

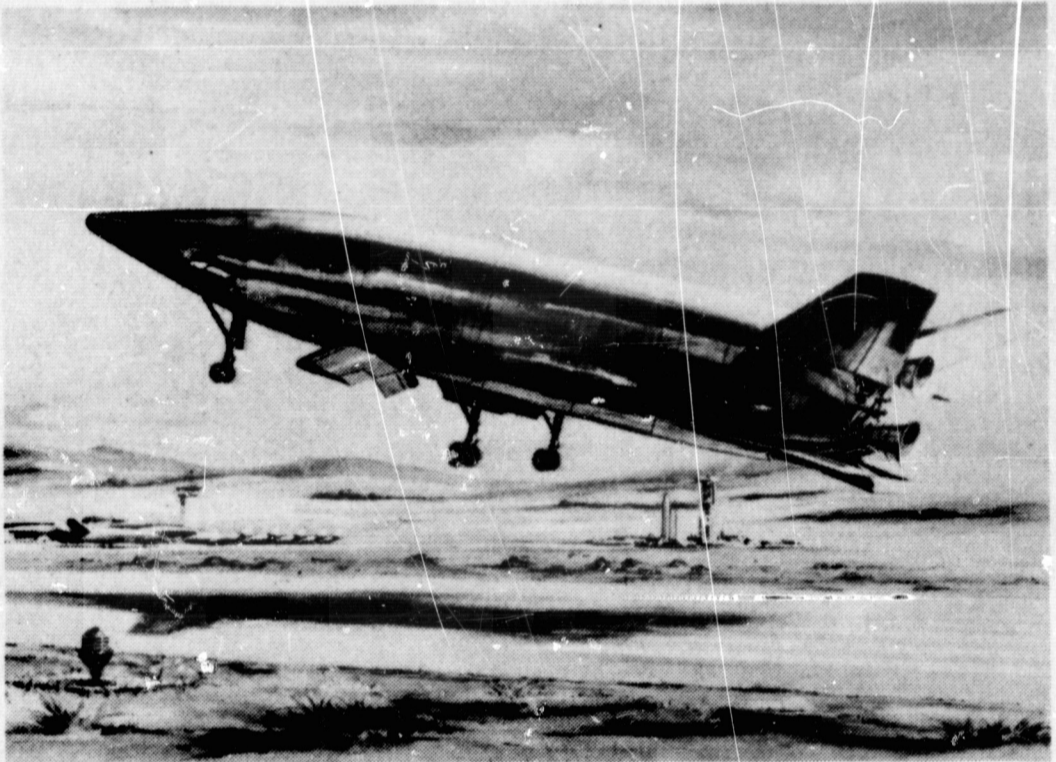
General Disclaimer

One or more of the Following Statements may affect this Document

- This document has been reproduced from the best copy furnished by the organizational source. It is being released in the interest of making available as much information as possible.
- This document may contain data, which exceeds the sheet parameters. It was furnished in this condition by the organizational source and is the best copy available.
- This document may contain tone-on-tone or color graphs, charts and/or pictures, which have been reproduced in black and white.
- This document is paginated as submitted by the original source.
- Portions of this document are not fully legible due to the historical nature of some of the material. However, it is the best reproduction available from the original submission.

X70-13384
CR-102554

REPORT NO. GDC-DCB69-046
CONTRACT NAS9-9207



SPACE SHUTTLE FINAL TECHNICAL REPORT

VOLUME VII + INTEGRATED ELECTRONICS

FACILITY FORM 602

N70-31542 (ACCESSION NUMBER)	
135 (PAGES)	1 (THRU)
CR-102554 (NASA CR OR TMX OR AD NUMBER)	31 (CODE)
	(CATEGORY)

GENERAL DYNAMICS
Convair Division

REPORT NO. GDC-DCB69-046

**SPACE SHUTTLE
FINAL TECHNICAL REPORT**

VOLUME VII ♦ INTEGRATED ELECTRONICS

31 October 1969

Prepared by
CONVAIR DIVISION OF GENERAL DYNAMICS
San Diego, California

FOREWORD

This volume of Convair Report No. GDC-DCB 69-046 constitutes a portion of the final report for the "Study of Integral Launch and Reentry Vehicles." The study was conducted by Convair, a division of General Dynamics Corporation, for National Aeronautics and Space Administration George C. Marshall Space Flight Center under Contract NAS 9-9207 Modification 2.

The final report is published in ten volumes:

Volume I	Condensed Summary
Volume II	Final Vehicle Configurations
Volume III	Initial Vehicle Spectrum and Parametric Excursions
Volume IV	Technical Analysis and Performance
Volume V	Subsystems and Weight Analysis
Volume VI	Propulsion Analysis and Tradeoffs
Volume VII	Integrated Electronics
Volume VIII	Mission/Payload and Safety/Abort Analyses
Volume IX	Ground Turnaround Operations and Facility Requirements
Volume X	Program Development, Cost Analysis, and Technology Requirements

Convair gratefully acknowledges the cooperation of the many agencies and companies that provided technical assistance during this study:

NASA-MSFC	Aerojet-General Corporation
NASA-MSC	Rocketdyne
NASA-ERC	Pratt and Whitney
NASA-LaRC	Pan American World Airways

The study was managed and supervised by Glenn Karel, Study Manager, C. P. Plummer, Principal Configuration Designer, and Carl E. Crone, Principal Program Analyst (all of Convair) under the direction of Charles M. Akridge and Alfred J. Finzel, NASA study co-managers.

ABSTRACT

A study was made to obtain a conceptual definition of reusable space shuttle systems having multimission capability. The systems as defined can deliver 50,000-pound payloads having a diameter of 15 feet and a length of 60 feet to a 55-degree inclined orbit at an altitude of 270 n.mi. The following types of missions can be accommodated by the space shuttle system: logistics; propellant delivery; propulsive stage delivery; satellite delivery, retrieval, and maintenance; short-duration missions, and rescue missions.

Two types of reusable space shuttle systems were defined: a two-element system consisting of a boost and an orbital element and a three-element system consisting of two boost elements and an orbital element. The vehicles lift off vertically using high pressure oxygen/hydrogen rocket engines, land horizontally on conventional runways, and are fully reusable. The boost elements, after staging, perform an aerodynamic entry and fly back to the launch site using conventional airbreathing engines. Radiative thermal protection systems were defined to provide for reusability. Development programs, technology programs, schedules, and costs have been defined for planning purposes.

During the study, special emphasis was given to the following areas: System Development Approaches, Ground Turnaround Operations, Mission Interfaces and Cargo Accommodations/Handling, Propulsion System Parameters, and Integrated Electronics Systems.

TABLE OF CONTENTS

Section		Page
1	INTRODUCTION	1-1
	1.1 SPACE SHUTTLE INTEGRATED ELECTRONICS	1-1
	1.1.1 Autonomous Operation	1-1
	1.1.2 Workload Considerations	1-1
	1.1.3 Data Multiplexing	1-2
	1.1.4 Navigation and Vehicle Control	1-2
	1.1.5 Automatic Landing Systems	1-3
	1.2 STUDY GROUND RULES	1-3
2	INTEGRATED ELECTRONICS	2-1
	2.1 INTRODUCTION	2-1
	2.2 DISPLAYS AND CONTROLS	2-1
	2.2.1 Introduction	2-1
	2.2.2 Display Task	2-4
	2.2.3 Types of Displays	2-5
	2.2.4 Discussion of Characteristics	2-11
	2.2.5 Display System Concepts	2-13
	2.2.6 Controls	2-16
	2.3 ONBOARD COMPUTERS AND SOFTWARE	2-19
	2.3.1 Introduction	2-19
	2.3.2 General Arguments	2-19
	2.3.3 Comparative Analysis	2-22
	2.3.4 Definition and Scope of Computer Hardware	2-28
	2.3.5 Computer System Estimates	2-31
	2.3.6 Definition and Scope of Computer Software	2-31
	2.4 MULTIPLEXED DATA BUS	2-37
	2.4.1 Introduction	2-37
	2.4.2 Basic Multiplexing Concepts	2-37
	2.4.3 Considerations	2-38
	2.4.4 Selection of Data Bus Technique	2-41
	2.5 GUIDANCE AND NAVIGATION	2-50
	2.5.1 Introduction	2-50
	2.5.2 Requirements	2-50
	2.6 COMMUNICATIONS	2-54
	2.6.1 Introduction	2-54
	2.6.2 Launch Phase	2-54
	2.6.3 On-Orbit Phase	2-54
	2.6.4 Entry	2-54
	2.6.5 Subsonic Flight Phase	2-54

TABLE OF CONTENTS, Contd

Section	Page
2.6.6 Effect on Configuration	2-55
2.6.7 Automatic Landing	2-55
2.6.8 Return of Unmanned Boosters	2-56
2.6.9 Impact of Change, Three-Element to Two-Stage Shuttle	2-56
3 ONBOARD CHECKOUT	3-1
3.1 INTRODUCTION	3-1
3.2 APPROACH TO THE PROBLEM	3-1
3.3 ONBOARD CHECKOUT OBJECTIVES	3-2
3.3.1 Prelaunch Confidence Testing	3-3
3.3.2 Performance Monitoring	3-3
3.3.3 Postflight Securing	3-5
3.3.4 Maintenance Assist	3-5
3.4 CHECKOUT CRITERIA	3-6
3.4.1 Prelaunch Criteria	3-7
3.4.2 Flight Performance Monitor Criteria	3-8
3.4.3 Maintenance Assistance Criteria	3-9
3.4.4 Instrumentation Criteria	3-10
3.4.5 Criteria Problems	3-10
3.5 Concept Development	3-11
3.5.1 System Test Processes	3-11
3.6 FAULT IDENTIFICATION METHODS	3-13
3.6.1 Direct Examination	3-13
3.6.2 Indirect Examination	3-14
3.7 PROGRAM DEVELOPMENT	3-14
3.7.1 Fault Disposition Routines	3-16
3.7.2 Instrumentation Selection	3-21
3.8 SYSTEM DESCRIPTION	3-23
3.9 SPECIAL EMPHASIS SYSTEMS DESCRIPTION	3-24
3.9.1 Environmental Control/Life Support System	3-24
3.9.2 Electrical Generating System	3-53

LIST OF ILLUSTRATIONS

Figure		Page
2-1	Integrated Electronics Subsystems	2-2
2-2	Display System Concept Block Diagram	2-14
2-3	Computer - Controlled Display Concepts	2-18
2-4	Flow Diagram of Selection Process	2-41
2-5	Bi-Phase Data Waveforms	2-43
2-6	Level Shift Transmitted Data Waveforms	2-44
2-7	Bi-Phase Transmitted Frequency Spectrum	2-44
2-8	Level Shift Transmitted Data Frequency Spectrum	2-45
3-1	Functions of Onboard Checkout	3-2
3-2	Prelaunch Functions	3-3
3-3	Performance Monitoring	3-4
3-4	Postflight Securing	3-5
3-5	Maintenance Assistance	3-6
3-6	Test Processes for Onboard Checkout	3-12
3-7	Fault Detection Program	3-15
3-8	Vehicle Readiness Fault Disposition	3-17
3-9	Performance Monitor Fault Disposition	3-19
3-10	Postflight Secure Fault Disposition	3-20
3-11	Maintenance Assist Fault Disposition	3-22
3-12	Onboard Checkout Subsystem	3-25
3-13	Atmosphere Supply and Pressurization Control	3-28
3-14	Atmosphere Supply and Pressurization Control Fault Detection Routine	3-29
3-15	Atmosphere Purification Loop	3-34
3-16	Atmosphere Purification Loop Fault Detection Routine	3-35
3-17	Water Management Subsystem	3-39
3-18	Water Management Fault Detection Routine	3-41

LIST OF ILLUSTRATIONS, Contd

Figure		Page
3-19	Waste Management Subsystem	3-44
3-20	Waste Management Fault Detection Routine	3-46
3-21	Personal Hygiene Subsystem	3-48
3-22	Thermal Control Subsystem	3-49
3-23	Thermal Control Loop Fault Detection Routine	3-52
3-24	Orbiter Electric Power System	3-56
3-25	Fuel Cell Output Fault Detection Routine	3-57
3-26	Fuel Cell Reactant Supply	3-59
3-27	Fuel Cell Reactant Supply Fault Detection Routine	3-61
3-28	Fuel Cell Water Removal	3-63
3-29	Fuel Cell Thermal Control	3-65

LIST OF TABLES

Tables		
2-1	Characteristics of Various Display Types	2-12
2-2	Power and Weight Estimates for Various Display Types	2-15
2-3	Optimum Configuration for Minimum Power and Weight Estimates	2-17
2-4	General Arguments Relative to Multiprocessor and Federated Computer Configurations	2-20
2-5	Processor Combinations	2-30
2-6	Computer System Estimates	2-32
2-7	Program and Data Estimates Unique to Orbiter	2-35
2-8	Program and Data Estimates Common to Booster and Orbiter	2-36
2-9	Program and Data Estimates for Booster and Orbiter Vehicles	2-36
2-10	Bus Options	2-46

LIST OF TABLES, Contd

Tables		Page
2-11	Baseline Guidance Accuracies	2-50
2-12	Estimated Power and Weight For Gimbaled and Strapdown Navigation Subsystems	2-52
3-1	Fault Identification Methods	3-13
3-2	Abbreviations and Chemical Symbols	3-26
3-3	Sensor Symbols	3-26
3-4	Component Symbols	3-27
3-5	Atmosphere Supply and Pressurization Control Redundancies	3-31
3-6	Atmosphere Purification Loop Redundancies	3-37
3-7	Water Management Subsystem Backup and Emergency Modes	3-43
3-8	Waste Management Backup Modes	3-45
3-9	Thermal Control Redundancies and Backups	3-50
3-10	ECS/LS Fault Detection Summary	3-54
3-11	Fuel Cell Onboard Checkout Removable Unit Fault Summary	3-67

SECTION 1
INTRODUCTION

1.1 SPACE SHUTTLE INTEGRATED ELECTRONICS

This report, while discussing the entire integrated electronics system for space shuttle is, at MSFC's direction, oriented toward a detailed discussion of certain limited areas. These areas, which are covered in detail, are:

- a. Onboard checkout, with particular emphasis on environmental control/life support and electrical power subsystems.
- b. Definition and the determination of the scope of the onboard computer system and its associated software.
- c. "State-of-the art" surveys and technology projections in the areas of display and control and automatic all-weather landing systems.
- d. Multiplexed data systems.

1.1.1 AUTONOMOUS OPERATION. The integrated electronics subsystem, like the space shuttle itself, is configured with the goal of lower total operating costs than those experienced with present-day systems. The key to lower total system costs lies in the area of almost completely autonomous operation of the shuttle, from checkout through countdown, flight, and landing. This autonomy, if achieved, will minimize the support required from large, expensive ground operations such as the launch control center at KSC, the mission control center at MSC, and the present NASA world-wide tracking and communication network.

This autonomy, however, does introduce new requirements into the vehicle's electronics subsystem, and some of these requirements and their implications are discussed in this report. It is emphasized that the particular implementations given in this report must be considered as a "baseline" or "strawman" system, which is subject to change as dictated by the mandatory tradeoff studies yet to be conducted. These studies will have to consider all the operational hardware and software aspects of the complete space shuttle transportation system.

1.1.2 WORKLOAD CONSIDERATIONS. Unless care is taken in implementation, the transfer to the vehicle of operations formerly performed by ground personnel could overload the flight crew. Particular attention must be given to the crew's capability and workload, the man-machine interfaces, and the vehicle's computers and their software.

1.1.2.1 Information Displays. Some of the requirements for onboard display of information may be determined by looking at the many mission phases and different vehicle modes. This examination will reveal that the display subsystem must present information to the crew that will allow them to check out their vehicle, launch it, perform the required orbital operations, entry, subsonic flight, and finally land it as a conventional aircraft. The electromechanical dials, gages, "8 balls", switches and similar devices in use on today's conventional aircraft and spacecraft do not have the flexibility to provide to the crew all of the information needed to enable them to efficiently manage the mission. The "state-of-the-art" of displays was therefore examined, and it appears that computer-driven cathode-ray tube displays come closest to meeting all the shuttle's requirements. Plasma displays, if their development continues at the present pace, may also be used for some alphanumeric display functions.

1.1.2.2 Computers and Software Organization. The computers carried on the shuttle must also handle many more functions than were performed by computers aboard previous spacecraft. The incorporation of these additional functions, such as checkout, display generation, mission management, and autonomous navigation, creates the need for a careful analysis to determine the optimum computer configuration. Complicating this analysis is the desired system characteristic of "fail operational, fail operational, fail safe", which in general means some form of multiple redundancy.

One section of this report considers this computer organization problem, a preliminary analysis of the software requirements, and an estimate of the resulting computer size. It can be seen from this analysis that the required computer capability will greatly exceed that carried by the Apollo spacecraft. These estimates of computer and software requirements should be used with great care, as examination of many other programs indicates that the final computer and software requirements often exceed the initial estimates by up to an order of magnitude. For example, the initial memory requirements estimated for the Apollo spacecraft computer was 4000 words, the final version had about 38,000 words, and many desired computer functions were found to be impractical due to the limited memory.

1.1.3 DATA MULTIPLEXING. The many different vehicle modes, the multiple redundancy, the resulting large number of "black boxes", and the requirements for low weight and reliability, have directed attention to the multi-pin connectors and wire bundles that abound on present generation spacecraft. The use of data multiplexing for onboard monitoring and control is examined in this report, and criteria for its application are developed. It should be noted that data multiplexing is now used for Apollo spacecraft checkout and control via the ACE equipment and the S-band telemetry and control links; and the extension of these techniques to onboard controls, monitoring, and checkout is a natural result of the miniaturization of electronic circuits.

1.1.4 NAVIGATION AND VEHICLE CONTROL. The various portions of the electronics subsystem used for guidance, navigation, and control are, in general, fairly conventional, with the choice between sensors made on the basis of development

status, accuracy, and probable reliability. Thus, this report recommends an installation of multiple gimballed inertial measurement units, but recommends "strapdown" instruments for starfield mapping, horizon tracking, and rendezvous laser radar.

1.1.5 AUTOMATIC LANDING SYSTEMS. The "state-of-the-art" of automatic landing systems was examined, and because of the requirement to land at any 10,000 ft runway, a system utilizing the present airline instrument landing system (ILS) was recommended for initial use, with later use of a scanning fan beam system when it becomes available.

1.1.6 AUTOMATIC ONBOARD CHECKOUT. The various aspects of onboard automatic checkout were examined with particular emphasis placed on a detailed analysis of the electrical power generation subsystem, and the life support/environmental control subsystem. It was found that once a vehicle is structured with an integrated electronics subsystem, containing powerful digital computers, flexible displays, and a multiplexed data system, the inclusion of onboard checkout becomes a fairly simple task, and will not burden the vehicle with a large number of additional transducers, wire bundles, or special switching networks. In fact, if properly done, the controls and monitoring equipment already required for the control of the various subsystems will provide the necessary means to accomplish almost all of the onboard checkout.

1.2 STUDY GROUND RULES

The original set of ground rules for this study is included in the work statement supplied by MSFC.

It seems pertinent to draw attention to a few factors that are akin to ground rules to provide additional perspective for the reader.

- a. Configurations for subsystems that serve as specific examples for onboard checkout analysis, namely, the environmental control/life support subsystem and power subsystems, were identified quite early in the study. The analysis of checkout tasks influenced and modified the configurations until a point where the configurations were frozen for reporting purposes. Further modifications of these two subsystems have occurred, but are not reflected in these pages.
- b. For the purposes of this study, the NASA "Desired System Characteristics" (Vol. II, Space Shuttle Task Group Report, revised 12 June 1969) were accepted as firm requirements, realizing that in Phase B many tradeoffs will be performed to eventually determine the final system requirements.

SECTION 2

INTEGRATED ELECTRONICS

2.1 GENERAL SYSTEM DESCRIPTION

To meet the requirements of reliability, minimum weight, and minimum operating cost, the space shuttle electronics subsystem was structured around the concepts of computer control, multiplexed data bus, cathode-ray tube displays, and onboard checkout.

The multiplexed data bus was chosen to permit the subsystem interconnections, while eliminating much of the weight and unreliability associated with conventional wiring. In this concept each "black box" communicates with the other portions of the electronic subsystem by means of time-multiplexed signals on a data bus consisting of redundant coaxial cables or shielded twisted pairs. The interface between this data bus and the "black box" is known as a data bus interface (DBI). It normally is an integral part of each "black box", containing error-checking circuitry and the triple or quadruple redundancy necessary to meet vehicle requirements.

The baseline integrated electronics subsystem is shown in Figure 2-1. The components are used in different combinations as the mission requires. The electronics subsystem in its onboard checkout and control roles interfaces with many other subsystems, such as propulsion and life support. The use of the data bus concept will greatly simplify the specification and control of these normally complex interfaces.

Cathode ray tube (CRT) displays provide the flexibility in the man-machine interface required by the multiphase missions of the reusable vehicle. This permits the display of information pertinent to the particular portion of the mission that is being performed, without requiring the crew to obtain this information by scanning several hundred indicators scattered around the flight deck.

2.2 DISPLAYS AND CONTROLS

2.2.1 INTRODUCTION. The displays and controls subsystem for the space shuttle has additional requirements over and above the subsystem requirements for prior manned spacecraft. First, the need for increased autonomy from ground mission control required additional information displays for more effective onboard mission management. Second, the inclusion of an onboard checkout capability presents another magnitude of display and control requirements. Third, the aircraft characteristics of the two system elements forces yet more requirements in both areas.

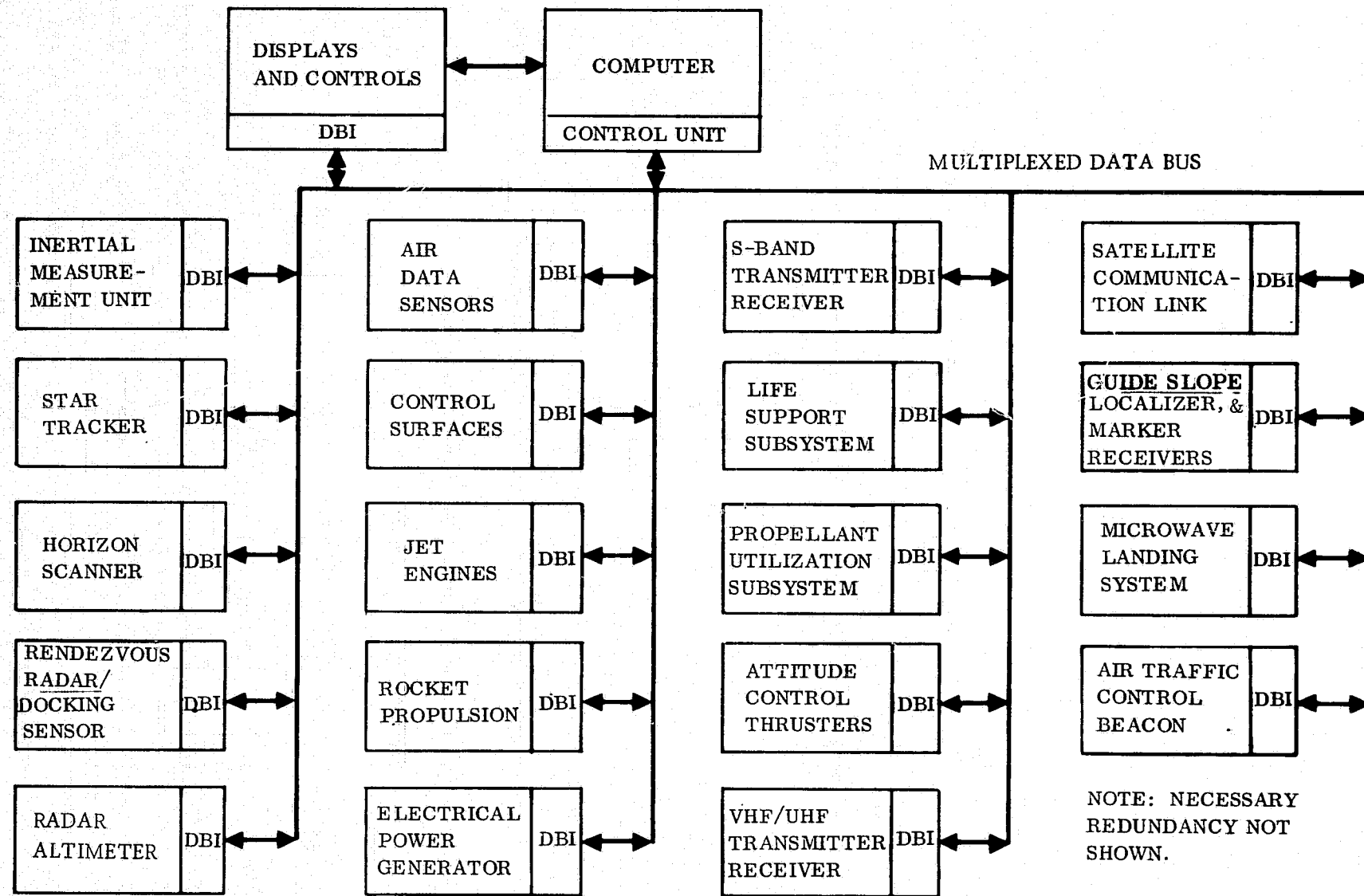


Figure 2-1. Integrated Electronics Subsystems

Additionally, the displays and controls subsystem for the space shuttle should overcome the problems encountered during operations in prior spacecraft. The display and control panels in manned spacecraft to date have been very cluttered, required too much area, and consumed too much volume. Circuit breakers and other electromechanical display and control devices have been troublesome to the crews because of high failure rates. The faces of some displays had to be red-lined and otherwise marked up by the crew to accommodate sensor calibration shifts and to provide greater clarity. Too much valuable crew time has been spent in the crew training area to acquire an intimate familiarity with the maze of displays and controls.

Innovation and ingenuity are required within the state-of-the-art to overcome past problems and at the same time to satisfy the greatly increased information display and vehicle control functions.

2.2.1.1 Requirements. What are some of the requirements for this space shuttle subsystem?

- a. Display devices should be of a more universal nature, capable of easily displaying any function or parameters instead of being reserved for a single function.
- b. Circuit breakers, mechanical switches, and electromechanical display devices should be eliminated.
- c. Software changes such as for sensor substitutions, sensor and transducer calibration shifts, and new operations limits for selected functions should not require alterations of display equipment.
- d. Measurement circuit, sensor, and transducer characteristics must be designed to prevent crew actions and perplexities in the event of measurement sensing equipment failures; i.e., the relationship between sensor intelligence input and voltage output might have to be inverted as it was for manual abort parameters in both the Gemini and Apollo spacecraft.
- e. More display of actual versus expected parameter variations and trending is required onboard, especially in the consumables area, to accommodate prior program groundbased mission control tasks.
- f. Two crew stations should be provided, with mission management capable from either station.
- g. An audio alarm should be implemented as part of the caution and warning subsystem, somewhat similar to the "night watchman" employed in the Apollo spacecraft. Not only is the reaction time decreased, but this concept fits in easily with the new approach to have crew members share the same work/sleep cycle.
- h. The number and types of displays and controls should be kept at a minimum to optimize display area, volume, clarity, and comprehension.

2.2.1.2 Equipment Approach. The list of requirements is incomplete and additional study is required to provide a comprehensive listing. More communication is also required with NASA crew systems personnel and mission control personnel to validate and optimize the requirements in light of all past problems in Apollo and Gemini spacecraft. However, the requirements provide sufficient visibility at this time to clarify the equipment approach:

- a. The input data for display and control should be predominantly of a digital type.
- b. A computer should serve as the interface between the measurement sensors and displays, and between the manual control provisions and functional subsystems.
- c. Extensive use should be made of CRT's and digital display devices.

The rationale for the above approach follows.

Digital data displays are precise and easy to read. Parallax and other sources of error, such as dual-pointer discrepancies, are eliminated. The use of more universal display devices requires a rapid handling of data. A computer is the most efficient information management mechanization that man has conceived.

Many of the complex and frequent routine command and control functions can be programmed, stored, called up instantly, and effected with precision with a computer. Crew time, decisions, and control provisions can all be minimized if a computer is provided as the interface between man and the machine for command and control or mission management. CRT's and other digital display equipment provide, in one device, a large number of alphanumeric displays. Coupled with a computer, pictures of subsystems' trends, consumables status, and expected-versus-actual performance variations can be instantly presented and easily understood. This use of a small number of digital display devices provides the capability for a two-crew-station mission management capability without the penalties of excessive areas, weight, and other trade considerations. During critical mission phases, both crew members can monitor the same information on their own displays; while during routine mission phases, tasks such as housekeeping can be easily shared by the two crewmen, with the same display equipment configuration. Crew loading will be minimized. The necessity to rotate crew positions that prevailed during Apollo missions can be abandoned.

2.2.2 DISPLAY TASK. The display task is the principal man-machine interface in the overall system. It is through the displays that the crew monitors the performance of all subsystems in the vehicle so that mission management can be performed with minimum assistance from external sources.

The display task can then be divided into two major categories, which may be identified as housekeeping and operational. Housekeeping includes the presentation of data related to the performance of the various systems and subsystems that comprise the vehicle, while operational is related to the relationship between the vehicle and the outside world.

2.2.2.1 Methods of Presentation. Information within these categories can be furnished visually to the crew in one or more of the following ways. Alphanumerics have long been recognized as an effective method of transmitting information to humans. We have been conditioned from early in our lives to extract information from the printed page, whether in the form of text or numerical values. This is a useful method for transmitting preprogrammed instructions, as might be used during preflight checkout, or for presenting quantitative data on the current status of important items such as the relative amount of fuel remaining compared to that planned in the mission schedule. A second method is the use of pictorial information from which the observer can determine the relative positions of various objects presented. A prime example of this is a radar plan position indicator (PPI) display or a television picture. Both fall primarily into the class of environmental displays. A third form of presentation is an analog display such as an aircraft vertical situation display or a simulation of a so-called "8 ball". This format also displays X-Y type plots, which permit rapid correlation and analysis of data that would be difficult to perform if the data were presented in a tabular format.

Other examples of analog type displays are bar graphs and simulated meter faces drawn on the display surface. This type of display is most easily achieved with a device capable of random plot capability, and the hardware requirements are different from those of the TV or radar display. A fourth type of display may be termed a status or go/no-go indicator. In the simplest configuration this could be a pilot light. Further versatility can be added by means of color change or text change in the display message; or even with separate indicators, each labeled to show the degree of relative performance of the system identified with those indicators.

2.2.2.2 Baseline Assumptions. Because specific display tasks have not yet been definitized, it becomes necessary to assume certain display capabilities to establish a baseline for comparative purposes. For example, it may be reasonable to assume that a minimum of 1,000 characters will be required for an alphanumeric display, and that there will be pictorial display capability requirement for radar and/or television. These may or may not appear on the same display surface, which is a feature that can be determined during the definition phase of the program.

2.2.3 TYPES OF DISPLAYS. Electronic displays may be divided into three general categories: X-Y flat panel, projection, and direct view cathode-ray tube. Other displays of possible interest in this program may be included in a fourth category for completeness. Major types of displays in each of these categories are discussed below.

2.2.3.1 X-Y Flat Panels. A recent development in display technology is the plasma display panel, which is a two-dimensional array of individually addressable cells, each filled with an inert gas. When ac voltage is applied across the cells, the gas is ionized and begins to glow. To maintain the light emission, a lower voltage is applied across

the cell. At the present time, the largest X-Y panel fabricated is 4×4 inches, with a cell density of 33 per linear inch. It is expected that in a few years panels measuring 10×10 inches with a density of 50 cells per linear inch will be available.

At this time, little is known about the expected lifetime of these panels, although in principle they should have a long life. However, some early models have exhibited failure of an individual cell or row of cells, which would cause dead spots on the array. Several failures such as this might be classified as serious failures that would impair the function of the display panel. At present, the brightness of 30 foot lamberts is adequate in a controlled ambient, but it may be insufficient for a cockpit display. Recently, a brightness of 750 foot lamberts has been observed in the laboratory.

Liquid Crystal Display. Another recently developed display uses an electro-optic effect in liquid crystals. As with the plasma display, individual X-Y addressing of cells is required to cause optical scattering in the medium. In this device, however, light is not generated; instead external light is used as the source of energy. In the off state, the crystals are transparent but become translucent when energized. Present models of the device range up to 4×4 inch panels with a resolution capability on the order of 700 lines per inch. This resolution, however, is that of the crystal medium itself; actual resolution would be a function of the spacing of transparent electrodes that must be applied to the panel. The line density is dependent upon the panel thickness, and present estimates indicate that a resolution of 30 to 50 lines per inch could be obtained. The response time of the device may be a limiting factor in this application, because a rise time of 1 to 5 milliseconds is required to activate an individual cell. This would preclude its use in a TV type display. Lifetimes have been estimated at greater than 30,000 hours with ac operation and 3,000 hours for dc operation.

Electroluminescent Panels. A great deal of work has been done on electroluminescent panels for display purposes. These panels consist of a suitable phosphor placed between electrodes separated a few thousandths of an inch. Voltage applied to transparent conductors on the panels causes the phosphor to glow. The light output is proportional to both frequency and voltage; although frequency has a more profound effect, because the light output is nearly linear with frequency. In general, light output is low, on the order of 10-12 foot lamberts for an applied voltage of 250 volts at 400 Hz. The resolution is limited to about 25 - 30 lines per inch because a phosphor thickness of several mil-inches is required. Lifetime, although good at low voltages such as 120 volts, 60 Hz, has been found to deteriorate rapidly with both higher voltage and higher frequency. Thus although adequate light output of 50 to 100 foot lamberts could be obtained at higher voltage and frequency, lifetime would be affected.

It is generally acknowledged that, although the panel itself requires relatively low power for illumination, the driving circuitry necessary to supply that power becomes quite extensive because of the low power factor in the system due to the high capacitance of the panel. Recent devices demonstrated in a TV mode have shown very low

brightness, poor resolution, and only two or three shades of gray. The recent use of evaporated film phosphors has increased the resolution to 32 lines per inch at a sacrifice in phosphor efficiency. Electroluminescent devices have been in active development for 15 years, with only minor improvements in performance. Expectation of breakthroughs in the next few years is small. At this time this device may be excluded from serious consideration.

Light Emitting Diodes. Recently, the light emitting diode (LED) has emerged as a potential display device with some attractive characteristics. These devices are capable of high light output (100 foot lamberts) with very small input voltages (less than 4 volts). The LED produces light by carrier injection electroluminescence across a p-n junction. Its switching time is very short (approximately 1 nanosecond), and its useful life is measured in hundreds of thousands of hours. A typical diode has a circular active region of 0.010 to 0.015 inch diameter and can be spaced on centers of 0.020 to 0.025 inch when fabricated using large-scale integration (LSI) techniques.

Power input for large arrays may be excessive (~ 0.03 watt per diode), but it is expected that greater efficiencies will be achieved in the next few years. The devices can be fabricated to emit different colors, ranging from green to red, although present diodes capable of green light have extremely low efficiency (10^{-4} or less). When used in arrays for numeric indicators, devices are available today with a character height of 0.25 inch, and other sizes ranging from 0.125 to 0.5 inch will be available shortly. These devices may be logical candidates for numeric readout or for status indicators if used as pilot lights. At the present time the cost is quite high ($\sim \$5$ per diode), but this may be because they are fairly new devices, and the cost should be reduced significantly in mass production.

2.2.3.2 Projection Displays. In general there are two types of projection displays, those which use an external light source such as an arc lamp or incandescent lamp and those in which the energy source is the device itself. In the first category a means must be provided to dynamically modulate the light beam for which a cathode-ray tube (CRT) is generally used. Thus a CRT and its complete set of driving circuits are required in addition to an external light source and associated optics system, which of course implies additional system weight.

Photochromic Film and CRT. One configuration for such a system uses photochromic film in contact with a CRT having a fiber optics faceplate. Photochromic materials change color upon excitation by ultraviolet radiation then revert slowly to their original state. Storage times are dependent upon the composition of the material, and range from 10 seconds to 30 minutes. Because of their low sensitivity, the writing rate is very slow, even when a high-energy CRT is used as the light source. The erase time can be reduced somewhat by subjecting the film to radiant energy in excess of 5,000 Angstroms, but it is still not considered a fast erase medium. The photochromic material has a finite life because of side reactions that occur in the

illumination process. Typical films exhibit complete fatigue at 500 to 1,000 cycles, but they can be replaced manually as necessary.

Light Valves and Schlieren Optics. Light valves employ a deformable surface which when used with a Schlieren optical system, projects the deformed pattern onto a screen. Perhaps the best known of the systems is the Eidophor, which is used for theatre television. In this device the deformable medium is an oil film that is activated by an electron beam. In some models the oil film is external to the CRT envelope to prevent cathode contamination. Some versions of this device use a thermoplastic medium which, when heated after electron bombardment, creates the deformed surface. All of these devices have been developed specifically for large-screen display applications, and because of their size, weight, and complexity, they are not serious contenders for this display application.

CRT and Schmidt Optics. A more direct form of projection display using a CRT is the device where the image on the screen of a small CRT is magnified onto a viewing screen by means of an optical system. Conventionally a Schmidt optical system is used because of its high light transmission. In general, a high-powered CRT is used, which results in a reduced tube lifetime on the order of 1,000 hours. A typical Schmidt optical system consists of a spherical reflector approximately 24 inches in diameter that has an effective speed of $f/0.7$. Alignment of the CRT in the optics is very critical because of the extremely small depth of focus.

Laser Projector. A discussion of projection schemes for display would not be complete without inclusion of a laser as the energy source. Although a great deal of work has been done in the past ten years, a satisfactory means for deflection of the laser beam has not been achieved. Solid-state schemes using electro-optic and birefringent crystals require very high voltages and are capable of deflecting to a maximum angle of about 5 degrees. Other means of deflection use a rotating mirror for horizontal and vertical scanning to produce a television type of presentation. It is obvious that serious stability problems can arise with such a system. Because of the extremely low efficiency of cw lasers, the input power to the laser for a display of the size and brightness typical of this application would be on the order of 3 kw. This power requirement alone would preclude the laser projector from consideration.

2.2.3.3 Direct View Cathode-Ray Tubes. Use of the cathode-ray tube (CRT) as a display device is well known and popular because of its great flexibility and proven effectiveness. Its high reliability has been well established. An MTBF for CRT systems is predictable. Additional reliability can be incorporated into the CRT by the use of redundant electron guns. This is an effective way of increasing the useful life of the tube, because cathode failure is the most frequent cause of tube failure. Recent use of solid-state circuitry has reduced the power and weight of commercial television receivers so that a typical 7-inch set requires only 15 watts and weighs about 9 pounds. Typical military displays capable of high performance weigh 30 pounds and require 200 watts for a 10-inch display.

Contrast Enhancement. Although brightness is generally limited to about 200 foot lamberts, which may be inadequate in a high ambient environment, considerable improvement in display legibility can be obtained by contrast enhancement. Some techniques that have proved successful are the use of a micromesh or a polaroid filter over the tube face, or the recently developed black-face CRT. If it is determined that color variation is a necessity in a display system, it can be incorporated at an increase in weight, power, and cost. Two colors may be obtained by the use of a multilayer phosphor, wherein changes in the electron beam energy determine screen penetration and the resultant color produced. This system requires high voltage switching with associated modulation of deflection gain. Three colors may be obtained by the use of a shadow mask tube of the type used in commercial television receivers; but it is doubtful that, even with appreciable development work, these tubes could withstand space shuttle shock and vibration.

CHARACTRON^R. When large quantities of alphanumeric data are required, consideration should be given to the CHARACTRON^R Shaped Beam Tube, which forms characters internally by extruding the electron beam through a stencil with a multiplicity of character-shaped openings.* This tube may also be used in a spot-writing mode for television or analog data. Other methods of character generation with standard cathode-ray tubes deflect a focused electron beam in a predetermined manner so that characters are generated by a series of strokes or dots. Virtually all CRT displays have inherent versatility and are easily adapted to computer-generated data.

A new development in shaped-beam tube technology has produced a significant brightness increase in CHARACTRON^R tubes, and additionally has simplified tube construction. Experimental tubes for large-screen projection systems have exhibited light output in excess of 3000 foot lamberts when 1000 characters are displayed flicker-free. Utilization of this technique in a 10-inch tube for direct viewing would achieve a brightness on the order of 1000 foot lamberts before filtering for contrast enhancement. Several types of CHARACTRON^R tubes have been qualified for use in military aircraft.

Storage Tubes. A special form of CRT is a storage display tube which retains the information written on the tube face for periods up to 10 minutes. This is accomplished by creating a charge pattern on a grid network behind the phosphor screen, which selectively transmits a flood beam of electrons from a second electron gun. In some models selective erasure is achieved by writing with an additional electron gun of a different accelerating voltage. In all tubes the entire display may be erased in a few milliseconds. Storage tubes have the obvious advantage of eliminating the need for buffer storage of the data displayed. However, for a 10-inch tube, resolution is limited to about 40 lines per inch because of the cellular construction of the storage surface. In addition, reliability suffers because of the need for several active electron

* CHARACTRON^R is a registered trademark of Stromberg DatagraphiX, Inc.

guns within the tube envelope and from excessive gas generated during use. Typical lifetimes are on the order of 1,000 hours.

A distinct advantage in addition to storage is the high brightness that can be obtained on the tube face. Typically, brightness levels on the order of 2,000 foot lamberts are readily attainable, which is the principle reason for this tube's use in aircraft cockpit displays where there is a high ambient light level. If it is desired to present a pictorial display without storage, a class of storage tubes known as multimode tubes have this capability by adjusting the accelerating voltage of the writing electron gun.

Helmet-Mounted Optical Projection System. A novel use of a CRT for spacecraft displays is the helmet-mounted optical projection system. This system consists of a one-inch cathode ray tube mounted on the side of the pilot's head. By means of a suitable optic system and appropriate mirrors, the image on the face of the CRT is displayed in front of the observer's eye. The display has a brightness capability in excess of 100 foot lamberts. The total package, including optics and CRT, weighs less than one-half pound. With appropriate color filtering in one of the mirrors, the observer can distinguish CRT-generated data from that within his normal field of vision. Conventional CRT circuits are used to generate the display.

2.2.3.4 Other Type of Displays. In applications where it is necessary for the pilot to observe information from the outside world as well as from his instruments, techniques have been developed to present data on a windshield. Such displays are known as headup displays. Various techniques for generating the information have been developed, which include a flat CRT with transparent phosphor, plasma panels with transparent electrodes, and various types of overhead projectors with contrasting colors.

