentralization. The optical navigation/attitude preprocessor serves to control the operation of five GNC assembly categories. Failure of an LRU in the preprocessor results in loss of capability with regard to the horizon detectors, attitude gyros, horizon sensors, star sensors, and star trackers; a total of nine required and one standby-redundant assemblies. If operational control were vested in the centralized multiprocessor, loss of one of the processors would affect only the function being performed at the instant of failure. Other functions would continue normally. The lost function might be recovered automatically in the centralized environment. However, in a decentralized environment, all the above functions would be lost until manual remove-and-replace activity could be effected.

6.5 MASTER EXECUTIVE DESIGN

The Master Executive is designed to perform the following:

- Handle interruptions
- Supervise tasks
- Control programs in main storage

- Control the Data Management Subsystem itself
- Supervise the interval timers of all processors
- Supervise the interface with man via display units
- Handle data logging
- Handle checkpointing
- Supervise exiting and termination procedures

The functions of the Master Executive are:

- Scheduling
- Support Services
- System Communications
- Resource Allocation
- Data Handling
- System Recovery
- Interruption Servicing

The Master Executive will perform multiprogramming; that is, fulfill two or more separate programming requirements concurrently by making decisions based on various conditions in the Data Management Subsystem. Therefore, it is a goal of executive design that modules will be reenterable. The reenterable attribute is ascribed to a program which is used concurrently in the performance of two or more tasks. The design of the Master Executive is such that it can perform its functions while being used by more than one processor in the DMS multiprocessor.

The basic service of the Master Executive is to provide an interface between software and hardware. In doing so, it enables programs to be largely independent from an evolving hardware environment.

The Master Executive serves to reduce redundant software development and reduce maintenance activities which arise in a dispersed design, by serving as a repository for common functions. Any function having multiple uses across systems (e.g., experiment, checkout), is designed with common interfaces and supplied as a service of the Master Executive.

6.5.1 SCHEDULING

The flow of processor control through the Master Executive is shown in Figure 6-2. Processor control is passed to the Master Executive via an interruption such as supervisor call, I/O, timer, program, or machine check. Any interruption causes processor control to be taken from the interrupted program and given to an interruption handling routine of the Master Executive. The interruption handling routines analyze the requirements for servicing the interruption; and, as a result, may pass control to one of the task specification routines which define a new task and record it in the task queue. The task queue is that portion of the data base containing the identity and characteristics of work being performed by the multiprocessor. After the task specification routine returns control to the interruption handling routine, or in the case where no new tasks are required, control is passed to the processor allocation routine which examines the task queue and chooses the highest priority task which is ready for execution. Control is then passed to this task. If no ready tasks are available, the processor is placed in a "wait" status until another interruption causes the above procedure to be repeated.

The task specification module determines the selection and priority of the tasks to be executed. The task specification function must recognize a request to execute a task, obtain and store enough information for the task to be initiated, and indicate when the task is ready for execution. Task specification identifies, locates, and evaluates in conjunction with the existing job mix, and specifies the order in which processors are to be allocated to each task.

Tasks are recorded in the data base of the Master Executive as a series of elements in the task queue, and ordered as to their priority. The elements record the task states of ready, waiting, and active, as appropriate, so that any processor can examine the queue and determine the highest priority task which is ready for processing. The ready state signifies that execution of the task can resume as soon as possible. The waiting state signifies that execution of the task must be suspended until the completion of a specific operation such as data transfer from the data bus. The active state signifies that a processor is currently engaged in executing the task.

The logic paths in the Master Executive are brought together into the processor allocation routine, which either selects the task which should next be executed, or enters the wait state, if all tasks are active or waiting. This results in a high service attention for tasks in the system.

A distributive task scheduling technique is used because the effects of processor or memory failure can be controlled in such a way that the failure does not disable the entire system. In most cases, remaining elements of DMS can continue to function in a normal way while corrective action and recovery is taking place.

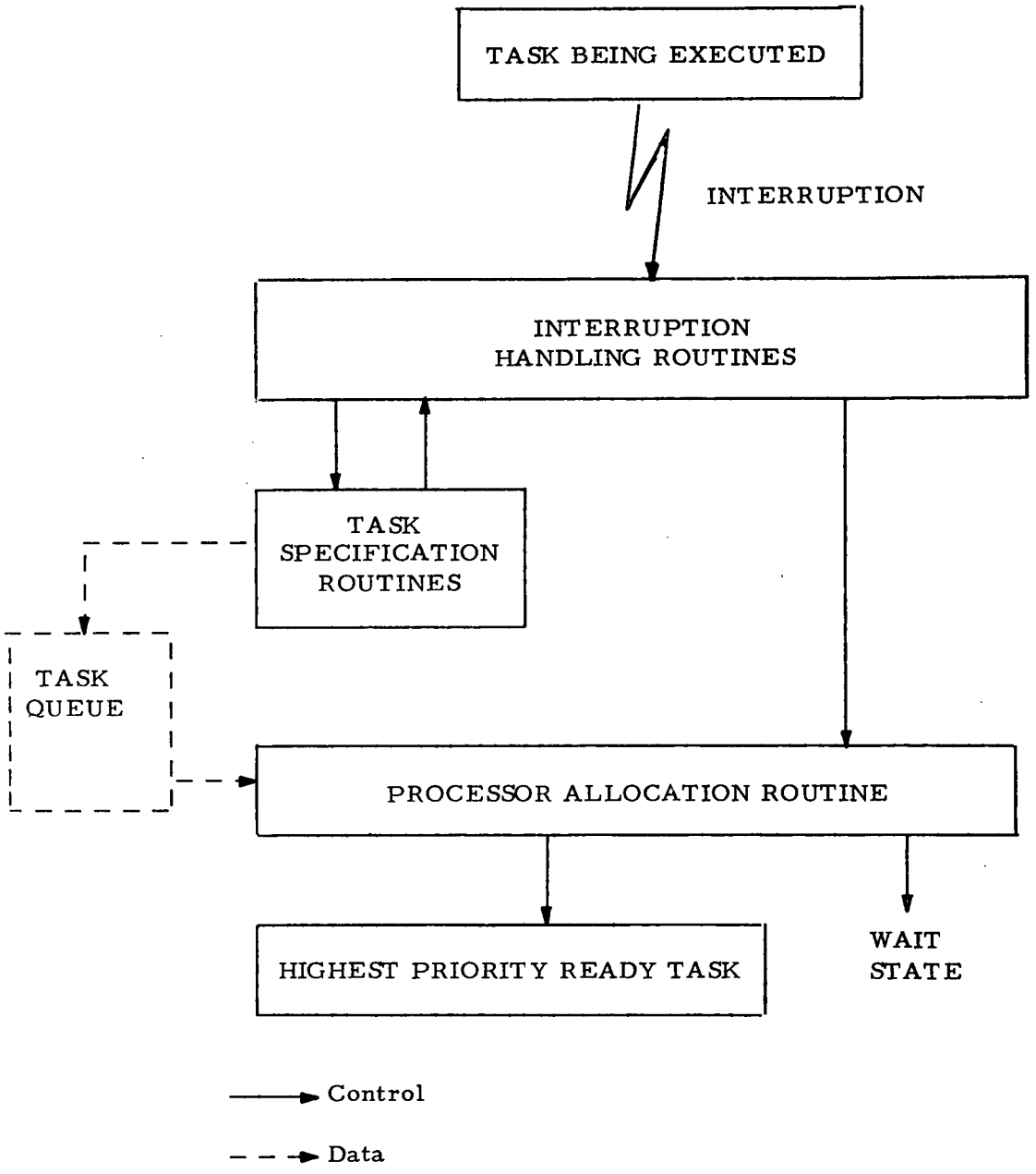


Figure 6-2. Master Executive Scheduling

The distributive technique allows any processor to execute any DMS task which is ready. As a result, during the lifetime of a task, it will receive the services of several different processors as the task states cycle through the normal sequence of ready, active, and waiting. The distributive technique eliminates the problems of interchanging master and slave roles, while utilizing more of each processor's potential.