The conventional approach to cockpit displays has been the use of a multiplicity of analog instruments, chiefly meters, dial gauges, and instruments similar to the flight director attitude indicator (8-ball). The Apollo vehicle, for example, uses some 400 different display functions with a weight in excess of 300 pounds. Many of the instruments display data that are used for only a small fraction of the mission.

All displays need not be visual. Information can be conveyed to the pilot by audio means. For example, a steady tone of a particular pitch can indicate that a particular system is operating according to schedule when queried by the pilot. In event of a malfunction, or if a warning is necessary, the pitch can be changed or the tone can be interrupted to form a beep. Quantitative data can be transmitted by assembling stored syllables or words in a manner similar to that used presently for quotations of securities. Recorded messages can be particularly useful for preflight checkout.

2.2.4 DISCUSSION OF CHARACTERISTICS

All flat panel displays require individual connections to each of the electrodes in the X and Y directions. An individual cell in the matrix is then addressed by selecting the desired pair of X and Y conductors. If the resolution requirement is on the order of 400 lines per display dimension (approximate commercial television resolution), a total of 800 individual wires must be attached to the panel. The reliability problems associated with such a multiplicity of connectors must be assessed as part of the consideration for this type of display. It is possible that the control and logic circuits can be an integral part of the panel, but development is needed.

Display Size. Most of the flat panels are available in sizes up to 4×4 inches at the present time. If a larger display is required, groups of modules must be assembled which will produce an undesirable discontinuity in the display. Of the panels considered above, the plasma display appears to offer the best chance for fabrication in a size large enough to present a usable pictorial display. It has been estimated by a manufacturer of plasma displays that in several years a 10×10 panel will be available.

Most of the projection displays have been developed for large-screen applications, for viewing by a group of observers. The associated optics for magnification of the image onto the screen is usually heavy and relatively inefficient. A high-powered CRT system is required to generate the image. For these reasons it is improbable that a device employing projection could be used for this application.

There has been a determined effort in recent years to eliminate the use of meters and gauges for flight instrumentation. People seem to be in general agreement that there is a better way to accomplish the display function by electronic means and thereby eliminate the clutter, weight, and power requirements of these devices.

Advantages of CRT Displays. The direct view cathode-ray tube is the most versatile display device in use today, and although much effort has been directed toward development of devices to replace the CRT, it is expected that it will be just as popular in 1973 as it is today. A vast amount of technology has been developed over the years in the design of CRT display systems. The tube itself can be made rugged and reliable, and the driving circuitry can be made compact with low power requirements. In addition, the CRT display has an attractive performance/cost ratio. For many spacecraft applications the physical size and bulk of a CRT may preclude its use, but in the present application this is likely to be a secondary consideration.

Summary of Display Device Characteristics. Pertinent characteristics of various display devices that may be considered candidates for this application have been gathered from various sources listed in the bibliography. Plasma and LED flat panels are included in the event that research continues to look promising. These characteristics are summarized in Table 2-1. The criteria chosen for determination of power and weight is that necessary for a 1000-character display of alphanumerics and/or a

Table 2-1. Characteristics of Various Display Types

Display Type	Mode	Brightness (foot lamberts)	Resolution (line/in)	Weight (lb)	Average Power (watts)	Reliability	% Prob. Avail. in 1972
Plasma Panel	TV	300	50	30	100	Unk.	60
	Random	500	50	25	55		75
	Alpha-Num	500	50	25	55		75
Light Emitting Diode Panel	TV	200	40	50	1500	High	40
	Random	200	40	40	750		
	Alpha-Num	200	40	35	500		
Cathode-Ray Tube	TV	200	100	15	25	High	100
	Random	50	100	70	320		100
	Alpha-Num	100	100	70	320		100
CHARACTRON ^R Tube	Alpha-Num	1000	200	75	350	High	100
Storage CRT	TV	2000	40	75	400	Medium	100
	Random	2000	40	75	350		100
	Alpha-Num	2000	40	75	350		100

2-12

pictorial or analog display with 500 resolvable elements per dimension. In addition, these values include the required control logic, data buffer, and power supplies necessary to drive the equipment. All data are calculated for a single display surface.

2.2.5 DISPLAY SYSTEM CONCEPTS

A block diagram for a typical display system is shown in Figure 2-2. It is assumed that the devices at the top of the diagram are located remote from the display system and serve as inputs and signal generators to the system. Three types of displays are provided.

2.2.5.1 Radar and Remote TV Camera Displays. For presentation of pictorial information from the radar (after scan-conversion) or remote television cameras, relatively unsophisticated television monitors using a CRT are used. It is visualized that a 7-inch rectangular tube would be adequate for this function. Two monitors are provided for redundancy, and if necessary, they can be made as pluggable units, so that in the event of failure the defective unit could be replaced by a standby unit. A switching selector is provided so that any of the pictorial information can be placed on either display surface. If necessary the selector may be under computer control.

2.2.5.2 Alphanumeric and Analog Displays. Two multiformat computer-driven displays are provided for alphanumeric and analog presentations. These are the main displays of the system, and again two are provided for redundancy. If a CRT is used for this display, additional reliability can be incorporated by the use of redundant electron guns in each CRT. It is assumed that a buffer for the display will be required to reduce the load on the computer. Because of their multiformat capability, these displays may also be used as a backup to the pictorial displays if necessary. If a storage CRT is chosen for these displays, then of course the buffer will be unnecessary.

2.2.5.3 Indicator Displays. A third type of display under computer control is a group called indicators. These may be visualized as light emitting diodes acting as pilot lamps to indicate the status of a particular system or subsystem. Each indicator consists of two different colors, red and amber, so that a color change would indicate a change in the system being monitored. Additional diodes of each color may be added to the indicator for redundancy. Further changes in status could be achieved by causing the diode to blink and/or by controlling its brightness. Other uses for indicators would be numerical readout devices to display certain functions that must be monitored continuously; for example, time elapsed from the start of the mission. If light emitting diodes are used for this function, a buffer would be required.

2.2.5.4 Power and Weight Estimates. Table 2-2 is an estimate of the power and weight requirements for each of the display devices tabulated in Table 2-1, according to the block diagram of Figure 2-2. Because the values in Table 2-1 include a prorated share of the logic circuits and power supplies, the data do not correspond directly with

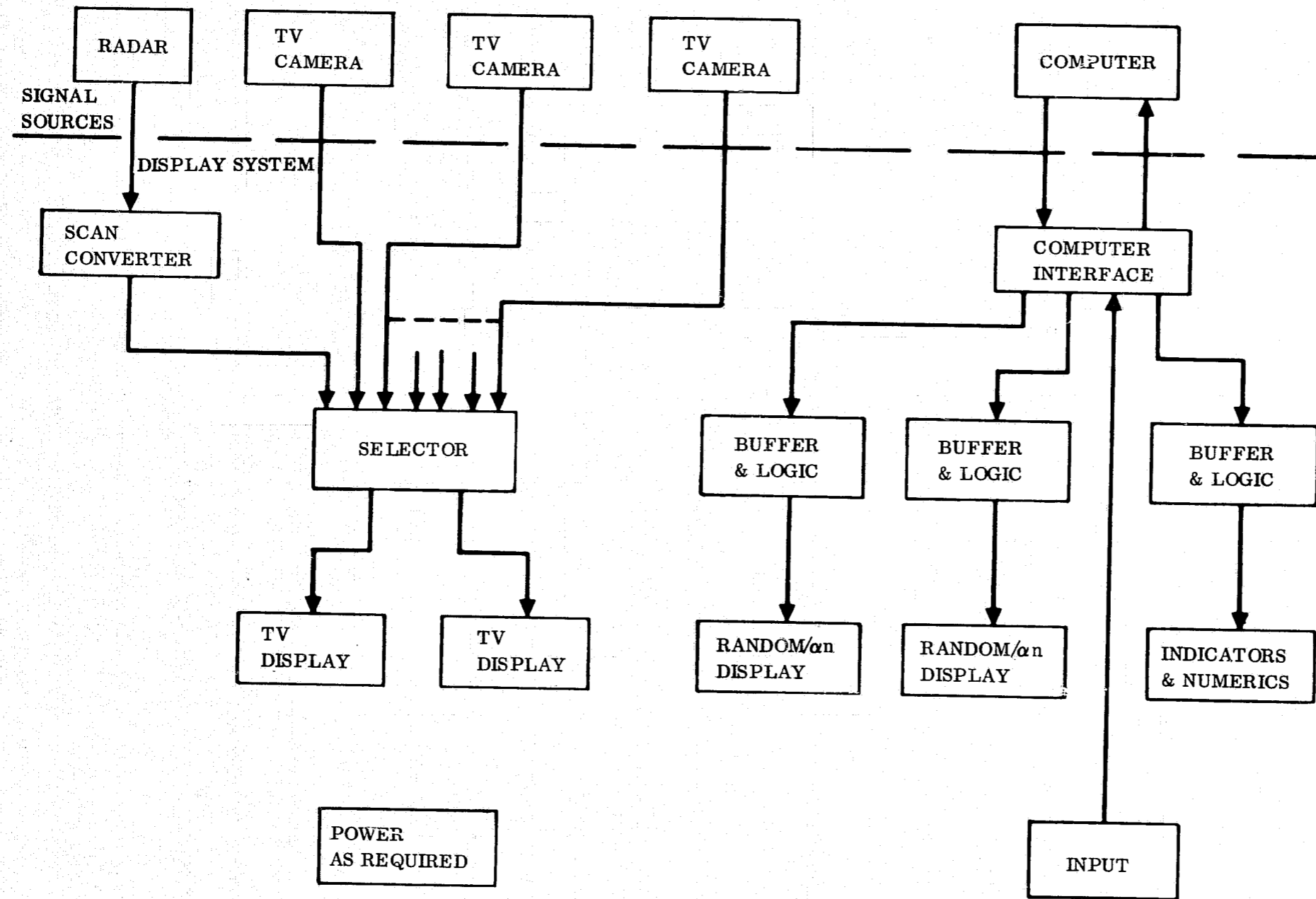


Figure 2-2. Display System Concept Block Diagram

Table 2-2. Power and Weight Estimates for Various Display Types

Item	Quantity	Plasma Panel		LED Panel		CRT		Storage CRT	
		Power (watts)	Weight (lb)	Power (watts)	Weight (lb)	Power (watts)	Weight (lb)	Power (watts)	Weight (lb)
TV	2	150	50	1200	65	50	25	650	120
Random/alpha- numerics	2	60	40	400	50	400	120	550	120
Buffer & logic	2	40	30	300	60	200	50	50	25
Interface	1	60	10	60	10	60	10	60	10
TV selector	1	—	2	—	2	—	2	—	2
Scan converter	1	150	30	150	30	150	30	150	30
Indicators & buffer	50	60	1	60	1	60	1	60	1
Input keys	50	5	5	5	5	5	5	5	5
Power supply	1	230	35	550	65	230	35	500	60
TOTALS		755	203	2725	288	1155	278	2025	373

2-15

the individual values of Table 2-1; however, the totals are approximately the same. The power supply is assumed to have an efficiency of 80%. The data indicate that plasma panels and CRT's consume the least power, with the former having a weight advantage. However, there is no certainty today that plasma panels will be sufficiently developed for the 1972 hardware phase. If they are available, it is interesting to calculate an optimum configuration using plasma panels for the random and alphanumeric displays, and CRT's for the TV displays. These data are shown in Table 2-3. However, the technology available today and in the near future indicates that CRT's are the safest selection today for these display requirements.

2.2.6 CONTROLS

A significant problem in display technology has been the interaction of man with his computers. The interaction requirements are further expanded when the computer is used for multiple purposes as is the case for the space shuttle.

2.2.6.1 Reprogrammable Switch Functions. Dedicating a separate switch to every function overcrowds panels, causes operator difficulties, and seems otherwise wasteful. It is more effective to perform the multitude of switch functions with a small number of switches. To make this possible, each switch must be reprogrammable to perform several functions; and, more importantly, all the choices that the pilot might wish to make at any one time must be available to him.

Implicit in this concept is that, at any one moment, the pilot's actions are by nature limited to a relatively small number of options, even when he performs complicated tasks. Complicated tasks usually are separated into a sequence of simpler steps. Real help would be in the form of cues that inform the pilot of his options.

Several solutions to reducing the number of switches use this concept. In each, the switch function is changed by having the switch interact with the computer. Switch closures are coded inputs to the computer. When an operator depresses one of the switches, a coded pulse is transmitted to the computer. The computer identifies the switch position, transmits a control signal, then reprograms the switch functions.

Display on Face of Pushbutton. The pilot must know what functions the switch will perform. This becomes convenient for him if the label on, or directly next to, the switch changes corresponding with the changing switch function. Figure 2-3a shows an example of pushbuttons with their programmable functions displayed directly on the button faces. This method uses a film slide that contains many individual messages with a bulb or optics behind each message. The switch legend is changed by activating the appropriate bulb, or moving the optics, or both. The message is projected onto a screen on the front portion of each switch. Reprogrammable function switches using the projection filmed message are currently being used with 24 and 48 individual messages per switch.

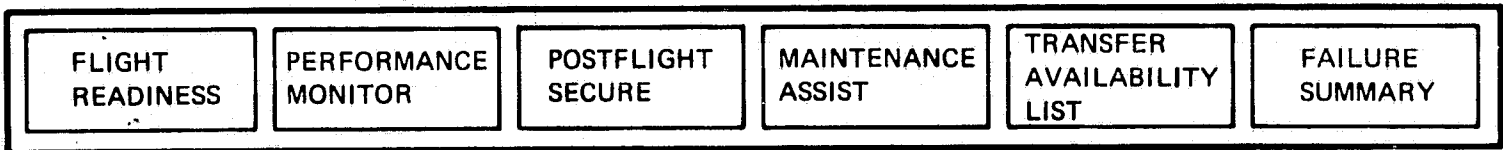
Table 2-3. Optimum Configuration for Minimum Power and Weight Estimates

Item	Quantity	Device	Power (watts)	Weight (lb)
TV	2	CRT	50	25
Random/alphanumerics	2	Plasma Panel	60	40
Buffers and logic	2		40	30
Interface	1		60	10
TV selector	1		—	2
Scan converter	1		150	30
Indicators and buffer	50		60	1
Input keys	50		5	5
Power supply	1		165	30
Totals			590	173

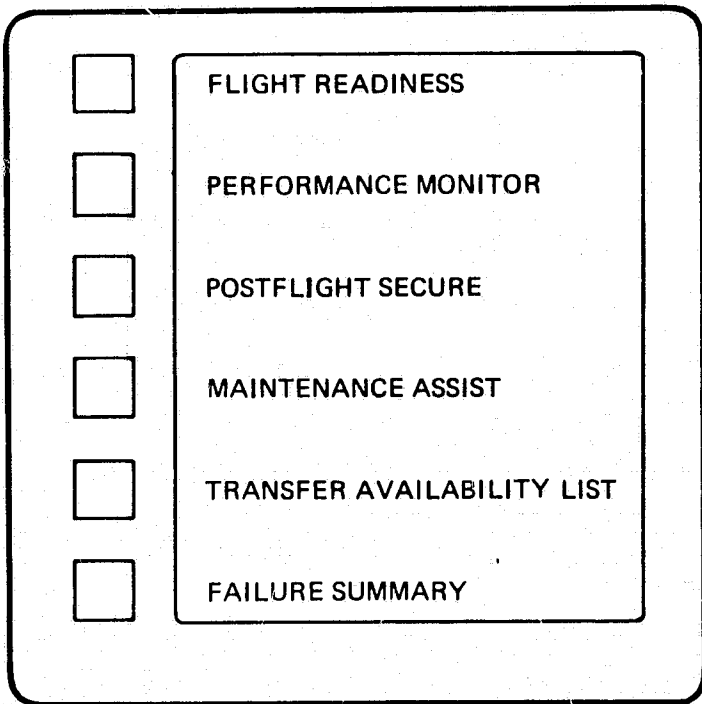
Display Next to Pushbutton. Figure 2-3b shows a second and highly flexible display method. The display is immediately next to the pushbuttons. Each message is close enough to its corresponding pushbutton that the face of the button can be left blank. The display medium can be cathode ray, plasma, or any other totally reprogrammable type. The quantity of messages is not limited as in the first method.

Keyboard Concept. Functionally less convenient for rapid response actions is the keyboard technique shown in Figure 2-3c, which identifies the changed switch function on a display near the pushbutton. The pushbutton has a fixed legend on its face, usually an alphanumeric or symbolic code. The nearby programmable display, such as a CRT, plasma, or some other digital device, shows the switch legend with the switch function spelled out next to it.

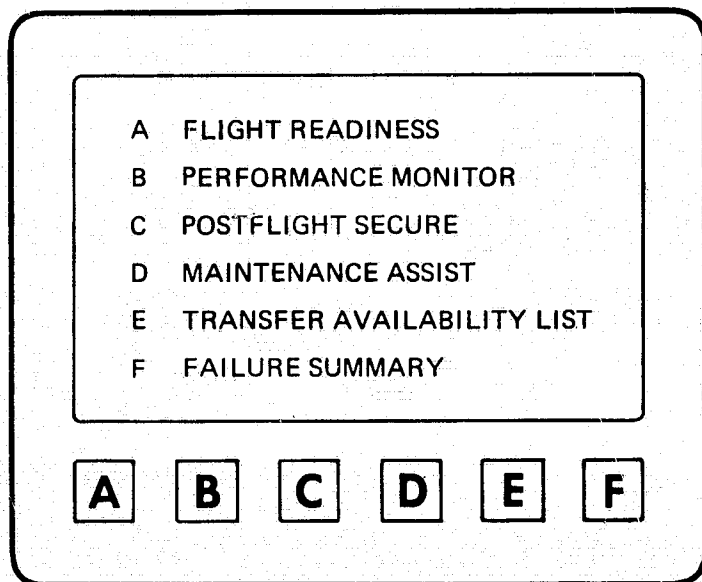
2.2.6.2 Final Concept. The control and display subsystem for space shuttle will probably include one or two of the methods shown in Figure 2-3 and conceivably could be a combination of all three.



(a)



(b)



(c)

Figure 2-3. Computer-Controlled Display Concepts

2.3 ONBOARD COMPUTERS AND SOFTWARE

2.3.1 INTRODUCTION. The onboard computers and associated software represent the focal point of electronics integration. The design and implementation of the computers and their software are significant engineering problems, which are becoming increasingly important.

Since there are many ways to use and design computer systems, it is important to investigate the advantages and disadvantages of various implementation schemes. The first discussion in this section identifies the characteristics of two possible basic approaches and lists their strengths and weaknesses. This overview of arguments does not lead to a quantitative decision applicable to any particular case. It was therefore necessary to take a similar but specific avionics system and develop a comparative analysis. This was done for two of the most likely basic computer configurations, (a) an integrated multiprocessor and (b) a federated computer system. The results of the comparative analysis indicated the general direction for the design to proceed. It is emphasized that the computer system can, and probably will, be a compromise between the integrated multiprocessor and the federated computer system. The trend is toward the integrated multiprocessor, and deviations from this trend will require definitive justification.

With this as a general guideline, the characteristics and sizing variations of the computer systems for the booster and orbiter stages were developed, Section 2.3.4.

A preliminary estimate of the weight, volume, and power for the computer and its peripherals is presented in Section 2.3.5.

The last section (2.3.6) presents the top overview of the software domain. Included are the preliminary estimates for booster and orbiter software.

2.3.2 GENERAL ARGUMENTS: MULTIPROCESSOR AND FEDERATED COMPUTERS.

Federated systems use several central processing units (CPU), each with its own memory and input/output (I/O) channels dedicated to a particular processing task. Each of the federated elements can be made to provide backup for other federated elements in the over-all system.

A multiprocessor also has more than one CPU, but it is organized with memory and I/O channels common to all CPU's. The multiprocessor system is multitask oriented and is therefore multiprogrammed.

The arguments presented in Table 2-4 are constrained to a real-time application that has an operational goal of "fail operational - fail operational - fail safe." This implies three successive failures to abort the intended mission operation while maintaining safety of flight.

Table 2-4. General Arguments Relative to Multiprocessor and Federated Computer Configurations

Characteristics	Multiprocessor Computer		Federated Computer	
	For	Against	For	Against
<u>Hardware</u>				
Reliability	Good for successive failures and degraded modes	Special vulnerability (in one location)	Low vulnerability (spacially dispersed)	For equal reliability requires more hardware
Maintainability	Excellent			May be difficult due to subsystem location
Efficiency	Low size weight, power, cost	Moderate memory interference	Low memory interference	Large size, weight, power and cost penalties
Flexibility and growth	Excellent			Poor
Integration/interfaces	Moderate - minimum interference			Difficult - many interfaces. Sequence dependent
<u>Software</u>				
Executive program	Generalized and consolidated for centralized control and conflict resolution	More complexity	Less complexity	Specialized and dispersed, requiring a higher authority for conflict resolution
Applications programs	Easiest to control consistent standard interface.	Less autonomy	More autonomy	Typically varying interface requirements
Flexibility-growth	Excellent			Very poor
Efficiency	Maximum - low overhead in memory and timing loads. Little duplication	Moderate memory interference	Low memory interference	Minimum - high overhead penalties in memory and timing loads. High duplication
Maintenance	Very good because of standardization			Typically poor because of minimum standardization
Simulation (system)	Straightforward - dependent upon executive and data bus			Complex - requires multiple executive asynchronous interaction

2-20

Volume VII

Table 2-4. General Arguments Relative to Multiprocessor and Federated Computer Configurations, Contd

Characteristics	Multiprocessor Computer		Federated Computer	
	For	Against	For	Against
Emulation (software)	Moderate complexity	Can be quite large unless multiple emulation modes exist	Moderate complexity. Always constrained in size	Timing interactions from other computers must be generalized
Integration	Moderate complexity	Requires excellent software systems management	Low complexity. Requires average software systems management	
Languages	Compiler base language. Applications language based on compiler	Slightly greater inefficiencies in execution time and memory required	Applications dependent compilers. Slightly greater efficiency in execution time and memory requirements	
Degraded modes	Powerful - requires minimal intercommunication. Minimal time to change modes			Difficult - requires complex intercommunication. Moderate time to change modes

2.3.3 COMPARATIVE ANALYSIS: MULTIPROCESSOR VS FEDERATED COMPUTERS. Insufficient data are presently available for space shuttle to perform an in depth tradeoff analysis of multiprocessor and federated computer systems. The nature of the problem dictated that a tradeoff study be conducted on an avionics system of comparable complexity to that envisioned for space shuttle. The system selected and considered quite similar to space shuttle's requirements was the Navy's S-3A avionics system. This is a carrier-based antisubmarine hunter-killer vehicle using a highly automated computer-centered avionics system. General-purpose displays and controls are used for the man-machine interface. Extensive self test and graceful degradation as a result of equipment failures were also requirements of the S-3A avionics system. Because of the many similarities, this system was deemed representative of the space shuttle electronics system and quite adequate for the comparative analysis of multiprocessor versus federated computer systems.

The avionics computer system implementation for the Navy's S-3A program evolved through tradeoff studies into a combination of dedicated special-purpose computers and a general-purpose multiprocessor. Many factors contributed to this mixed implementation.

The purpose of this discussion is to assess the effects on volume, weight and power as if the S-3A avionics implementation had been constrained to a federated computer system concept.

By way of definition, a federated computer system consists of a number of central processors, each having dedicated memory and input/output capability. The multiprocessor also has many central processors, but the memory modules and input/output channels are shared by the central processors.

2.3.3.1 Technical Approach. To conduct the comparative analysis, realistic ground rules and constraints were imposed. Common hardware modules were used to implement the individual federated computers. The number of potential backups for a specific processor was varied from two to four. Time loading, memory loading and input/output loading per processing function were extracted from the available S-3A software analysis.

The technical approach proceeded through the following steps:

1. Identify the computer hardware modules and their parameters for implementation of the federated computer system.
2. Determine the software overhead functions and their parameters required to implement any processor in the federated system.
3. Allocate the software functions of the S-3A multiprocessor to dedicated federated computers.

4. Determine the maximum percentage time loading for each of the federated computers.
5. Determine the maximum memory loading for each of the federated computers.
6. Analyze the degraded modes for complete failure of one, two and three federated computers and allocate additional hardware modules to allow for graceful degradation and future growth.
7. Compute volume, weight, and power for the federated computer system.
8. Compare the federated to the multiprocessor parameters.

STEP 1. Identify computer hardware modules which may be used as building blocks in either a federated or in multiprocessor system.

Modules	Volume (ft ³)	Weight (lb)	Power (watts)
Central processing unit	0.85	47.3	304
Memory storage unit (16 k)	0.95	44.2	79/175*
Input/output	0.61	32.3	160
Control panels	1.22	74.9	120

*Standby and operational power requirements

Additional weights for each processor are volume dependent
(Examples: Racks, cabling, connectors, vibration isolators, etc.)

STEP 2. Determine software overhead functions and their parameters required to implement any processor in the federated system.

Function	Main Store (words)	Execution Time (sec)
Inflight readiness test support	1,100	
CPU test (2)	2,000	0.590
MSU test (6)	500	9.000
I/O test (2)	500	0.010
	4,100	9.6
	(4K words)	(8.5%)

STEP 3. Allocate the software functions of the S-3A multiprocessor to the federated computers.

Processor	Function
C-1	Navigation
C-2	Communication
C-3	Acoustics
C-4	Nonacoustics and stores management
C-5	Control and display

STEP 4. Determine the maximum percentage time loading for each of the federated computers.

Processor	Maximum Time Loading (percent)	Maximum Core Loading (K words)
C-1 NAV	31.5	21.7
C-2 COMM	23.5	10.0
C-3 Acoustics	63.7	68.0
C-4 Nonacoustic and Stores	12.5	10.2
C-5 Control and Display	33.5	17.0

STEP 5. Determine maximum core loading for each of the federated computers. (Place data in 3rd column of Step 4.)

STEP 6. Analyze degraded modes for one, two, and three failures of the federated computers and allocate additional hardware modules to allow for graceful degradation and future growth.

Processor	Time Loading (T_L)*	Possible Backups					No. of Possible Backups
		C-1	C-2	C-3	C-4	C-5	
C-1	31.5	—	** Yes	No	** Yes	** Yes	3 vs 3 required
C-2	23.5	** Yes	—	—	** Yes	** Yes	3 vs 3 required
C-3	63.7	No	No	—	** Yes	** No	1 vs 2 required
C-4	12.5	Yes	** Yes	Yes	—	** Yes	4 vs 2 required
C-5	33.5	** Yes	Yes	No	** Yes	—	3 vs 2 required

*If ($\% T_L > 80\%$) the resultant answer was No.

**Indicates selected backups for degraded mode capability.

C-3 processor has only one potential backup. C-4 processor has four potential backups. The other processors each have three potential backups. Processors C-1 and C-2 (navigation and communication) are required for safety of flight. (The S-3A was required to be flyable manually, without benefit of electronic display and controls.)

Each nonsafety-related processor requires two potential backups to satisfy (a) first failure-operational, (b) second failure-operational and (c) third failure — safety of flight. In order to meet the safety requirement, the safety-related processors C-1 and C-2 need three backups each.

To satisfy the degraded mode criteria "fail-operational, fail operational, fail safe" all three potential backups for C-2 and C-3 must be implemented. C-3 requires an additional backup. At least two of the potential backups for C-4 and C-5 need to be implemented.

The double asterisks in the previous time-loading table indicate the selected backup to meet the degraded mode criteria. The selection of the obvious choices for C-1 and C-2 strongly conditions the selection for backing up the remaining processors. The backup selection for C-3 was determined to be an augmented C-5, because it would add an additional CPU to this heavily used backup.

This gives the following requirements:

Processor	I/O	CPU	Control Panel	Memory (K words)*	100% Growth (K words)	MSU (16K each)
C-1	4	1	1	21.7 + 17.0 = 38.7	77.4	5
C-2	4	1	1	10.0 + 21.7 = 31.7	63.4	4
C-3	4	1	1	68.0 + 17.0 = 85.0	170.0	11
C-4	4	1	1	10.2 + 68.0 = 78.2	156.4	10
C-5	<u>5</u>	<u>2</u>	<u>2</u>	17.0 + 68.0 = 85.0	160.0	<u>10</u>
Totals	21	6	6			40

*Summation of initial memory requirement plus largest memory requirement of selected backup modes.

STEP 7. Compute volume, weight, and power for the federated computer system.

VOLUME

Modules	Quantity Required	Subtotals (ft ³)
1. Central Processing Unit (0.85 ft ³)	6	5.10
2. Memory Storage Units (0.95 ft ³)	40	38.00

VOLUME (CONT.)

Modules	Quantity Required	Subtotals (ft ³)
3. Input-Outputs (0.61 ft ³)	21	12.81
4. Control Panels (1.22 ft ³)	6	7.32
	Total Volume	63.23

WEIGHT

Modules	Quantity Required	Subtotals (lb)
1. Central Process. Unit (47.3 lb)	6	283.8
2. Memory Storage Unit (44.2 lb)	40	1,768.0
3. Input-Outputs (32.3 lb)	21	678.3
4. Control Panels (74.9 lb)	6	449.4
	Total Weight	3,179.5

POWER

Modules	Quantity Required	Power Subtotals (watts)
1. Central Process. Unit (304 watts)	6	1824
2. Memory Storage Unit (79/175 watts*)	40	4312
3. Input/Output (160 watts)	21	3360
4. Control Panels (120 watts)	6	720
	Total Power	10,216

*Standby and operational power requirements assuming that on the average two MSU's were operational per CPU (Total 12), and the remaining 28 were in standby.

STEP 8. Compare the federated to the multiprocessor parameters.†

	Multiprocessor*	Federated
1. Volume	28.36	63.23 (ft ³)
2. Weight	1454.4	3,179.5 (lb)
3. Power	5008.0	10,216.0 (watts)

*The multiprocessor has 4 CPU's, 16 MSU's and 8 I/O channels

2.3.3.2 Conclusion. In this comparative analysis between the multiprocessor and the federated computer systems concepts, it seems that the multiprocessor holds a 2-to-1 advantage in desirability over the federated approach.

The multiprocessor advantage in the weight and cost analysis is further increased by considering the electrical power and environmental control system penalties. For example: the weight requirement for an additional 5 kilowatts for 7 days in orbit would require approximately 4,000 pounds of additional liftoff weight.

The advantages of the multiprocessor are:

- a. More design flexibility.
- b. Better capability to handle degraded modes.
- c. Better growth flexibility.
- d. Higher reliability.
- e. Lower weight.
- f. Lower volume.
- g. Lower life cycle cost.

2.3.3.3 Recommendations. In recommending a multiprogrammed integrated multiprocessor, it is recognized that some attempts to implement multiprocessors have been less than unqualified successes. On the other hand, others have been successfully implemented with a reasonable amount of effort. It is important to understand the reasons for these differences.

Those who have been successful in implementing a multiprocessor such as computer time-share operations, the Navy's VS A-NEW aircraft avionics program, and the Air Force's manned orbital laboratory project, have provided adequate amounts of simulation and testing, and have established carefully worked-out software development ground rules prior to implementation.

† Data based on S3A analyses with space shuttle ground rules, not to be interpreted as space shuttle volume, weight, and power estimates.

Those who have had difficulties in implementation commonly were found deficient in simulation, verification, and in setting software ground rules.

Since on other programs the goal has been achieved, it is recommended that the space shuttle program take advantage of the benefits of an integrated multiprocessor computer and ensure success of the effort by taking the necessary developmental steps.

2.3.4 DEFINITION AND SCOPE OF COMPUTER HARDWARE. Primary considerations are physical and functional characteristics. Physical characteristics are volume, weight, and power. Functional characteristics are those other hardware features that result from the space shuttle design characteristics and the operational and maintenance concepts as defined by NASA.

Preliminary tradeoffs considering a multiprocessor computer versus a federated system of computers indicate the likely desirability of a multiprocessor computer. Although this is a general guideline, the multiprocessor approach cannot be considered a universal panacea.

Exceptions to the integrated multiprocessor typically encountered are unintentional, personal, or political preference; subsystem autonomy requirements; high data load; or higher speed special processing tasks. The latter two are technically rational, justifiable by tradeoff study results. Subsystem autonomy may be justifiable when either (a) sensitive security processing is encountered, or (b) the subsystem is totally autonomous because it is a fixed invariant element attached to the vehicle, while other processing functions are highly variant loads not required for all intended uses of the vehicle. This could allow more efficient payload adaptability to varying missions.

2.3.4.1 Computer Concepts. Three computer concepts were initially considered. Two were federated and the third an integrated multiprocessor. The two federated concepts were:

- a. Dedicated computers for primary tasks having the capacity to backup other dedicated computers.
- b. Dedicated computers having sufficient self-contained redundancy to act as their own backup.

The second federated concept with its self-contained redundancy was not evaluated in the comparative analysis because of the following reasons:

- a. Each of the multiredundant computers would end up being a multiprocessor.
- b. A federated system of multiprocessors would require much more volume, weight, and power than either of the other two concepts. It tends to have the disadvantages of both without their advantages.

2.3.4.2 Comparative Analysis Results. The results of the comparative analysis of an aircraft avionics system similar to space shuttle indicated that for the space shuttle, the federated approach would require a computer with net volume, weight, and power approximately double those of one equivalent to the integrated multiprocessor system.

Power and Weight Requirements. For the space shuttle the gross penalty of the federated system is actually considerably more than this factor of two. This is caused by the increased power requirement propagating to (a) a substantial increase in fixed and expendable fuel-cell weight requirements for in-orbit, which in turn requires (b) a substantial increase in the environmental control system capacity. An estimated gross penalty for the federated system is four times the weight of an integrated multiprocessor for the orbiter, and two times the weight for the booster.

Maintenance. Another consideration was the requirement of maintenance of the computer(s). Assume that federated computers are dispersed throughout the vehicle. Thus repair activity must also be dispersed. Environmental control would have to be extended to these areas to allow shirtsleeve maintenance. The rocket engine computers seem to be a good example. To avoid these penalties it seems desirable to have the computer(s) located in a centralized area for maintenance.

Backup Communication. Each of the federated computers requires communication to nearly all other federated computers to allow for backup capability. Two methods of backup take-over are possible. The first is to have the allocated backup unit receive periodically the significant parameters from the prime unit to allow the backup to take over without loss of continuity. The remaining alternative is to accept the continuity loss to minimize the periodic status and parameter update. The prospect of continuity losses and potentially difficult recovery procedures seems quite undesirable. Data, information, and control parameters are also necessary in intercomputer communication to coordinate their common purpose of safely conducting and fulfilling the mission objectives.

Intercommunication. Communication between the computer and its subsystem elements is also required. The number of data buses from a centrally located federated computer system is much greater than the number required from an integrated multiprocessor. Each federated computer must be connected not only to its own subsystem elements, but also to all those other elements for which it is to serve as a backup computer.

Reduction of the quantity of intercomputer communication and the number of data busses from computers to subsystem elements appears to be a desirable goal. Since (a) the computers are centrally located for ease of maintenance and minimization of environmental control penalties, and (b) a design goal is to avoid interruption of processing due to the loss of a computer, a solution that circumvents these problems and penalties would be to allow each computer to communicate directly to the memories of all other computers. This solves (a) intercomputer communication problems, (2) the abundance of data buses connecting computers to subsystem elements for backup operation, and (c) the loss of data and processing due to an intermittent or hard failure.

Processor Alternatives. With memory in common and centralized location, the processors must be analyzed with respect to their capability and application. Table 2-5 shows the alternative processor combinations that can be considered. Capabilities can be the same or different, and the application can be dedicated or nondedicated.

Table 2-5. Processor Combinations

Alternative	Capabilities	Applications	Remarks
1	Different	Dedicated	Possible
2	Different	Nondedicated	Quite improbable
3	Same	Dedicated	Possible
4*	Same	Nondedicated	Possible

*Best over-all choice.

Alternative 1 uses central processors with different capabilities, each dedicated to specific processing tasks. Although this is feasible, it does not satisfy the failure mode criteria of "fail operational, fail operational, fail safe."

Alternative 2 uses central processors that have different capabilities, with each processor nondedicated or supposedly capable of doing any of the processing tasks. This is illogical.

Alternative 3 uses identical processors capable of doing any processing task, but the processing tasks are allocated to specific processors. Although this is a feasible solution, it restricts the effective use of the potential processing power.

The fourth alternative represents a general solution in which all processors have the same capability, and processing tasks can be performed by any of the processors. This alternative is best for growth, flexibility, and processing efficiency; and it readily satisfies the failure-mode criteria.

Instruction Repertoire. If the processors have like capability, this implies that the instruction repertoires are identical and should be flexible to accommodate new (growth) requirements. This, in turn, implies that the instruction set be implemented with read-only storage (ROS). This method of implementation allows for both standard instructions and special applications of dependent macros. Used as a control element, it eliminates the need for complex instruction decoders and sequencing networks.

The instruction set should be capable of floating point, fixed point, logical, branching, status switching, and I/O. Floating point should have single and double precision capabilities. ROS cycle time should be approximately 200 nanoseconds.

Failure Mode and Growth Requirements. At least four processors are required to satisfy the failure mode criteria and growth requirements. Main computer memory should be organized by four, nine-bit bytes per word. Parity shall be included per byte. Main memory should be organized into sixteen thousand-word modules. Memory protect codes are desired for each 512-word segment. Access time should be approximately one microsecond. A minimum of four memory modules are required with an upper limit of sixteen. Memory modules should have 8 to 16 input-output ports to accommodate at least four central processors and 4 to 12 I/O channels. The high number of ports significantly reduces the memory timing interference between I/O's and processors.

I/O Modes. Input/output channels should be capable of both burst and multiplex modes of operation. Channels should operate with stored programs modifiable by the processors under executive program control. Word size and parity should be common with memory requirements. Crossover capability is required between I/O channels to accommodate the failure-mode criteria.

System Clock. A multiple redundant time-code generator should be part of the digital computer. The computer requires a real-time clock plus a number of internal timers. Analog raw data recording, including voice, will require an IRIG-B timing clock, which should be incorporated into the over-all time code generator within the computer.

Data Storage. Magnetic drums and tapes are required for program and data storage to accommodate system initialization, recovery modes, roll-in and overlay executive philosophy, and mission history recording. Both digital and analog tapes are required. Analog tapes are primarily for voice, possible sensor data, and test signal stimuli.

2.3.5 COMPUTER SYSTEM ESTIMATES. Preliminary estimated weight, volume, and power for the computer system with its peripherals is given in Table 2-6 for the orbiter and booster vehicles respectively.

2.3.6 DEFINITION AND SCOPE OF COMPUTER SOFTWARE. The computer software for space shuttle deserves technical and management attention comparable to that given the electronics hardware. Although software does not have easily recognized characteristics of weight and volume, it is nevertheless just as much an integral part of the system as any piece of hardware. Each piece of hardware is required to carry out certain system functions and must be designed to accomplish this. In like manner, each item of software is required to carry out certain system functions and must be designed to accomplish them. The software in a computer-oriented system is analogous to the wiring in an electronics system. The system does not exist as a system without it, and its design is an integral part of the system design. In both instances (software and electronics wiring), the appearance of the end result to the uninitiated is one of tremendous and somewhat mysterious complexity. In each case, however, the complexity consists simply of a very large number of essentially simple elements designed

Table 2-6. Computer System Estimates

Modules	Qty	Orbiter			Qty	Booster		
		Weight (lb)	Volume (ft ³)	Power (watts)		Weight (lb)	Volume (ft ³)	Power (watts)
1. Central process units	4	20	0.4	120	4	20	0.4	120
2. Memory storage units	16	352	8.0	740	8	176	4.0	370
3. Input/output	12	39	0.7	200	8	26	0.5	134
4. Control panels	1	60	1.3	200	1	60	1.3	200
5. Drums	4	280	6.0	160	4	280	6.0	160
6. Digital tape	4	120	1.5	80	4	120	1.5	80
7. Analog tape	4	200	8.0	160	4	200	8.0	160
Totals:		1071	25.9	1660		882	21.7	1224

Note: Computer estimates were derived using Table 2-8 (Program and Data Estimates for Booster and Orbiter Vehicles) in conjunction with 1972 hardware projection and do not include a growth factor. The growth factor should be in the order of 4 to 10 times memory capacity.

to work together to produce the desired result. Software must be defined, designed, developed, and tested in a systematic manner that will ensure the proper operation of the over-all system.

2.3.6.1 Software Categories. The software task starts with mission analysis. Functional requirements defined by mission analysis are subjected to tradeoff studies, where applicable, to decide upon the method of implementation. Implementation of functions can be by hardware alone or in conjunction with software. The failure-mode criteria for hardware is equally applicable to software.

The software for space shuttle can be defined in three broad categories:

- a. Onboard software.
- b. Developmental support software.
- c. Operational support software.

The onboard software consists of an executive program, applications programs, and checkout test procedures and systems monitoring program.

Developmental support software includes software languages; software assemblers, compilers, and emulators; system simulators; software and hardware testing and integration; and software for flight test and evaluation.

Operational support software is comprised of premission initialization; possible surface monitoring of inflight operations in rare critical situations; update to the vehicle of data it requires and could not otherwise acquire; postflight analysis, evaluation, records, and reporting; software maintenance and modifications for special mission requirements; and software for training simulators.

The basic software should have a higher level basic language foundation with possibly two special applications languages built upon that foundation. The special applications languages would be for checkout and possibly navigation. The higher order language foundation should be machine independent. The inefficiency of the higher-order language foundation should not exceed 15% in time loading and core loading when compared to equivalent assembly coding.

2.3.6.2 Software Design Characteristics. Software commonality should be maintained across the over-all scope of the space shuttle program to maximize meaningful communication and to reduce cost and calendar time expenditures.

The software design philosophy should have the following characteristics:

- a. Modular organization including modular name common.
- b. Use relocatable subroutines in fixed segments.
- c. Use reenterable subroutines.

Schedule. The software schedule is quite important. Particular early emphasis is anticipated in the following ordered software areas because of the persistent calendar time problem.

- a. Display format and control testing.
- b. Master executive.
- c. Language definition.
- d. System simulation.
- e. Compiler and emulator development.
- f. Software specifications.
- g. Off-line verification of hardware checkout test procedures.
- h. Software integration and testing.
- i. Hardware/software integration and testing.

Design Objectives. The software higher level language, commonality, and machine independence for the development and operational phases seem to be highly desirable software objectives.

Some of the autonomous processing functions that must be investigated are those required to contend with space junk, solar flare, terminal weather, political and defense constraints, biomedical monitoring, and onboard request for surface assistance due to apparent unresolvable onboard systems problems.