Programs are scheduled to be initiated by the following means:

- By the crew or ground using the execute element of the high level language
- By the routine which handles timer interruptions
- By the routine which logs real-time data
- By other programs using either the execute or the call elements of the high level language

Program initiation is performed in the following steps:

a. Bring in program characteristics table

b. Verify that the parameters required by the program are available

c. Allocate memory and other DMS resources required by the program

d. Fill out or complete the program characteristics table

e. Format the working storage used by the program

f. Give control to the program

If the crew or ground requests a checkout program be executed, and one or more of the DMS LRU's required are inactive, an indication is received that the executive is unable to allocate from available resources.

6.5.2 SUPPORT SERVICES

In contrast to the in-line services of the Master Executive which are obtained when an interruption occurs, the support services operate as separate tasks.

6.5.2.1 Language Support

The language support services of the Master Executive consist of a compiler which organizes language statements into data lists, an interpreter which processes the data lists as a program, and a library of routines which provide detailed functions to support the compiler and the interpreter.

6.5.2.1.1 Compiler

Since the high level language is used for system communication as well as programming, the compiler is provided to transform keyboard entries into data lists for efficient processing by the interpreter. The compiler is used for batch processing of language stored on card, tape, or direct access media, as well as for real-time processing of keyboard entries. The data lists which are prepared during the batch process are stored in a compact form for later processing by the interpreter.

When used in the real-time mode, the compiler keeps a low profile in main storage by using overlay techniques which load only the compiler modules needed for the element being processed. As soon as a data list is formed from one language statement, control is given to the interpreter for actual processing.

From the keyboard user's standpoint, there is both a define and an execute mode of the language. When the compiler is in the execute mode, language statements, consisting of elements and modifiers, are passed to the interpreter one-by-one, as they are entered from the keyboard. The interpreter performs the specified operations and returns results, or status to the user in a conversational manner.

When the compiler is in the define mode, the data lists from language statements are accumulated until the user commands that the execute mode be entered. Transition between modes is effected by the BEGIN and the END language elements.

6.5.2.1.2 Interpreter

In general, an analysis of two or more programs written in a high-level language reveals a high degree of redundancy in the instructions which have been prepared for execution by the language translator. These programs may differ only in the parameters or data lists which are to be processed by the instructions. By removing the executable instructions from the high-level language programs and consolidating them in an interpreter, a savings in main storage results from the elimination of the redundancy. In addition, the data lists which now comprise the program can be made independent of the main storage addresses actually used to store the program during execution.

For the Space Station multiprocessor with shared main memory, the above characteristics result in more efficient use of main storage by eliminating redundant instructions which might otherwise appear in concurrent tasks. In addition, should a memory LRU fail, the programs in the LRU can be relocated without having to be restarted. A disadvantage in consolidating the executable instructions is the increase in memory contention, which results when several processors use the same set of instructions in the interpreter.

Two or more tasks are concurrently processed by the interpreter as a result of storage allocation and interpreter design techniques. The interpreter uses a block of main storage allocated to the program for storing the data required in the interpretation process, and the data required by the program itself. The interpreter routines are made reenterable by this storage technique. The reenterable attribute allows use of a routine by subsequent tasks, prior to the time when the initial task completes its use. For example, the interpreter routine which processes the MEASURE element for Task A may start an I/O operation and be waiting for its completion when Task B requires use of the MEASURE routine. Since working storage is used for all changes, Task B may enter the routine before Task A leaves it, thus decreasing the time spent waiting for task processing.

The interpreter provides general processing, such as recognition of the language element represented in the data list, and passing processor control to the appropriate library routine for detailed processing. The interpreter also controls the loading of non-resident library routines from auxiliary storage into a transient area of main storage.

6.5.2.1.3 Library Routines

Library routines of the language support services provide detailed processing necessary for the language elements. Depending on their frequency of use, they may be stored in auxiliary storage and transferred to main storage as required, or kept in main storage. Principal services provided by the language support library are as follows:

- Symbolic Test Point Translation - permitting hardware-independent development and multiple use of program modules. (See Figure 6-3).
- Data Handling - employing a data base definition, storage, and accessing technique for both the high-level language programs and for the interpreter.
- Message Assembly - permitting concise language references to skelton messages stored in the data base.

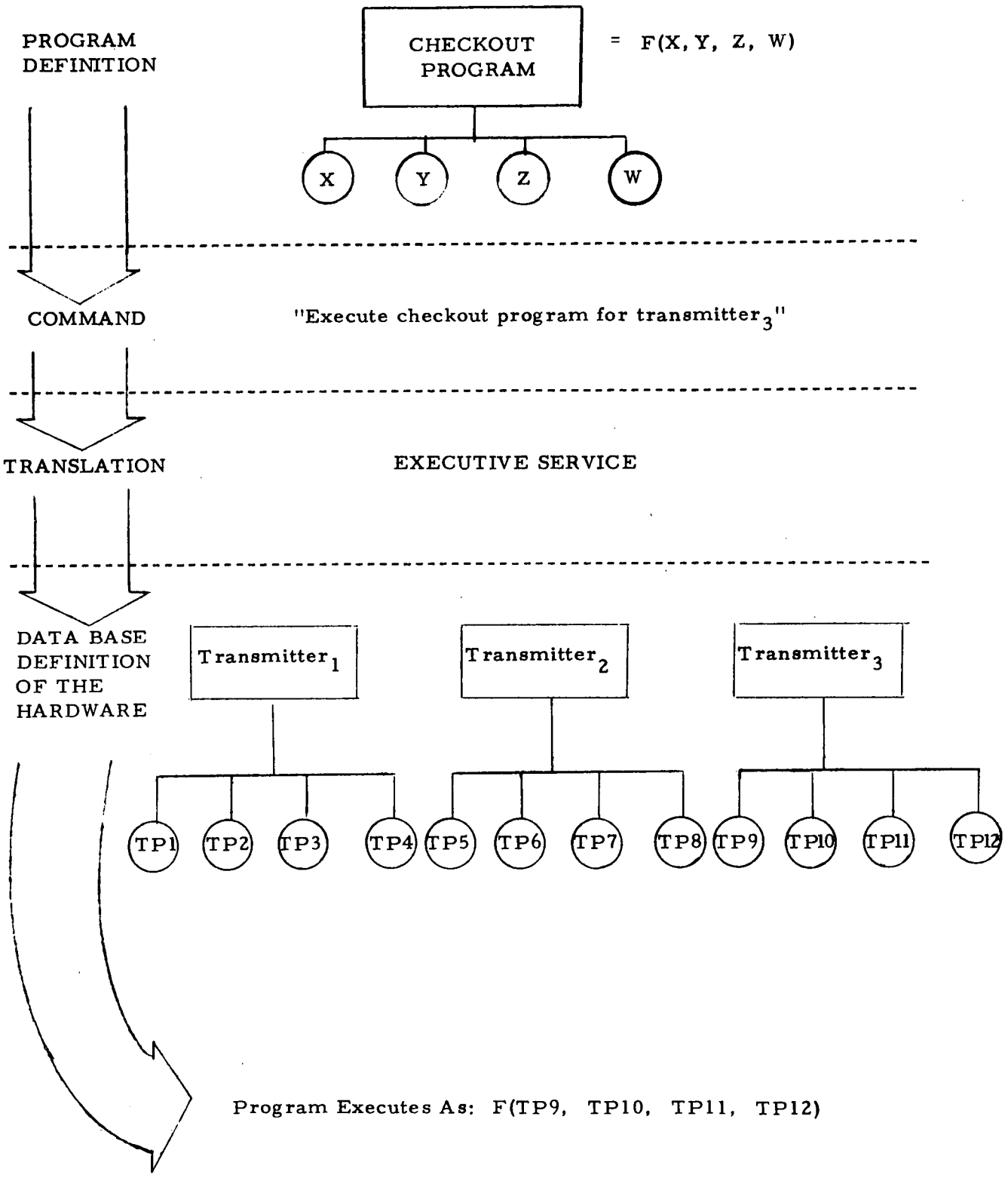


Figure 6-3. Symbolic Test Point Translation

- Arithmetic Processing - in support of the SOLVE element.

- Documentation and Debugging - to provide display, retrieval, and modification of programs; and, to provide facilities for tracing program execution.

6.5.2.2 Time-Based Services

When large numbers of programs must be initiated repetitively on a scheduled basis, a machine is a more reliable initiator than man. Examples of programs of this type are those used for trend analysis, periodic checkout, and data path verification. To relieve crew or ground personnel from the burden of remembering when to execute these tasks, a Master Executive routine called the Pacer is provided which sets the interval timer of a processor to a value which will cause a timer interruption when initiation of a scheduled task is required. A flow chart of the Pacer is shown in Figure 6-4.

6.5.2.3 Utility Services

The utility services are provided by a collection of general purpose programs which are used as required to aid man in establishing the data base, retrieving data, and modifying the Rate Table used by the Pacer.

6.5.2.4 System Initialization

The initialization procedure is invoked by crew or ground, and establishes the division between processors used for operations and those used for experiments. Initialization is invoked by a hardware command to one of the DMS processors. Included as a parameter is the address of the auxiliary storage device which contains the initialization program and the executive. Other processors are activated by the first, using the processor-to-processor communications feature. The initialization function determines the DMS configuration; loads the executive into shared main storage; establishes the initial executive data base; and finally causes each processor to execute pending tasks; or await further communication from crew, ground, or data acquisition path.

6.5.3 SYSTEM COMMUNICATION

The system communication function of the Master Executive is designed to enable man to obtain the services of the Master Executive; and, through those services invoke the functions necessary to provide data processing for the on-board subsystems. It is a design goal to implement the system communication function within the structure of the high-level language, in order to minimize the amount of "non-language" which man must know in order to make use of the Data Management Subsystem.

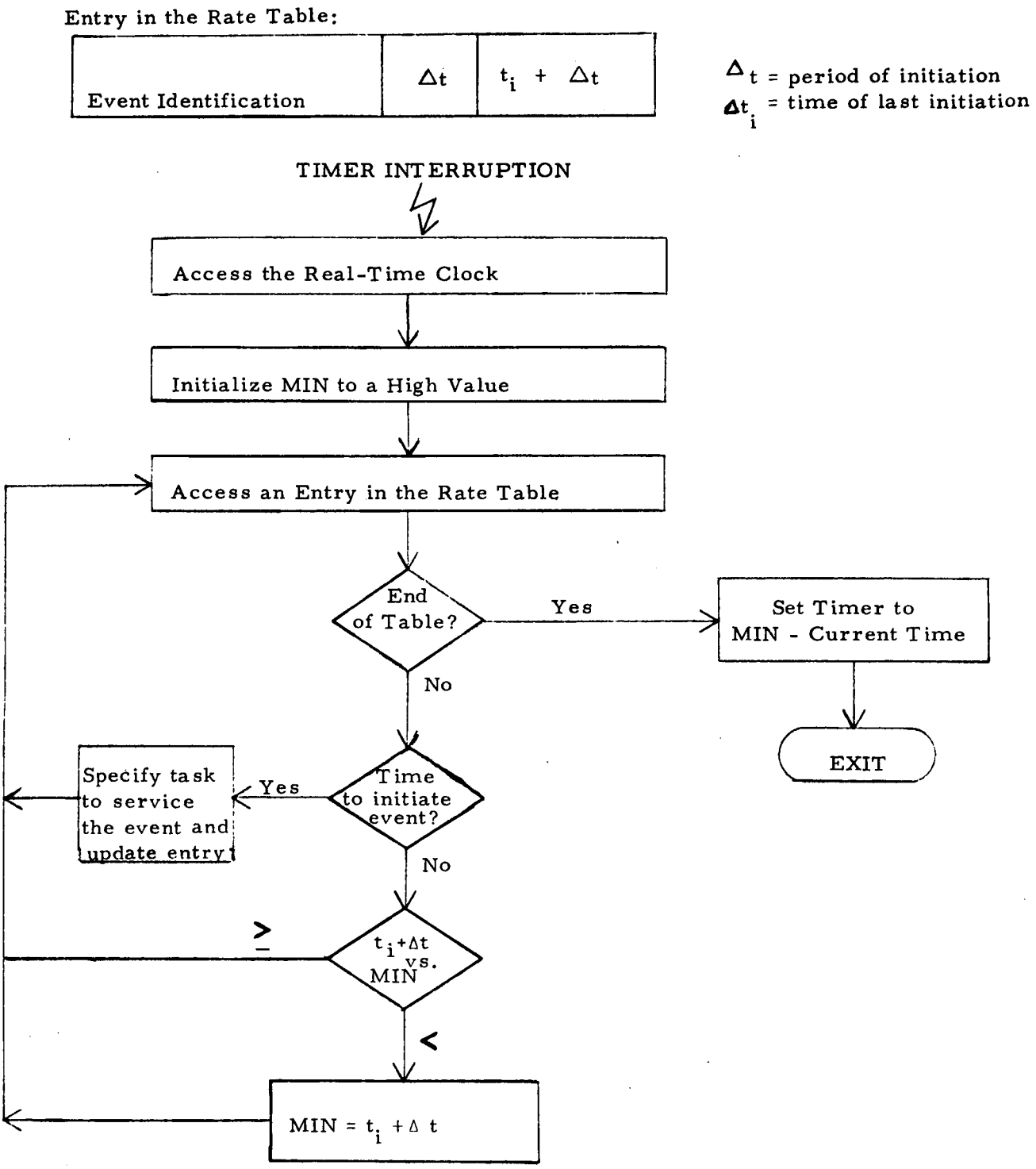


Figure 6-4. Pacer Logic Flow

6.5.4 RESOURCE ALLOCATION

The allocation and use of resources function of the Master Executive is primarily a supervisory one, and the routines that perform this function are collectively referred to as the Supervisor. The routines of the supervisor control the allocation and use of the processors, shared main storage, data bus controller, data bus terminals, and other devices of the Data Management Subsystem. The supervisory functions are as follows:

- Interrupt Supervision, which involves analysis using specific routines to handle each type of interruption.