2.3.6.3 Program and Data Requirements Estimate. Program and data requirements for the booster and orbiter vehicle computers were estimated. These estimates are preliminary and have a confidence approximation of 60%. This includes processing functions that have not yet been identified.

The estimating approach was to identify two sets of processing functions: those unique to the orbiter vehicle (Table 2-7) and those common to the booster and the orbiter (Table 2-8). Estimates were compiled from knowledgeable personnel having at least 5 years, and up to 15 years experience in the applicable processing technology areas of concern. Estimators indicated that estimates were intentionally set high to conform with a conservative minimum risk approach.

Orbiter Estimates. These estimates are given in Table 2-7.

Relative to use requirements it appears that all single processing tasks for a particular mission phase are mutually exclusive.

Estimates Common to Orbiter and Booster. (See Table 2-8.)

Table 2-9 shows the estimated loads for each combined processing booster and orbiter vehicle.

It is felt that the time loading requirements could easily be satisfied using the quadruple multiprocessors dictated by the NASA operational requirement and the previous computer configuration comparative analysis.

Table 2-7. Program and Data Estimates for Processing Functions
 UNIQUE to the Orbiting Vehicle (must be added to the
 Booster Processing Requirements)

Functions	Program (K words)	Data (K words)	Use†
1. Rendezvous and docking	5.0	1.0	S
2. Processing horizon scanners	0.5	0.1	C & P
3. Mission scheduling*	100/50‡	10.0	P
4. Satellite servicing**	10.0	2.0	S
5. Weight and balance	2.0	2.0	P
6. Reentry	10.0	5.0	S
7. Landing site update	2.0	5.0	P
8. Orbital displays	4.0	32.0	C & P
9. Orbital communications	5.0	10.0	C & P
10. Orbital navigation	5.0	10.0	P
11. Checkout	5.0	20.0	C & P
Totals	148.5/73.5	69.1/61.1	

*Mission scheduling includes: maneuver planning, resources budgeting, target ephemeris, etc.

**Satellite servicing includes: deployment, retrieval, checkout, repair, and replenishment.

†Use: P-Periodic, C-Continuous, S-Single executions within particular mission phases.

‡A/B symbolizes: A-Total program words and B-Program word used at any one time.

Table 2-8. Program and Data Estimates for Processing Functions
COMMON to the Booster and the Orbiter Vehicles

Functions	Program (K words)	Data (K words)	Uset
1. Executive	3	5	P
2. Guidance and navigation	8	5	C
3. Control and display	7	4	C
4. Propulsion	4	3	C
5. Checkout	300/30‡	100/2	C
6. Biomedical monitoring	3	2	C
7. Communications	4	8	C
8. Radar	0.1	0.1	C & P
9. Mission control system	10/1	1	C
10. Environmental control system	3	2	C
11. Automatic landing system	5	3	S
12. Television system	0.2	0.1	P
Totals	344.3/65.3	133.2/33.1	

†Use: P-Periodic, C-Continuous, S-Single executions within particular mission phases.
‡A/B symbolizes: A-Total program words and B-Program word used at any one time.

Table 2-9. Program and Data Estimates for Booster and
Orbiter Vehicles

	Per Booster (K words)	Orbiter* (K words)
Program	344.3/65.3	492.8/138.8
Data	133.2/33.1	202.3/94.2
Minimum core	98.4	233.0
Minimum Blk Store	477.5	694.1

*Unique orbiter + common requirements

2.4 MULTIPLEXED DATA BUS

2.4.1 INTRODUCTION. The interrelations between the many subsystems on the space shuttle generate a large amount of control and data signal traffic between them. Using conventional methods to handle this signal traffic results in miles of cabling and thousands of connections with attendant weight and reliability problems. This is exemplified by the massive cable harnesses in Apollo and other space systems.

Several ideas come to mind that would reduce the number of cables required for moving signals around the vehicle. But as soon as minimizing the cables becomes the objective, short of putting all the electronics into one box, multiplexing becomes a necessity.

Multiplexed data bus is a label frequently given to multiplexed wire systems used primarily for data transfer.

This section contains a short explanation of multiplexing concepts, discussion of considerations affecting multiplexed data buses, discussion on selection of data bus techniques, and finally considers criteria for applying data bus techniques to the space shuttle.

2.4.2 BASIC MULTIPLEXING CONCEPTS. To multiplex means to share the same circuit or channel for transmission of a number of messages simultaneously. A classic example of multiplexing is available in telephony, where several thousand conversations may be transmitted simultaneously over the same circuit. Multiplexing is possible in two domains: frequency and time.

Frequency division multiplexing works by imposing each message signal on a different frequency carrier signal, and mixing the carrier signals together. At the receiving end, first the carriers are separated from each other, then each message signal is separated from its carrier. When the multiplexing process has adequate quality, the user of the message is unaware that his message was multiplexed.

Time division multiplexing achieves multiple transmissions a different way. Each message is sampled as often as necessary to maintain fidelity. The sample itself, or a representation of the sample, is transmitted. Transmission is controlled so that one sample at a time is transmitted. Samples from the different messages are interleaved.

By this means messages are transmitted simultaneously, although their samples are sent one at a time. At the receiving end, the samples are unscrambled, and the original message can be reconstituted if that is desired. Again the user need not be aware that his signal was multiplexed, so long as the sampling and other factors were treated properly.

As implied earlier, several time division multiplexing methods exist. When instead of sending a sample itself, the numerical value of the sample is generated, the sample

has been "digitally encoded." Many codes with varying attributes are available to represent numbers and letters. For example, some codes are constructed to detect transmission errors, others to enhance transmission efficiency. When digital methods are used for time division multiplexing, codes are most usually expressed by combinations of binary signals; i. e. each signal can take on only two values or meanings. Telephony has advanced digital time division multiplexing technology to the degree that 224 million bits/second are transmitted for voice and data messages. Pulse code modulation (PCM) is a popular example of digital time division multiplexing.

2.4.3 CONSIDERATIONS. The control and data transfer media on a complex vehicle such as the space shuttle has many requirements and constraints. The transmission medium required to handle the exchange of control and data signals between systems and computer(s) must be flexible, reliable, and light weight. The equipment must also be readily maintainable and capable of operating generally without error in various environments.

The vehicle environment itself imposes several requirements such as operating temperatures, vibration, electromagnetic compatibility, exposure to mechanical stresses, corrosion, and minimum weight. A multiplexed data bus system generally meets these requirements and provides sufficient weight reduction over conventionally wired systems to materially contribute to mission effectiveness. Operation of systems involving volumes of data from an array of subsystems, sensors, and processors requires a fully integrated system. The interaction between subsystems, computer, and sensors frequently dictates precise timing and detailed planning of time-oriented functions. Data quantities and priorities change from phase-to-phase within a mission and from mission-to-mission. Requirements for complex control and data signal transfers need to be incorporated in the design.

The trend toward computerized control of missions — whether in boost mode or another mode — is cause for the requirement for basic digital interfaces through which communications are established with radio, navigational systems, and numerous other sources of data. Digital techniques are favored to achieve accuracy. Examination of space shuttle subsystems reveals substantial data transfer complexity. But these subsystems use data rates well within time division multiplexing capabilities. Some tradeoffs for considering this type of system are:

- a. Complexity of point-to-point wiring versus a standardized time shared "party-line" cable.
- b. Weight tradeoffs between massive cables with associated connectors versus the encoding and sampling hardware used in a "party-line" network.
- c. Flexibility — The fixed rigid characteristics of a hardware system versus the flexibility of software reprogramming associated with a multiplex system.
- d. Failure Resistance — The nonredundant cables of conventional systems versus the use of redundant "party-line" cables.

The following paragraphs will discuss other consideration factors such as electromagnetic compatibility, reliability, maintainability, flexibility, weight savings, and integration.

2.4.3.1 Electromagnetic Compatibility. The data bus is a key element to overall integrated electronics electromagnetic compatibility, since it interfaces with most, if not all, other subsystems and is physically of extensive dimensions. The electromagnetic compatibility (EMC) of the data bus is its capability to operate with a specified margin of safety in the operational electromagnetic environment. The data bus should be neither a source of, nor be susceptible to, electromagnetic interference (EMI). Accordingly the data bus EMC plan, as part of the integrated electronics EMC plan, will require emphasis on interference-free design.

To minimize interference generation, design of the data bus signal has the objective of minimizing spectrum occupancy. Toward this goal sinusoidal waveforms rather than pulses are more desirable. Signal amplitudes should be chosen to ensure satisfactory probability that the desired signal exceeds the decision threshold of the data bus receiver; at the same time the decision threshold must be sufficiently high to eliminate, to sufficient degree, ambiguities attributable to noise.

Thus if interference emitted by a signal source and susceptibility of a receiver are reduced to the lowest value consistent with operational requirements, the effectiveness of other techniques for achieving EMC is enhanced. These techniques include the use of:

- a. Electrically balanced circuits, which may be expressed by the symmetry of twisted-pair wiring.
- b. The use of cable shields.
- c. Physical separation from power and control circuit conductors.

Electrical balance of the data bus circuits will both minimize the emission of, and susceptibility to, extraneous electromagnetic energy, but only if interconnecting wiring does not compromise the balance by its distributed reactance. Twisted pair wiring is particularly effective in reducing the magnetic field aperture a circuit presents. It also minimizes electric field coupling. Adding a cable shield improves electric field isolation by at least 60 dB. Shields should be grounded at both ends and provisions made to ensure their continuity through connectors, junction boxes, and bulkheads. Data bus wiring should, as a goal, be a minimum of three inches from cables containing ac and dc power and high-level signals. Maximum use should be made of the principle of orthogonality in data bus wiring and cable layout.

In addition, appropriate attention must be given to the EMC of the data bus terminations to ensure that components containing integrated circuits and devices with low break-

down potentials are properly protected from electromagnetic impulse in the operational electromagnetic environment where impulse type interference could damage them.

2.4.3.2 Reliability. By locating subsystem interfaces to the data bus inside an electronic component or element, the number of connector pins and the number of wires in the mating harness are materially reduced. This more than offsets the reliability degradation of adding the interface in series. In a conventional system the A/D and D/A conversion would likely be done at one, or at most a few, central converters. With a data bus concept these functions are dispersed to the interfaces.

Redundant twisted shielded pair cables can be used for all intrasystem communications. Twisted shielded pair cable is light weight, of small diameter, tolerant of damage, and minimizes connector problems. The redundant cables are connected to each unit through isolated couplings, which removes any requirement for cable switching and allows any pair to be terminated at random, tapped at random, shorted, shorted to ground, shorted to shield, opened, or stubbed without adversely affecting system operation.

2.4.3.3 Maintainability. Preliminary analysis of the space shuttle electronics indicates no special maintainability problems if maintainability is given proper attention during specification and design phases.

Implementation of a multiplexed data system will materially improve the maintainability of the total system. Regimenting the entire electronics to a common form of control and data interface will ultimately result in a special benefit — the multiplexing elements are designed to have maximum commonality throughout, thereby reducing the logistics problems that might occur with the conventional array of interface units.

2.4.3.4 Flexibility. A software programmable data transfer system permits optimization of the system for each phase of a given mission and for each mission as a whole. The computer controls channel sampling rates, format sizing, bit rates, and logic sequences. The digital computer can be programmed to perform the data transfer in several fixed modes or possibly even operate in an adaptive mode.

2.4.3.5 Weight Savings. The magnitude of weight savings on a given space shuttle version has not yet been determined. However, the complexity of the electronics is a very good indicator of the complexity of a conventional wiring system. The volume and weight of conventional point-to-point wiring is not a linear function, but rather a higher-order function of the complexity of the electronics. Some feeling for the magnitude of the savings possible can be gained by comparison with other multiplexed systems. On the S-3A ASW aircraft concept, the net weight savings was estimated at 478 pounds or about 10% of the total electronics system weight. In entertainment and passenger service system alone, on the 747 commercial airliner, the weight savings is estimated to be in excess of 1000 pounds.

2.4.3.6 Integration Tool. A beneficial byproduct of incorporating a multiplexed data bus into the space shuttle is that it requires a very thorough and detailed study of all interfaces very early in the program. The benefits from this total systems approach are already in evidence and will become more obvious as the design of the space shuttle system continues. In the past insufficient concern of the total system interface has sometimes resulted in incompatibilities. The reduction of installed electronics weight by about 10 to 15% and the attendant improvement in mission effectiveness are real benefits derived from the multiplexed data bus approach.

2.4.4 SELECTION OF DATA BUS TECHNIQUE. Using the considerations discussed in the previous paragraphs, one possible configuration will now be developed that may be used as a baseline for future tradeoffs. In the following paragraphs, first a selection method is delineated, signal selection is discussed by examining spectrum generation and coupling methods, a clock method is selected from several candidates, and cable selection is discussed as are message structures.

2.4.4.1 Selection Process. Selecting the type of control and data transfer system has many facets. The flow diagram in Figure 2-4 shows the various inputs, constraints, decisions, and optimizations, that go into the design of a multiplexed data bus subsystem.

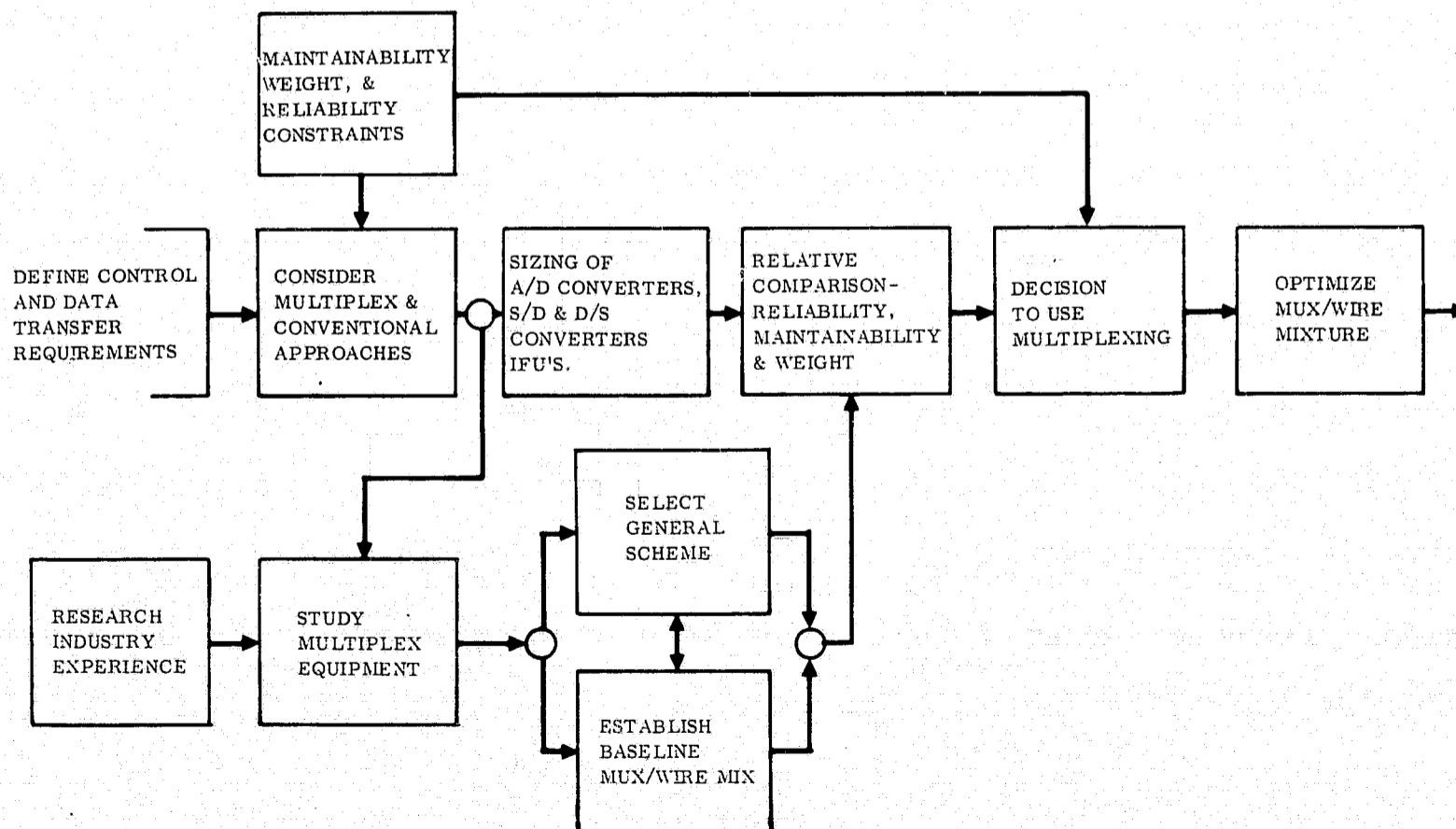


Figure 2-4. Flow Diagram of Selection Process

It appears that a basic consideration for use of wire sharing techniques is volumes of data requiring transfer to one or more remote areas of distribution. Each application, however, must be studied relative to other factors — for example, the length of a space vehicle can be considered a long distance when a complex and heavy cable is required to carry a large number of signals. Yet this same distance would be considered insignificant in a telephone substation application. Thus, each application must be placed in a realistic context and tradeoffs must be made to determine system effectiveness. As technology improves, these tradeoffs must be necessarily reexamined.

2.4.4.2 Signal Selection. A number of signal types could be utilized for a multiplexed data bus. Examination of a few of their characteristics makes it possible to select a signal that appears well suited for space shuttle application. The following signal techniques were considered:

NRZL	Nonreturn to zero level
RZ	Return to zero
Bi Polar RZ	
PDM	Pulse duration modulation
PAM	Pulse amplitude modulation
LSK-AM	Level shift keying— amplitude modulation
Bi-Phase Digital Modulation	
Bi-Phase Carrier Modulation	
LSK-SW	Level shift keying—sine wave modulation

LSK-SW was selected as the baseband technique, based on the following considerations.

Spectrum Analysis. The spectrum of the various baseband techniques was examined to determine transmission bandwidth, magnitude of high-frequency components capable of generating RFI, and power level for clock.

Examination of the modulation spectrum eliminates square pulse modulation as a candidate unless it is accompanied by heavy filtering to remove high-frequency components which generate RFI. Some forms of pulse modulation such as PDM, RZ, and PAM have greater high-frequency components than NRZL and the bipolar RZ. Since the space shuttle contains a multitude of electronic and radio frequency functions, the sinusoidal data signal should be used rather than the rectangular pulse train to minimize electromagnetic interference problems between the numerous electronic systems within the vehicle.

Two of the simplest forms of sine wave modulation are LSK-SW and bi-phase carrier modulation. Bi-phase carrier generates larger amplitude high-frequency spectrum

components due to the 180 degrees phase reversal at the 1-0 switching point. The waveform for this technique is shown in Figure 2-5. In LSK-SW the level of the signal is switched by the data pulse train. This modulation waveform is shown in Figure 2-6. The resultant frequency spectra generated by the waveforms in Figures 2-5 and 2-6 are shown in Figures 2-7 and 2-8.

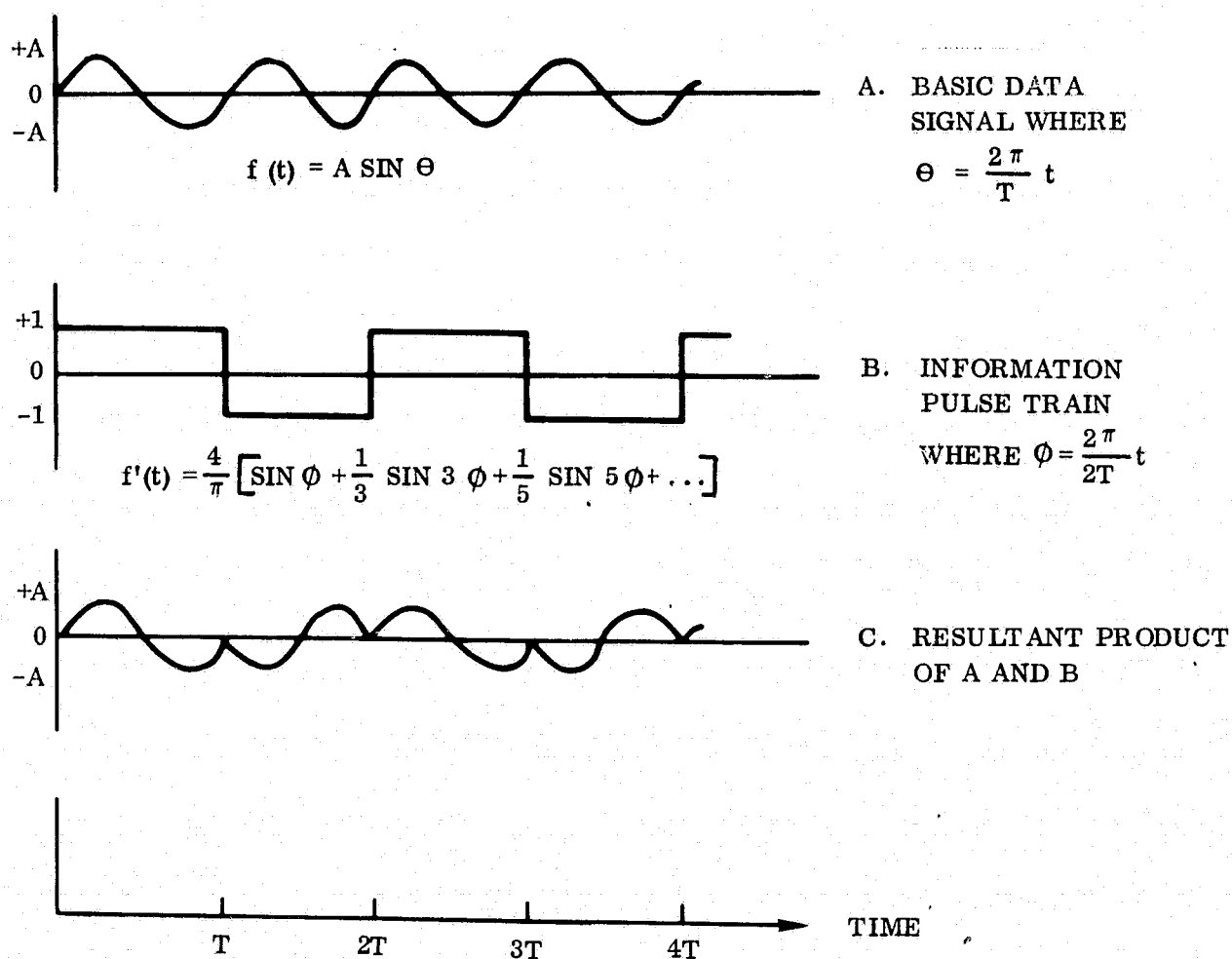


Figure 2-5. Bi-Phase Data Waveforms

Transformer Coupling. Direct coupling versus transformer coupling is a consideration. With balanced lines and high common mode rejection with differential receivers, the noise problems with direct coupling are reduced. However, another factor is the susceptibility of semiconductor circuitry to high reverse voltages. Prior experience with transients on the ground bus of magnitude from 350 to 500 volts with frequencies up to 10 MHz on the Atlas and Centaur boosters indicates that use of filters and limiters is at best a difficult solution. For this reason transformer coupling is selected for complete ground isolation. Use of a sine wave signal simplifies the transformer design.

Clock Transmission. The selection of a baseband technique is partially dependent upon the means for providing system clock.

Table 2-10 lists some of the possible clock options with advantages and disadvantages. Without a clock bus, separate clock generators are required at each data bus interface

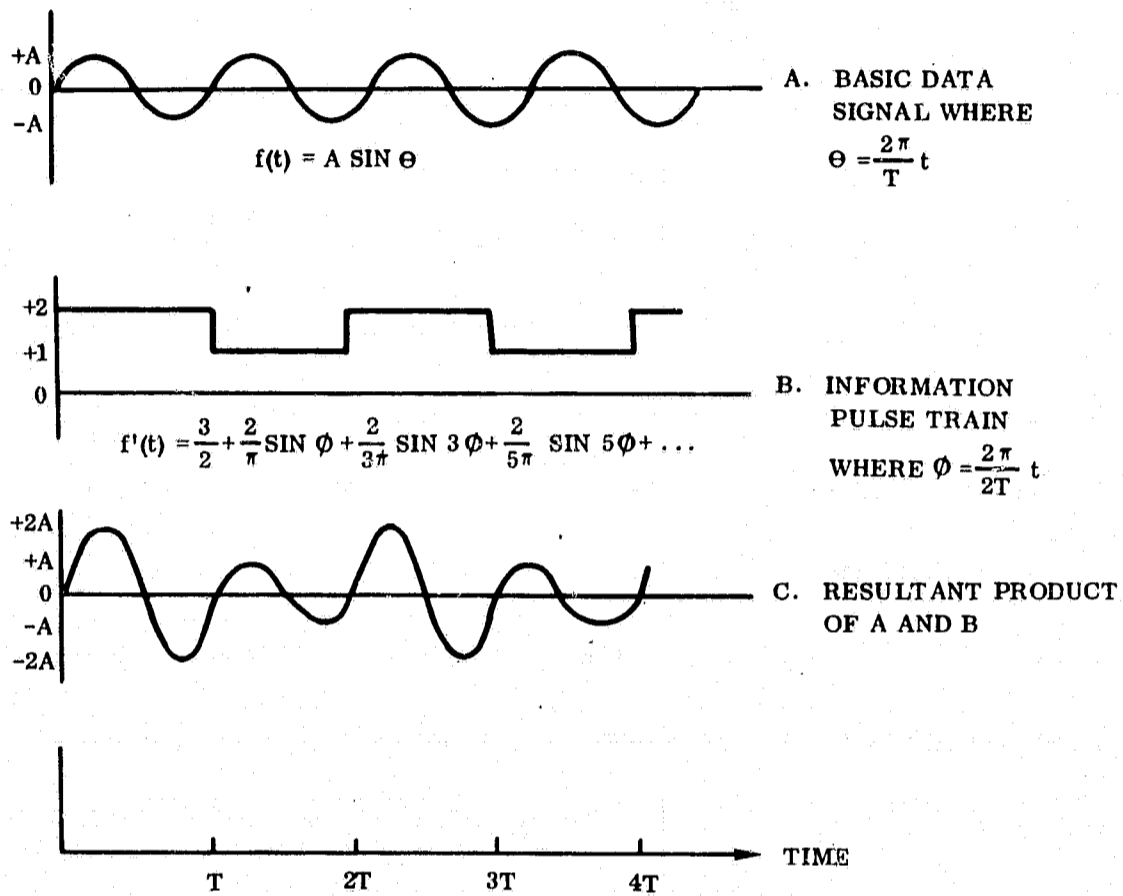


Figure 2-6. Level Shift Transmitted Data Waveforms

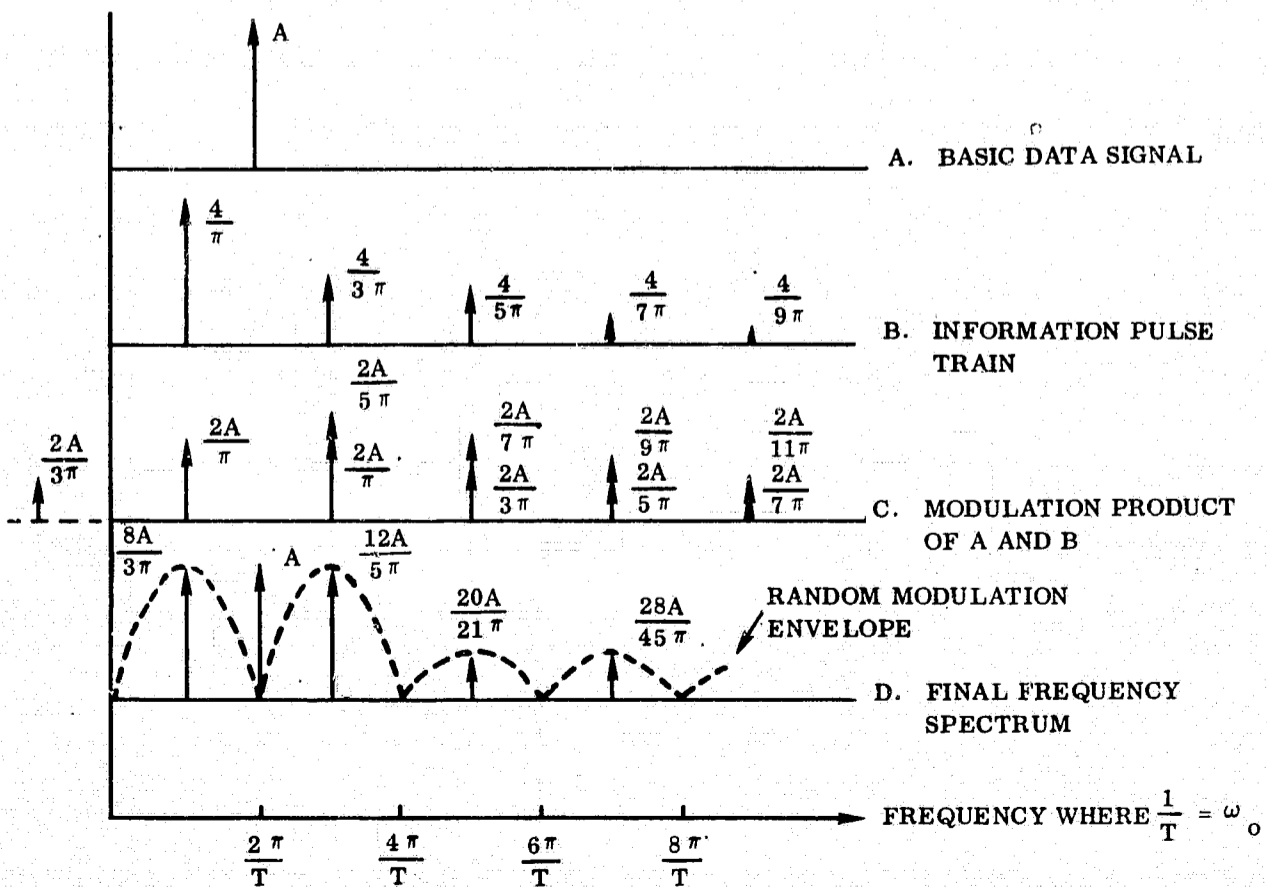


Figure 2-7. Bi-Phase Transmitted Frequency Spectrum

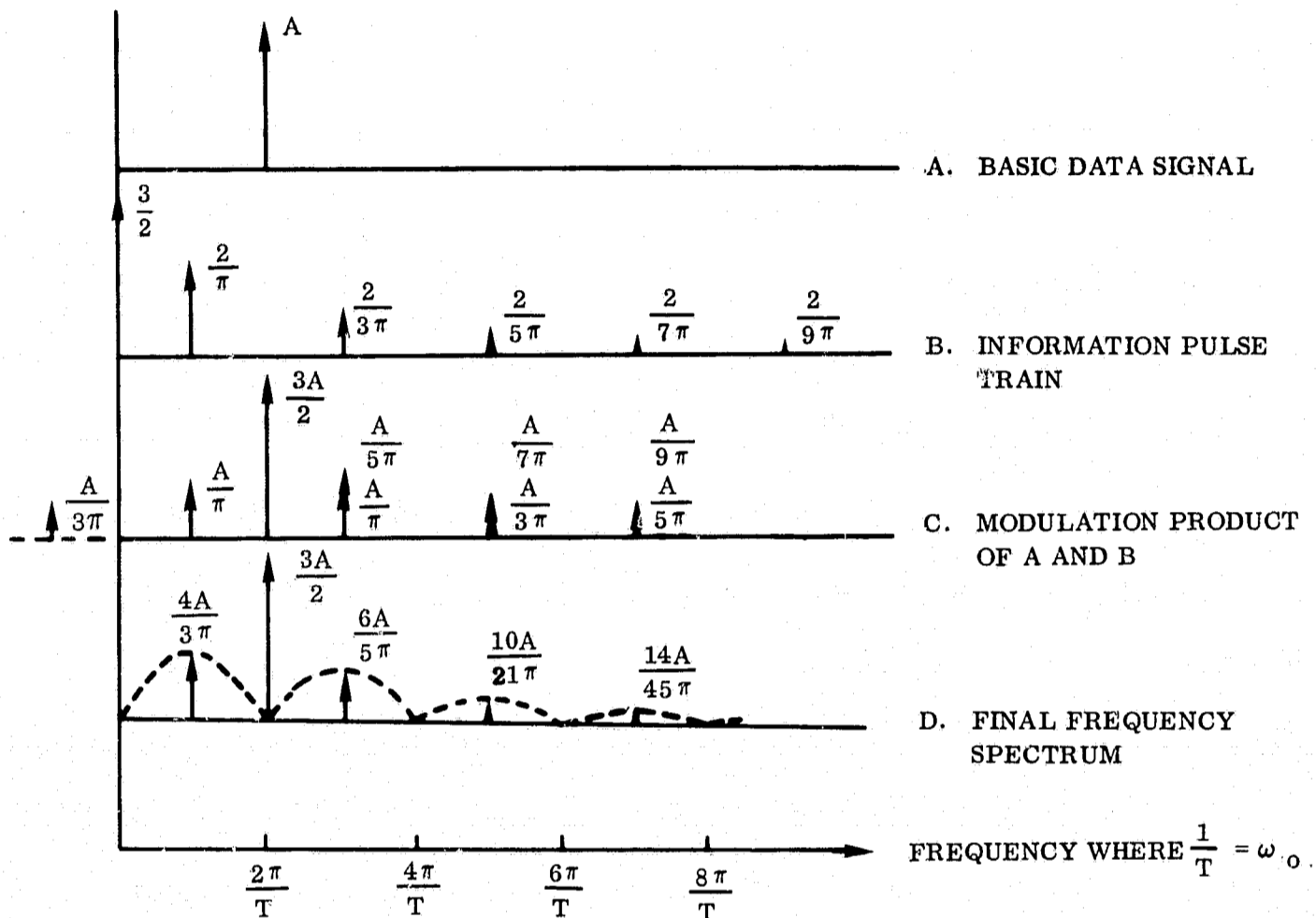


Figure 2-8. Level Shift Transmitted Data Frequency Spectrum

(DBI). Because of this hardware penalty, the clock bus choice is preferred. A separate clock bus can interconnect all the DBIs without creating impedance matching and power level problems.

One of the considerations in implementation is whether the modulation technique includes readily available clock with data. As pointed out above, a clock line is required to avoid having clock generators in each DBI. Therefore there is another factor; that is, it is desirable to have clock with data so that phase delay difference between a separate clock and data lines is not a problem for high bit rates. NRZL does not include clock with data except by expensive, time-consuming data correlation. RZ has clocking problems for a string of 0's. Bi-phase digital and bi-phase carrier are somewhat difficult to obtain clock from data.

Adequate signal-to-noise margin is provided by the LSK-SW technique. It generates less RFI than bi-phase carrier, and clock extraction is simpler with LSK-SW. LSK-SW is the choice for the baseband system.

2.4.4.3 Cable Selection. Two basic transmission-line types have desirable characteristics for baseband use: a double shielded coaxial cable or a shielded balanced twisted-pair type (Twinax). The shielded, twisted-pair cable is more lossy for the equivalent

Table 2-10. Bus Options

OPTION	ADVANTAGES	DISADVANTAGES
1. Two-bus type (a) A clock bus (b) Address and data on second bus	1. Easy control transfer to subsystem. 2. Low cable weight penalty. 3. Simple second bus interface.	1. Longer communication time.
2. Two-bus type (a) Address and clock on bus 1 (b) A data bus	1. Shorter communication setup time.	1. High cable weight penalty. 2. Hardware penalty of two bus interface. 3. Difficult control transfer to subsystem.
3. Single-bus type (a) Address and data on bus (no clock)	1. Easiest control transfer. 2. Lowest cable weight penalty. 3. Interface with a single bus.	1. Hardware penalty of clock generators in each DBI. 2. Longer communication setup time.
4. Two-bus type (a) An address bus (b) A data bus (no clock)	1. Shorter communication setup time.	1. Hardware penalty of clock generators, and two bus interface. 2. High cable weight penalty.

size, but attenuation is not a serious consideration for the required cable lengths. An appropriate coaxial cable type is RG-142 A/U, and a good shielded twisted-pair cable is RG-108 A/U. These are good representative cables since they are relatively small in diameter, resulting in a minimum cable weight.

The cable to be used must be selected to achieve optimum signal transfer characteristics with a minimum of size and weight. The cable shielding must be sufficient to inhibit interference to or from other electronic or rf equipment. The shielded twisted-pair cable RG108-A/U will better meet these requirements than the RG142-A/U. The shielded balanced transmission line will offer better shielding properties than the coaxial cable as indicated in NASA Report N68-20827. In this report, the coupling between a rod antenna and RG108-A/U and RG58-A/U is compared. The spacing between the 1-meter-long rod antenna and the test cable was two inches. The shielded, twisted pair cable offers better attenuation at low frequencies. In another test, the crosstalk between two shielded twisted-pair cables was less than 100 microvolts for a signal level of 500 millivolts differential in the transmitting cable, or an attenuation of 74 dB. The better shielding properties of the RG108-A/U make it the better choice over the RG142-A/U for the multiplex data bus.

2.4.4.4 Message Formatting. A variety of methods have been used to structure message transmissions in systems which use data bus concepts and computers. These methods may be generally classified as follows:

- a. Fixed frame format.
- b. Interrogate reply.
- c. Polling.

Fixed-Frame Format. In this particular format, the data to be transferred is organized into a recurring sequence and is usually transmitted serially. Each data word is assigned a "time slot" or a time duration following some frame synchronizing word(s) that recurs periodically. Standard pulse code modulation (PCM) telemetry is a prime example of this type. Fixed-frame format may be used in either simplex or duplex modes. In duplex mode, the various sources are synchronized to no less than word slots. If the separation is such that time delays are significant, the systems usually operate word synchronous and bit asynchronous.

Interrogate-Reply. This mode utilizes a "question-and-answer" routine, which is sometimes called "hand shaking." The computer requests data by signalling on the data bus. Once a subsystem has been interrogated it responds with the requested data. This operation is used by most off-line computer complexes, except that with off-line computers a dedicated line is used for signalling. Interrogate-reply techniques make relatively inefficient use of time. In a large complex requiring the transfer of large volumes of data between subsystems, it seems inefficient to use the computer as a switching device.

Even though this method may not make maximum use of time; i. e., using time for addressing, requests, setup time, etc., it usually simplifies the hardware required at the peripheral subsystem and simplifies software. It may be implemented for either serial or parallel data.

Polling. In this technique a central logic device (it may or may not be a computer) performs a "roll call" of the subsystems. If they have data to transfer, the central device initiates the transfer to either the computer or to some specified subsystem. In the latter case the data must be preceded by an address or must otherwise be directed to the proper destination.

If the polling is performed externally to the computer, the computer is relieved of a certain portion of the loading. The sequencing may be controlled by either hard-wired logic or computer-controlled logic as the requirement for flexibility dictates. The peripheral hardware is essentially the same as in the interrogate-reply.

Format Selection. Selecting the most appropriate format for space shuttle is much less dependent on data bus considerations than on computer hardware and software considerations. The effect of format on the data bus is primarily message capacity, because different formats may require a different total number of bits to accomplish transmissions, and they may impose peculiar timing constraints.

The effect of format on the data bus interfaces may be pronounced, depending on detail design; but is still less significant than the computer software problems.

Studies to date indicate the optimum format for space shuttle is a combination of the interrogate-reply and polling modes. In this concept the repetitious transfer of data is handled by a computer-controlled polling device external to the computer proper. The equipment would be designed to receive and store instructions from the computer regarding the polling sequences. At any time the computer requires data, it interrupts the polling sequence and requests the appropriate peripheral. Once the data are transferred, the control is returned to the polling logic.

Advantages of Polling Format. A major advantage of polling versus frame format operation is the complete control of data transfer sequence within computer software. Any format change occasioned by subsystem modification is more likely to be accomplished without hardware rework with the polling type of system. Both the source of data and the destination of data would be specified by address bytes stored either in the computer core memory or control sequencer. Since it is desirable to limit the amount of I/O traffic, an address designation may apply to one word of data or a block of data words, depending upon the particular transmission. The traffic routing is primarily to and from the computer with some amount of traffic between DBIs.

Criteria may be established for deciding when to multiplex and when not to. If the idea is accepted, in general, that the advantages are on the side of multiplexing, it becomes

Even though this method may not make maximum use of time; i. e., using time for addressing, requests, setup time, etc., it usually simplifies the hardware required at the peripheral subsystem and simplifies software. It may be implemented for either serial or parallel data.

Polling. In this technique a central logic device (it may or may not be a computer) performs a "roll call" of the subsystems. If they have data to transfer, the central device initiates the transfer to either the computer or to some specified subsystem. In the latter case the data must be preceded by an address or must otherwise be directed to the proper destination.

If the polling is performed externally to the computer, the computer is relieved of a certain portion of the loading. The sequencing may be controlled by either hard-wired logic or computer-controlled logic as the requirement for flexibility dictates. The peripheral hardware is essentially the same as in the interrogate-reply.

Format Selection. Selecting the most appropriate format for space shuttle is much less dependent on data bus considerations than on computer hardware and software considerations. The effect of format on the data bus is primarily message capacity, because different formats may require a different total number of bits to accomplish transmissions, and they may impose peculiar timing constraints.

The effect of format on the data bus interfaces may be pronounced, depending on detail design; but is still less significant than the computer software problems.

Studies to date indicate the optimum format for space shuttle is a combination of the interrogate-reply and polling modes. In this concept the repetitious transfer of data is handled by a computer-controlled polling device external to the computer proper. The equipment would be designed to receive and store instructions from the computer regarding the polling sequences. At any time the computer requires data, it interrupts the polling sequence and requests the appropriate peripheral. Once the data are transferred, the control is returned to the polling logic.

Advantages of Polling Format. A major advantage of polling versus frame format operation is the complete control of data transfer sequence within computer software. Any format change occasioned by subsystem modification is more likely to be accomplished without hardware rework with the polling type of system. Both the source of data and the destination of data would be specified by address bytes stored either in the computer core memory or control sequencer. Since it is desirable to limit the amount of I/O traffic, an address designation may apply to one word of data or a block of data words, depending upon the particular transmission. The traffic routing is primarily to and from the computer with some amount of traffic between DBIs.