- Task Supervision, which is the recording of tasks currently in the Data Management Subsystem, and their associated priorities, status, and the programs they require.

- Shared Main Storage Supervision, which is the allocation and deallocation of various portions of shared main storage.

- Contents Supervision, which is the loading of programs into shared main storage, and the recording of the characteristics of these programs for use in allocation and recovery procedures.

- Timer Supervision, which is the setting and maintaining of the interruptable timers of all processors in the Data Management Subsystem.

Shared main storage in the DMS is allocated by the Master Executive based on pre-defined program requirements, and requirements which arise during program execution. In order that the effect of a memory failure may be assessed, a memory table of contents is redundantly maintained in separate line replaceable units.

Programs are designed so that during execution, they may be moved about in shared main storage to eliminate fragmentation of unused storage.

6.5.5 DATA HANDLING

When a task of the Data Management Subsystem requires data outside its own working storage, it must use the data handling services of the Master Executive to obtain that data. The reason for this is to control access to the data and resolve possible conflicts. The data handling function of the Master Executive provides a unified interface with using programs so that the data location (main storage or auxiliary storage) is transparent to the programs.

6.5.5.1 Capabilities

The principal rationale for providing extensive data handling capabilities for the Space Station On-Board Checkout Subsystem is that an accurate account of status and configuration must be maintained, at least down to the LRU level. Most high-level language programs are involved indirectly in data handling; however, the interface provided through the READ and WRITE language elements allows data handling specifications to be made in general terms, consistent with the abilities of the language in other areas. Operations such as indexing, buffering, physical storage management, etc., are performed by executive routines. Data base definitions are maintained external to either executive or checkout programs, in order to provide a central reference for all routines gaining access to the data base.

6.5.5.2 I/O Operations

The processing of I/O operations is divided into the processing required to start the operation, and the processing which is required when the operation is terminated.

The use of a READ or a WRITE language element results in control being passed to the language support services routine which determines what further action should be taken. If an I/O operation is required, information required to initiate the operation is gathered, and a supervisor call instruction is executed which causes a supervisor call (SVC) interruption. The SVC interruption handler of the Master Executive gives processor control to the I/O supervisor, which either starts the I/O operation using the start I/O instruction, or enqueues the operation if the data path is busy.

When the I/O operation terminates, an I/O interruption occurs causing processor control to pass, first to the I/O interruption handler, and then to the I/O supervisor which records the fact that the operation is completed in the table provided for that purpose by the routine which requested the operation (usually the language support services routine). If an error is indicated, the appropriate error handling routine is scheduled. The queues are examined to determine if another I/O operation can be started on the data path prior to returning control to the interruption handler.

6.5.5.3 Data Logging

Many potential sources for real-time data exist in the Space Station. In order to respond to the unpredictable arrival of such data, the Master Executive provides a logging and reduction service which records the arrival of real-time data, and performs preliminary compaction prior to logging.

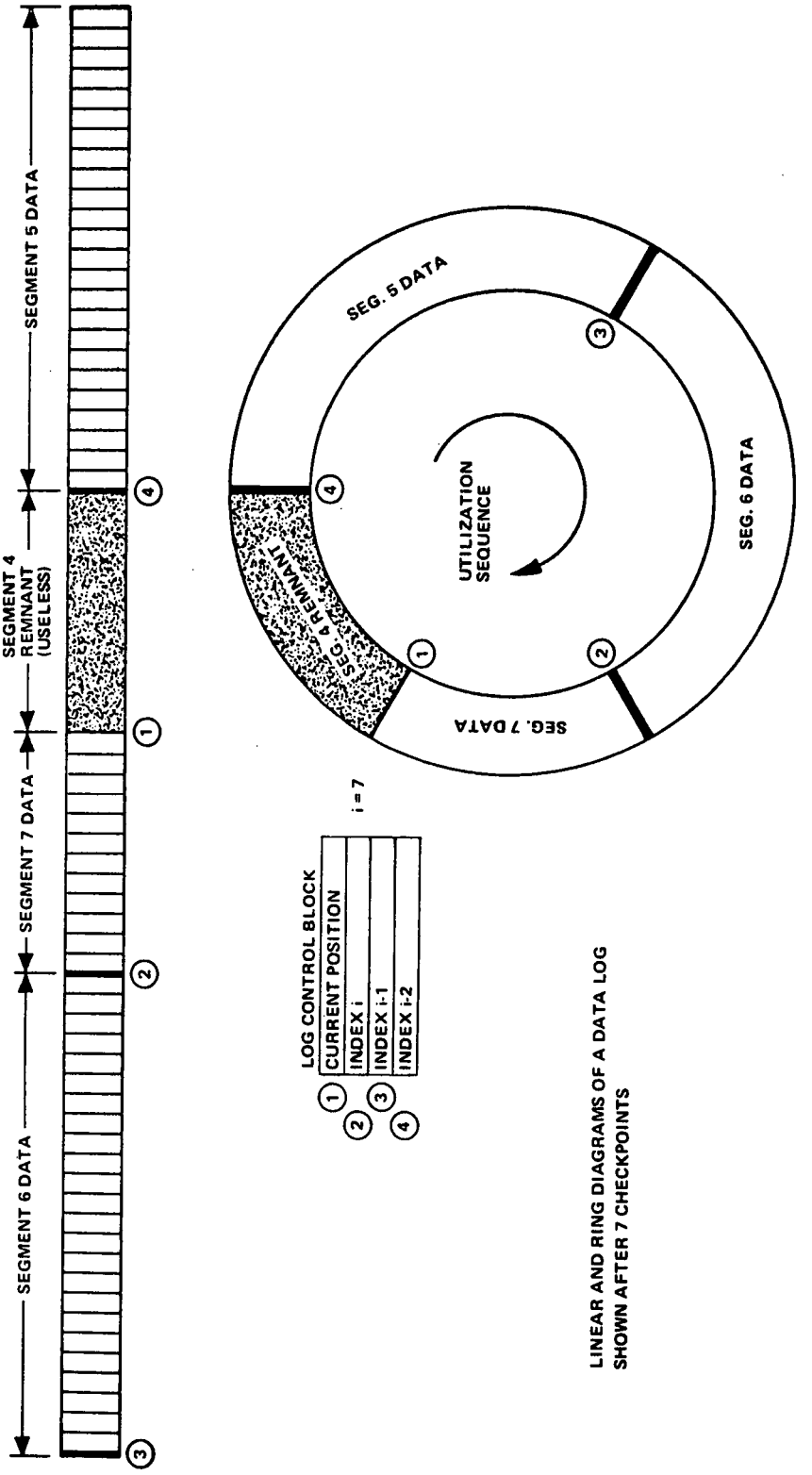


Figure 6-5. Data Log

Programs which process real-time data may be scheduled for execution by the arrival of the data, or the accumulation of a threshold quantity of data. The executive service is designed so that processing does not lock out further arrivals; and when no further data is available, the program is checkpointed so that main storage may be used for other purposes.