Criteria may be established for deciding when to multiplex and when not to. If the idea is accepted, in general, that the advantages are on the side of multiplexing, it becomes

necessary to establish methods to decide only when not to multiplex. The process requires, and begins with, a thorough traffic analysis of data to be handled. This means examining all subsystems that use and generate data and control signals. Each signal then has criteria applied to determine if it should be exempted from being multiplexed:

- a. Analog signal that is to be used in the same form as generated by equipment physically close to its source.
- b. Signal is "ultracritical."
- c. Wideband analog signal with one point of origin and only one destination.
- d. Multiple signals traveling exclusively between two terminals physically very close together.

2.5 GUIDANCE AND NAVIGATION

2.5.1 INTRODUCTION. The first question that always comes up when a guidance system is discussed is "what is the required accuracy?" For space shuttle, with a single vehicle performing all phases of the complete mission, providing an answer to the accuracy question becomes difficult. The required accuracy can only be determined after completion of a series of tradeoffs and other studies, such as:

- a. Guidance accuracy vs. on-orbit velocity expenditures.
- b. Guidance accuracy required for various rendezvous techniques.
- c. Entry heating constraints on guidance accuracy
- d. Landing system coverage and resulting entry guidance scheme accuracy.

Pending the results of these studies, and after examining the results of similar studies for other vehicles, a baseline inertial measurement unit component accuracy set was selected (Table 2-11). For comparison, the Saturn and Centaur accuracies are also shown in the table.

Table 2-11. Baseline Guidance Accuracies

SENSOR	ACCURACIES		
	BASELINE 3σ	CENTAUR 3σ	SATURN 3σ
Accelerometers			
Bias	40 parts/million	40 parts/million	10 parts/million
Scale Factor	40 parts/million	40 parts/million	50 parts/million
Gyros			
CT	0.15 deg/hr	0.15 deg/hr	0.1 deg/hr
MUIA	0.20 deg/hr/g	0.20 deg/hr/g	0.25 deg/hr/g
MUSA	0.30 deg/hr/g	0.30 deg/hr/g	0.25 deg/hr/g

2.5.2 REQUIREMENTS. The requirement is for an autonomous navigation subsystem usable for all portions of the mission with an on-orbit time of seven days. An inertial subsystem is the only type that can be considered autonomous, but even the best inertial subsystem will need assistance to enable it to provide accurate angular reference after a seven-day period in orbit. Star sights obtained by the use of star trackers, a star-field mapper, or manual sextant can provide the necessary reference to maintain accurate orientation.

The present state of the art in items such as star trackers and inertial measurement units is such that the mission can easily be accomplished if all equipment is operating; however, the requirements for redundancy (fail operational-fail operational-fail safe) lead to some interesting tradeoffs.

2.5.2.1 Tradeoff Considerations. For example, the inertial measurement unit will be mechanized in either gimballed or strapdown configuration. If the redundancy/reliability requirements permitted the use of a nonredundant reference, the weight and power for equivalent strapdown and gimballed units turn out to be very similar, and choice of a gimballed configuration would probably be made on the basis of the large amount of existing experience with gimballed inertial measurement units. However, the redundancy requirements do exist, and the use of a redundant sensor concept such as the 6-gyro, 6-accelerometer skewed orientation strapdown cluster now under low-level development by several organizations appears to be very attractive. If properly mechanized, this arrangement can permit any two similar instruments to fail, compare instrument outputs, identify the failed instruments, and use data from the remaining good instruments to complete the mission. The loss of a third instrument would still permit normal subsystem operation, if a means other than comparisons of instrument output were available to identify and thus eliminate the failed item.

When the use of redundant sensors as above is considered, then the resulting strapdown subsystem will be simpler and lighter, consume less power and take up less space than a gimballed system with the same redundancy. The choice between strapdown and gimballed systems, however, will still be difficult when consideration is given to problems of calibration, alignment, and possible effects on performance of unknown system environments. The lack of large funded programs for strapdown system development over the past few years has not made this choice any easier. For the baseline system, a multiple installation of conventional 4-gimbal platforms will be assumed, similar to that now being installed on large commercial transports.

This could require a total of four platforms, if "fail safe" is assumed to be a configuration that requires the use of an inertial reference, and a total of three platforms if some other backup means of attitude reference and navigation is available. A comparison of typical power and weight for present day state-of-the-art hardware is shown in Table 2-12. A detailed tradeoff between the strapdown and gimballed configurations should be conducted in Phase B, with consideration given to a laser gyro strapdown mechanization. The possibility of using an electrostatic suspension gyro/accelerometer should also be investigated, as recent progress has been made in this area.

2.5.2.2 Alignment. Due to the length of time required for typical missions, the inertial measurement unit will require in-flight alignment and/or monitoring and correction of gyro drifts. The information required to accomplish the above functions may best be obtained using measurements of angles to the stars. This may either be accomplished by the Apollo technique of a space sextant operated by an astronaut and requiring his full attention whenever making a measurement, or by an automatic star

Table 2-12. Estimated Power and Weight for Gimballed and Strapdown Navigation Subsystems

	Gimballed Configuration		Strapdown
	Single Platform	Triple Installation	Redundant Config.
Weight	85 lb	255 lb	140 lb
Power	330 watts	1000 watts	270 watts

Note: The above comparison table was based on present state-of-the-art hardware with the baseline guidance system accuracies as shown in Table 2-11.

tracker/mapper. The state of the art in such devices is such that a strapdown star tracker/mapper can obtain the necessary angular measurements with a one-sigma uncertainty of about 10 seconds of arc and a total field of view of 30 degrees (square field). This type of star tracker is very attractive as it may also be used as the major component of a laser radar, capable of providing rendezvous and docking guidance.

2.5.2.3 Earth Reference. In addition to an accurate angular reference system, the navigation function will require some means of locating the vehicle with respect to the Earth, and several methods of accomplishing this have been considered.

The autonomy requirement eliminates any ground-based radar tracking or reliance on navigation systems (such as Loran, Omega, Navsat) in structuring the guidance system. Their use as additional aids, of course, should still be considered.

The use of a landmark tracker, tracking either known or unknown landmarks, was also briefly investigated; but considering the present state of the art it does not appear feasible to rely on this type of device, unless we are willing to have one of the crew operate the tracker in a manual mode.

The best way at this time to implement the on-orbit navigation function appears to be the use of horizon trackers. These devices, operating in the 14-16 micron CO₂ absorption band, measure the angle from vehicle reference to the horizon with a one-sigma accuracy between 0.05 to 0.1 degree, including the effects of horizon radiance profile uncertainties. As an example of state of the art, a strapdown horizon tracker using a balanced thermopile sensor with "essentially no moving parts", now in advanced development by Quantic Industries, Inc. for the Air Force, is scheduled for flight test in late 1970. Weight of this system in a six head redundant sensor configuration would be about 50 pounds with a power consumption of 30 watts.

2.5.2.4 Rendezvous Sensor. The choice of a rendezvous sensor will, of course, depend upon the mode of rendezvous selected for use by space shuttle. This mode selection will determine the maximum detection range, the volume to be searched, the time available for search, and the required tracking accuracy of the sensor. The

choice of mode, however, will conversely be affected by the capabilities of the rendezvous sensor, the accuracy/fuel consumption tradeoffs, and many other operational requirements such as maximum time allowed to rendezvous, accuracy of target ephemeris, and probable desire to avoid having either the astronauts or the rendezvous sensor look directly at the sun. In addition, for rendezvous with a passive satellite, information such as the radar and/or optical cross section model, or expected temperature and minimum-area emissivity product must be specified.

The possibility that the "passive" satellite might, for most missions, be required to carry radar or optical corner reflectors should not be overlooked. In fact, looking briefly at mission requirements, the provision of a long-range (50 n.mi. or more) sensor capable of skin track on a truly passive satellite of small size, would put what might be an unacceptable weight burden upon the normal logistics mission. It is suggested that the long-range detector of passive satellites be made a part of the mission payload, and not a part of the basic vehicle. This would be consistent with the provisions for inspecting, probing, repairing and/or retrieving the passive satellite all being considered as payload. The requirement for rendezvous on a normal logistics and/or space rescue mission can then be examined, and the sensor type chosen.

Considered as candidates for the rendezvous sensor were the Gemini and Apollo rendezvous radars (which require transponders on the target vehicle), and a laser radar, similar to the equipment that has been under development by ITT for Marshall Space Flight Center during the last five years. This equipment has undergone successful aircraft tracking tests and performed many successful dockings in a six-degree-of-freedom hardware docking simulator.

Considering the time schedule, the requirements for automatic approach and docking can only be met by the above. The baseline rendezvous and docking sensor selected for space shuttle is the laser radar. The possibilities of using multi-mode radar or long long-wave infrared sensors for all phases except docking should be investigated in Phase B studies.

2.6 COMMUNICATIONS

2.6.1 INTRODUCTION. Only the operational vehicle is considered in this analysis. A major goal of the space shuttle is low system-operating cost. One method of achieving this goal is by means of virtually completely autonomous operations.

This desire for autonomy and low cost leads to a philosophy of minimum communication (i. e. low data rate, no requirement for continuous communication, and use of available commercial communication satellites such as Intelsat IV.

The total communication requirements of space shuttle may best be analyzed by considering the various flight phases and the specific requirements of each phase.

2.6.2 LAUNCH PHASE. The launch phase communications between the vehicle and the launch site will be direct, via either vhf or S Band. The communication bandwidth will be limited to that required by voice or 1 to 2 kilobits of digital data. Antennas may be either short blades or cavity types, located so as to approximate an omnidirectional pattern.

To eliminate the need for real-time telemetry from the operational vehicle during boost phase, the use of a self-separating, aircraft-type crash recorder with recovery beacon will be considered.

2.6.3 ON-ORBIT PHASE. The on-orbit communications may be accomplished using commercial satellites such as Intelsat IV, with the data rate restricted again to no more than 1 to 2 kilobits, or voice.

Link analyses performed by Comsat Corporation and by Convair show that a 4-foot-diameter steerable paraboloid or its equivalent will be adequate to support a satellite-shuttle down-link data rate of about 1 kilobit with an error rate of 1 in 10^6 . The use of this antenna for the shuttle-satellite up-link will require an average transmitter power of approximately 70 watts. Inherent in these computations is the assumption that continuous communication is not required, and that waiting until the satellite is well above the horizon before attempting to communicate is acceptable. Delays in establishing communication of 20 minutes or more may result, depending on the number of satellites used. This is similar to the present capability of the NASA tracking network when used with spacecraft in low earth orbit. Direct vehicle-to-vehicle communication while on orbit will not require use of the satellite link, but may be accomplished via either the S-band or vhf systems.

2.6.4 ENTRY. The entry period is assumed to require no communications.

2.6.5 SUBSONIC FLIGHT PHASE. Subsonic flight communications will be accomplished via vhf/uhf radio compatible with the present air traffic control system. An L-band beacon compatible with the air traffic control system will also probably be carried.

2.6.6 EFFECT ON CONFIGURATION. The only antenna requirement that might have an effect upon vehicle configuration is the 4-foot paraboloid or equivalent. This antenna, used for shuttle satellite communication, is only required when on orbit, and will be retracted at all other times.

The heaviest weight items in the communication area will be the 70-watt, 6-GHz transmitter and the antenna with its pointing/tracking controls.

2.6.7 AUTOMATIC LANDING

2.6.7.1 Requirement. The primary requirements that define the landing system are that the shuttle be capable of automatic blind landings, and that it be capable of performing these landings on any 10,000-foot runway in the world.

2.6.7.2 State of the Art. The major problem that this requirement introduces is that no practical scheme now under development has this capability without the use of some form of ground equipment. This ground equipment, whatever it may be, is certainly not now installed at every 10,000-foot runway. The system that comes closest to universal installation is the instrument landing system (ILS), which is installed at major airports all over the world. Unfortunately, however, this system operates at vhf frequencies and is susceptible to multipath distortion of the commanded flight path. Unless great care has been taken in installation and maintenance, it is not suitable for completely automatic landing; in fact, even if properly installed, it is marginal.

An upgrading of ILS installations is underway, and certain airports will have Category III ILS systems. These could support blind landings, although some questions still exist as to the resulting system performance and reliability.

The Radio Technical Commission for Aeronautics (RTCA)*, recognizing the inherent limitations of the present vhf ILS, issued to industry in early 1969 a call for proposals for a new guidance system for approach and landing (RTCA paper 24-69/SC117-48). The operational requirements for this system are called out in RTCA paper 19-69/SC117-46. Evaluating the 23 resulting proposals, an RTCA subcommittee concluded that the system chosen will probably be a microwave scanning fan beam system. Present plans are for system selection by the end of 1969, and for some special installations to be completed in the 1972-75 period.

A system meeting the RTCA requirements will provide the guidance for space shuttle, and it is recommended that this become the primary system for space shuttle

*Composed of representatives of the airlines, military, electronics industry, FAA, and certain foreign countries.

automatic landings. However, inasmuch as worldwide installation will not occur until the 1975-85 period, compatibility with the present vhf ILS will be required. The automatic landing system may, if required, combine ILS and inertial measurement data in an optimum manner to minimize the effects of ILS multipath.

2.6.8 RETURN OF UNMANNED BOOSTERS. The reusable boosters, if unmanned, must be able to return to the launch site and land. Almost all drone aircraft now being flown are equipped with either an autopilot or a combination of autopilot and inertial navigator, which actually fly the aircraft. The command link is used only to change modes or direction of flight. The shuttle booster, containing similar guidance, control, and computing equipment to that in the orbiter, could easily be automatically returned to the launch site and landed. However, considering the cost of this type of vehicle and the abilities of man, a very careful tradeoff study must be performed before committing the program to an unmanned booster.

2.6.9 IMPACT OF CHANGE FROM THREE-ELEMENT TO TWO-STAGE SHUTTLE CONFIGURATION. The orbiter portions of either configuration (two-stage or three-element) will, in the electronics area, be almost identical. This results from the basic requirement that the boosters must be able to fly independently from the orbiter when returning to base after boost and when being ferried. This means that electronics for guidance, control, communications, and landing, as well as on-board check-out of these systems, should be in the boosters. Therefore, the orbiter's electronics subsystem will be almost independent of the booster electronics. The major impact of substituting a two-stage vehicle for the baseline three-element configuration will be the deletion of one full set of booster electronics from the complete vehicle.

SECTION 3 ONBOARD CHECKOUT

3.1 INTRODUCTION

This section of the report describes a possible mechanization of onboard checkout for the space shuttle. This configuration was developed as part of the special emphasis study and was conducted in three basic increments.

The first study increment developed the objectives to be accomplished by the onboard checkout system. These were derived together with the current mission profiles and present maintenance requirements for the space shuttle.

The second and third increments were accomplished simultaneously as each phase relates directly to the other. The second increment developed a baseline subsystem configuration to implement the onboard checkout objectives. The third phase applied the configured system to two preselected vehicle subsystems. These were: 1) the environmental control/life support subsystem, and 2) the electrical power generation subsystem. The second and third study phase were iterative processes with each tending to refine and modify the other.

3.2 APPROACH TO THE PROBLEM

The primary objective of the onboard checkout function is to verify that all of the vehicle subsystems are operable. This philosophy has been extended to include additional related test processes. These related processes of checkout are performance monitoring, post flight securing, and maintenance assistance (Figure 3-1). Performance monitoring is flight or operations oriented and directed toward corrective action following a failure or detectable impending failure. The post flight secure process assists the flight crew in deactivating and making the vehicle safe after flight. The maintenance assist program aids the ground crew in the isolation and repairs of defective subsystems.

Three types of subsystem test methods are used for the onboard checkout system:

- a. Demandable built in self test.
- b. Continuous built in self test.
- c. Onboard computer evaluation.

The use of any particular type or combination of test types follows a tradeoff analysis to determine the most effective subsystem process.

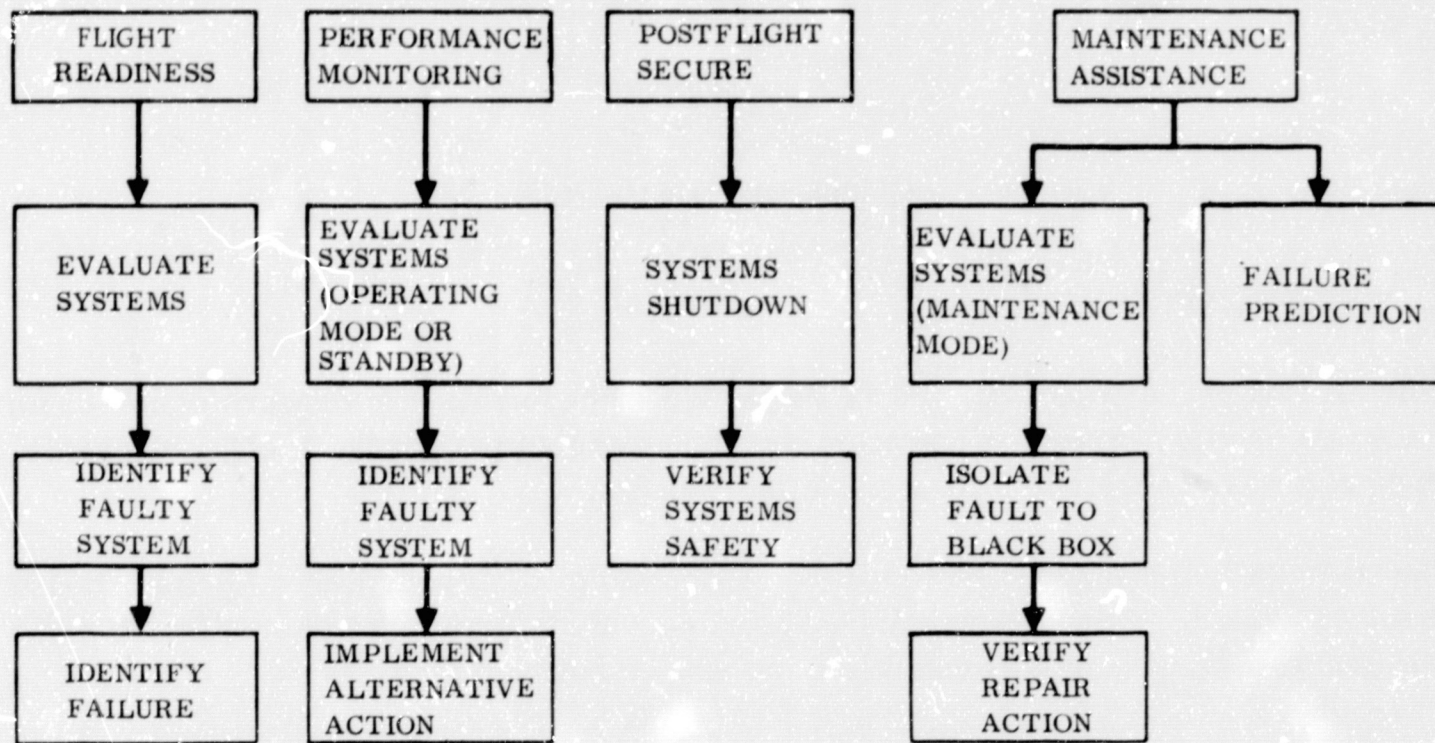


Figure 3-1. Functions of Onboard Checkout

The onboard checkout concept developed in this report places heavy emphasis on data management. Data management software costs, which can exceed the costs of systems hardware, require special emphasis to make the overall system realizable. The algorithms structured for this study are based on a general fault-detection routine and variable fault-disposition routines.

The fault-disposition routines are a function of the phase of vehicle operation. The routines are dictated by the different methods of handling a failure. Flight readiness, as an example, is concerned with identifying the failure for analysis by the crew, while the performance monitoring program is concerned with reconfiguring the vehicle by the redundant modes selection.

The onboard checkout subsystem is a functional entity only and uses the data system of the vehicle. When operating as a functional entity it uses the central computing complex, the multiplexed data bus, and the crew station controls and displays. All test processes are conducted from the crew stations.

3.3 ONBOARD CHECKOUT OBJECTIVES

The primary objective of the onboard checkout system is to verify that all vehicle subsystems will operate to perform a specific mission. The process of assurance should be accomplished by a system that is totally self-contained in the vehicle. The system should be capable of being operated at any time, including flight, and as such should not require support by ground personnel or ground equipment.

In the construction of a system that identifies operability, the instrumentation and logic requirements result in a configuration that has an inherent additional capability. To determine if a system operates within a desired specification requires measuring and comparison to tolerance limits. Deviation from a tolerance limit indicates the system has some characteristics of nonoperability. By expanding the logic of a checkout system and using the same measurements, the nature of the failure can be determined. Expanding this concept, a desirable set of secondary objectives can be met that are related to specific operational modes. These modes are prelaunch, flight performance monitor, postflight securing, and ground maintenance. The requirements of the onboard checkout systems are unique for each of these operating modes.

3.3.1 FLIGHT READINESS. Prior to launch a confidence test is required. This provides assurance to the flight crew that the vehicle can perform the desired mission. The process determines that all subsystems and subsystem redundant modes will operate (Figure 3-2). In the event that a subsystem does not perform to specification in all operating modes, a status report must be provided. To achieve effective status reporting, the faulty subsystem and the type of failure must be identified.

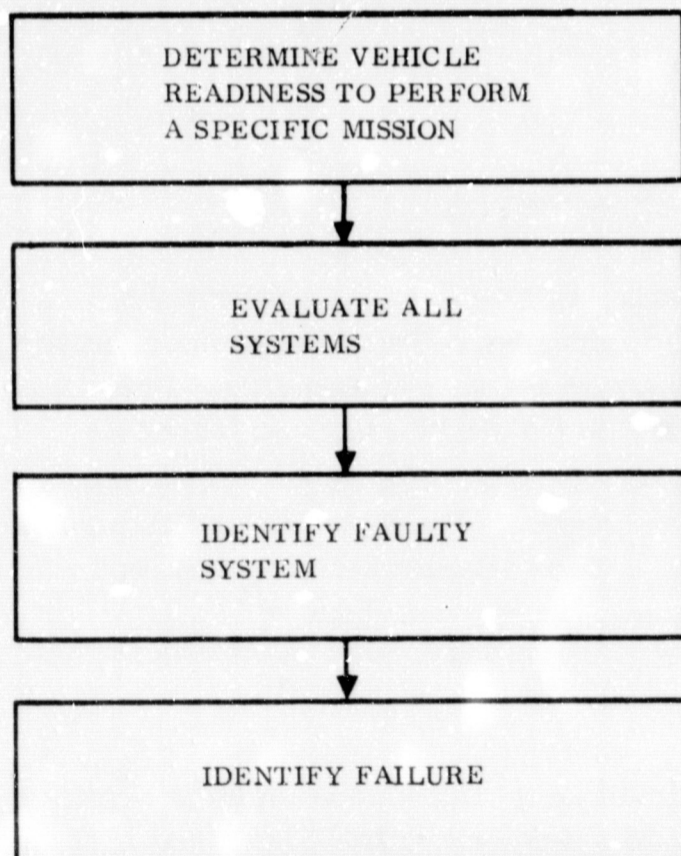


Figure 3-2. Prelaunch Functions

With this information, the flight crew can evaluate the impact to the mission and make critical operational judgments.

3.3.2 PERFORMANCE MONITORING

3.3.2.1 Corrective Action. The performance monitor mode of the onboard checkout system is used during the flight phases of the space shuttle. It consists of a set of instruments and logic similar to that used for the prelaunch confidence test. However, the algorithm emphasis is directed toward detecting a failure and either implementing alternative action or informing the crew of status and possible alternatives (Figure 3-3). This is the prime objective of performance monitoring. Corrective action is accomplished by activating a subsystem redundant mode and disabling the defective subsystem

component. The performance monitor program need only isolate a failure to the lowest subsystem level for which redundancies exist and can be controlled.

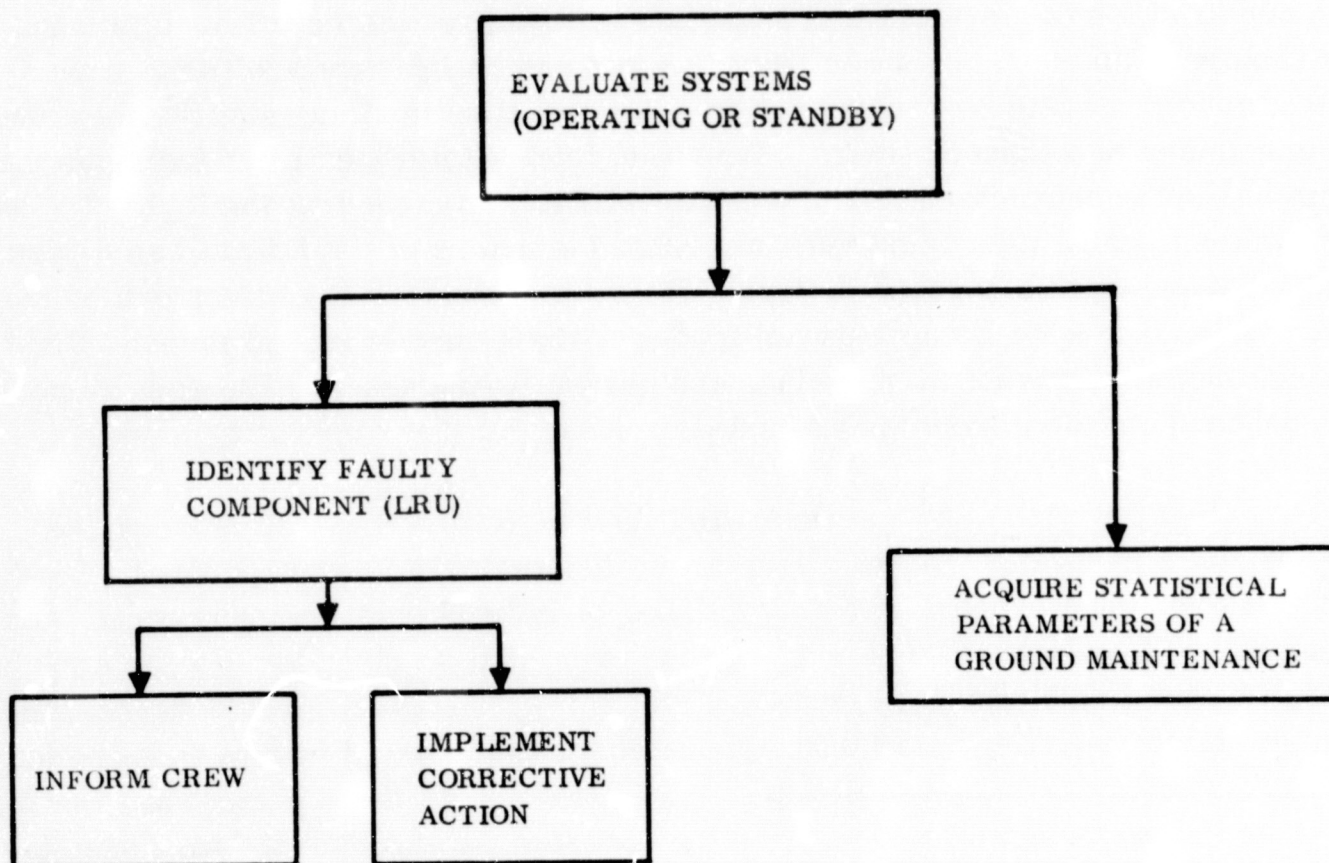


Figure 3-3. Performance Monitoring

3.3.2.2 Failure Data Presentation. The secondary objective of the performance monitor program is to present failure data to the flight crew. Two categories of information derived from the performance monitor program require enunciation. Information in the first category is automatically presented to the flight crew and identifies critical subsystem and system failures. In the severest case this would include data on failures that would jeopardize the mission performance. However, not all failures will be automatically presented to the flight crew. The general rule determining automatic display is that failure information will only be presented for which the flight crew can take action. This eliminates from the displays a large portion of minor subsystem failures.

The second category of displayed data resulting from the performance monitor program is a failure summary. This information is not automatically available but must be requested by the flight crew. This summary will also be of extreme importance to maintenance personnel.

3.3.2.3 Maintenance Data Acquisition. The tertiary objective of the performance monitor program is to acquire data for maintenance activities. Vehicular failures and operational parameter data will be recorded. The failure data will be used to assess failure modes, while the parametric operational data will be used in predictive analysis. Some predictive analysis will be performed to assist in preventing inflight failure.

3.3.3 POSTFLIGHT SECURING. Postflight securing is an assigned function of the onboard checkout system (Figure 3-4). The checkout system assists the flight and ground crew in deactivating the vehicle. This includes detanking propellants and reactant fuels as well as assisting in shutting down the subsystems. Upon completion of the shutdown but before final power disconnect, the onboard checkout system would verify that all the subsystems are properly secured.

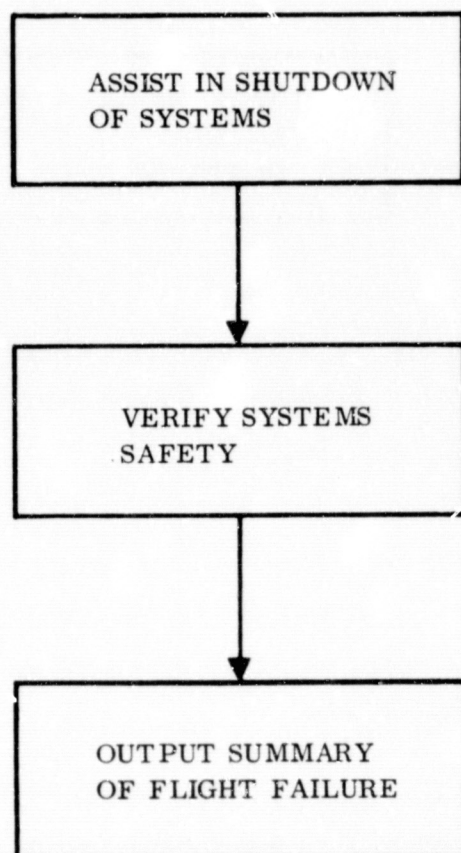


Figure 3-4. Postflight Securing

based computers and skilled personnel. The onboard checkout system compiles the parametric data during operational conditions and transfers the intelligence to the ground computers.

Both of the objectives may be automated to virtually any level of fault isolation, but their practical economic and weight constraints limit the depth of fault isolation to be achieved onboard. As an example it is probably sufficient to localize a failure to a subsystem component and not to the piece part within the component. This constraint produces a ground rule of fault isolation: isolate faults within a subsystem to the lowest level unit that can be conveniently removed from the vehicle.

The onboard checkout system places primary emphasis on subsystem control and functional evaluation. To adopt this to the maintenance mode, additional instrumentation and logic are required, which may be added at very minimal increase in weight.

An important aspect of the postflight securing mode is the compilation of the flight failures into a maintenance action report. This report will list all failures occurring before and during the flight. Listing will be by components or component groups.

3.3.4 MAINTENANCE ASSISTANCE.

The maintenance assistance mode is a natural extension of the onboard checkout system. A commonality of instrumentation and computer logic exists between each of the functional modes that allows the system to be used in the maintenance mode.

The maintenance assist program (Figure 3-5) has two primary functions; the first is to isolate a failure to the lowest practical level within a subsystem, and the second is the prediction of potential system failures. This failure prediction appears best accomplished by ground-

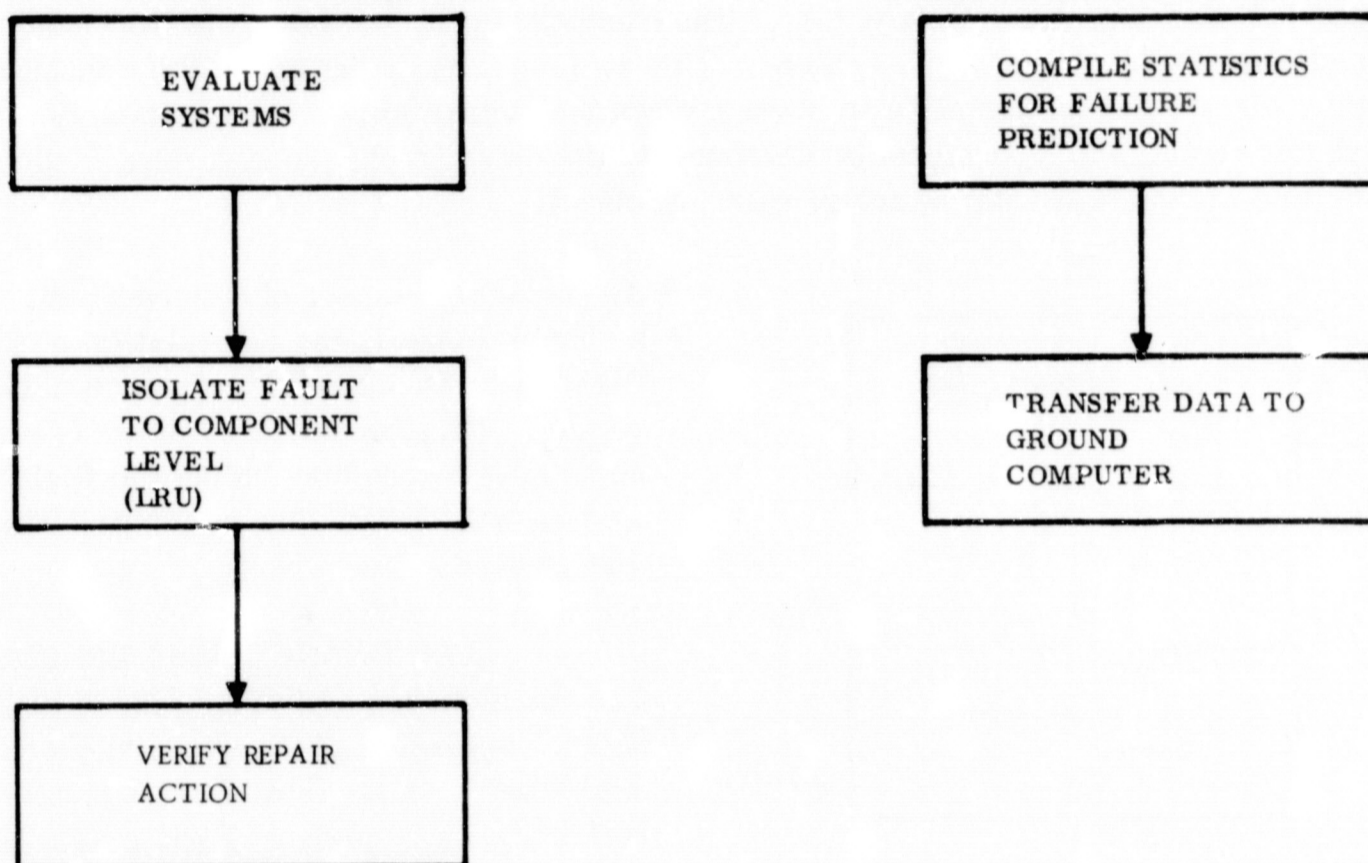


Figure 3-5. Maintenance Assistance

However, some types of instrumentation can reduce the system reliability. This produces a rule of thumb; i.e., no instrumentation will be added solely for the maintenance mode that degrades system reliability.

Careful attention must be directed toward the additional computational logic for the maintenance assistance program. The logic required is essentially a subset of the logic for the checkout function.

In the area of multiple failures, the logical process becomes quite complex. This is especially true in the continuous systems because of multivalued variables and the interrelationship of closed-loop functions. In order to avoid unreasonable software costs for a multiple failure isolation, the operator will assist in the diagnostics. In fact, the ability of skilled maintenance personnel will be used extensively in multiple failure isolation.

3.4 CHECKOUT CRITERIA

One of the goals of the onboard checkout study is to establish criteria by which proposed checkout ideas, techniques, and implementation may be evaluated. Criteria are needed to determine what to check out and how to perform the check out. The ideal

process for establishing criteria is very basic. It is the same, theoretically, as for any information system. The fundamental rule is: Gather enough data, but only enough data, to make the decisions. Therefore, the analysis begins by determining the decisions that have to be made. We then determine what knowledge is needed to make these decisions. Necessary knowledge is obtained from evaluation of data that are properly gathered, processed, and displayed.

The ultimate criteria for assessing the checkout system, its hardware, and software can be stated in terms of the checkout system's effect on three fundamental measures:

- a. Probability of crew/vehicle survivability.
- b. Probability of accomplishing assigned mission.
- c. Total program cost.

However, these criteria are expressed at a too high level of abstraction to be applied directly to specific problems. It becomes necessary, then, to develop lower level criteria that can be directly applied to design requirements, evaluation of solutions, etc.

Checkout criteria are selected to satisfy the purpose of each mission phase. Candidate criteria are evaluated to see how well they fit these purposes. It can be expected that checkout criteria will change with mission phases.

3.4.1 PRELAUNCH CRITERIA

- a. Detect all faults within a subsystem that affect redundancy reserve or could impact the mission.
- b. Determine the magnitude of the fault in any subsystem that could continue to operate in a degraded mode.
- c. If the fault can be corrected by switching to redundant hardware, the fault should be isolated to the lowest level at which redundancy is available.

Ground Rules

- a. No ground test equipment.
- b. No ground support personnel assistance.
- c. Subsystem not operated during prelaunch operation should be evaluated.
- d. Prelaunch checkout must be accomplished in reasonable time (target 60 minutes without faults).

Prelaunch Development

In the prelaunch checkout process, whenever a fault occurs three alternatives are possible:

- a. Fly with fault as is.
- b. Do not fly — make repair.
- c. Need more information before decision to fly or not fly can be made.

Consequence (b) "make repair" requires that fault be isolated to enable an acceptable type of repair, for example, to replaceable unit(s).

Consequence (c) "need more information" requires additional testing and may possibly call for judgement by pilot.

Checkout criteria for the prelaunch phase are selected to meet these objectives.

3.4.2 FLIGHT PERFORMANCE MONITOR CRITERIA

- a. Detect and display all faults that will result in decision to abort or to implement an alternate mission plan.
- b. Isolate all faults to the lowest level at which corrective action can be implemented.
- c. Monitor and evaluate at sufficient frequency to determine faults and implement corrective action before damage to other subsystems occurs.
- d. Monitor and evaluate subsystems whose operation is required at a future time in the mission early enough to implement corrective or alternate action.

Ground Rules

- a. Subsystem should be evaluated in passive (nonoperating) mode if it will be required in a scheduled future flight phase.
- b. Minimum disturbance of the flight crew.
- c. No instrumentation will be used that materially reduces the subsystem reliability.

Flight Performance Monitoring

During any mission phase, whenever a fault occurs, the possible decision to be made are:

- a. Continue with the mission.

- b. Abort.
- c. Implement an alternate mission plan.

Choice (a) "continue with the mission" can be selected when the fault does not sufficiently diminish mission success probability, usually expressed in terms of mission ground rules, to warrant the other alternatives. The reasons for this choice might be that redundant equipment or modes are available, or that the function was not critical. Urgency of peculiar missions may dictate a decision to continue the mission with increased risk despite a fault that normally would call for a different decision.

Choice (b) "abort" may be selected because the probability of accomplishing the assigned mission or alternative missions is below an acceptable level. The reasons for this choice may be because a critical failure has occurred, or insufficient redundancy remains available.

Choice (c) "implement alternate mission plan" is elected when the probability of original mission success is not sufficient, but alternate missions are available for which sufficient success probability remains.

Performance monitoring criteria should be selected and evaluated on the basis of 1) how well they help the crew in the decision process affecting the conduct of the mission, and 2) how well they help identify the more immediate consequence and aid implementation of the proper corrective action.

3.4.3 MAINTENANCE ASSISTANCE CRITERIA

- a. Detect failures within the subsystem and isolate without ambiguity to a failed replaceable unit.
- b. Determine the operability of subsystems and assure the potential of flight operations.

Ground Rules

- a. Repair of a single failure must result in a single break within a subsystem.
- b. Maximum use of control, prelaunch checkout, and performance monitor instrumentation will be made for maintenance assistance.
- c. Instruments may only be added for enhancement of subsystem reliability.
- d. Where ground support equipment is required, it must not have any opportunity to interfere with the subsystem normal operating mode.

Maintenance Assistance

The decisions that have to be made in the onboard maintenance phase are:

- a. Does equipment require maintenance or repair action?
- b. If yes, which replaceable unit needs to be replaced?
- c. After replaceable units have been replaced, is the subsystem ready to operate properly?

The effects of assistance to maintenance are in two areas:

- a. Cost — including factors usually stated in other terms that are readily translated into cost.
- b. Time — as related to mission assignment (for example, rescue) rather than as related to cost.

Implementing instrumentation to assist maintenance has its negative side as well. Criteria needs to be established to prevent compromising probabilities of crew/vehicle survivability or mission success just for the sake of maintenance ease.

3.4.4 INSTRUMENTATION CRITERIA

- a. Instrumentation must fail safely.
 1. Instrumentation failure must not damage subsystems.
 2. Failure of an instrumentation to measure properly (false reading) must result in normal operation of the subsystem.

3.4.5 CRITERIA PROBLEMS. Some test situations exist for which criteria are difficult to establish, despite the fact that the elements for the criteria can be identified. The difficulty arises because we cannot readily attach values to all the elements. For example, consider a subsystem comprising several replaceable units. Assume that the instrumentation and fault isolation process are straightforward only to the point where the failure is determined to be in one of the two replaceable units. Assume that further isolation to one or the other of these two replaceable units is much less obvious, let's say, because of the added weight, or reliability effect. The solution, then, is a trade study based on the specific conditions of the program. Eventually, criteria to evaluate solutions for such situations can be developed, but not before a number of such cases are examined in detail. Past programs are only a guide from which projections might be made. They indicate that for electronics equipment isolation to a specific replaceable unit may be practical in 95-97% of faults encountered. For non-electronic hardware, a lower percentage is anticipated.

3.5 CONCEPT DEVELOPMENT

Developing the hardware for a system that effectively evaluates vehicle health is reasonably achievable with current state of the art. This is manifest in current ground checkout equipment used on the present space programs. The principle area of difficulty in the present program is to compress the man-machine operations into the operational vehicle. It is obvious that the role of man must be sharply curtailed, and this creates an increase in the automation logic.

In analyzing the development of the present ground checkout systems, it is apparent that the data management and software costs far exceed those of the hardware. This was evident when man was extensively included in the evaluation loop. It must be anticipated that the data management function will increase, because the operator activities are curtailed when the checkout system is totally self-contained.

In order to create the optimum system, design priority must be directed toward the task of data management. This does not imply that the hardware is ignored, but the emphasis is on data management with the hardware adapting to the requirements of the software.