Specific advantages can be gained in real-time systems which accept the random arrival of data initiated by external devices, by providing routines to accomplish special analysis. Tolerance checking and data compaction typify such requirements. Tolerance check routines compare the data with user specified values, and the operator is notified only when limits are exceeded. The technique of compressing data of like characteristics or values during real time processing reduces the amount of time and space required for storage.

The log supervisor function of the Master Executive provides the following services:

- Receiving, time stamping, and logging real-time data
- Initiating the program which processes the data
- Retrieving data from the log at the request of the program

The first service continues while the other two are in progress. Note that the application program, not the log routine, coordinates transfer of data from the log to the program for processing. The log routine is responsible for insuring that the program is initiated. It is the program's responsibility to read the data by requesting retrieval from the log supervisor. If no further data is available, the log supervisor returns an indication to the effect to the program which may wait or terminate, as appropriate.

It is the joint responsibility of the log supervisor and the restart supervisor to record the progress made by the program in processing data in the log.

The association between the data source and the program required to process it is pre-defined and recorded in the data base.

A fixed number of auxiliary storage tracks, divided into several segments, are allocated for each log and used in a cycle as shown in Figure 6-5. The segments contain groups of data which have arrived since a checkpoint of the program was recorded. A log control block is used to record the segment boundaries, and maintain coordination with the associated checkpoints. Although the responsibility for initiating checkpoint procedures lies primarily with the program, the log supervisor will initiate a checkpoint if the latest segment begins to overlay the oldest segment.

The Data Retention module is a function which must accomplish the retention of data which will be required for analysis at a later time. This can be accomplished by allocating areas of peripheral storage to hold the data, and periodically deleting the data which is no longer needed.

6.5.6 SYSTEM RECOVERY

The system recovery function of the Master Executive is concerned with the activities necessary to maintain a high level of DMS operating capability when a DMS failure occurs. Reconfiguration is performed automatically by making use of redundantly maintained tables which reflect the configuration of active and spare elements at all times; and by changing the configuration control registers of the hardware.

Malfunctions in the processors and in main storage are handled by the recovery management function and initiated by a machine check interruption. Failures in the data acquisition path are also handled by this function; however, initiation is by way of the I/O interruption and subsequent analysis of associated status indications. It is a goal of the recovery management function that system operation may be permitted to continue even though failures have occurred that would otherwise cause the system to stop. If normal retry procedures are unsuccessful, the recovery management function automatically prohibits further use of the failed LRU, so that system operation can be resumed in the remaining operative portion of DMS. Recovery management then analyzes the effect of the failure, in order to restart or recover those tasks which are affected.

Recovery from certain memory failures can be achieved by refreshing the contents of the memory cell causing the problem. Separating program text from working storage makes it possible to refresh a program module if a machine check occurs during a reference to the instructions. Having working storage and instructions intermingled reduces the frequency with which this technique can be employed.

Since damage to certain infrequently used data management tables due to program error, may go undetected for a time, a data base audit function is provided to check the integrity of the data base periodically and after the failure of a memory or processor-associated LRU. Programs which provide this function verify that the relationships among components of the data base are correctly established, and that conditions that exist in the hardware are accurately reflected in the data base.

Termination procedures must provide for both scheduled and unscheduled termination of the activities of DMS software and hardware. It is a goal of the termination process to enable a restart of the system without losing task continuity, while providing a means for activities to be selectively resumed by crew or ground specification.

Providing for unscheduled termination increases system overhead. Several methods are employed in existing ground-based systems, including checkpoint, logging of changes, and emergency or backup power supplies. As Space Station requirements evolve, trade studies in this area are indicated.

6.5.7 INTERRUPTION SERVICING

The interruption is the basic means by which hardware and programs obtain the services of the Master Executive. For each type of interruption, a first level routine exists to determine detailed requirements of the requested service and route processor control to the appropriate executive routine.

The interruption is a demand to the Master Executive to recognize that an event has occurred, and to consider that event when scheduling the processor activity. While a keyboard interruption indicates that there is a console entry which should be serviced, an alarm condition may indicate a system failure. It is reasonable to assume that the alarm requires action of a relatively higher priority than the keyboard.

The design of an interruption monitor is heavily dependent upon the hardware interruption system in the computer. The software must complement the hardware design while performing the following functions:

- Save machine status (processor status and register contents if needed) at the point of interruption
- Identify the interruption source and type
- Select and execute the appropriate program module
- Restore machine status and return to the interrupted program

6.6 OCS EXECUTIVE DESIGN

The OCS Executive is designed to provide services which are unique to checkout, and common to more than one subsystem. By locating such services in the OCS Executive, redundant software development is avoided.

The OCS Executive consists of routines closely associated, or in line, with the Master Executive, and routines which operate as separate tasks. The closely associated routines are handled in the same way as the Master Executive's own in-line routines in that they are resident with the Master Executive, or established as transient routines. The separate task routines are invoked as needed by other tasks which require their services.

An example of a separate OCS Executive task is the utility which facilitates RDAU memory management. An example of an in-line OCS Executive routine is the second-level I/O interruption routine which verifies the limit check.

In the following paragraphs, the data base and the services of the Onboard Checkout System Executive are discussed.

6.6.1 DATA BASE

Operations of the OCS Executive are centered about a data base in which the configuration and status of all Space Station assemblies are continuously maintained. By storing the representation of the logical relationships which exist among assemblies of the onboard subsystems, the data base provides the reference for coordinating conflicting tasks. Hardware status can be determined without interrupting the active functions of the hardware in order to make tests, because the data base is maintained in real-time by executive programs. Use of the data base by both the Master and the OCS Executives results in more concise application programs, since the coordination procedures do not have to be provided in each program module.

6.6.2 CHECKOUT SERVICES

The functions which are determined to be associated principally with checkout, yet are not unique to a particular subsystem, are selected for implementation in the OCS Executive. This choice does not restrict in any way the selection of whether or not the high level language is used when programming these functions; rather, the choice of language may be made based on suitability relative to the specific application.

In the following paragraphs, OCS Executive services which support status monitoring, fault isolation, reconfiguration, trend analysis, and checkout program debugging are discussed.

6.6.2.1 Status Monitoring

Although the continuous measurement of test point parameters and the comparison of their values to upper and lower limits is performed by the Remote Data Acquisition Units RDAU, the OCS Executive plays an important role in status monitoring. When the I/O interruption handler detects an RDAU limit check, it passes control to a module of the OCS Executive known as the RDAU Second-Level Interruption Handler. The function of this module is to verify that the RDAU limit check is a proper one. This is done by accessing the RDAU memory contents stored in shared main storage, and comparing them with the contents of the RDAU memory. The test point which has gone out of limits is then read, and an in-storage limit

check is performed to verify that the test point is out of tolerance. Upon verification, the RDAU channels which read that test point are then masked to prevent further interruption until analysis is complete. The identity of the RDAUs involved are placed on a restore queue so that, after analysis is complete and the failure is corrected, the RDAU limit-checking mode can be re-instituted.

A functional flow chart of the Second-Level Interruption Handler is shown in Figure 6-6. Prior to passing control to the subsystem fault isolation routine, an analysis is made to determine whether the test point is out of limits is within the scope of a fault isolation task already in progress. If this is the case, then no further action is taken. If the test point is not within the scope of existing fault isolation, then a new subsystem fault isolation task is enqueued for execution.

The Second-Level Interruption Handler uses the test point identification as a key to search the data base for the indication that special processing is required for particular test points. In the interest of brevity, this is not shown in Figure 6-6. The most important type of special processing is the analysis to determine if a caution or warning indication is required when the measurement is out of limits. An example of other special processing is that used for certain Electrical Power Subsystem test points which are measured repeatedly after the initial out-of-limit indication. A fault indication is provided only if the measurement remains out of limits for a pre-determined number of consecutive measurements.

6.6.2.2 Fault Isolation

When a fault is detected and has been verified by the limit check interruption handler, the OCS Executive routine for fault isolation is given control. This is a routine written in the high-level language which utilizes key test points and the configuration data base to evaluate the performance of each Space Station subsystem, and to determine which sequence of fault isolation programs should be utilized in isolating the fault. Thus, the OCS Executive performs fault isolation at the subsystem level.

Additional functions which support fault isolation are: loss-of-capability analysis, GO-NO-GO processor,and the repair rate monitor. These functions are discussed in the following paragraphs.

6.6.2.2.1 Loss-of-Capability Analysis

The loss-of-capability function uses the configuration data base to determine the relationship between an LRU failure and hardware functions and capabilities, which are being used at the time of failure. The relationship is examined with regard to the effect of the failure on vital functions and capabilities.

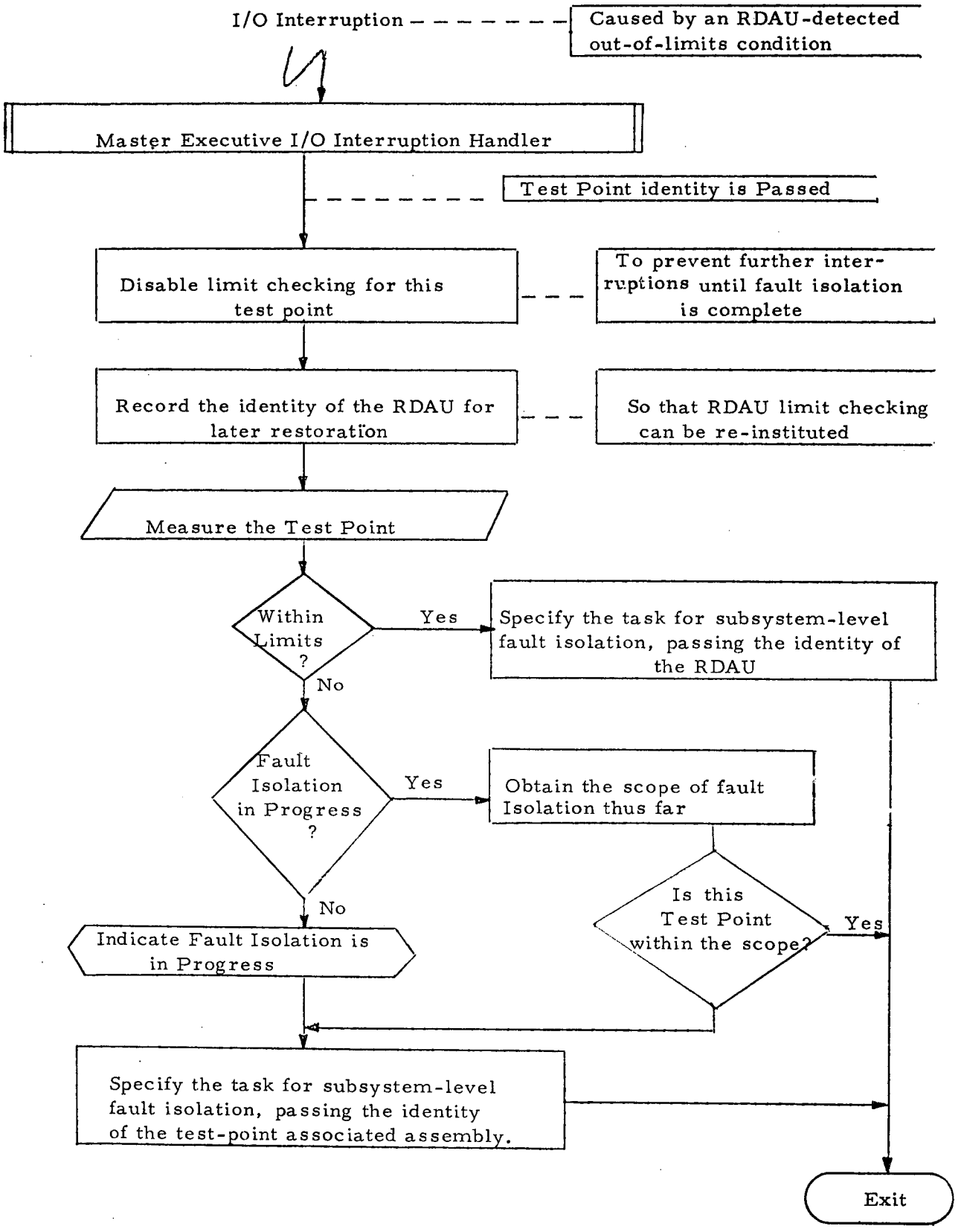


Figure 6-6. RDAU Second-Level Interruption Handler

6.6.2.2.2 GO-NO-GO Option Processor

In order to permit the operator some flexibility in dealing with situations where a reading is detected out of tolerance, the application program requires the ability to respond to keyboard direction. Subsequent to detecting an out-of-limit situation, a message is displayed and the program enteres the GO-NO-GO processor. The available options are presented, the operator enters his selection, and program to continue as if no error has been detected, to re-execute the part of the program which detected the error, and to terminate the program.

6.6.2.2.3 Repair Rate Monitor

When a failure has been isolated, the actual remove and replace activity may be delayed in order to optimize crew activities by having all such functions performed according to a schedule. The repair rate monitor function serves as a log to record fault incidences for use in scheduling activities requiring crew intervention. A reminder feature is provided which acts to insure that a failure, once detected and isolated, is not forgotten. Use of the Pacer is made to send a message to the crew if action has not been taken within a pre-determined time interval. Reminders may be rescheduled or cancelled by appropriate manual entries at the display keyboard.

6.6.2.3 Reconfiguration

The reconfiguration update utility program facilitates changing the configuration tables of the data base to reflect changes to the configuration of the subsystems. The utility also is used as a tool when establishing the configuration data base for use by the fault isolation and operational procedures. This function has an extensive interface with man, and is not intended to be used as a real-time update function.

6.6.2.4 Trend Analysis

The trend analysis functions are implemented as a library of several different types of routines which are designed to fulfill all trend analysis requirements of the Space Station Subsystems.