Several unique features in the baseline data configuration tend to ease the impact of data handling. One is that all the vehicle systems are operated and controlled by the central computing facility. Communication between the computer and the systems is digital and transmitted over a multiplexed data bus. This provides data in the correct format at a convenient point for processing. Data processing is accomplished in the central computer, thereby diminishing the need for special processing equipment. This commonality of use of the central control computer is economical if the checkout function can use the computer during times of low system activities. A secondary benefit accrues from this configuration in that no special processing hardware is required for the checkout function.

3.5.1 SYSTEM TEST PROCESSES. In analyzing methods to perform the onboard checkout function, three basic test methods are identifiable (Figure 3-6). All subsystem testing is categorized into one of those methods or a combination of the three methods. The choice for a particular subsystem will be determined by tradeoff studies. The tradeoffs will consider the relative merits of implementing a particular test process as well as the impact on the vehicle data processing system.

3.5.1.1 Demandable Built-In Self Test. The first category, Type A or demandable built-in self test, uses test equipment designed and packaged within the subsystem.

This method is applied to subsystems that require status reporting over relatively long periods and is generally limited to electronic equipment. The primary advantage of this test system is the preservation of central data processing and data bus capacity. A secondary advantage is that it tends to expedite certain maintenance activities.

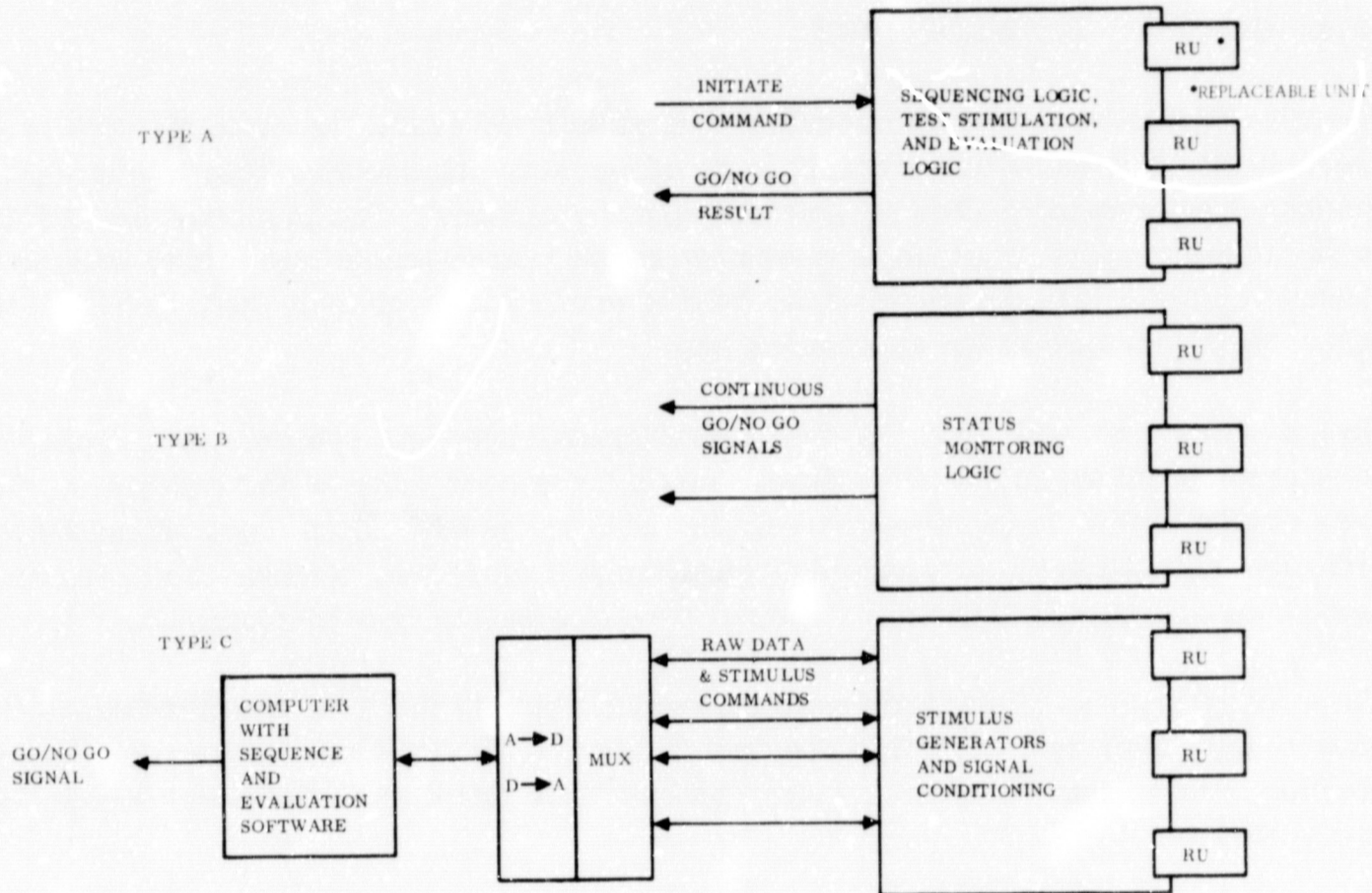


Figure 3-6. Test Processes for Onboard Checkout

One of the most serious disadvantages is the intermittent nature of the test and the resulting inability to detect intermittent failures. Another disadvantage is that being go-no-go, it gives no indication of approaching limits that indicate impending failure. This system also may impose a weight penalty which, in general, increases as a function of the thoroughness of the testing.

3.5.1.2 Continuous Built-In Self Test. The second category, Type B or continuous built-in self test, also uses equipment designed and integrated within the subsystem. Unlike Type A, this method continuously evaluates the system during operation. If a failure occurs, it interrupts the data bus, signalling the failure. This method is most efficient when the system under test has high data rates, or where the detection of intermittent failures is essential.

The primary advantages of this method are in the preservation of central data processing capacity as well as the transmission bus capacity. This method also eliminates the need for stimulus generators and the control sequencers. The most pertinent disadvantage is that the system must be operational to be evaluated.

3.5.1.3 Onboard Computer Test. The third category, Type C or onboard computer test (external to the system under test, but contained within the vehicle), uses the central computer for system evaluation. This requires that the data be converted to a digital signal and transmitted to the computer for processing. If additional hardware must be developed to achieve this, the process might be uneconomical. However, in the baseline configuration, the capability already exists as part of the vehicle control configuration. The use of the control configuration for checkout weighs heavily in favor of this test process in subsystem tradeoffs.

Stimulus generators are required in some of the systems, but these may be reduced in number, because the computer is capable of controlling all subsystems. Outputs of one portion of a subsystem might well serve as a stimulus to the portion of the subsystem under test.

This test method appears to be the only practical method of evaluating some of the vehicle's physical systems. This test type generally conserves weight and tends to reduce the unit cost for subsystem checkout. If it is possible to use the control computer for checkout during the computer's idle time, then only one major disadvantage exists. This disadvantage is the increased data management and software expenses during the development phase.

3.6 FAULT IDENTIFICATION METHODS

Several methods are used in fault detection and isolation to the lowest practical level. This methodology is defined as either direct or indirect examination of the unit under test (Table 3-1).

Table 3-1. Fault Identification Methods

Direction Examination
1. Component Instrumentation
2. Introspection
Indirect Examination
1. Functional Testing
2. Correlation Testing

3.6.1 DIRECT EXAMINATION. Direct examination is subdivided into two types: One is introspection and the other is component instrumentation. The method of introspection is generally limited to digital computers and systems with monitored voting logic. Introspection is the process whereby the subsystem evaluates itself using its own operational logic. This process is best demonstrated by the digital computer periodically inserting a test problem and determining its own health by the correct solution.

The component instrumentation method of fault identification uses instruments solely as a method of component fault detection. Essentially this is the "brute force" method and is resorted to when the other methods are impractical.

3.6.2 INDIRECT EXAMINATION. The indirect examination method uses all related information to isolate faults to a component or group of components. This information includes all intelligence available regarding the subsystem and components, then logical algorithms are used to locate the fault to the most probable failed component.

The majority of the subsystem checkout functions, as defined to date, will use the indirect fault identification method. This method can be further subdivided into functional fault isolation and correlation fault isolation. The functional methodology uses information obtained from within the subsystem. Information is obtained from the system status instrumentation and then analyzed to locate the most probable failed component or component group. If the fault is not localized to a component level, the computer selectively controls valving and the redundancy modes to refine the probable fault process. This continues, if possible, until the faulty component is located. Two or more related systems may produce similar functional outputs. In correlation fault isolation, the parameters of these systems are compared. System operational faults may be isolated to a parameter that deviates from the parametric group. The fact that the majority of control information is available in the computer(s) makes this test process an important means of evaluating system health as well as localizing faults.

Correlation testing is of importance in isolating faults in subsystems that contain built-in test equipment (Type A). For example, if a system indicates a fault, but the correlation analysis program suggests the system is operational, then the test equipment would be suspected.

3.7 PROGRAM DEVELOPMENT

The program structure was developed from the process requirements of the special emphasis study. This produced a basic algorithm set that operates effectively with the two subsystems that were studied in detail. It is expected that the program organization developed for these special emphasis subsystems will perform effectively for the remaining vehicle subsystems.

It became obvious from the study efforts that checkout is primarily concerned with detecting failures. Whether the failures are detected on the ground or in flight, the process of failure isolation is essentially the same. While the detection of the failure is not operating-mode dependent, the disposition of the failure is acutely mode dependent. This dependency dictates that a portion of the program, the fault disposition routine, must be variable (Figure 3-7).

These routines are dictated by the disparate needs of the analysis modes. Flight readiness, as an example, is concerned with identifying the failure so the crew can evaluate

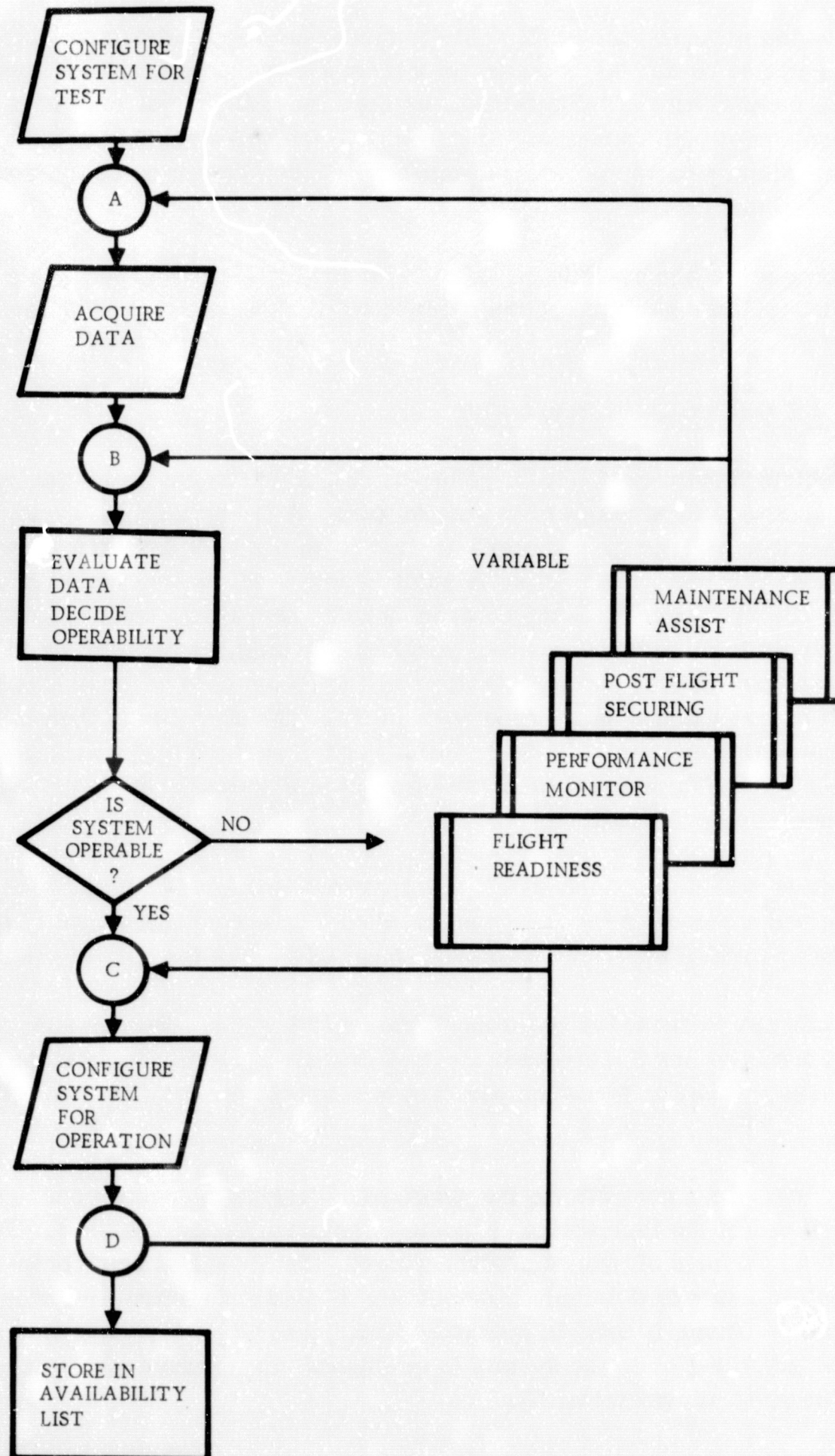


Figure 3-7. Fault Detection Program

the impact on the proposed mission. This implies that this specialized fault disposition program is going to be display oriented to present the intelligence to the operators. Performance monitoring fault disposition, as opposed to the flight readiness fault routine is concerned with reconfiguring the vehicle from one redundant mode to another. The only time display becomes involved is when failures jeopardize the safe performance of the scheduled mission.

The postflight secure emphasis is on safteying the vehicle after flight, while the maintenance assist fault disposition routine's emphasis is on isolating a fault for repair action.

3.7.1 FAULT DISPOSITION ROUTINES

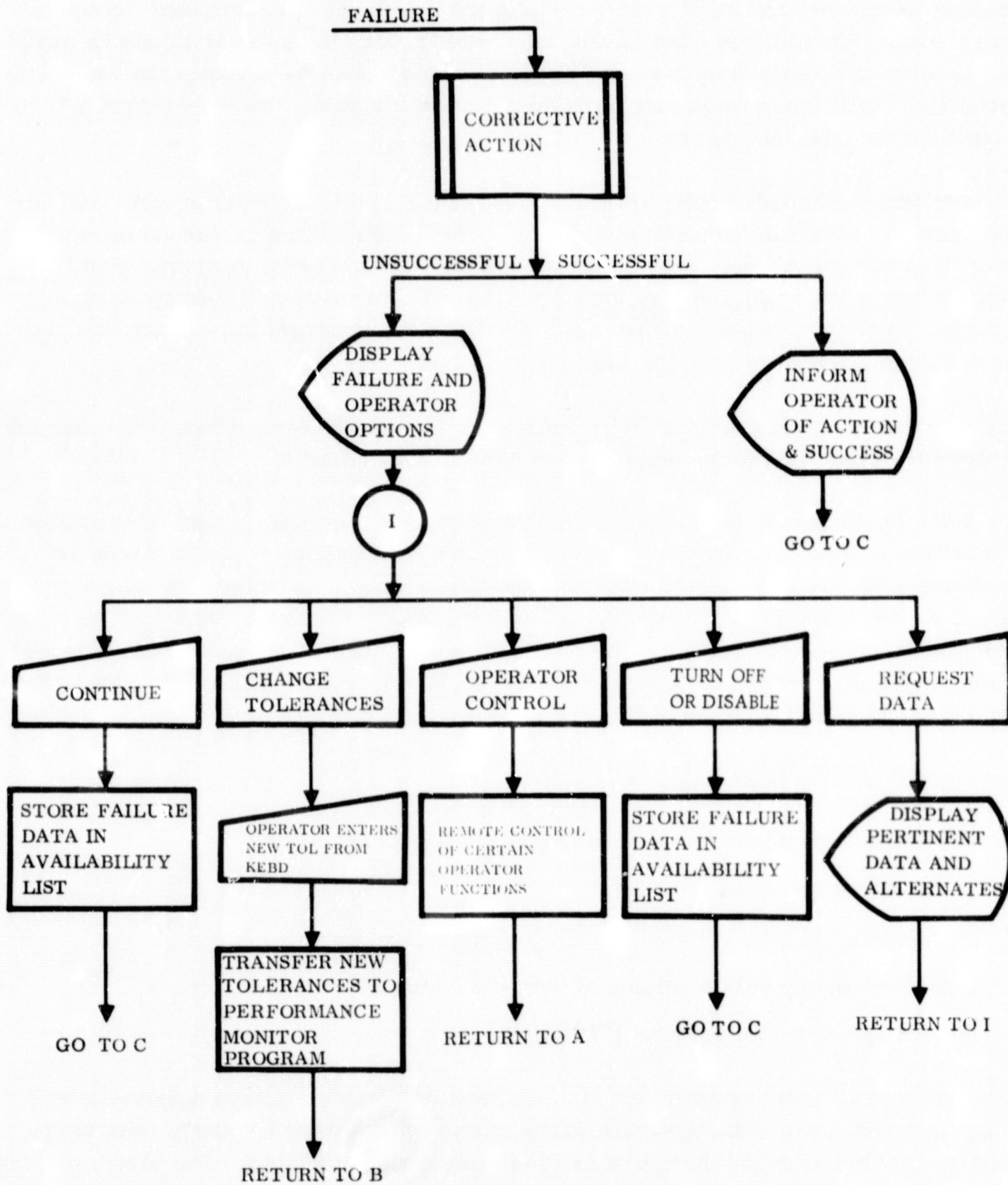
3.7.1.1 Vehicle Readiness Fault Disposition. Figure 3-8 illustrates the logic flow of the vehicle readiness fault disposition subprogram. A failure of a subsystem component to meet prescribed tolerances transfers control from the fault detection program to the fault disposition routine. The routine is entered with a corrective action subroutine. This routine attempts to restore the component to an operating state. This does not necessarily apply to all subsystems; but purging, bleeding, loads, etc., can correct some of the component deficiencies. Following the completion of these actions, the system must be evaluated to determine operability. The operator is then informed of the corrective action and the success or failure of the restorative process. If the process was successful, the fault disposition routine is exited and control is returned to the fault detection program.

If the corrective action is unsuccessful, the operator is informed of the subsystem failure and given a choice of five responses. Four of the responses modify the program, which in effect provides the operator dispositional control of the defective subsystem.

The fifth action is a request for additional data regarding the defective subsystem. The data request tabulates for the operator the test process, tolerances, and the results of the test process. Other information peculiar to a subsystem may be included, if pertinent.

A request for data does not advance the program. Program advancement is accomplished only if one of the four action requests is selected by the operator. The "turn off or disable" is a form of program advancement. This request shuts down the portion of the subsystem that was determined defective. It also set a warning flag so the subsystem cannot be normally used in operating situations. If redundancy modes exist, they would be activated when the system is configured upon return of control to the fault detection program (terminal C).

The "operator control" response turns over limited operations of the subsystem to the operator. In effect, it allows the operator to override computer controls so he can obtain a better understanding of the failure. The functions that the operator can control



NOTE: THE LETTERS A THRU D REFER TO POINTS ON FAULT DETECTION PROGRAM

Figure 3-8. Vehicle Readiness Fault Disposition

appear as options on the display. One of the options will be a request for a retest of the subsystem. This option returns control to the fault detection program. The "change tolerance" option, like the previous option, allows operator modification of the program. In this case, the tolerances for evaluating the subsystem can be modified to allow the subsystem to "pass" the test. This alerts the operator to a possible borderline condition by requiring positive action on his part. The subsystem will be flagged for maintenance action upon return to base.

For systems evaluated in the passive or nonoperating state, a separate operator action must be provided. The systems, being passive, can neither be turned off nor be controlled manually. Actually, the only significant action by the operator would be a verification of the receipt of a failure message. This is accomplished by an operator "continue" action response. This response allows the program to proceed, storing the subsystem failure flag in the availability list.

The "continue" option allows a faulty subsystem to continue to operate. This could be desirable if this subsystem output is used as a stimulus source.

3.7.1.2 Performance Monitoring Fault Disposition. The performance monitor fault disposition routine is activated upon a failure and, if possible, replaces the faulty hardware with a minimum disturbance to the flight crew. If a failure is being corrected by selection of a redundant mode, and if sufficient reserve redundancies exist, no message need be presented. The messages that should be presented are those for which the flight crew can take corrective action or are deemed essential to the operation of the vehicle (Figure 3-9).

The normal routine is as follows:

- a. After a failure determine available replacement.
- b. Activate the replacement.
- c. Verify that the replacement is operating satisfactorily.
- d. Shut down the defective portion of the subsystem.
- e. Record the above on the availability list.

Two alarm paths exist in which the fault disposition routine displays a message and requires a response. The highest priority alarm occurs when a system fails to operate to specification and there are no redundant modes available. The alarm message informs the crew of the subsystem failure and requires operator response.

There are two choices for action and a choice requesting further data. The action choices are: 1) a change in tolerance, or 2) a request for system shutdown. The second-level alarm informs the crew that no redundant mode exists. The crew responds to this second level warning by indicating that they have observed the message.

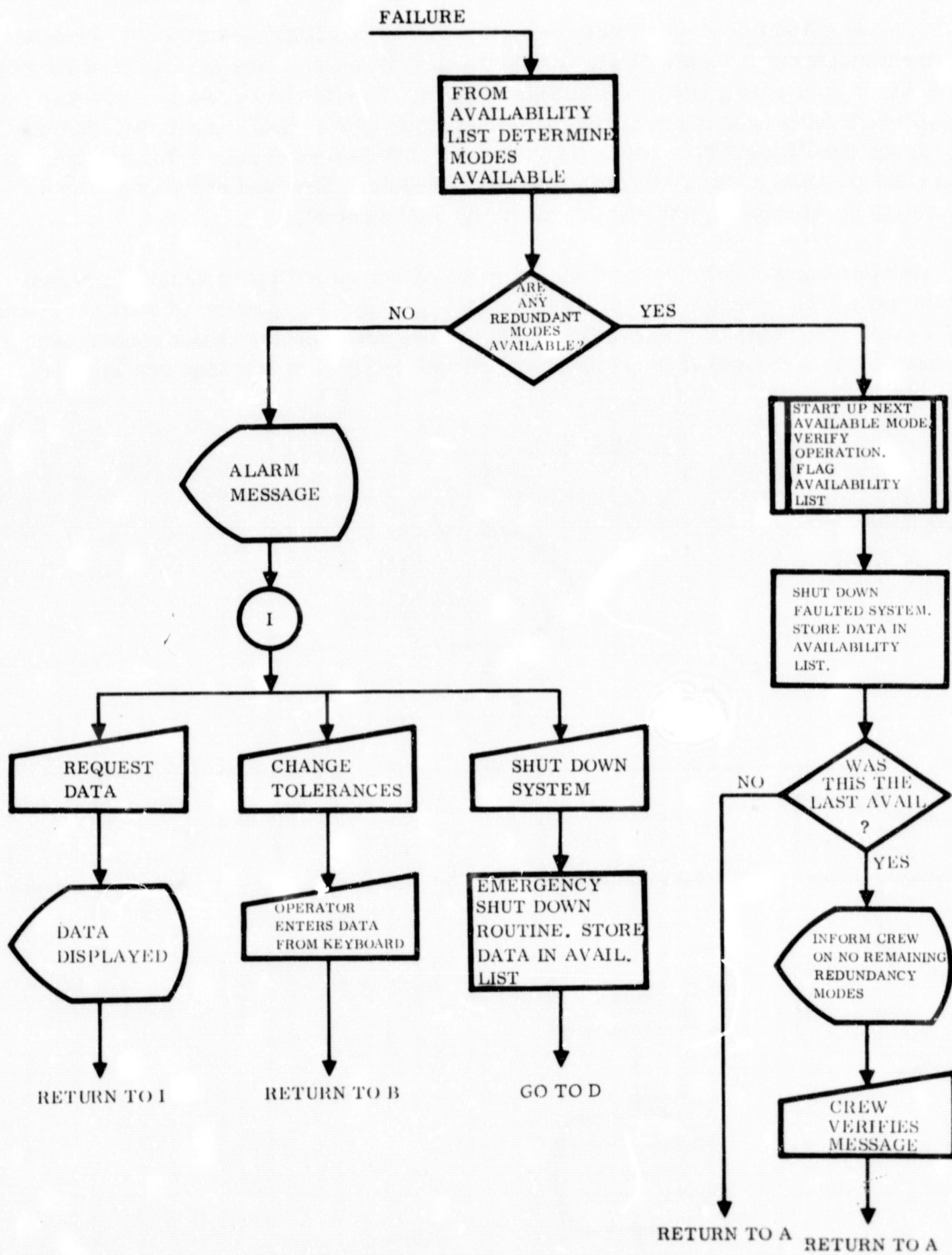


Figure 3-9. Performance Monitor Fault Disposition

3.7.1.3 Postflight Securing Fault Disposition. The postflight secure fault disposition routine's emphasis is on the display of alarm messages which are the result of the vehicle being in an unsafe configuration (Figure 3-10). This routine evokes a response from the operator for a decision regarding the disposition of the unsafe condition. In many cases, the unsafe condition can be flagged, but related circumstances that affect a decision must be made available to the operator. These are provided at the operator's discretion by depressing the "data request" function control.

The operator control option allows the operator direct inspection of vehicle parameters. In this mode, the operator not only obtains data but has the capability of subsystem control by use of the operator's keyboard. This allows the operator direct control over the unsafe situation until it is rectified or until sufficient data are acquired to make a decision.

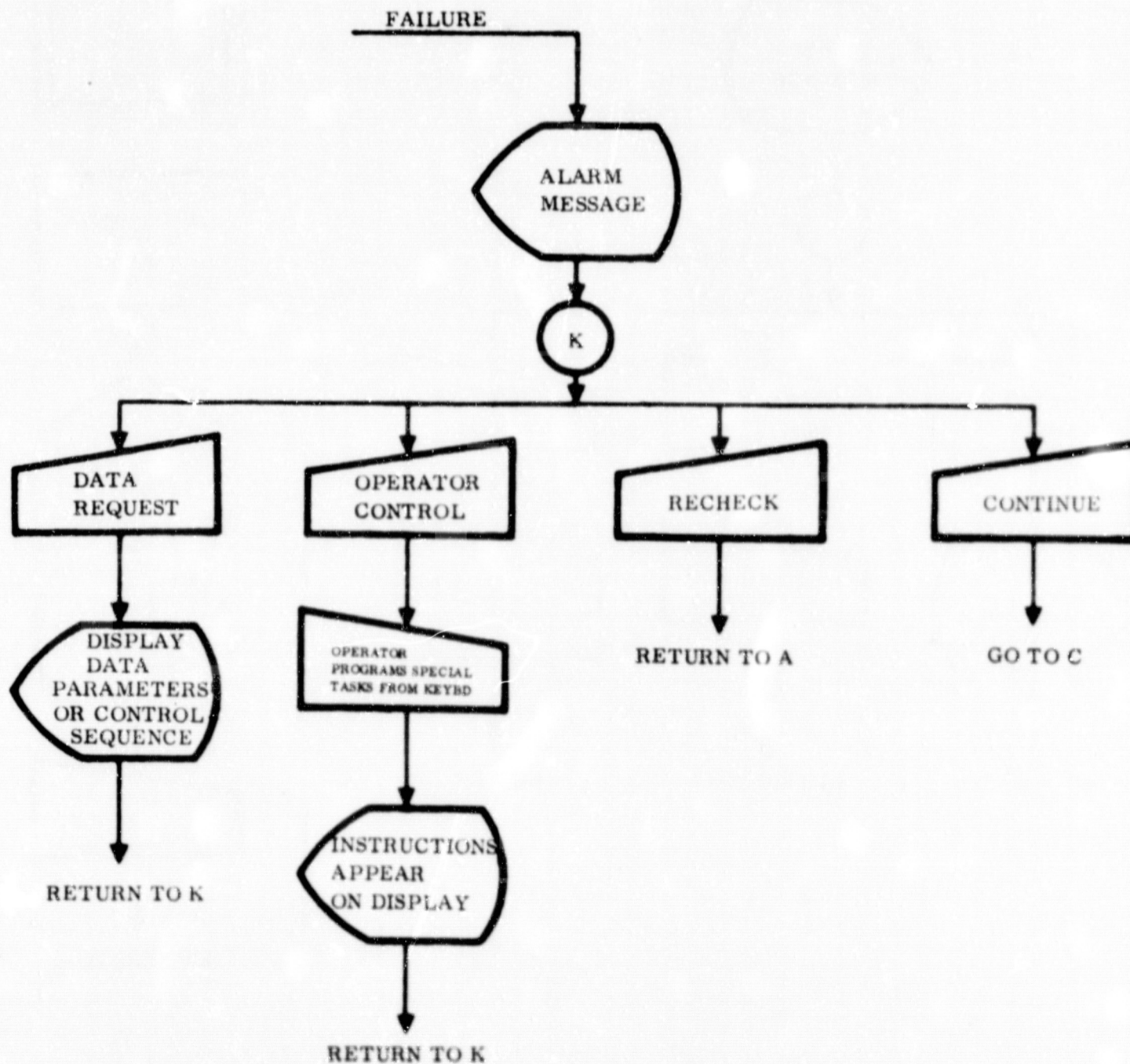


Figure 3-10. Postflight Secure Fault Disposition

If the condition was corrected by manual control, or if the operator's knowledge of the external situation leads him to believe that the system fault has been corrected, he would select the "recheck" option. This directs the fault detection program to re-evaluate the system. If the system is found to be in the proper state, the program continues normally. If the fault persists, the alarm flag will be reactivated. If no further action can be accomplished, or if the fault would require maintenance action, the operator would activate the "continue" mode. This allows the fault to remain on the display, but allows the fault detection program to proceed beyond the fault.

3.7.1.4 Maintenance Assistance Fault Disposition. The primary function of the maintenance assistance fault disposition program is to identify a failure to the lowest practical level within the subsystem. The fault detection program, having identified a subsystem failure, transfers control to the fault disposition routine (Figure 3-11). Entry into this routine is through a fault isolation subroutine. This routine uses the control and fault detection instrumentation and the control functions to isolate the fault to the lowest removable component level. If the routine was able to isolate to the desired level, the identity of the defective component is displayed. If, on the other hand, the routine was unsuccessful in the isolation of the fault, computer control is given to the maintenance operator. When this is accomplished, the display indicates a subsystem failure and the fact that the standard program could not isolate the fault. The transfer from automatic to manual control is necessary, because all probable failure modes or combinations of failures are not programmed. The system uses the diagnostic capability of the maintenance personnel to continue fault isolation. The operator commands the computer, via a test language, to control the system and format the display. Subsystem test data is displayed to the operator and he continues to manipulate the system until he isolates the fault or faults. He then designates the faulty components to the computer and exits from the manual control program to the automatic fault detection program.

3.7.2 INSTRUMENTATION SELECTION

3.7.2.1 Instrument Commonality. During the development of this system, it became obvious that a commonality exists between the instruments necessary for control of the vehicle subsystems and the checkout instruments. This commonality exists because many of the checkout fault isolation requirements are present in the control function. Control is dedicated not only to operating the systems, but to implementing redundant modes following component failures. This redundancy control requires fault isolation instrumentation. An optional checkout configuration uses the control fault isolation instrumentation.

Requirements dictate that the control function have a higher priority in a conflict with checkout, but there is considerable latitude in the placement of both instrumentation types. Optimum placement of the control instrumentation would allow it to be employed in the checkout phase. In this respect, it might be desirable to complicate the logic necessary to process the checkout data to permit common instrumentation. This

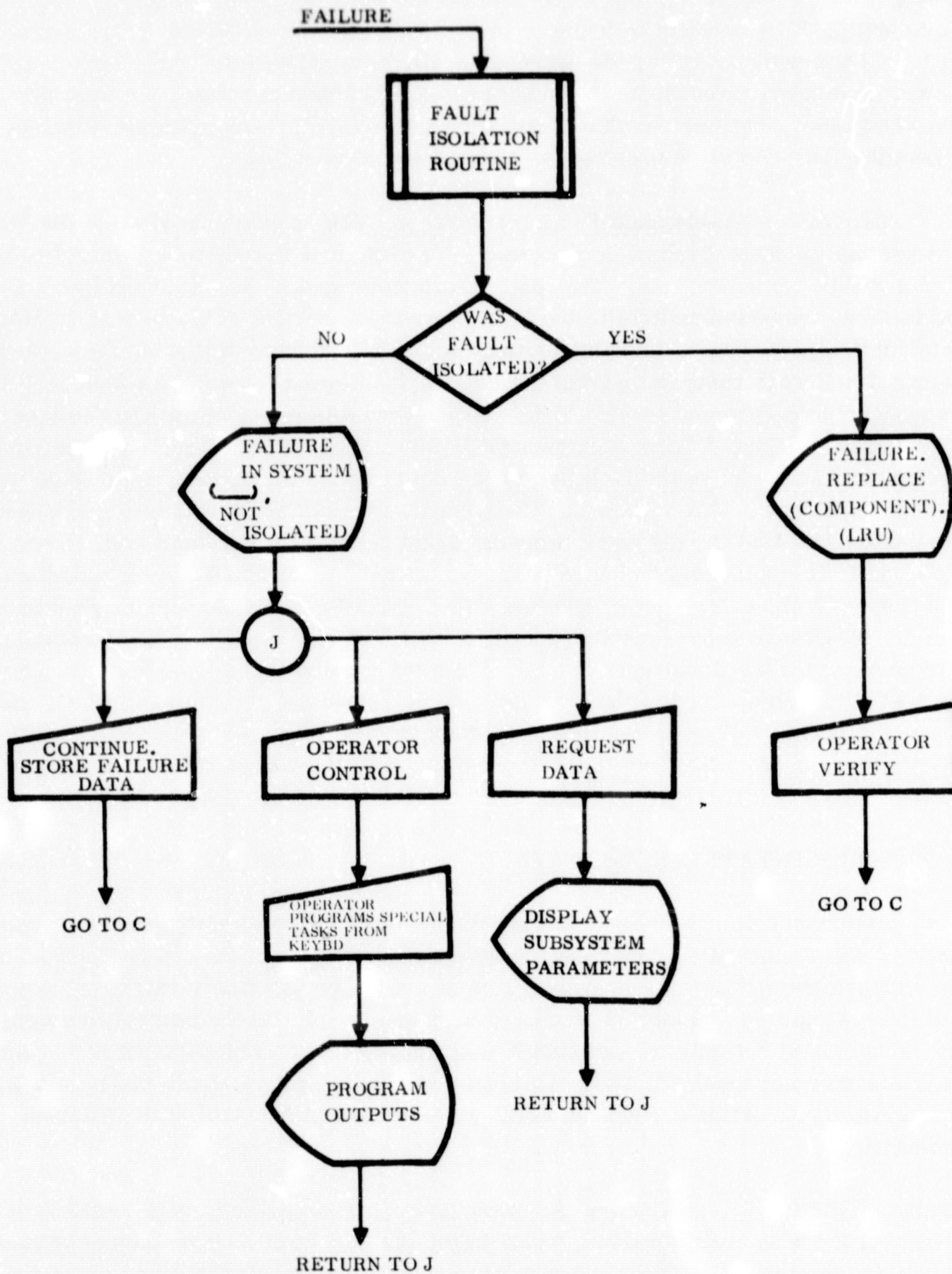


Figure 3-11. Maintenance Assistance Fault Disposition

expansion of logic is natural, as the inherent vehicle processing capacity is relatively large and can accommodate the additional logic capacity. Many of the programs can also be implemented sequentially; and with no time constraints, the additional logic has little operational significance.

3.7.2.2 Test Point Determination. A failure-modes-and-effects analysis should be used to determine the location of the subsystem test points. The instrumentation can be placed to monitor the most critical failure modes or subsystem and vehicular effects. Fault isolation considerations would also be used to determine the measurement assignment. This should be accomplished during the conceptual design phase, because it allows test instrumentation to be included as part of the basic system. It is generally impossible to add internal test instrumentation without a major redesign effort.

3.7.3 IMPENDING FAILURES. The detection of an impending failure is a consideration during the performance monitoring mode of operation. This process should be implemented when it is effective and meaningful to have information relating to the probability of continued mission success. With redundant systems, the decision to continue a mission in the event a failure is predicted will be dependent upon where in the mission such a prediction is made. It is implied that for impending failure detection, one or more subsystem parameters undergo a measurable change. In general, the deterioration of the subsystem would be indicated by a migration of the data toward the tolerance limits. For the failure mode where the subsystem is characterized by an apparently instantaneous catastrophic failure, research will undoubtedly uncover some parameter that can be used for prediction.

Two predominant methods exist for implementing failure detection processes. One method employs the philosophy of the static near limit or caution limit. In this approach, a second set of fixed amplitude tolerances is inserted into the evaluation hardware. These tolerances are arranged so that a warning or caution flag is indicated before the subsystems deteriorates to the point of exceeding the final specifications. The second method of impending fault detection is through the use of trend analysis. This is similar to the maintenance assist failure prediction method. The impending fault detection method compiles statistical data during early operating phase of the mission. This data would be evaluated for the rate of progression toward failure. The rate toward failure, once established, would be extrapolated to determine probable time to failure. This time to failure would be tested against mission time remaining. If it becomes apparent from this analysis that a failure occurs during the remaining portion of the mission, the equipment would be flagged with a caution warning.

3.8 SYSTEM DESCRIPTION

The onboard checkout system is a functional entity only and requires no major equipment on board the vehicle. Essentially, the checkout operates within the hardware confines of the vehicle control data system and exists fundamentally as a software function.

The onboard checkout system, Figure 3-12, uses three major vehicle equipment groups during the test process. These are the cockpit controls and displays, the vehicle central computing facility, and the system under test. These are integrated into an operating system by a multiplexed data bus, which is the transmission media between these devices.

The system is activated by an operator who enters a computer instruction from the cockpit keyboard. This consists of alphanumeric instructions as well as discrete control inputs. The operator-initiated control signals are coded for transmission to the computer on the multiplexed data bus.

The cockpit controls, as well as the vehicle subsystems, require a buffering device for operation on the multiplexed data bus. This device is the data bus interface (DBI), which is uniquely organized for each subsystem in which it operates. The DBI translates incoming digital data to signals that operate the subsystem. The DBI also translates the signals from the subsystem components into a common digital language for transmission to the computer. Translation of input signals is accomplished by decoding the instructions and test signal words and converting these, after checking, into signals directly usable within the subsystem under test. The DBI recognizes its unique address, demultiplexes, checks parity, and converts to analog or discrete signals. In the transmission mode, the DBI converts and encodes test and identification signals, adds parity, and multiplexes the signals into the data bus.

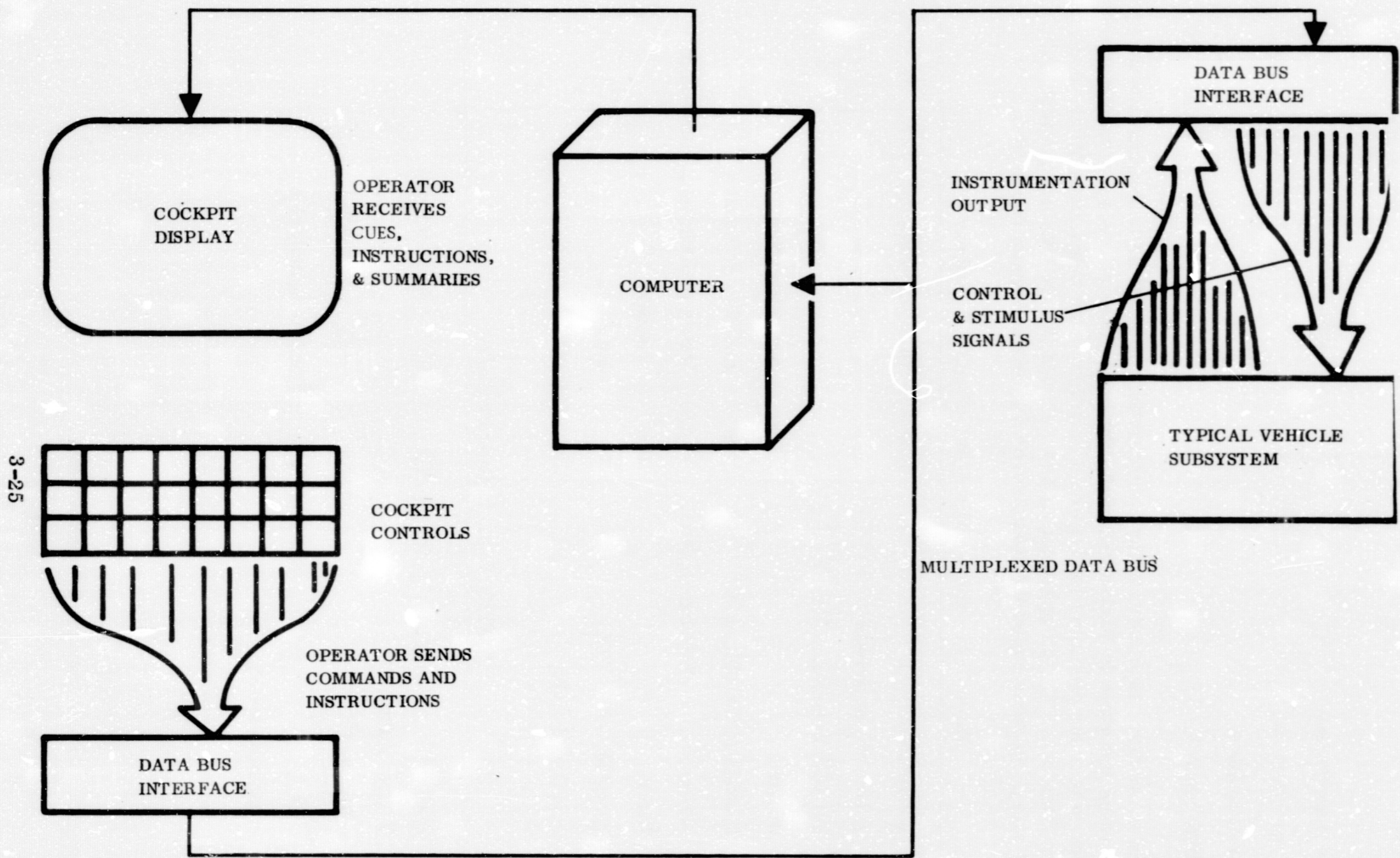
The multiplexed data bus, a high-speed digital transmission link under computer control, serves all vehicle systems. For checkout, this bus transfers command and test signals between the DBI, computer, and display.