The executive is involved in the following steps when a trend measurement is required:

- The Pacer detects the need to perform a trend measurement
- Restart retrieves the last copy of working storage
- If the program is not already in storage, it is loaded

- Control is passed to the program which makes the measurement, logs it, and updates the working storage

- If the processing results dictate, crew communication is performed

- Checkpoint-and-terminate is invoked to save the updated copy of working storage and relinquish processor control

For certain trend analysis applications, the data is merely stored for later recovery and review. The trend data display function provides the means by which man can retrieve trend data, and control the presentation of it in the form most suitable for his purposes. Facilities are provided for processing the data in tabular or graphical form.

6.6.2.5 Program Verification Facilities

An important aspect of checkout which is too often overlooked is that of software verification. The Executive services capability should contain sufficient software verification techniques to determine the validity of the high-level language test sequences in real time. A requirement further exists for a complete software verification facility to be provided in a ground environment "Hanger Queen" to perform checkout verification on both operational and checkout software.

The program verification facilities of the OCS Executive serve to provide an interface with checkout programs indistinguishable from actual hardware, yet controllable by man. The facilities use random number generation techniques to unpredictably assume all possible situations which can arise from a given arrangement of test points, so that program performance can be assessed rapidly and without extensive time consuming breadboard techniques.

Section 7

MAINTENANCE

There are two aspects of maintenance which entered into the basic study. Basic maintenance concepts were provided as part of the baseline resulting from the Phase B Space Station study; they are discussed in subsection 7.1 below. Additionally, one of the study tasks was aimed at implementation of an onboard electronics maintenance capability. The results of that task are summarized in subsection 7.2.

7.1 BASELINE MAINTENANCE CONCEPTS

Maintenance concepts defined for Space Station subsystems are intended to facilitate their preservation or restoration to an operational state with a minimum of time, skill, and resources within the planned environment.

7.1.1 GENERAL SPACE STATION MAINTENANCE POLICY

It is a Space Station objective that all elements be designed for a complete replacement maintenance capability unless maintainability design significantly decreases program or system reliability. This objective applies to all subsystems wherever it is reasonable to anticipate that an accident, wearout, or other failure phenomenon will significantly degrade a required function. Estimates of mean-time-between-failure, or accident/failure probability, are not accepted as prima facie evidence to eliminate a particular requirement for maintenance. Should the accident/failure probability be finite, the hardware is to be designed for replacement if it is reasonable and practical to do so.

As a design objective, no routine or planned maintenance shall require use of a pressure suit [either EVA or internal vehicular activity (IVA)] . Where manual operations in a shirtsleeve environment are impractical, remote control means of affecting such maintenance or repairs should be examined. However, EVA (or pressure suit IVA) is allowable where no other solution is reasonable, such as maintenance of external equipment.

Time dependency shall be eliminated as a factor of emergency action insofar as it is reasonable and practical to do so. This includes all program aspects of equipment, operations, and procedures which influence crew actions. When time cannot be eliminated as a factor of emergency action, a crew convenience period of 5 minutes is established as the minimum objective. The purpose of the convenience period is to provide sufficient time for deliberate, prudent, and unhurried action.

7.1.2 ONBOARD MAINTENANCE FACILITY CONCEPTS

In addition to OCS/DMS capabilities, other onboard maintenance support facilities provided on the Space Station include:

- Special tools for mission-survival contingency repairs such as soldering, metal cutting, and drilling, as determined from contingency maintenance analyses, although repairs of this type are not considered routine maintenance methods.

- Protective clothing or protective work areas for planned hazardous maintenance tasks (such as those involving fuels, etc.).

- Automated maintenance procedures and stock location data for both scheduled and unscheduled maintenance and repair activities.

- Real-time ground communication of the detailed procedures, update data, and procedures not carried onboard.

- Onboard cleanroom-type conditions by "glove box" facilities compatible with the level at which this capability is found to be required.

- Maintenance support stockrooms or stowage facilities for spares located in an area that provides for ease of inventory control and ready accessibility to docking locations or transfer passages.

7.1.3 SUBSYSTEM MAINTENANCE CONCEPTS

Space Station subsystems utilize modular concepts in design and emplacement of subsystem elements. Subsystem modularity enhances man's ability to maintain, repair, and replace elements of subsystems in orbit. Providing an effective onboard repair capability is essential in supporting the Space Station's ten-year life span since complete reliance on redundancy to achieve the long life is not feasible. The need for a repair capability, in turn, requires that a malfunction be isolated to at least its in-place remove-and-replace level. The level of fault isolation is keyed to the LRU, which is the smallest modular unit suitable for replacement. The identification of subsystem LRUs is addressed as a separate, but interdependent, part of the Onboard Checkout Study.

Specific subsystem maintenance concepts, of course, depend upon examination of the subsystems. These concepts are discussed in subsequent subparagraphs. General subsystem-related maintenance guidelines that have been established for the Space Station are:

- It is an objective to design so that EVA is not required. However, EVA may be used to accomplish maintenance/repair when no other solution is reasonable.

- Subsystems will be repaired in an in-place configuration at a level that is acceptable for safety and handling, and that can be fault-isolated and reverified by the integrated OCS/DMS. This level of maintenance is referred to as line maintenance and the module replaced to effect the repair is the LRU.

- A limited bench-level fault isolation capability will be provided on the Space Station, but is only intended for contingency (recovery of lost essential functions beyond the planned spares level) or for development purposes. Limited bench-level support is also provided in the form of standard measurement capabilities which are used primarily to reduce the amount of special test equipment required.

- Subsystem elements, wherever practical, will be replaced only at failure or wearout. Limited-life items that fail with time in a manner that can be defined by analysis and test will be allowed to operate until they have reached a predetermined level of deteriorated performance prior to replacement. Where subsystem downtimes for replacement or repair exceed desirable downtimes, the subsystem will include backup (redundant) operational capability to permit maintenance. Expendable items (filters, etc.) will be replaced on a preplanned, scheduled basis.

7.2 ONBOARD ELECTRONIC MAINTENANCE (STUDY TASK 3)

The objective of this task was to generate recommendations of supporting research and technology activities leading to implementation of a manned electronics maintenance facility for the Space Station. Early in the task it became apparent that attention could not be confined to a central maintenance facility; it was necessary to refocus the task to address implementation of an on-board maintenance capability encompassing in-place as well as centralized maintenance activities. The critical questions are the following:

- What is the optimum allocation of onboard maintenance functions between in-place and centralized maintenance facility locations?

- What is the optimum level of onboard repair (i.e., to line-replaceable unit, subassembly or module, piece part, or circuit element)?

7.2.1 MAINTENANCE CYCLE

In order to place the task in the proper context, a generalized Space Station electronic maintenance cycle is depicted in Figure 7-1.

A convenient place to enter the cycle is with detection of a fault ("In-Place Maintenance" block). The fault is isolated to a Line Replaceable Unit (LRU). The affected subsystem is restored to full capability by replacing the failed LRU with an operable one from spares storage.