The system under test contains all the test instrumentation stimulus generators necessary in the test process. Manipulation of the subsystem's controls are also possible in the performance of the test, but this manipulation is exclusively under computer control. The computer requests the control functions, stimulus requirements, and data conversion; then it evaluates the status of the subsystem. The status of the subsystem tested is then presented to the operators on the cockpit display.

3.9 SPECIAL EMPHASIS SYSTEMS DESCRIPTION

3.9.1 ENVIRONMENTAL CONTROL/LIFE SUPPORT SYSTEM. This section describes the baseline environmental control life support system (EC/LSS) in terms of composition, normal operation, failure modes, failure sensing, and the redundancies and backups for restoration of function. The subsystems of the EC/LSS thus described are:

- a. Atmosphere supply and pressurization control.
- b. Atmosphere purification.
- c. Water Management.



3-25

Figure 3-12. Onboard Checkout Subsystem

- d. Waste management.
- e. Food management.
- f. Personal hygiene
- g. Thermal control.

Each of the subsystems is illustrated by a schematic. Symbols and abbreviations used on the diagrams are given in Tables 3-2, 3-3, and 3-4. The rationale for redundancies and backups is to make provision for failure in functions such that a first failure does not require mission abort (fail operational) and a second failure does not prevent safe abort (fail safe). In some cases there are several levels of backup capability.

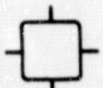

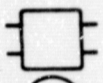







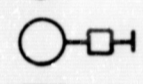


Table 3-2. Abbreviations and Chemical Symbols

A	accumulator	HX	heat exchanger
a	absolute, as in psia	L	liquid, as in LO ₂
ACF	activated charcoal filter	LiOH	lithium hydroxide
Ag	silver	MF	multifiltration unit
BAC	benzalkonium chloride	psi	pounds per square inch
D-50	Dowex 50 ion exchange resin	WMS	water management subsystem
F	filter	Po	position
G	gaseous, as in GO ₂	S	sterilizer
g	gage, as in psig		

Table 3-3. Sensor Symbols

Ⓟ	pressure	Ⓡ	electrical current
Ⓣ	temperature	Ⓥ	voltage
Ⓠ	quantity	Ⓢ	electrical conductivity
Ⓛ	flow	Ⓟ	position indicator
Ⓡ	rotational speed		

Table 3-4. Component Symbols

	or		shut-off valve
	heat exchanger		remotely-actuated valve
	pump		manually-actuated valve
	blower		selector valves
	check valve		
	relief valve		remotely-actuated valve with manual override
	pressure regulator		flow restrictor

3.9.1.1 Atmosphere Supply and Pressurization Control. Figure 3-13 shows the major components of the subsystem. The O_2 is stored in four vessels, of which one is redundant. Table 3-5 lists other redundancies. The N_2 is stored in two vessels with no redundancy. Figure 3-13 also shows the concept of sensor locations for automatic checkout.

Description of Operation. Multiple insulated vessels, located external to the cabin, store cryogenic O_2 and N_2 . Pressure within the vessels is maintained supercritical by a combination of heat leak through the insulation and internal electrical heaters. Uninsulated accumulators for the gases provide some capability for rapid flow response. The two-gas pressure control causes withdrawal of the gases from storage such that partial pressures of O_2 and N_2 are maintained within their respective control bands. The flows are from the gas accumulators through components in sequence as follows: 1) a filter; 2) a flow restrictor, which prevents flows greater than the capacity of the cabin pressure relief valve; 3) a first-stage pressure regulator: for the 50 psig N_2 gas only, and 10 psig for the O_2 ; 4) a second-stage pressure regulator for N_2 , which controls to 10 psig; and 5) the two-gas pressure control, which maintains O_2 partial pressure at 2.7 psi and cabin total pressure at 10 psia.

The cabin pressure relief valve vents gas to relieve cabin pressure greater than 10.5 ± 0.2 psig. It also provides negative pressure relief when the vehicle is descending into the lower atmosphere.

N_2 is supplied to the water management subsystem at 50 psig and at 10 psig for pressurization of expulsion devices.

First Failures, Atmosphere Supply and Pressurization Control

Insulation Failure in One Vessel (Figure 3-14a). Heat influx will cause rapid pressure rise and fluid loss by venting through relief valves. Loss is detected by quantity gaging

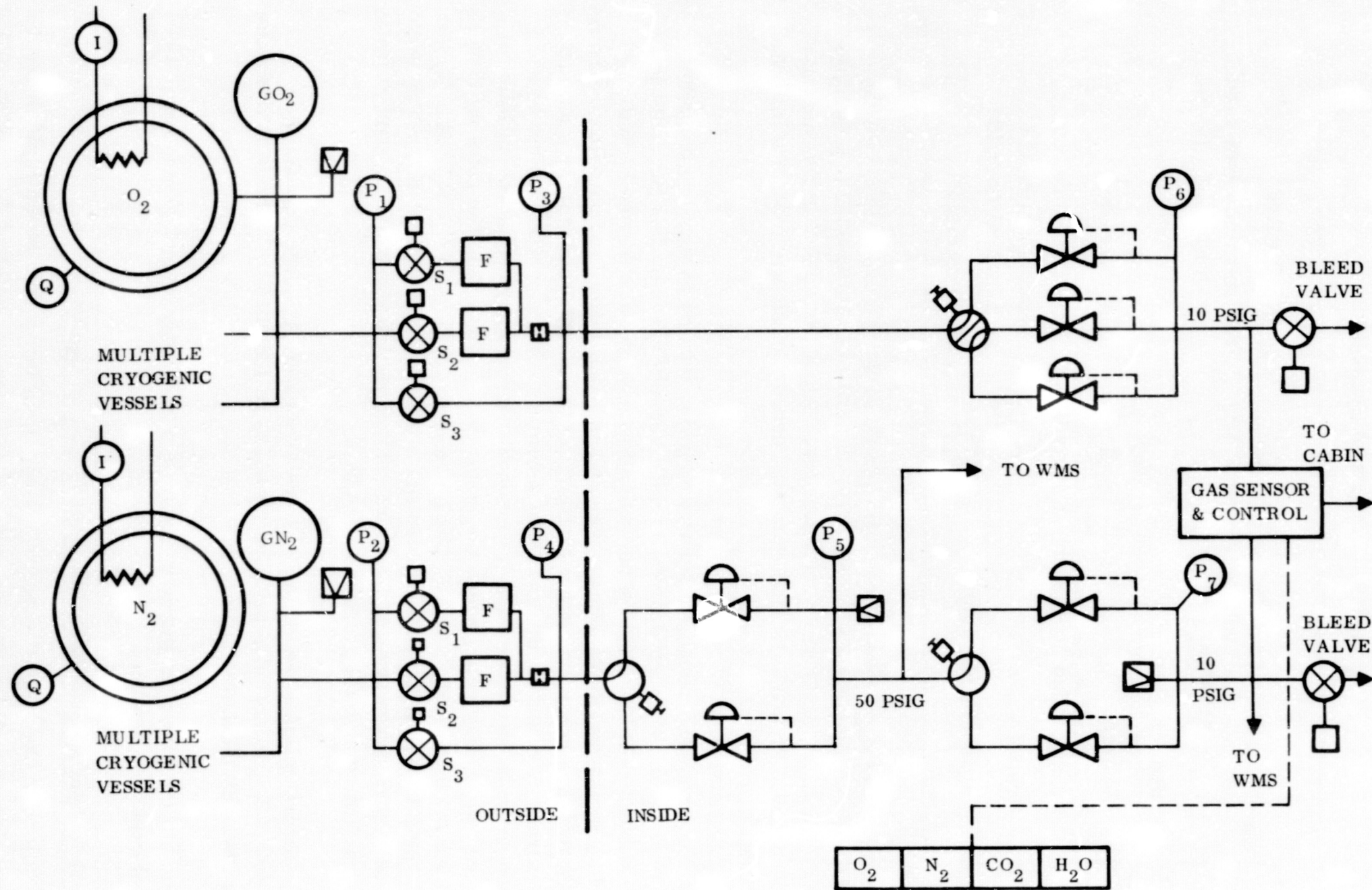
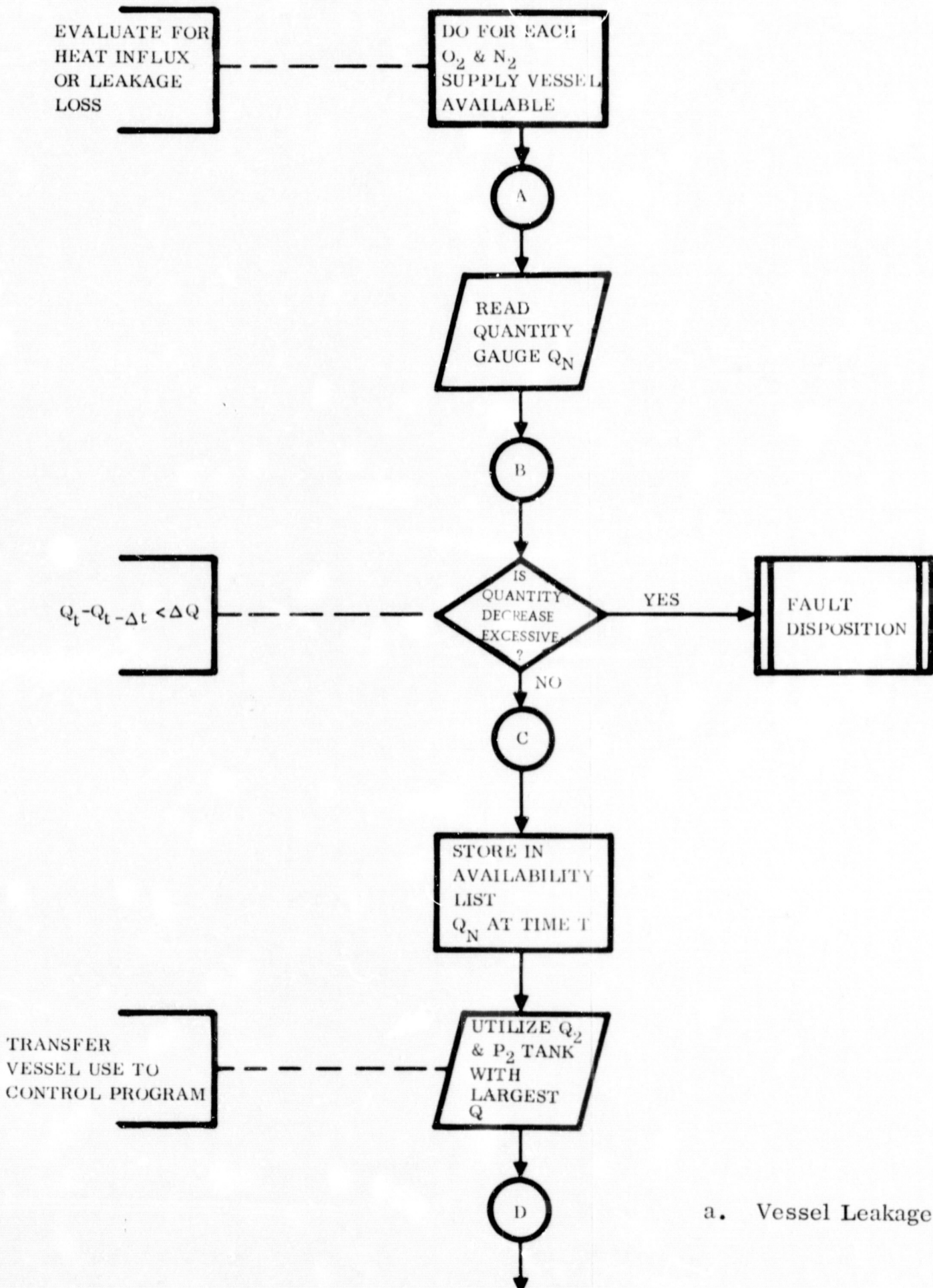
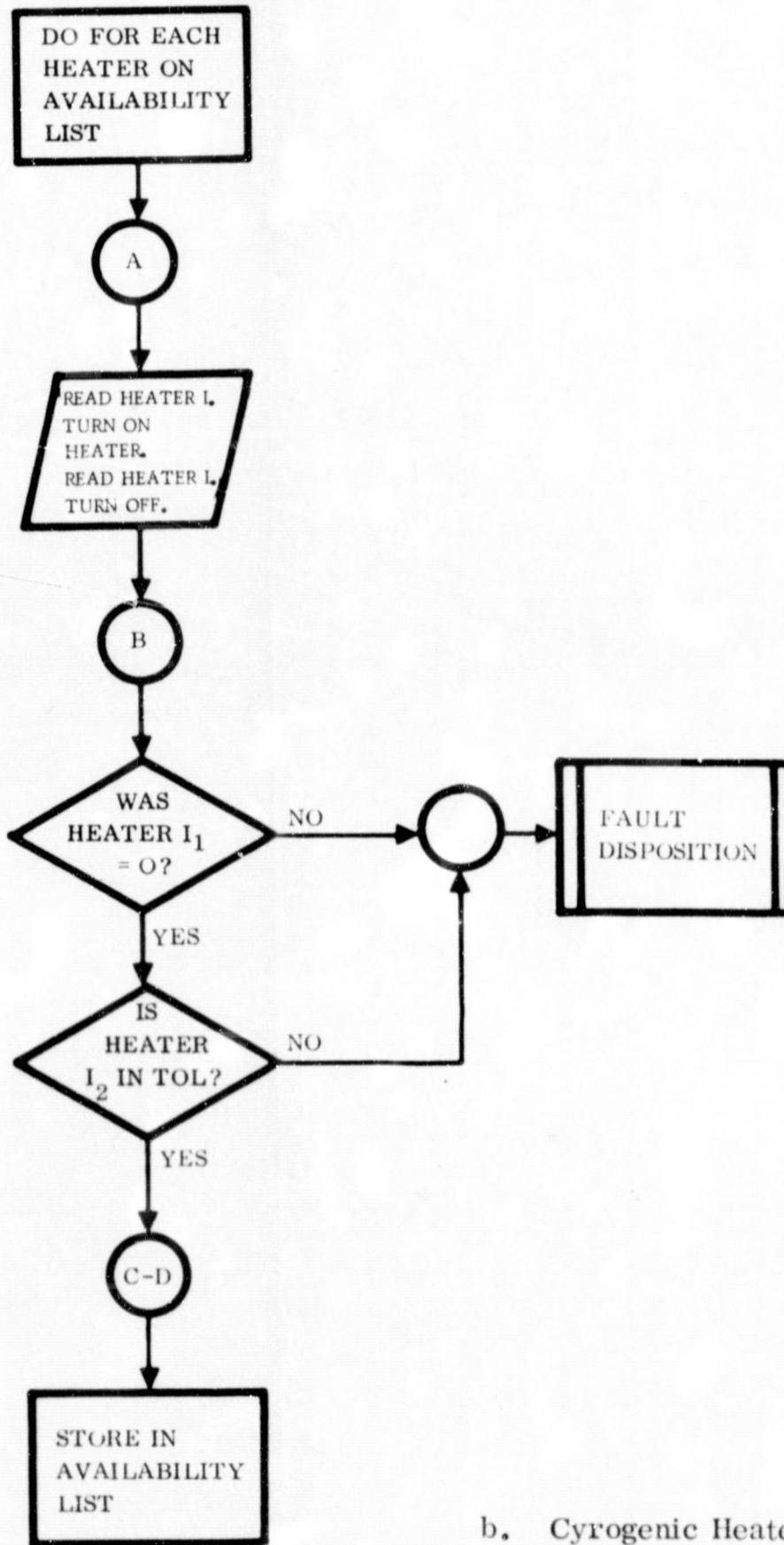


Figure 3-13. Atmosphere Supply and Pressurization Control



a. Vessel Leakage

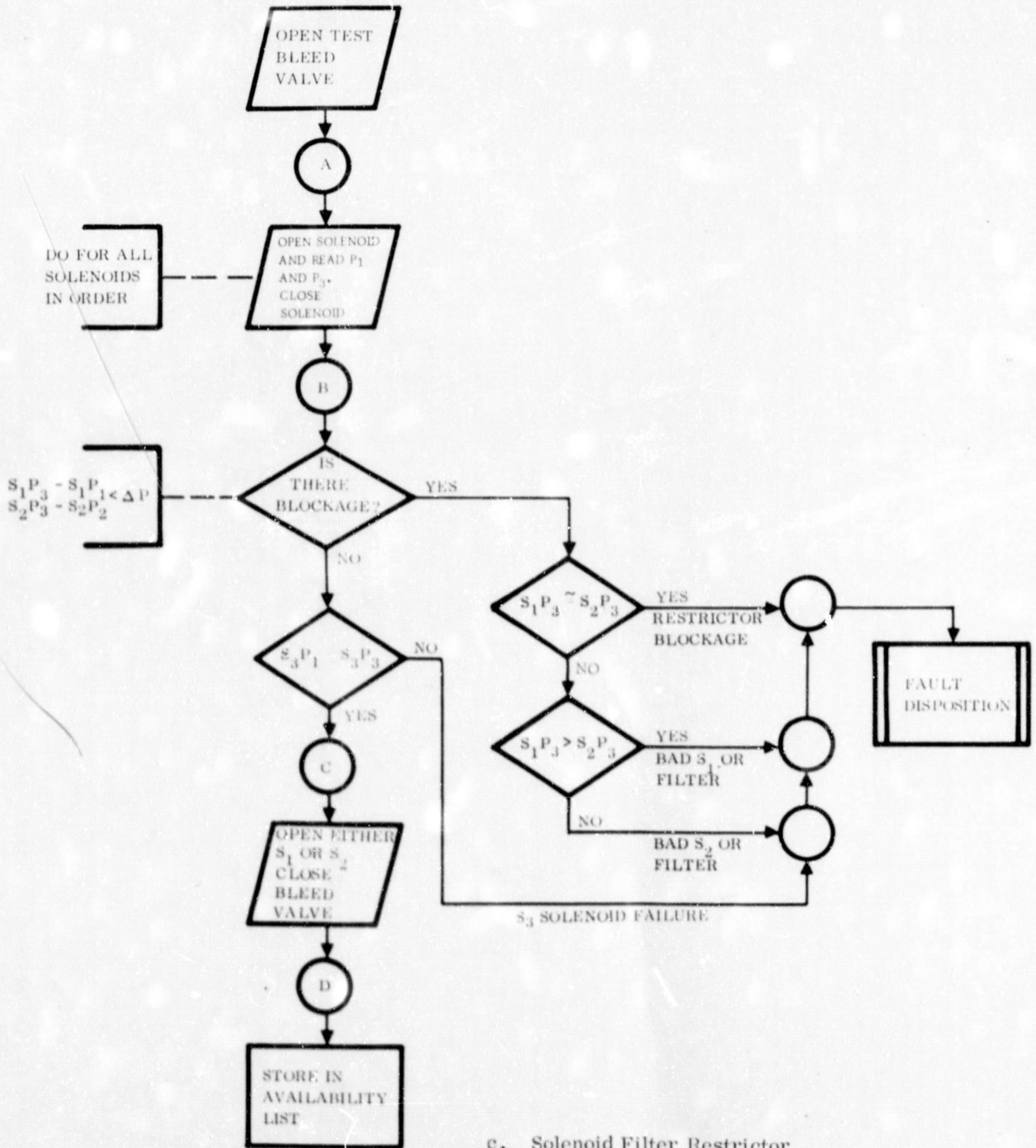


b. Cyrogenic Heaters

FOLDOUT FRAME 2

DO FOR
SOLENOID
IN ORDER

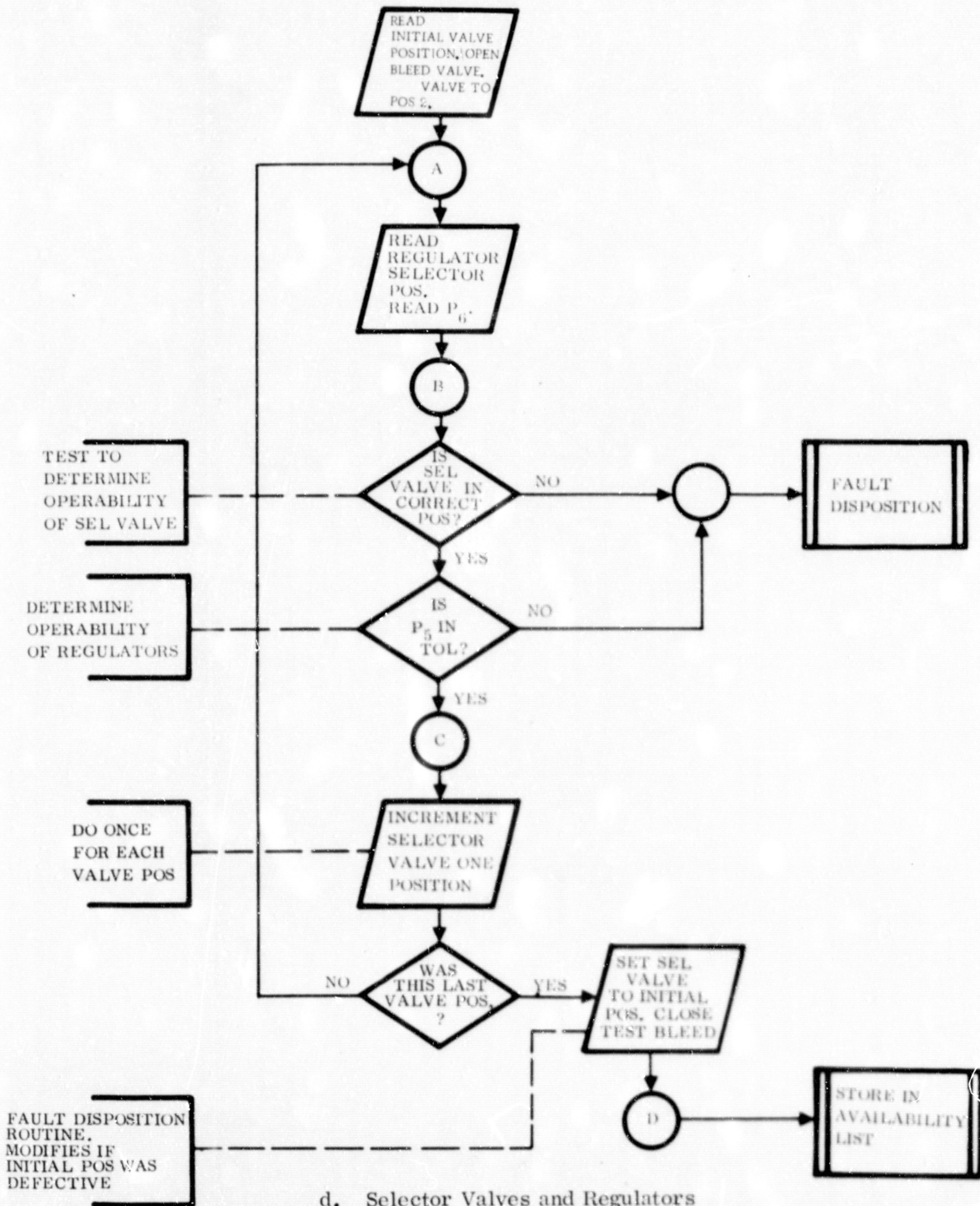
$S_1 P_3 - S_1 P_1$
 $S_2 P_3 - S_2 P_1$



c. Solenoid Filter Restrictor

DE
OF
OF

FAU
ROU
MOD
INIT
DEF



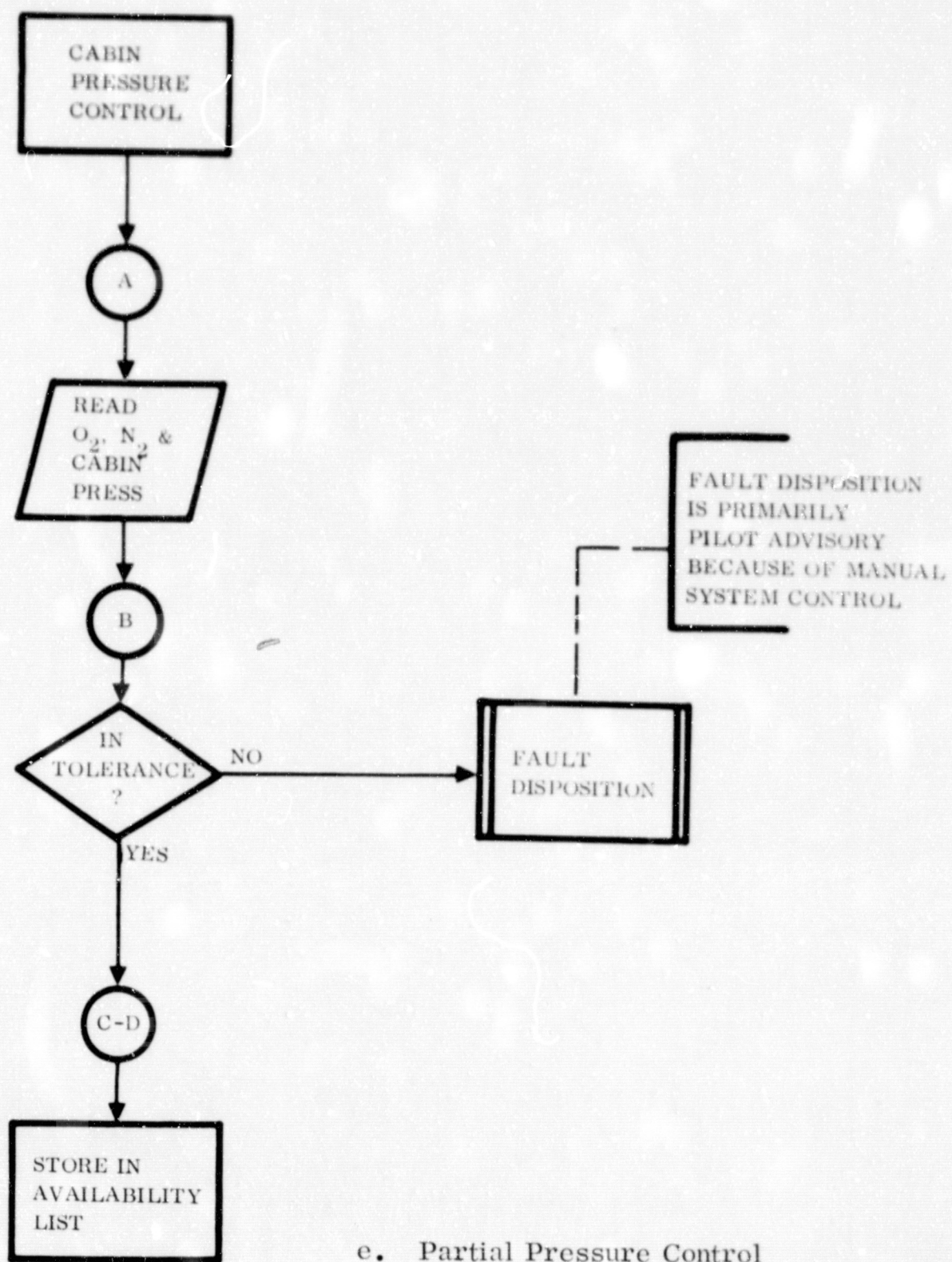


Figure 3-14. Atmosphere Supply and Pressurization Control Fault Detection Routine

Table 3-5. Atmosphere Supply and Pressurization Control Redundancies

Component	Redundancies
O ₂ cryogenic vessels	Multiple vessels, one redundant. Redundant heater in each vessel.
N ₂ cryogenic vessels	Multiple vessels, none redundant. N ₂ content of cabin atmosphere provides backup.
Cabin pressure relief valves	Redundant valves for inflow and outflow relief. Manual overrides for inflow and outflow.
Gas filters	Redundant filters. Filter bypass.
O ₂ pressure regulators	Two redundant regulators in each stage.
N ₂ pressure regulators	One redundant regulator in each stage. N ₂ content of cabin atmosphere provides backup.
Gas sensor and control	Redundant sensor and control elements. Manual overrides.
Other Functions	Backup
Cabin pressure integrity	Suit loop.
Pressurization for WMS	Separate gaseous N ₂ container.

in the defective vessel. Redundancy is such that sufficient O₂ and N₂ remains in other vessels to complete the mission. Capability to completely repressurize the cabin may be lost.

Leakage of One Vessel (Figure 3-14a). Loss is detected by quantity gaging. Redundancy is such that sufficient O₂ and N₂ remains in other vessels to complete the mission. Capability to completely repressurize the cabin may be lost.

Heater Failure (Figure 3-14b). Failure is indicated by measurement showing zero current in the heater. Each vessel contains a redundant heater, which is switched on to restore function.

Flow Restrictor Blockage (Figure 3-14c). Failure is detected by high Δp across the restrictor. Flow is restored by opening a solenoid-operated bypass valve. This valve is also opened to achieve high flow for rapid cabin repressurization.

Filter Blockage (Figure 3-14c). Failure is detected by high Δp across the filter. Flow is restored by opening the solenoid-operated valve to a redundant filter.

Failure of Pressure Regulators (Figure 3-14d). Failure open is detected by abnormally high pressure downstream of the regulator, and/or by opening the relief valve, which prevents over-pressure damage to downstream components. Failure closed is detected by abnormally low downstream pressure. Function is restored by actuating a selector valve that switches flow to a redundant regulator.

Two-Gas Pressure Control (Figure 3-14e). Failure is detected by periodic analysis of the cabin atmosphere for O₂ partial pressure and by reading cabin total pressure. An over-pressure failure is indicated by the performance monitor program and presented on the display for crew action. Function is restored by manual switching to redundant sensing and control elements in the unit.

Cabin Pressure Relief Valve (Figure 3-14e). Failure closed will cause the function to be assumed by a redundant relief valve. No switching is required. Failure open is detected by sound or by abnormally high flow from atmosphere stores. This failure is corrected by manual override.

Cabin Leakage (Figure 3-14e). High rate loss of cabin atmosphere is detected by sound or drop in cabin total pressure due to limited inflow. Low rate loss may be detectable only by periodic quantity gaging of atmosphere stores, which will show abnormally high use rate. High rate loss may be stopped or reduced by locating the defect and applying a sealant. Atmosphere stores have sufficient reserve to sustain a low rate loss without mission abort.

Second Failures, Atmosphere Supply and Pressurization Control

If a second O₂ vessel fails in a mode causing loss of supercritical fluid, sufficient O₂ is available in the cabin atmosphere and/or in other vessels to sustain the crew for several hours. If the failure is in the second N₂ vessel, sufficient N₂ will remain in the cabin so that no additional inflow is required. The N₂ partial pressure will decrease slowly due to leakage. Failure of the second heater in a vessel results in partial failure of the vessel. Gas will be delivered at a reduced rate as limited by heat leak through the insulation. Redundancy is such that sufficient O₂ and N₂ can be delivered from other vessels to complete the mission.

If a redundant filter fails by blockage, flow is restored by opening a solenoid-operated bypass valve. If a redundant O₂ pressure regulator fails, function is restored by switching flow through another redundant regulator. If the redundant N₂ regulator fails closed, N₂ partial pressure in the cabin is allowed to diminish slowly due to leakage. This does not create a hazard to the crew. If the regulator fails open, N₂ flow is stopped by closing three solenoid-operated valves upstream of the filters. If the redundant elements of the two-gas pressure control fail, manual overrides are used to admit O₂ and N₂ into the cabin periodically to restore correct partial pressures.

If a combination of failures is such that function of the primary N_2 source cannot be restored, the water management subsystem is supplied pressurant from a backup source. If serious leakage or a combination of failures is such that cabin pressurization cannot be maintained, the crew dons pressure suits that are connected into a suit loop for O_2 supply, atmosphere purification, humidity control, and temperature control. The same backup applies to gross atmospheric contamination, which may require intentional venting of the cabin without capability to repressurize.

3.9.1.2 Atmosphere Purification. Figure 3-15 shows the major components of this subsystem, which includes a pressure suit loop as backup to cabin pressurization. The redundancies are summarized in Table 3-6.

Description of Operation. Cabin atmosphere is circulated through the atmosphere purification loop by a motor-driven blower. Flow from the cabin is through components in the following sequence: 1) coarse and fine elements of a particulate filter assembly; 2) a canister containing an activated charcoal filter for removal of gaseous contaminants, and lithium hydroxide for removal of CO_2 ; 3) a cabin loop blower; 4) a pressure suit boost blower, which is inactive in the normal operating mode; 5) a humidity control heat exchanger, which cools the cabin atmosphere and causes condensation of water vapor to liquid droplets; and 6) a motor-driven separator, which delivers gas-free condensate to the water management system and liquid-free atmosphere to the cabin.

The pressure suits provide backup capability for crew survival if cabin pressurization fails for any reason, or if there is accidental gross contamination of the cabin atmosphere. To convert the atmosphere purification loop to a pressure suit loop, the suit hoses are connected, and the loop is isolated from the cabin by closing two valves. A suit boost blower is switched on to compensate for added pressure drop through the suits. A valve is opened to provide O_2 , which flows through a regulator for control of suit pressure. The suit loop is vented for sufficient time to purge most of the N_2 and enrich O_2 to at least a normal partial pressure.

The expendable CO_2 absorbers have a capacity of 36 manhours. Once each 9 hours the crew will remove a spent cartridge and replace it with a fresh one.

First Failures, Atmosphere Purification Loop

Particulate Filter (Figure 3-16a). The particulate filter receives almost no loading in normal operation. A channeling or by-pass type failure reduces effectiveness and may be detected by an abnormally low Δp across the filter. A blockage or contamination-type failure will require removal of the failed filter elements, and may be detected by an abnormally high Δp across the filter.

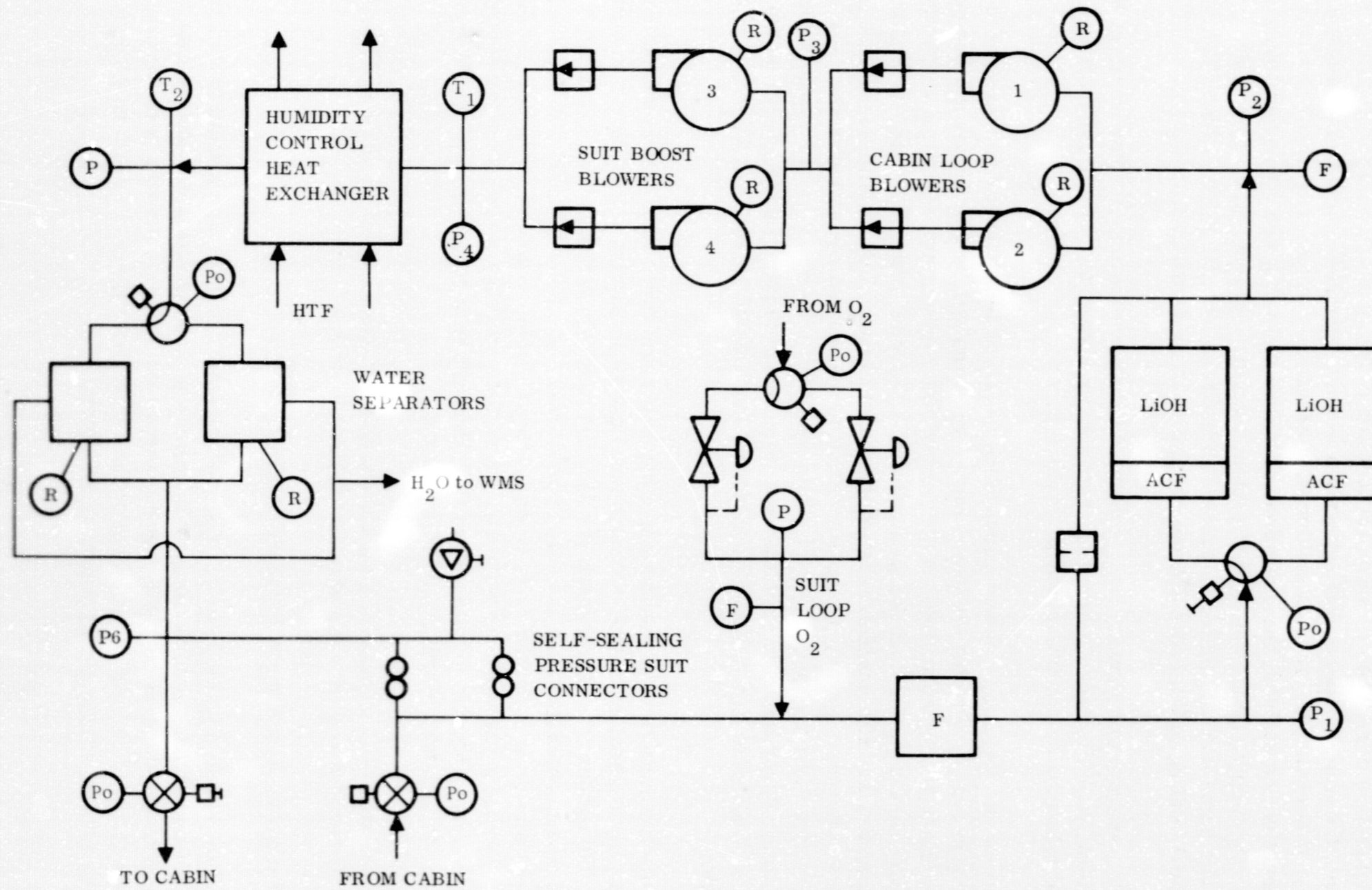
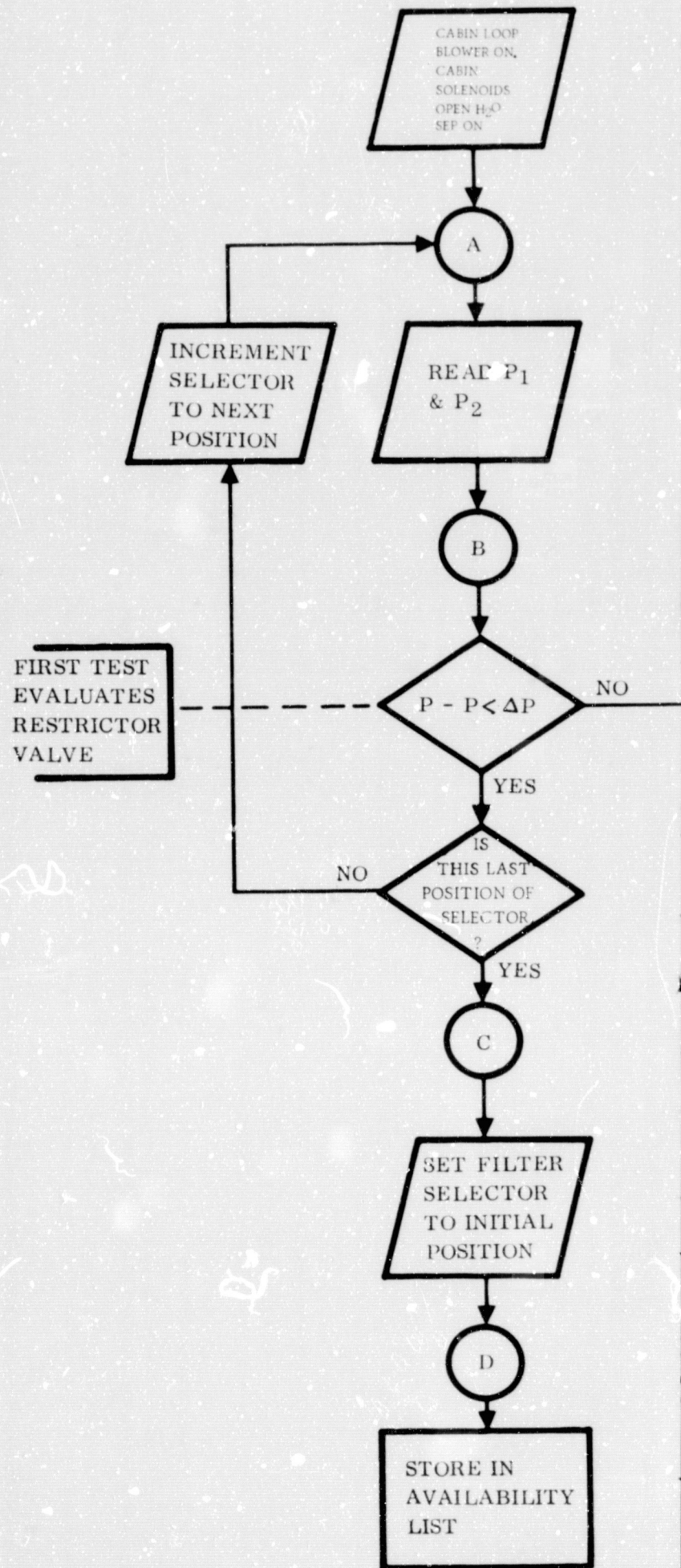
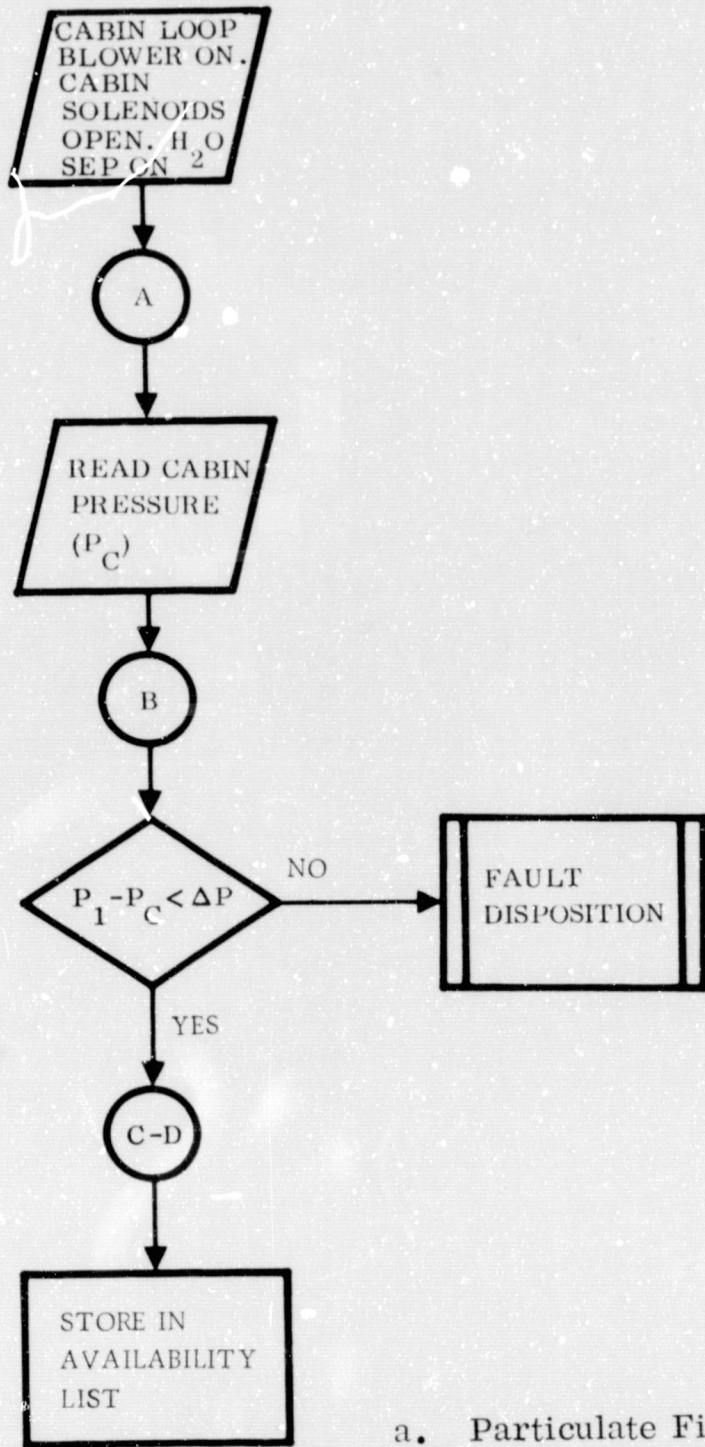
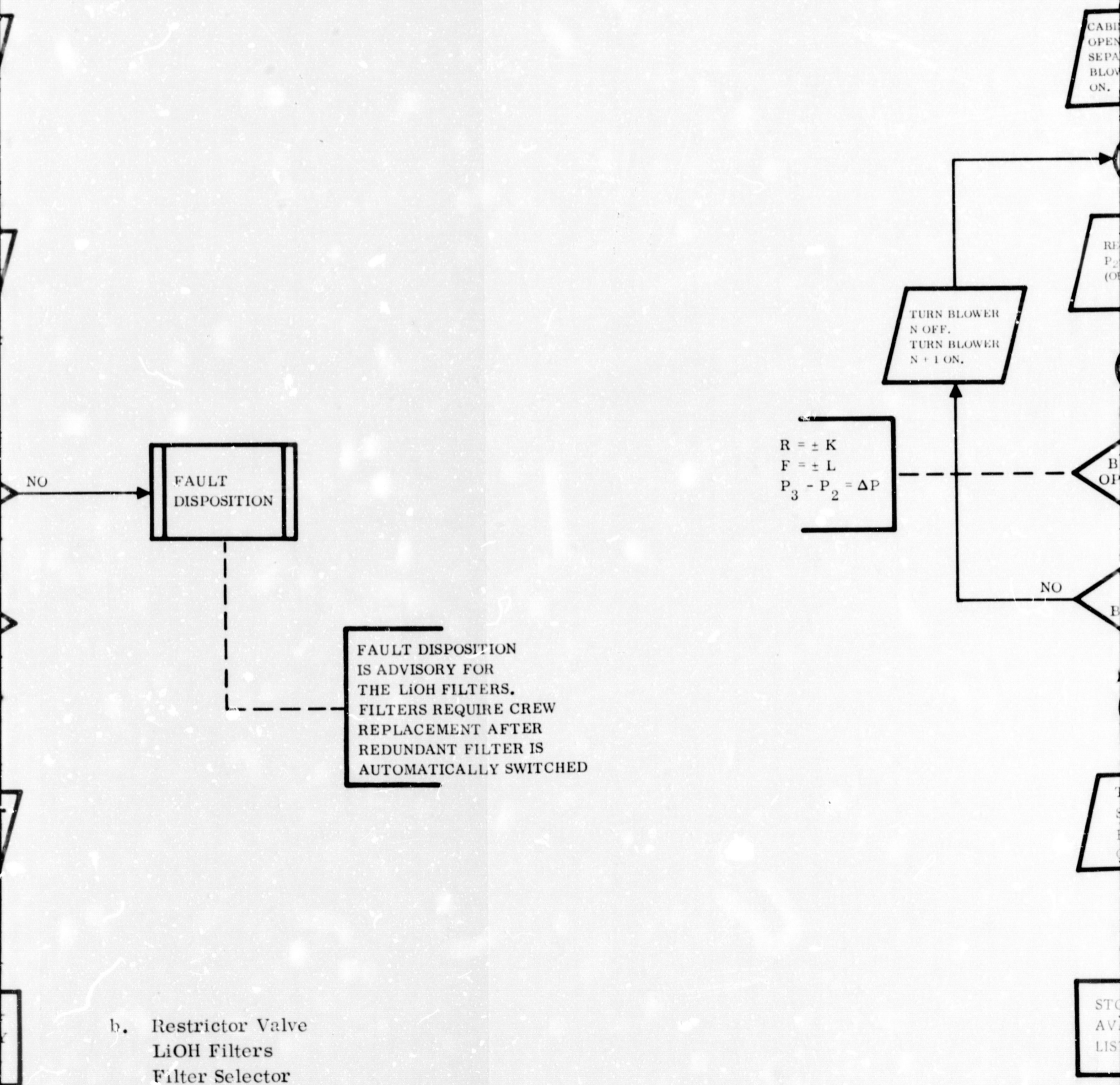


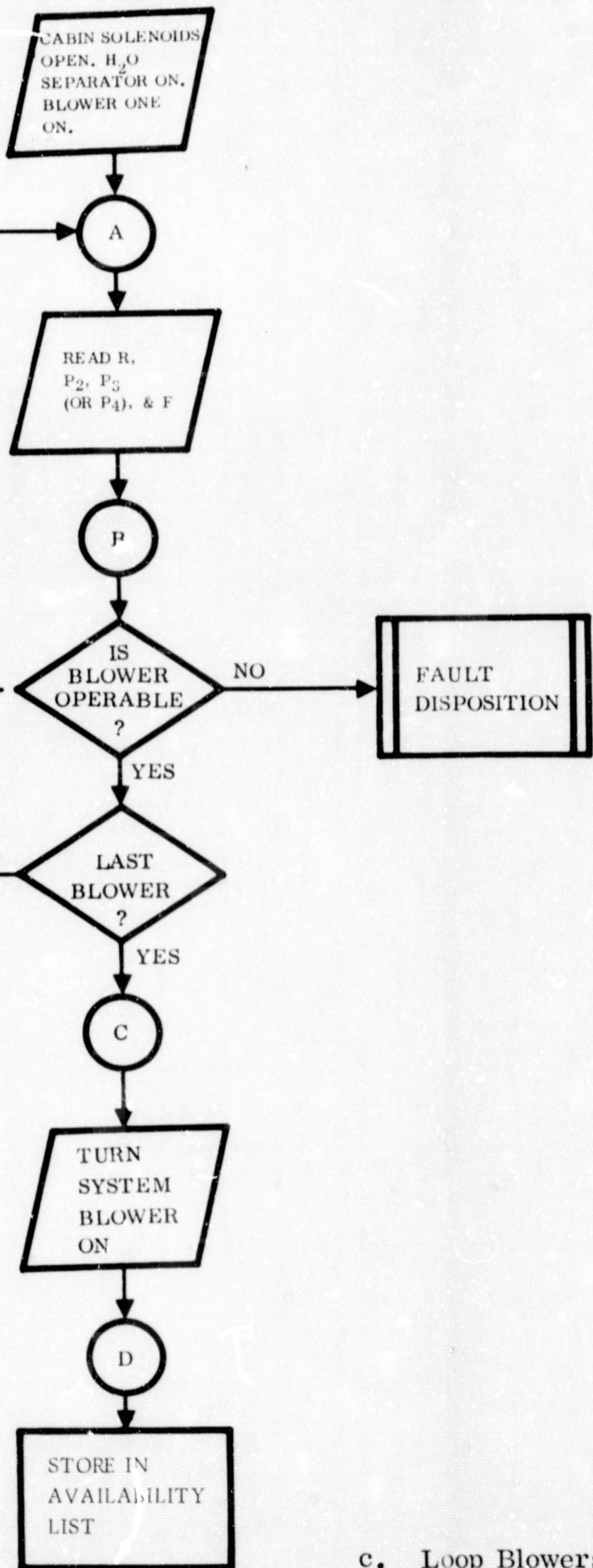
Figure 3-15. Atmosphere Purification Loop



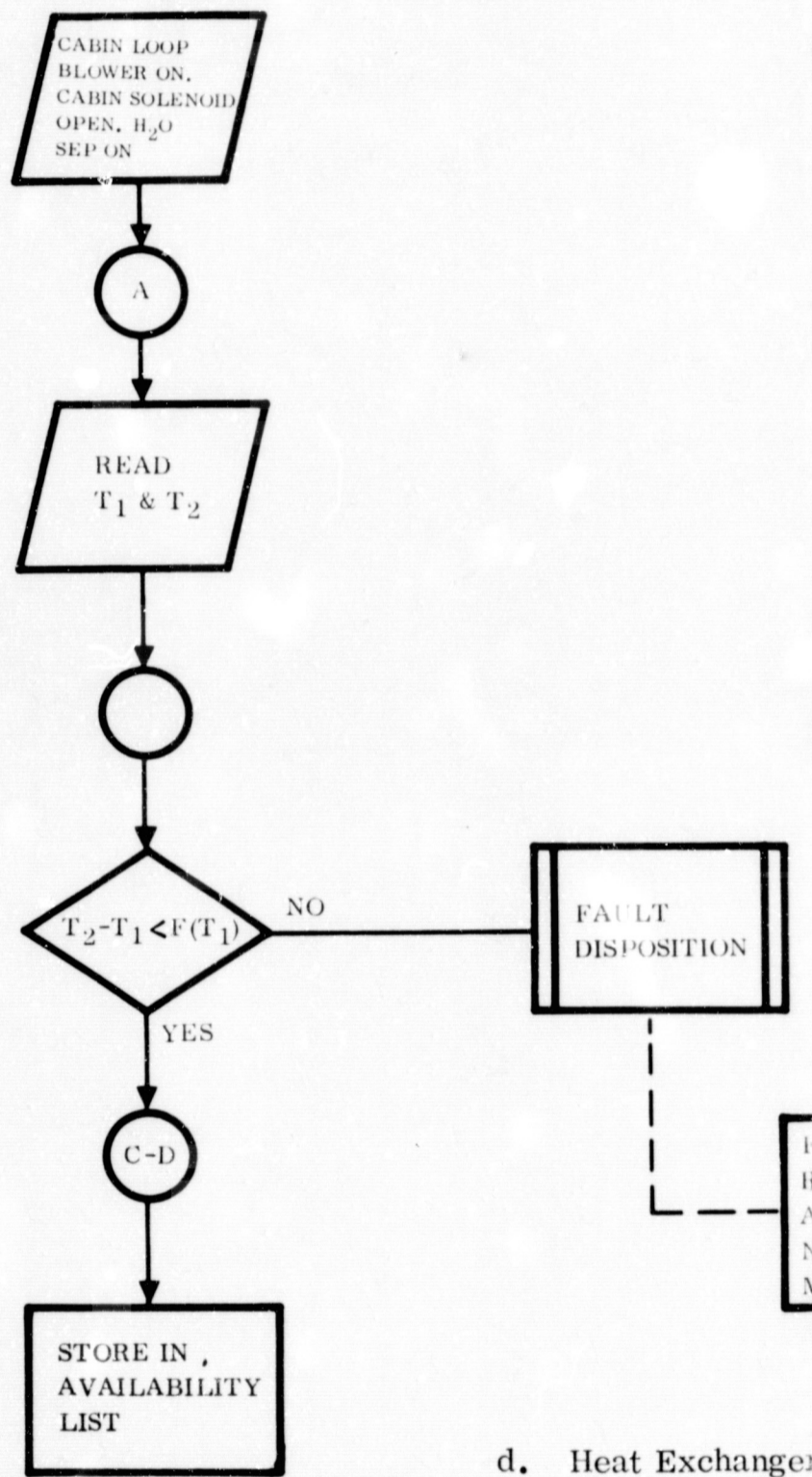
FOLDOUT FRAME



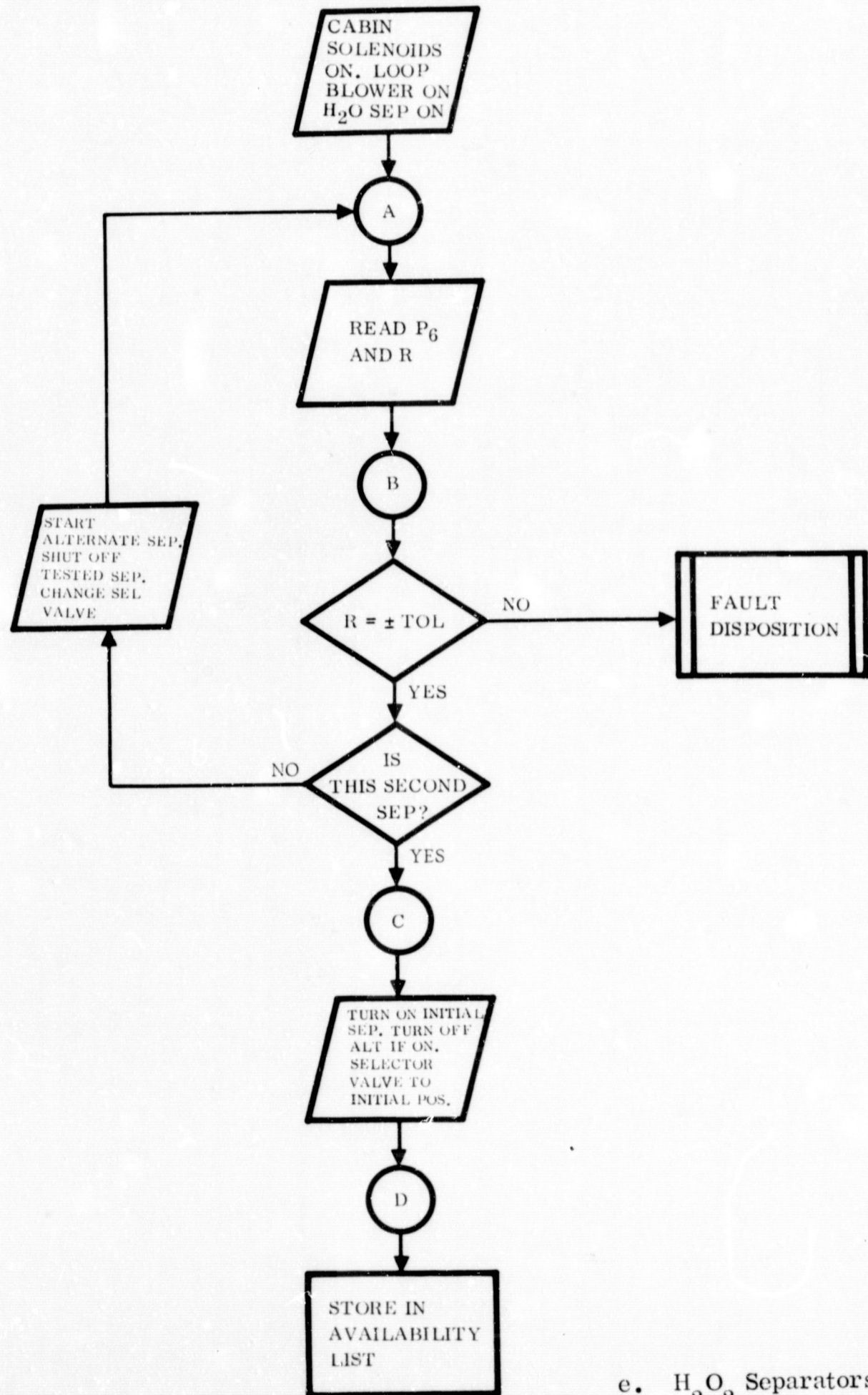
b. Restrictor Valve
LiOH Filters
Filter Selector



c. Loop Blowers



d. Heat Exchanger



FAULT DISPOSITION ROUTINE IS ADVISORY ONLY. NO REDUNDANT MODES

e. H₂O₂ Separators

Figure 3-16. Atmosphere Purification Loop Fault Detection Routine

FOLDOUT FRAME
4

Table 3-6. Atmosphere Purification Loop Redundancies

Component	Redundancies and Backups
LiOH and ACF	Redundant filter housing. Expendable LiOH and ACF cartridge is replaced periodically.
Cabin loop blower	Redundant blower. Suit boost blower is backup.
Suit boost Blower	Redundant blower.
Humidity control heat exchanger	Redundant liquid passages in heat exchanger.
Water separators	Redundant water separator
Suit loop pressure regulator	Redundant regulator.

ACF/LiOH Filter Assembly (Figure 3-16b). The cartridge within the filter assembly is expendable and is replaced on an established schedule. Depletion of the LiOH may be detected by gas analysis showing increased CO₂ in the cabin atmosphere. Depleted ACF capacity may be detected by odor. Depletion will not occur in normal operation if the cartridges are replaced on schedule. To restore function after any type failure, a redundant filter assembly is switched on the line by means of a selector valve.

Cabin Loop Blower (Figure 3-16c). Failure is detected by abnormally low (or zero) rotational speed of the impeller, or by failed Δp across the blower. Function is restored by switching on the redundant blower.

Humidity Control Heat Exchanger (Figure 3-16d). Liquid side redundancy is discussed in the Thermal Control section. The gas side of the heat exchanger is assumed to be equivalent to ducting in which no uncorrectible failures will occur.

Water Separators (Figure 3-16e). Failure is detected by sensing abnormally low (or zero) rotational speed or by abnormal pressures in the gas stream. Function is restored by switching on the redundant water separator.

Second Failures, Atmosphere Purification Loop

If the second cabin loop blower fails, function is restored by switching on a suit-boost blower. One ACF/LiOH cartridge is carried in excess of scheduled replacement needs. If there is a second failure in the water separators or humidity control heat exchanger, some backup exists in the capability of the cabin atmosphere to take on added moisture up to a point of near saturation. Additional backup is attainable by manually venting moisture-laden cabin atmosphere and making replacement with dry gases from storage.

In addition to other redundancies of the atmosphere purification loop, there is a redundant suit boost blower and a redundant O₂ pressure regulator. Failure of a blower will be immediately apparent to the crew and will also show as reduced Δp across all components. Correction is by switching on the redundant blower. Failure of the O₂ pressure regulator will show on the suit pressure gage and is corrected by switching flow through the redundant regulator.

3.9.1.3 Water Management. Figure 3-17 shows the water management scheme, including waste liquid storage and jettison. Backup and emergency modes are summarized in Table 3-7.

Description of Operation. Water from the fuel cells is used for drinking and food and beverage preparation, with some of the excess stored for use in the thermal control sublimator for heat rejection. Humidity condensate, from the water separators of the atmosphere purification loop, is processed for sterility and is used for personal hygiene and for flushing the urinal. Urine and used wash water are jettisoned. Storage is provided for water from all sources, which permits the backup uses and some choice of time and place for dumping wastes. Storage is in positive expulsion tanks, which are pressurized with N₂ from the atmosphere stores.

Processing the humidity condensate is through components in sequence as follows: 1) a cyclic accumulator pressurized with N₂ at 50 psig, which raises pressure for flow into the 10-psig water management system; 2) a multifiltration unit, consisting of a bacteria filter, an ion exchange column, and an activated charcoal filter; and 3) a sterilizer, which adds a silver compound at sufficient concentration to arrest micro-organism activity. Fuel cell water is processed in a parallel set of components. If either set fails, humidity condensate is diverted to waste, and fuel cell water is processed in the remaining set for continued use by the crew. A Dowex-50 ion exchange column removes the silver before the water is used in food and beverages.

First Failures, Water Management

Pressurization. Gross failure in pressurization is detected by pressure measurement in the pressurant lines and in the water lines. If failure is in the N₂ pressurant supply, redundant components restore function. (See Atmosphere Supply and Pressurant Control section.)

A low-rate leak can be sustained for the mission duration. A high-rate leak requires that the failed portion of the plumbing be isolated by valves.

Humidity Condensate (Figure 3-18). Normal use of humidity condensate is for personal hygiene and urinal flush; both uses can be terminated without requiring mission abort. However, selector valves permit use of fuel cell water for these purposes. Failure of the multifiltration unit purification function may be detected by a conductivity sensor, (Figure 3-18a), but this kind of failure would not necessarily preclude

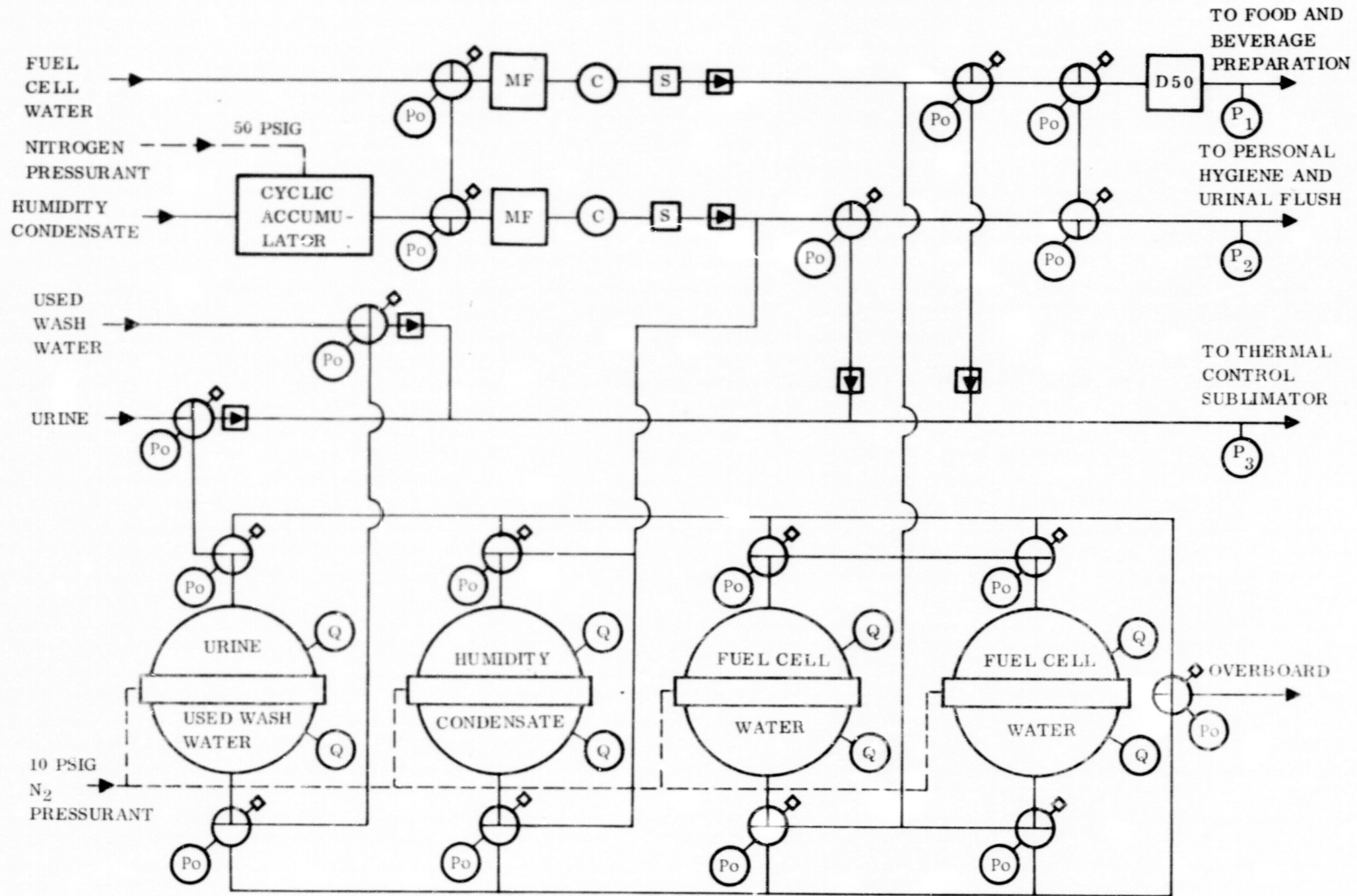
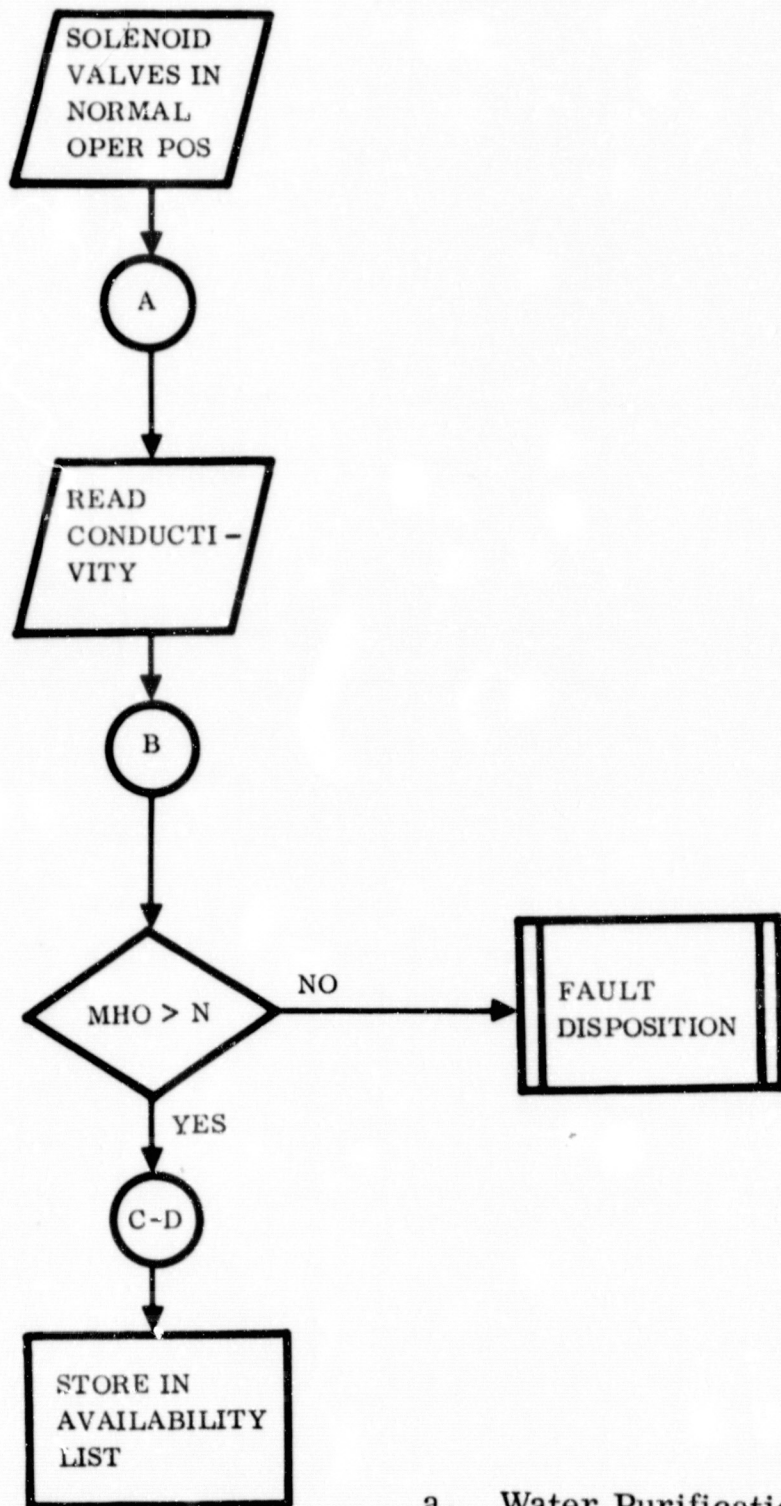


Figure 3-17. Water Management Subsystem



a. Water Purification

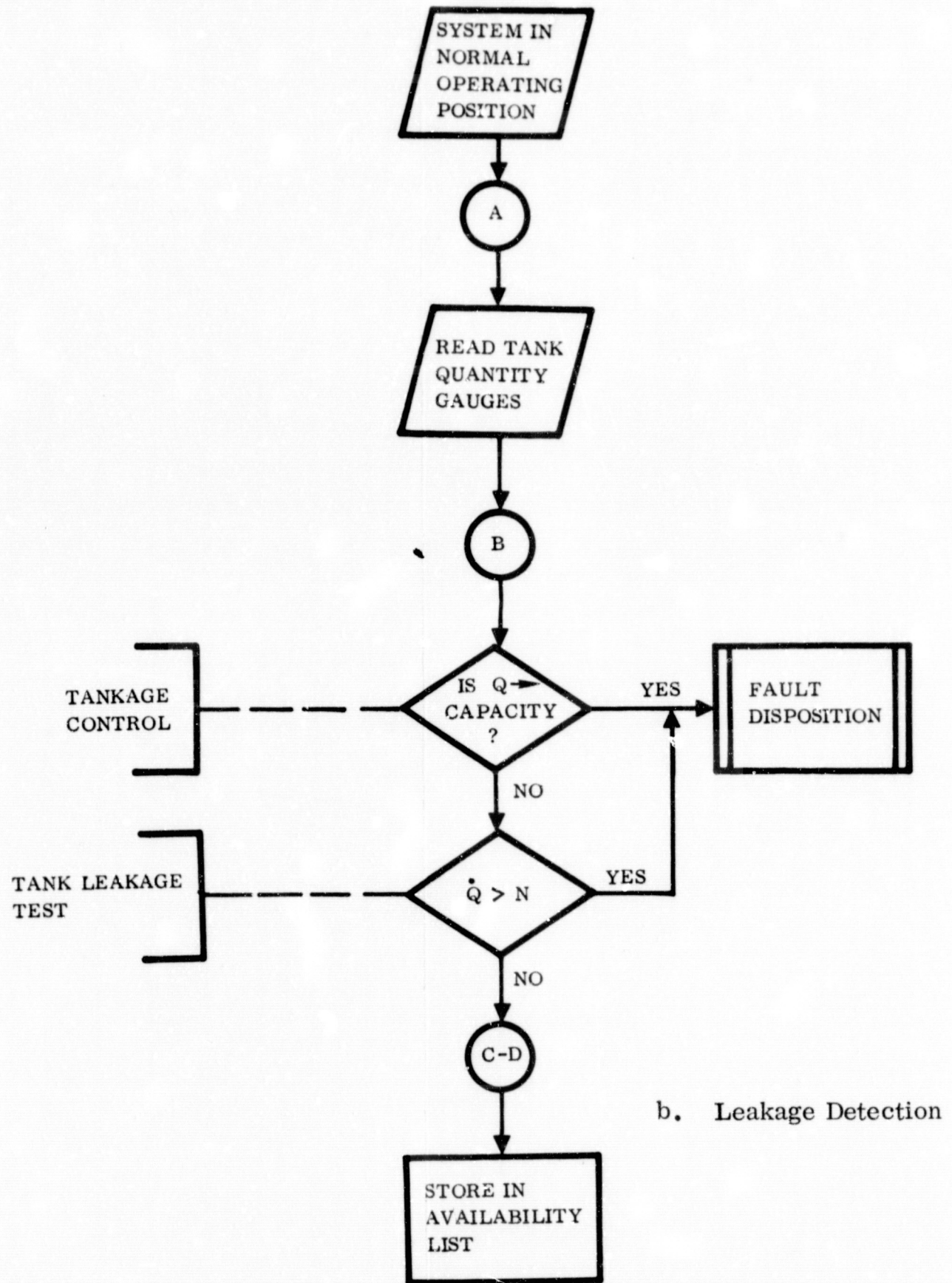


Figure 3-18. Water Management Fault Detection Routine

Table 3-7. Water Management Subsystem Backup and Emergency Modes

Water Source	Primary Uses	Backup Uses	Emergency Use and Priority
Fuel cell water	Food and beverage Heat rejection	Personal hygiene Urinal flush	Heat rejection 1
Humidity condensate	Personal hygiene	Food and Beverage	Heat rejection 2
Used wash water	Dump overboard		Heat rejection 3
Urine	Dump overboard		Heat rejection 4

use of the water. A failure of the cyclic accumulator pressurization function, or a blockage downstream, would cause water accumulation in the water separators. This would be detected by discharge of water drops into the cabin and by abnormal Δp across the separator. If one of these failures occurs, the humidity condensate is collected in a plastic bag, which is periodically emptied manually into either the urinal or the waste wash water collector. A leakage-type failure is detected visually or by storage tank gaging (Figure 3-18b), which shows abnormally low quantity. Water that leaks may evaporate into the cabin atmosphere and be returned as humidity condensate or it may be picked up manually in a sponge and returned to the personal hygiene waste water.

Fuel Cell Water. Normal use of fuel cell water is for drinking and for food and beverage preparation. These uses take only about one-third of the water produced; the remainder is stored. Although this storage is primarily for potential use in the thermal control sublimators as a backup mode of heat rejection, the water can be used for any other purpose. If the fuel-cell water supply fails completely, and the stored water has been used, needs for drinking and food preparation can be partially met by using processed humidity condensate.

Second Failures, Water Management

Several levels of backup capability exist for failures beyond the first. A separate source of gaseous N_2 is available for emergency pressurization of the water system. If this also fails the O_2 will be used as a pressurant. Isolation of the various water sources precludes loss of all water in a second plumbing or component failure. In the event of a heat rejection emergency, selector valves permit use of any water on board for this purpose. After using all available fuel-cell water, the priorities in emergency diversion of other water to the thermal control sublimator will be 1) humidity condensate; 2) used wash water; and 3) urine.

Performance Monitoring, Servicing, and Selector Valve Checkout. Performance of the multifiltration units is monitored during flight by periodically measuring conductivity of the product water. Failure in purification is indicated by high conductivity. If this occurs in water for food and beverage preparation, valves are actuated to select the alternate source. If it occurs in water for personal hygiene and urinal flush, these uses can continue. As soon as the vehicle is committed to entry, all fresh and waste water on board is jettisoned. Valves are actuated to isolate the water management system, and all lines and components are evacuated to space. After landing, the system is flushed with water and disinfectant and purged dry with clean nitrogen. Adequate flushing will require valve actuation, which will serve as a valve function checkout. Valve actuation can also be checked at any time while the system is dry.

3.9.1.4 Waste Management. Figure 3-19 illustrates the waste management subsystem. Backup modes are summarized in Table 3-8.

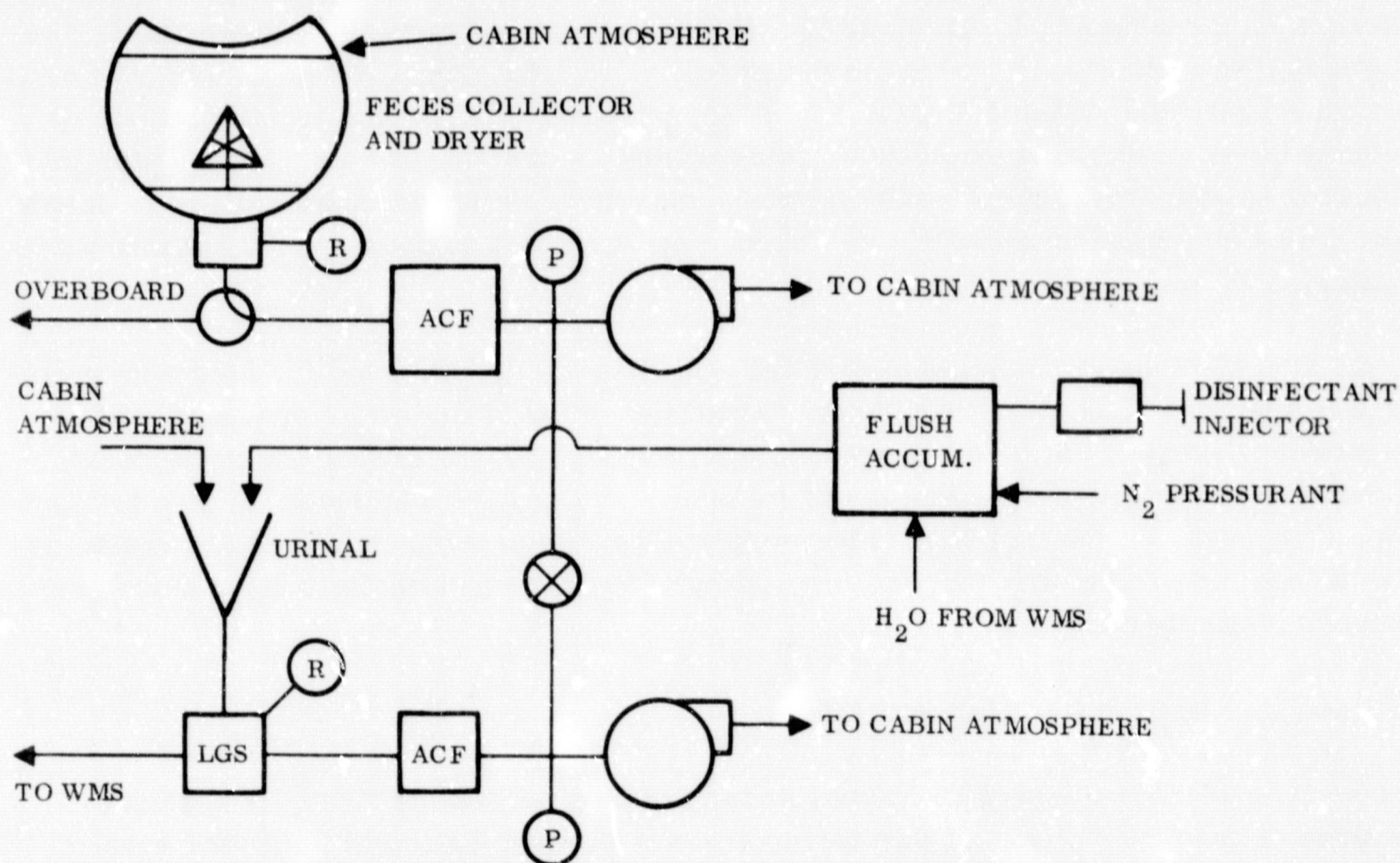


Figure 3-19. Waste Management Subsystem

Description of Operation. Urine is collected in a relief tube, into which cabin atmosphere is drawn to facilitate liquid capture in zero-g. Flow of the liquid-gas mixture is into a motor-driven separator, which includes a pump for pressurized flow of the liquid into a storage tank of the water management subsystem. The separated gas flows through an activated charcoal filter for odor control, through the blower, and then

Table 3-8. Waste Management Backup Modes

Function	Component	1st Backup	2nd Backup
Feces Collection	Blower	Urine collection blower	Emergency collector*
	Slinger	Reduced capacity	Emergency collector
	Others	Emergency collector	Emergency collector
Urine collection	Blower	Feces collection blower	Emergency urinal**
	Flush accumulator	Emergency urinal	Manual flush
	Liquid-gas separator	Emergency urinal	Plastic bag

*Plastic glove type emergency feces collector.

**Personal hygiene waste water collector serves as an emergency urinal.

returns to the cabin. The urinal is flushed with a metered quantity of water, which contains a metered quantity of disinfectant. After each use, the flush accumulator automatically refills with water and disinfectant.

A flow of cabin atmosphere transports waste into the feces collector. Cabin atmosphere return from the collector is through an activated charcoal filter and a blower to the cabin. The waste impinges on a motor-driven device that spreads the material onto a plastic liner on the inner surface of the collector sphere. After use, the lid of the collector is closed and sealed. A selector valve exposes the sphere interior to space vacuum, which dries the thin layer of material. When thus dried, microbiological activity and decomposition are arrested. For the next use of the collector, the selector valve is moved to connect the sphere with the blower, at the same time shutting off the vacuum and allowing the sphere to repressurize with cabin atmosphere. Opening the lid actuates switches that start the motor and the blower.

First Failures, Waste Management Subsystem (Figure 3-20)

Blower failure may be detected by sound, by sensing rotational speed of the impeller, or by sensing pressure rise across the blower. If either blower fails, the other blower can be turned on to cause the flow of cabin atmosphere required for zero-g waste collection. Selector valves and electrical switches are used for transfer of the function. Failure of the feces collector motor or liquid-gas separator will be detected by sensing rotational speed. If the liquid-gas separator fails, the waste water collector of the personal hygiene subsystem is used as an emergency urinal. If the feces collector fails, collection can continue but at less capacity of the container.

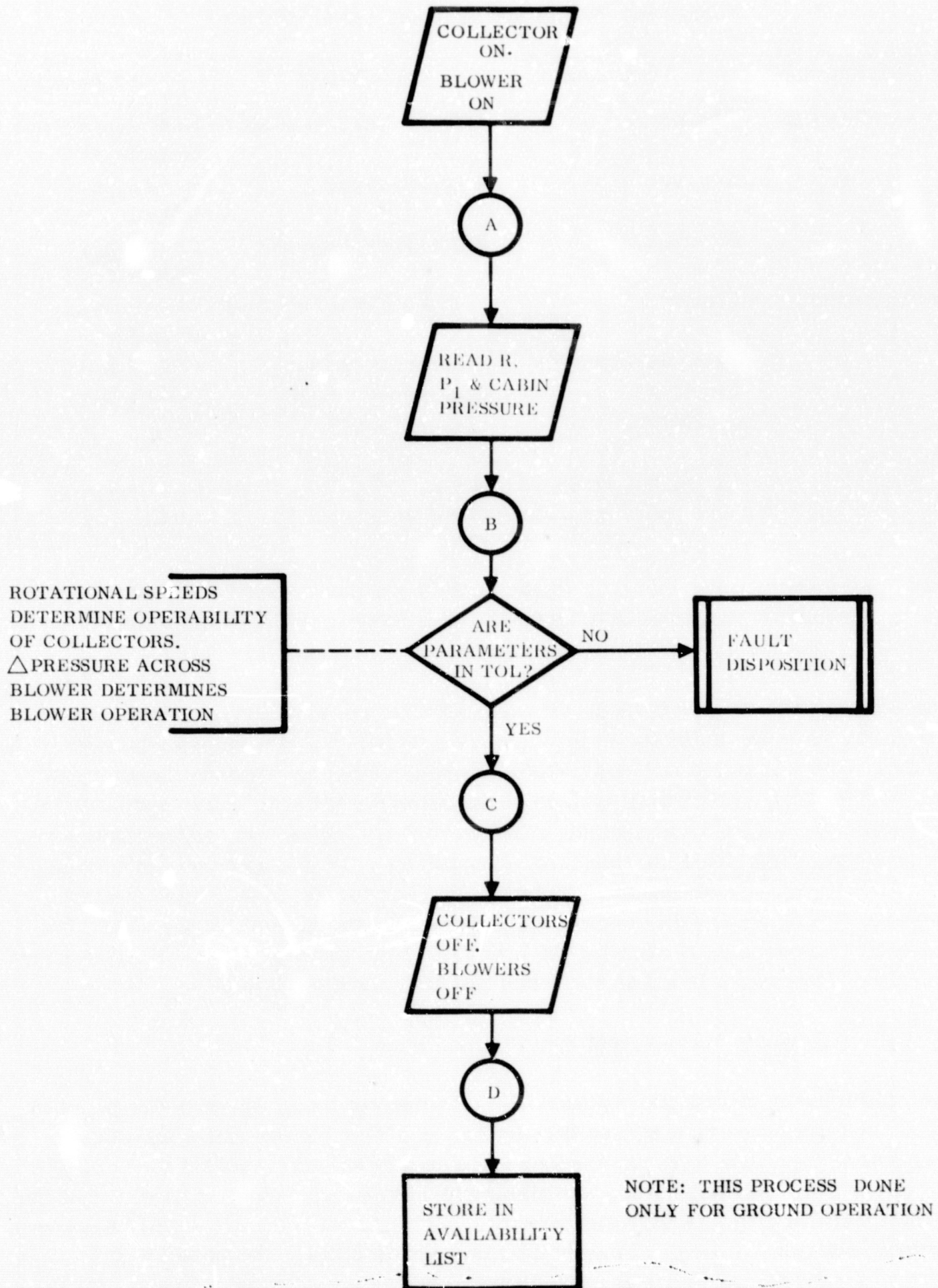


Figure 3-20. Waste Management Fault Detection Routine

Also, the material will not dry sufficiently to inhibit bacterial activity. If the flush accumulator fails, the urinal can be flushed manually by discharging water into it from a plastic bag or from a sponge. The failure would be observed visually.