The failed LRU is taken to a maintenance facility (assumed for the moment to have a fixed location in the Space Station) where it is first classified as repairable or non-repairable. Classifications will likely be predetermined, and a listing should be retained in the Data Management Subsystem. If the LRU is non-repairable, it is placed in segregated storage. If the LRU is repairable on board, the fault is further isolated to the failed Shop Replaceable Assembly (SRA). The LRU is then repaired by replacing the failed SRA with one from spares storage. The repaired LRU is then calibrated (if necessary), and its operation verified before it is placed in spares storage.

Logistics requirements (replacement LRUs and SRAs needed) are transmitted to ground-based logistics support functions by RF communications and/or Space Shuttle. Failed units are taken away from and replacement units are delivered to the Space Station by the Space Shuttle.

7.2.2 SUMMARY OF RESULTS

The study confirmed and emphasized the necessity of onboard maintenance for any manned mission of any complexity and duration measured in months (up to 10 years for Space Station). Formulation of recommendations for implementing such a capability required consideration of other topics first, and achievement of certain interim results. The principal conclusions of this study task are summarized below. The analyses leading to them are explained in the Task 3 Final Report.

- Prior studies and developments of in-space maintenance have emphasized justification of first-level (in-place) maintenance, fasteners, and tools for space application and human factors criteria. Much less attention has been devoted to test equipment, maintenance training, or definition of shop level maintenance requirements.

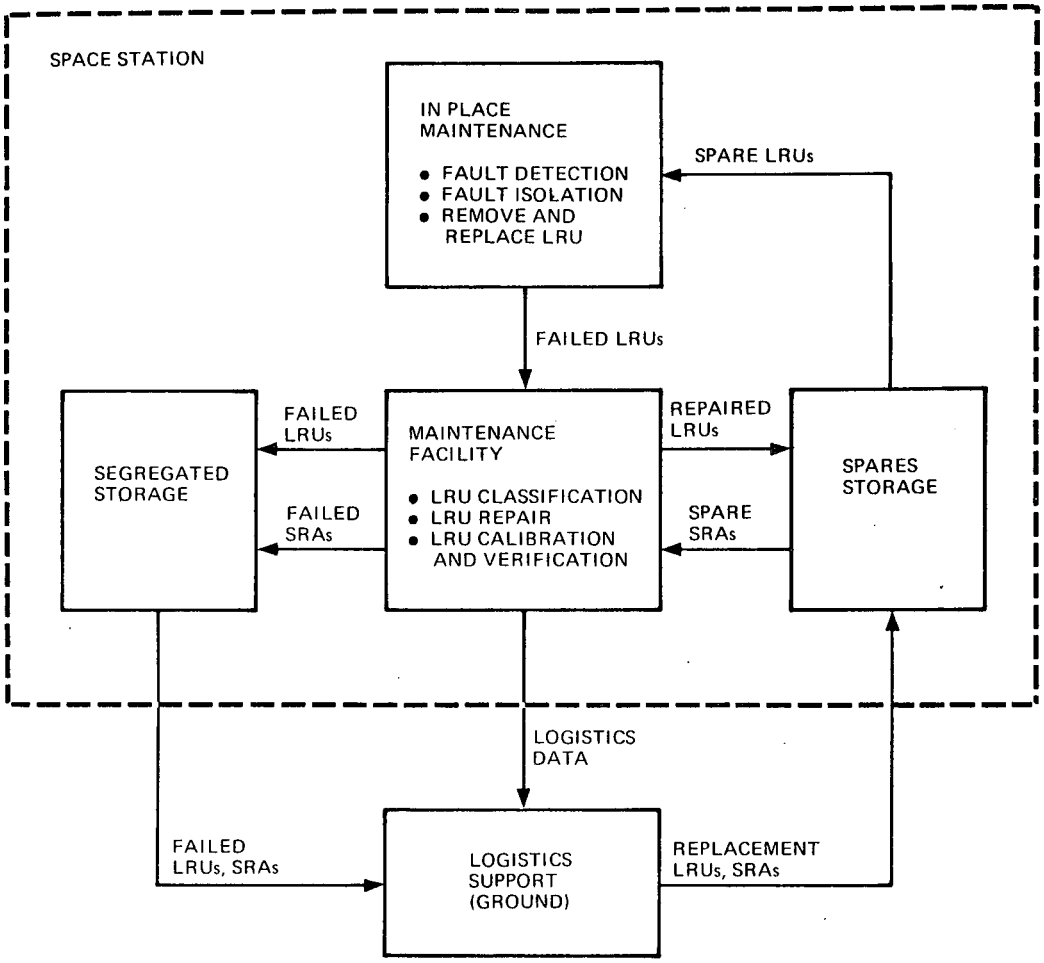


Figure 7-1. Space Station Maintenance Cycle

- The baseline subsystem descriptions, checkout requirements analysis, and software requirements analysis indicate that approximately 60 percent of all faults (over a long period) can be isolated to the failed LRU automatically under software control, without crew intervention. In an additional 27 percent of failure cases, fault isolation to one LRU can be achieved by the crew using the onboard Data Management System as a tool. In the remaining failure cases, additional fault isolation capabilities are needed. This is a good result for a "first iteration" and can probably be improved considerably with a modest effort to modify stimulus and measurement provisions.

- Crew involvement in scheduled and unscheduled maintenance (including participation in fault isolation) is estimated to average 7.2 manhours per week over the total mission time. This estimate is most sensitive to equipment reliability and levels at which onboard repair is performed. It is affected little by the efficiency of automated fault isolation under control of the Data Management Subsystem (DMS).

- The recommended approach to maintenance in the baseline Space Station is in-place removal and replacement of LRUs, without attempts to repair LRUs onboard, if the resupply interval is less than nine months. Onboard spares should be LRUs.

- For long resupply intervals or non-resupplied missions (as in a manned interplanetary mission), in-place maintenance should be by removal and replacement of LRUs. Repair of LRUs should be by removal and replacement of Shop Replaceable Assemblies (SRAs). Onboard spares should be SRAs.

- The Earth-orbital Space Station should include provision for development of onboard maintenance capability and techniques applicable to long duration non-resupplied missions and/or the larger, more complex Space Base.

- The baseline subsystem descriptions are at such a level of detail that precise specification of onboard tools and test equipment is neither feasible nor desirable. Anticipated needs identified qualitatively in the study are: (1) a portable test module to supplement software fault isolation as well as to assist mechanical adjustments and calibrator, (2) hand tools for removal and replacement of electronic assemblies, (3) devices for transporting and positioning spare assemblies, and (4) a central maintenance/repair bench.

- Several tasks have been identified and recommended for future performance, as part of a system study/design program or as separate supporting research and technology tasks. The principal ones deal with (1) development of a portable test assembly, (2) development of a repair/test bench with special provisions for small parts retention and for debris collection, (3) design for accessibility of test points and subassemblies, and (4) devices for transporting equipment within the Space Station.

The foregoing conclusions apply to the Modular Space Station as well as the 33-foot diameter, four-deck configuration.

The results of the study rest upon several assumptions and estimates, derived wherever possible from related experience. The results are not sensitive to small variations of the assumed or estimated values, except for equipment failure rates, which are most influential. Furthermore, it has not been practicable to pursue all trade analyses to include all relevant factors. Nevertheless, the study has generated valid insights into Space Station onboard maintenance and useful visibility of the path to implementation of that capability.