Second Failures, Waste Management Subsystem

If the second blower fails, the waste water collector of the personal hygiene subsystem is used as an emergency urinal. The emergency feces collector is a "defecation glove". After use, the collector and contents are stored in the feces collection sphere. Partial drying may be achieved if sphere vacuum is maintained and the selector valve is intact.

3.9.1.5 Food Management. The hardware consists of a food storage container, a water heater, a water chiller, and a water dispenser. The water heater and chiller are shown in the thermal control subsystem schematic. The food is considered to be of the Apollo type, with supplements selected for compatibility with zero-g. If failures occur in water heating or chilling, the water is consumed at the temperature available. An emergency water dispenser is provided.

3.9.1.6 Personal Hygiene. Figure 3-21 illustrates the facility for bathing with a sponge. The facility can be used for bathing the entire body or for limited washing, such as for face and hands. The waste water collector serves as a backup to the urinal in the waste management subsystem.

Description of Operation. The apparatus is designed for zero-g control of the wash water to minimize chance of cabin contamination. The user operates the apparatus and washes to the extent desired in a cycle as follows: 1) he opens the hinged lid on the end of the sponge wetter-squeezer, inserts the sponge, closes the lid, and presses a START button; 2) he waits a few seconds while the pneumatically-powered unit automatically cycles to a) compress the sponge with the piston, expelling water and air, b) release piston pressure on the sponge, c) admit a metered quantity of water with detergent into the sponge, d) vent the cylinder to admit cabin atmosphere and permit full return of the piston, and e) unlatch the lid on the cylinder; 3) the user removes the sponge and washes a portion of his body; and 4) he repeats the cycle as many times as desired for partial or whole-body bathing.

When the sponge is compressed, the expelled water flows into a waste water collector identical to the urinal. The waste-water collector has a motor-driven liquid/gas separator with a pump to transfer the liquid into a waste storage tank, and a blower that returns entrained gas back to the cabin atmosphere. An activated charcoal filter adsorbs odors from the cabin atmosphere return.

The water for washing is from the stored, processed, humidity condensate. It passes through a liquid-to-liquid heat exchanger, where it is warmed by heat transport fluid from the thermal control subsystem. A liquid nonfoaming detergent such as benzalkonium chloride (BAC) is metered into the wash water.

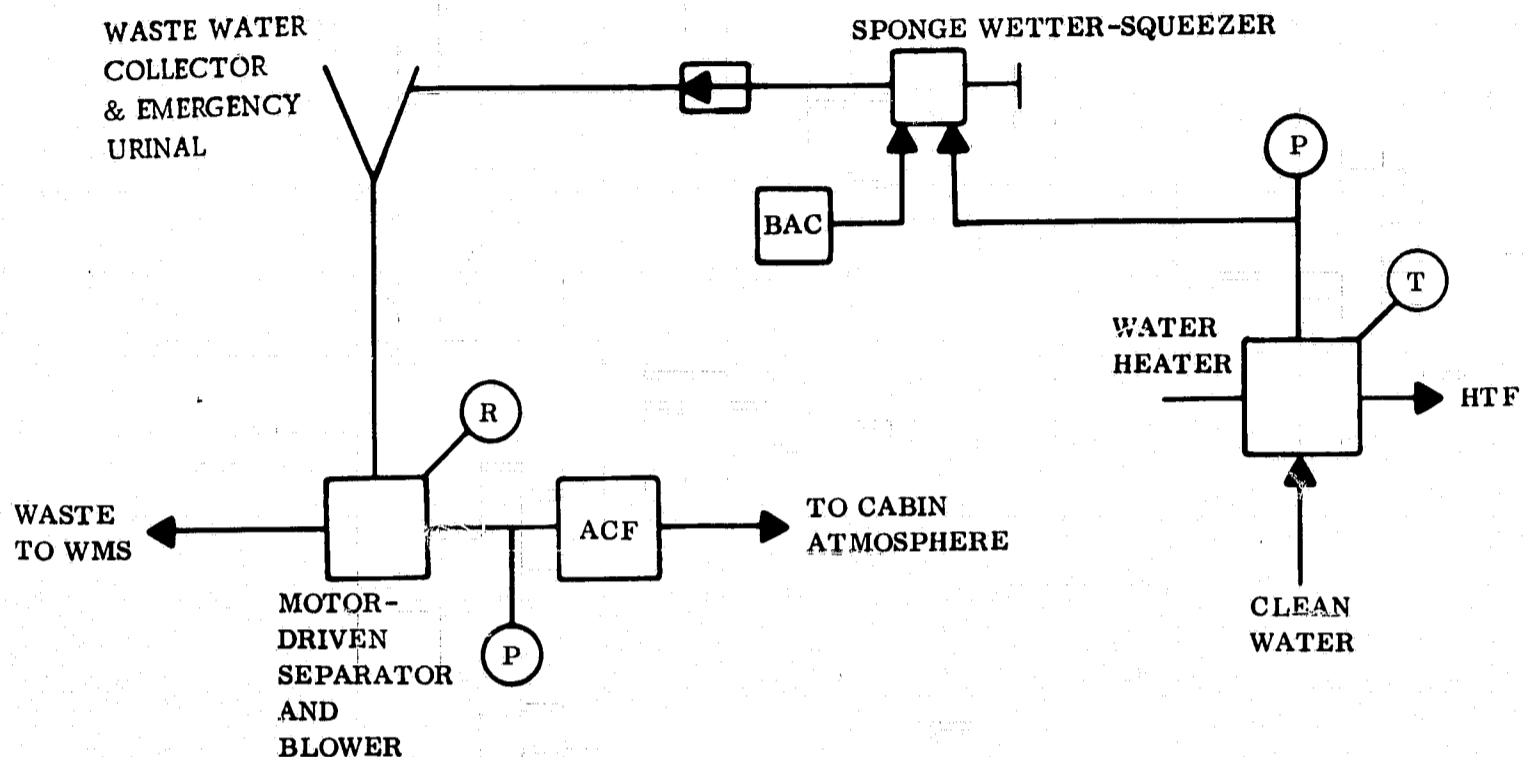


Figure 3-21. Personal Hygiene Subsystem

Failures, Personal Hygiene Subsystem. Whole-body bathing is terminated upon failure of the personal hygiene subsystem. A backup mode is available for cleansing the hands and face, consisting of chemically-treated wipes. Used wipes are disposed into the feces collector. Another mode is available if the supply and control of water and detergent are intact. In this case small, untreated disposable wipes are wetted by manually controlling water flow into the cylinder then used for cleaning the hands and face. Drying is by another untreated, disposable wipe. Disposal is also into the feces collector.

3.9.1.6 Thermal Control. Figure 3-22 is a schematic of the thermal control subsystem. The redundancies and backups are summarized in Table 3-9.

Description of Operation. The thermal control subsystem cools cabin atmosphere, cools equipment, and transports and rejects heat.

Cabin Atmosphere Cooling. The load is shared between the humidity control heat exchanger and the cabin heat exchanger. The former operates in the atmosphere purification loop at temperatures low enough for moisture condensation and removal. The latter operates at temperatures low enough for cooling, but high enough that moisture does not condense; it is independent of the atmosphere purification loop. Both transfer heat from the cabin atmosphere to a heat transport fluid (HTF). The humidity control heat exchanger has fixed flows that maintain relative humidity within the control band. The cabin heat exchanger has bypass variable flow in response to thermostat signals, so that nearly constant atmosphere temperature is maintained. The thermostat has an adjustable set point for selection by the crew as desired.

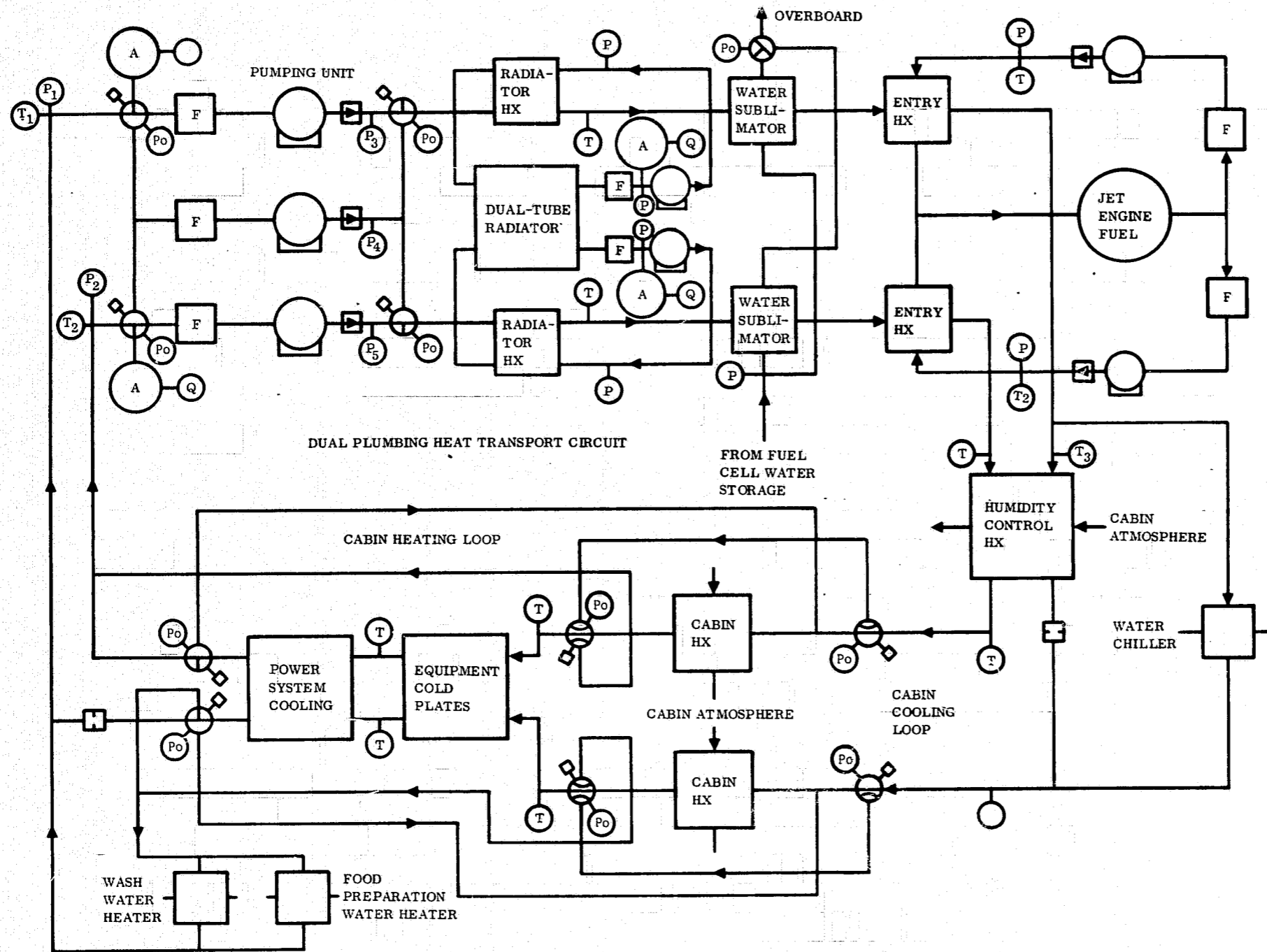


Figure 3-22. Thermal Control Subsystem

Table 3-9. Thermal Control Redundancies and Backups

Component	Redundancies	Backups
Radiator	Redundant tubing. Redundant pumping unit	Water sublimator Entry HX
Piping	100% redundancy except in heating and cooling water for crew use.	
Pumps	Pump in redundant plumbing	Additional redundant pump. Valves are controllable so that any one of the three pumps can operate in either plumbing circuit
Filters	Same as pumps	Same as pumps
Humidity control HX	Redundant liquid passages	
Cabin HX	One redundant	Suit loop
Entry HX	One redundant	

Provision is made for operating the cabin heat exchanger in a heating mode. A selector valve diverts cold HTF around the heat exchanger and supplies it with hot HTF from the point of maximum temperature.

Equipment Cooling and Heating. Both the cabin atmosphere and liquid-cooled cold plates participate in cooling electrical and electronic equipment. Since the cabin atmosphere is cooled by the same heat transport fluid as the cold plates, all heat from the equipment contributes to temperature rise in the HTF. The components are arranged in a series-parallel network, so that HTF flows and temperatures are consistent with component heat loads and temperature requirements. The chiller for crew drinking water is at the cold end of the HTF circuit, and the heaters for personal hygiene and food preparation water are at the hot end.

Heat Transport. The heat transport fluid is water with a corrosion inhibitor. It is filtered before entering the motor-driven pump, which circulates it at a rate consistent with the heat loads and temperature limits. An accumulator compensates for temperature-caused volume variations and also has a small fluid reserve for minor leaks.

Heat Rejection. In orbital flight, the HTF is cooled in a liquid-to-liquid heat exchanger that transfers the heat into the radiator subsystem. The radiator fluid is Freon-21, selected for its viscosity characteristics at low temperatures. The radiator subsystem has 100% redundancy in pumps, fillers, and plumbing. The radiator concept is of panels in the upper and lower surfaces of the wings, thereby utilizing wing deployment mechanisms to deploy the radiator. The wing skin is designed of a thickness to serve as radiator fin material, and the dual tubing shares common fins.

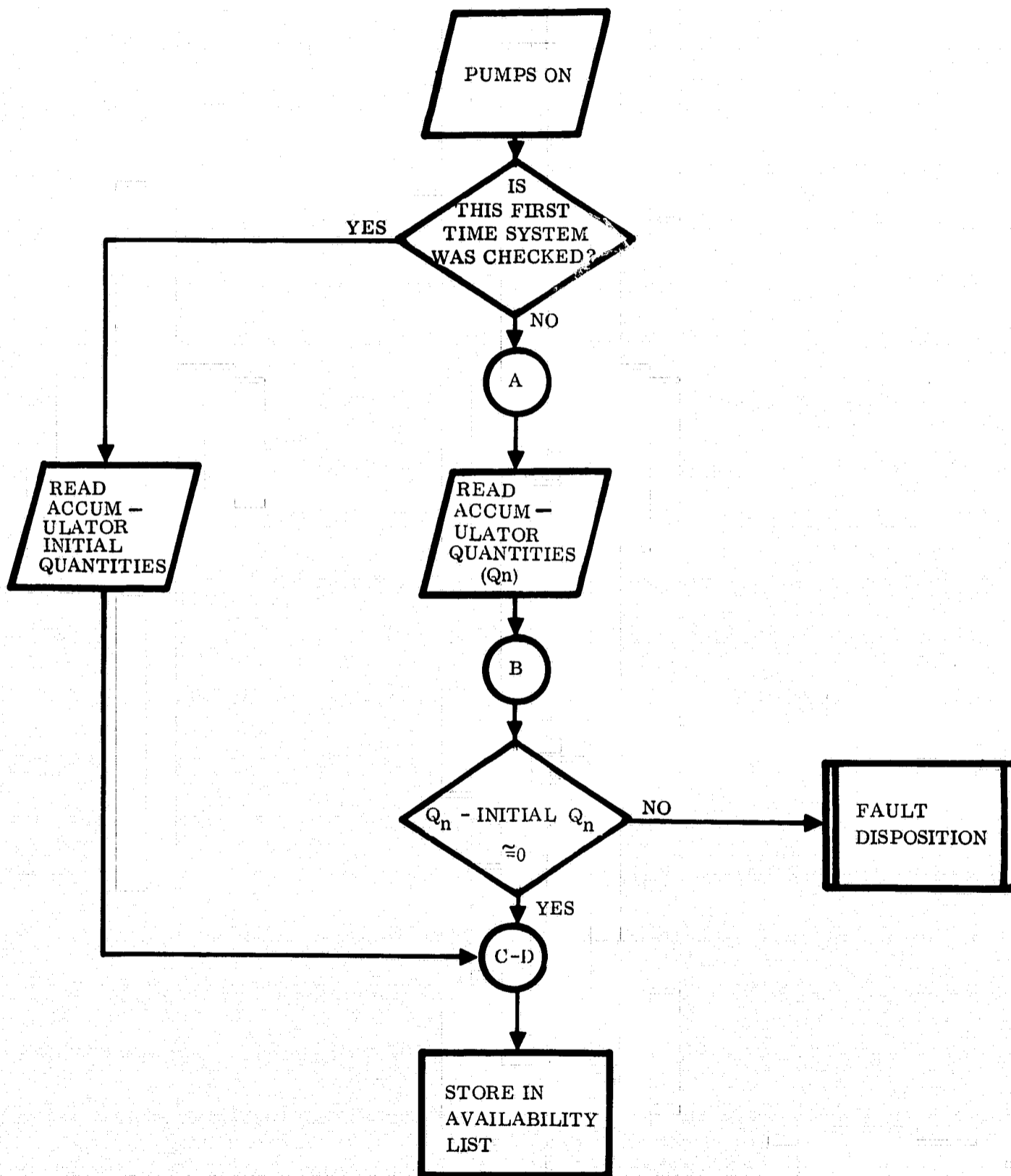
Heat rejection capacity of the radiator is supplemented by a water sublimator which uses fuel cell water. This use is for brief periods of peak heat loads or of unfavorable thermal radiation exposure for the radiator. This heat sink is available only during flight above the atmosphere and is limited by the amount of water available.

Another liquid-to-liquid heat exchanger is used during the period of entry and atmospheric flight. The cabin HTF transfers heat into the turbojet fuel, causing a slight temperature rise in the fuel. This heat sink loop can be placed in operation at any time during flight and has considerable thermal capacity if the fuel is initially at a low enough temperature.

First Failures, Thermal Control (Figure 3-23). The thermal control subsystem has 100% redundancy in plumbing and in all components except the water coolers and heaters for personal hygiene and for food and beverage preparation. Failure of these components would not require abort. The 100% redundancy amounts to two independent heat transport circuits, two independent radiator heat rejection loops, and two independent fuel heat sink loops. Each of these elements can handle the full thermal load. The failure of any pump or loss of fluid in any loop causes automatic switching to the redundant loop. Fluid loss failures are detected by accumulator quantity sensors (Figure 3-23a). Pump failures are detected by measurement of Δp (Figure 3-23b).

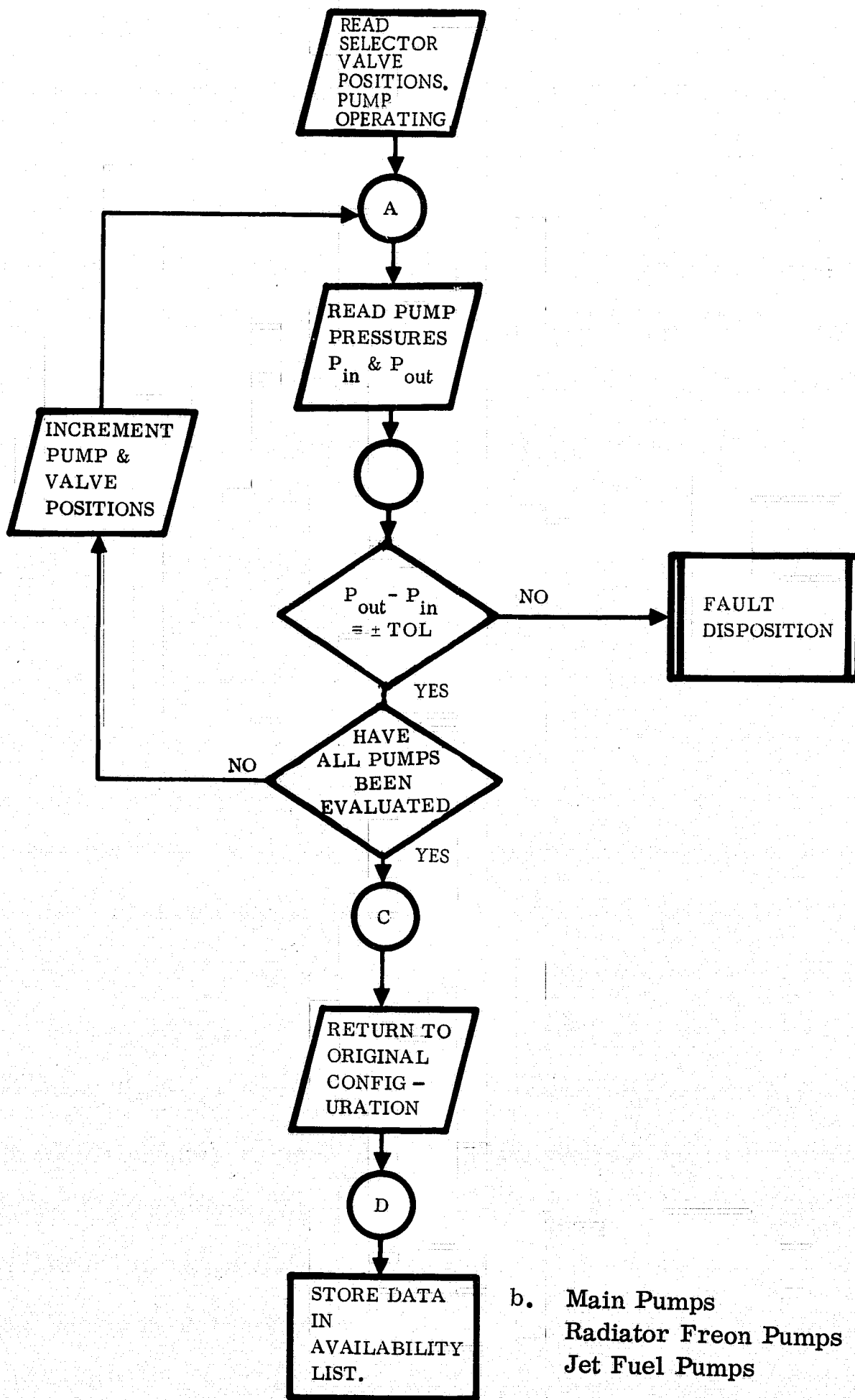
Second Failures, Thermal Control. Triple redundancy is provided in the heat transport fluid pumping unit. By actuating electrical switches and selector valves, any of the three pumps can be used in either heat transport circuit. Pump failure is detected by Δp measurement.

The heat rejection function has several levels of backup. Each of the redundant radiator loops is backed up by a water sublimator and by a jet fuel heat-sink loop. The priority in employing the backups is to use the water sublimator until the water supply is exhausted or until the vehicle descends into the atmosphere. Thereafter, the jet fuel heat sink loop is activated by switching on a pump. If all heat rejection fails, the ultimate backup is in the thermal inertia of the cabin atmosphere, the heat transport fluid, and all the thermal control hardware. This backup has an estimated capacity for 15 minutes of operation at degraded thermal performance.



- a. Fluid Loss
Refrigerant Manifold
Coolant Manifold

Figure 3-23. Thermal Control Loop Fault Detection Routine



3.9.1.7 ECS/LS Fault Summary. Table 3-10 summarizes the environmental control and life support subsystem fault detection process. This table lists the components (replaceable units) evaluated in preflight as well as the fault isolation processes for repair action and the methods used for evaluation. The performance monitor portion outlines the instruments monitored during the fault detection program and the instruments used during fault disposition routines. The performance monitor section also includes the corrective action control necessary to make a failed portion of the system operational.

3.9.2 ELECTRICAL GENERATING SYSTEM

3.9.2.1 Description of Operation. Refer to the block diagram, Figure 3-24. The requirements for the orbiter vehicle are satisfied with the system elements shown. The operational sequence follows.

Operation. The fuel cells are activated by opening the H₂ and O₂ valves, using ground power. The fuel cell outputs rise in voltage and energize the bus. Ground power is removed, and all vehicle loads associated with the boost, orbiting, and entry may be energized as required. The fuel cells remain activated during the entire mission and share the system load. If either unit fails, the remaining unit continues to supply the entire load, and the mission continues without affecting capability.

If a second failure occurs, the battery is activated by dumping the stored KOH electrolyte into the cells. Power is now supplied only to those loads required for safety of return. Time limits imposed by limited energy storage require that the vehicle de-orbit and enter within a two-hour period. Stored electrolyte provides long battery life in the inactivated state. Rarely will the battery be used, since it is an emergency energy source. Once used, the battery is replaced as an expendable item.

Entry Period. The entry period is considered to end upon engine deployment. After the engines are started, an additional electrical power system is activated to accommodate those loads peculiar to the aircraft operating mode. The magnitude of this composite load suggests that the prime power be generated as alternating current. A variable-speed, constant-frequency (VSCF) system is shown. The oil-cooled, wide-speed-range ac generator is coupled directly to a high-speed engine pad (10,000-20,000 rpm). The high output frequency of the generator (1000-2000 Hz) is converted to three-phase, 115/200-volt, 400-Hz power by the cycloconverter. Direct current power is obtained simply by a transformer-rectifier (T-R). In addition to supplying aircraft mode loads, this system also supplies power to all of the loads on the fuel cell/battery bus in proportion to demand. All the dc sources can operate in parallel in any combination since their volt-ampere characteristics will be similar.

Fuel Cell Checkout. For the purposes of this study, the checkout of only the fuel cell portion of the system was chosen. The procedures and techniques demonstrated for this part of the system are generally applicable to the remaining part.

Table 3-10. ECS/LS Fault Detection Summary

Subsystem	Components Evaluated During Startup	Performance Mon	
		Instruments Monitored	Failure Mode Instr
Atmosphere supply and pressurization	Same as fault isolation list	<ol style="list-style-type: none"> 1. O₂ supply manifold press. 2. O₂ storage vessel quan. 3. O₂ low pressure man. 4. N₂ supply man. pressure 5. N₂ storage vessel quan. 6. N₂ low press. manifold 7. O₂ and N₂ partial press. 8. CO₂ content 9. H₂O content 	<ol style="list-style-type: none"> 1. LO₂ quantity 2. LN₂ quantity 3. Heater currents 4. O₂ and N₂ manifold press. 5. O₂ and N₂ partial 6. Cabin CO₂ and H₂O content 7. Heater continuity 8. Hi press. select valves 9. Int press. select valves
Atmosphere purification loop	Same as fault isolation list	<ol style="list-style-type: none"> 1. Temp heat ex output 2. H₂O separator RPM 3. Blower output press. 4. Filter out flow meter 	<ol style="list-style-type: none"> 1. Suit loop O₂ flow 2. Suit loop O₂ pres 3. LiOH input press 4. LiOH output pres 5. Blower output pr 6. Heat exchanger p 7. Loop output pres
Water management	Same as fault isolation list	<ol style="list-style-type: none"> 1. Conductivity 2. Vessel quantity 	<ol style="list-style-type: none"> 1. Manifold pressu

Performance Monitoring		Fault Isolation	
Failure Mode Instruments	Corrective Action Control	Components	Fault Isolation Method
O ₂ quantity	1. O ₂ manifold solenoid	1. Cryogenic vessel heaters	Instrument
N ₂ quantity	2. O ₂ hi lo sel valve	2. Oxygen supply solenoid	Functional
heater currents	3. N ₂ hi and int sel valve	3. O ₂ high press. selector	Functional
O ₂ and N ₂ manifold press.	4. Emer pressurant valve	4. O ₂ high press. regulator	Instrument
O ₂ and N ₂ partial press.	5. O ₂ and N ₂ test bleed valve	3. O ₂ low press. selector	Functional
Cabin CO ₂ and H ₂ O content		4. O ₂ test bleed valve	Functional
heater continuity		5. O ₂ emer. press. valve	Functional
low press. selector		6. N ₂ supply solenoid	Functional
valves		7. N ₂ high press. selector	Functional
high press. selector		8. N ₂ high press. regulator	Instrument
valves		9. N ₂ low press. selector	Functional
		10. N ₂ low press. regulator	Instrument
		11. N ₂ test bleed valve	Functional
Suit loop O ₂ flow meter	1. Filter selector valve	1. Cabin shut off sol.	Functional
Suit loop O ₂ pressure	2. Cabin loop blower	2. Particulate filter	Functional
LiOH input pressure	3. H ₂ O separator selector valve	3. Filter selector	Instrument
LiOH output pressure	4. H ₂ O separator	4. LiOH and ACF filter	Instrument
lower output pressures	5. Suit loop sel valve	6. Suit and loop blowers	Functional
heat exchanger press.	6. Suit loop regulators	7. Humidity heat exchanger	Instrument
Suit loop output press. (P _c)		8. Water separators	Instrument
		9. Suit O ₂ regulators	Instrument
		5. Filter restrictor	Functional
Manifold pressures	1. Selector valves	1. Storage vessels	Instrument/correlation
		2. Storage vessel selector valve	Instrument
		3. Cyclic accumulator	Functional
		4. Selector valves	Instrument
		5. Filters	Instrument
		6. Sterilizer	Replaced periodically
		7. Ion tower	Replaced periodically

Subsystem	Components Evaluated During Startup	Performance M	
		Instruments Monitored	Failure Mode Ins
Waste management subsystem	None - system determined operational prior to launch activities by ground personnel	No inflight monitoring	1. Gas pressure 2. Feces coll. R 3. Blower pressu
Personal hygiene system	None - system determined operational prior to launch activities by ground personnel	No inflight monitoring	1. Gas pressure 2. H ₂ O temp & p
Thermal loop	<ol style="list-style-type: none"> 1. Filter/pumps 2. Radiator filter pumps 3. Pump selector valves 4. Water sublimator 5. Jet fuel coolant pumps 6. Humidity control heat exchanger 7. Cabin heat exchanger 8. Equipment cold plates 9. Power system cooling 	<ol style="list-style-type: none"> 1. Coolant quantities 2. Freon quantities 3. Coolant temp T₁ or T₂ 4. Coolant out temp T₃ or T₄ 	<p>All system temps</p> <p>All system press</p> <ol style="list-style-type: none"> 1. Coolant quanti

FOLDOUT FRAME /

Table 3-10. ECS/LS Fault Detection Summary, Contd

Performance Monitoring		Fault Isolation	
Failure Mode Instruments	Corrective Action Control	Components	Fault Isolation Method
Gas pressure Feces coll. RPM Lower pressures	1. Crossover valve (manual)	1. Feces collector 2. Charcoal filters 3. Blowers 4. Urinal 5. Liquid gas separator 6. Flush accum 7. Disinfectant injector 8. Crossover valve	Instrument Replace periodically Instrument Functional Instrument Functional Functional Functional
Gas pressure O ₂ temp & press.		1. Waste water collector 2. Waste water separator 3. Charcoal filter 4. Water heater 5. Disinfectant dispenser	Functional Instrument Replace periodically Instrument Functional
System temps. System pressures Coolant quantities	1. Filter pumps 2. Pump selector valves 3. Radiator pumps 4. Sublimator control 5. Jet fuel coolant pumps 6. Cabin coolant sel. valves 7. Equipment sel valves	1. Filter pumps 2. Pump selector valves 3. Radiator 4. Radiator heat exchanger 5. Radiator pumps 6. Water sublimator 7. Jet fuel heat exchanger 8. Jet fuel coolant pump 9. Water chiller 10. Humidity cont. heat exchanger 11. Cabin heat ex. sel. valve 12. Cabin heat exchanger 13. Equipment cold plates 14. Power system cool 15. Wash water heater 16. Food prep heater 17. Equip coolant sel. valve	Instrument Functional Functional Functional Instrument Functional Functional Instrument Functional Correlation/instrument Functional Functional Instrument Correlation Functional Functional Functional

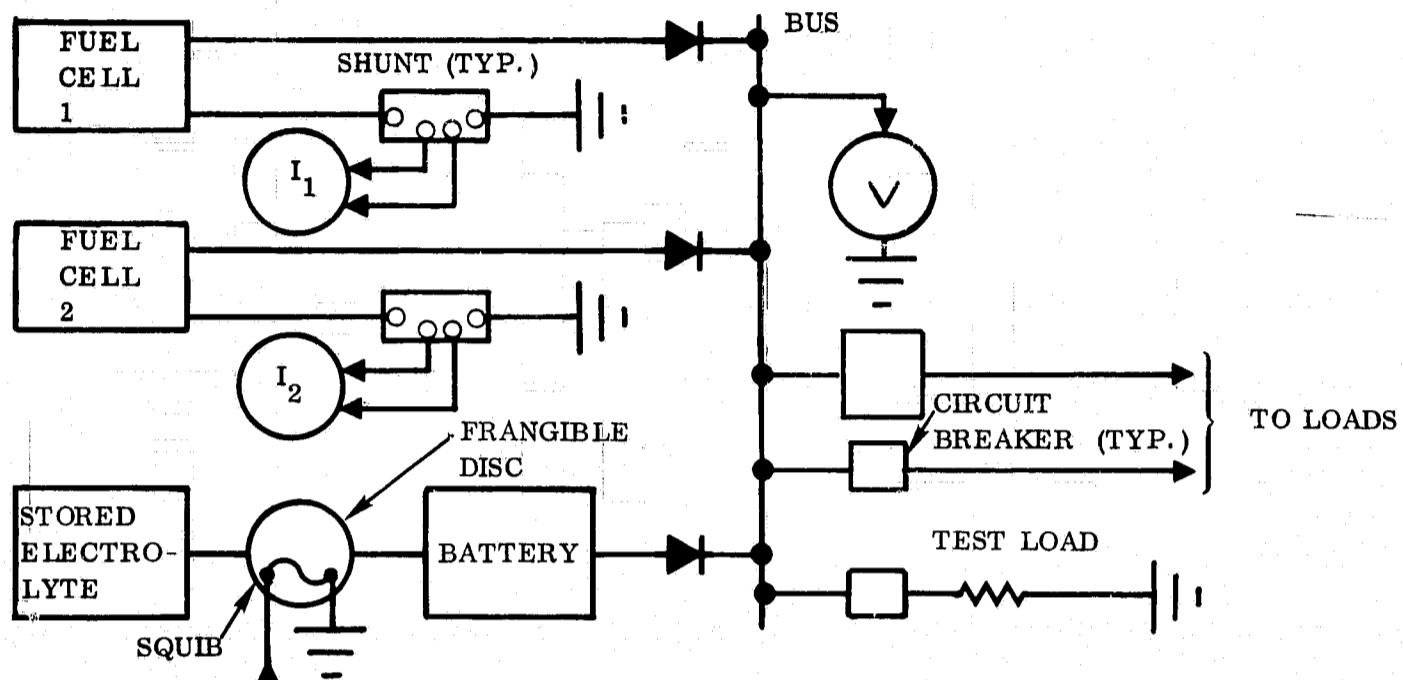


Figure 3-24. Orbiter Electric Power System

Measurements conducted on the output of the fuel cells cannot be made until they have reached normal operating temperature (160° - 180° F). This is because of the change in the slope of the volt-ampere curve with temperature; i. e., at low temperature (say 70° F), the slope is relatively steep, resulting in poor inherent voltage regulation. Within the normal operating temperature range, however, the slope is quite flat. The no-load to full-load voltage will be approximately 31 to 27 volts at the main bus. A thermal control system maintains the correct temperature range.

Measurements (Figure 3-25). Checkout is accomplished by measurement of each fuel cell current and bus voltage. Voltage is measured to establish that the minimum acceptable bus voltage is available for any given load condition. The current output of each unit is measured to assure that load sharing is within acceptable limits. An appropriate test load will be used to achieve a level of current per fuel cell that will provide confidence that the fuel cells and their associated feeders can transmit the required power.

The mathematical equation of each fuel cell and the composite equation of the paralleled fuel cells may be written from test data. These mathematical models are stored in the computer, and fuel-cell performance is measured against the standard. The general equation of a fuel cell may be approximated by a linear representation, sufficiently accurate for all purposes, as follows:

$$E - IR = V,$$

where E is the open circuit voltage, taken as the straight-line intercept, I is the load current, R is the apparent internal resistance of the fuel cell plus the resistance of connections, wire and isolating rectifiers between the fuel cell and the bus, and V is the resulting terminal voltage at the bus.

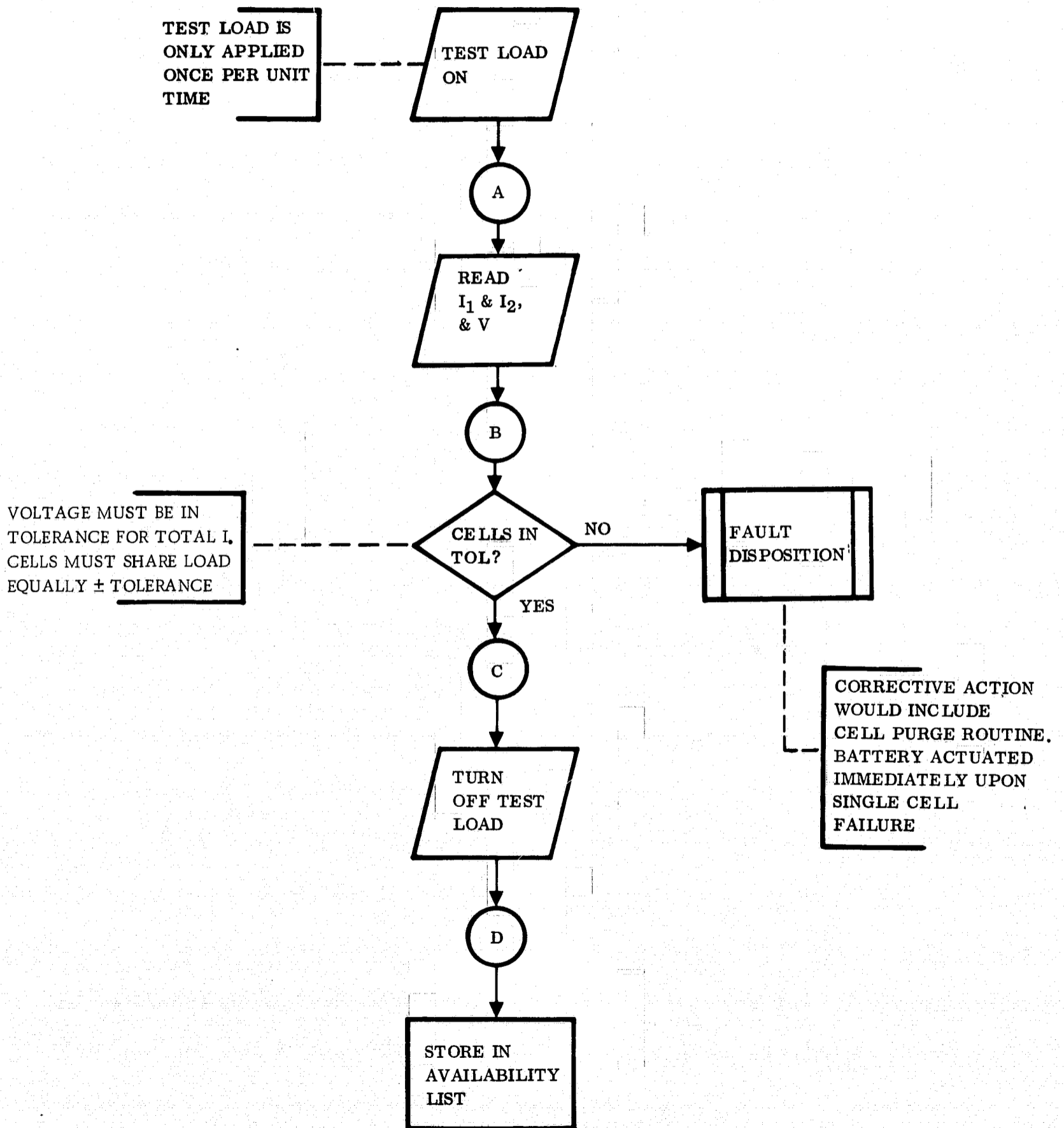


Figure 3-25. Fuel Cell Output Fault Detection Routine

Load sharing will be calculated by the computer by dividing the ratio of the difference and sum currents:

$$\frac{I_1 - I_2}{I_1 + I_2}$$

and comparing this index with a minimum standard value for the load condition.

For example, if the load sharing index is exceeded, the corrective action would involve examination of one or more of the following:

- a. Fuel cell temperature control.
- b. Reactant pressure.
- c. Purge control.

If the corrective actions do not result in improved load sharing, the faulty fuel cell may be shut down automatically or manually.

3.9.2.2 Reactant Supply.

Description and Operation. Figure 3-26 shows the major components in this accessory system. The oxygen and hydrogen are stored supercritically with two vessels per fluid. Each vessel can supply either fuel cell module and contains adequate fluid to last the entire mission. The vessels are filled with two-phase fluid at ambient pressure. The vessels are then brought to operational pressure by applying electrical power to the internal heaters. Selected shut-off valves are opened, and gases are admitted to the fuel cell. Normally the fuel cell modules would have been stored pressurized with an inerting gas such as N₂ or He. Purging is then required to clear the gas cavities of the inerting gas. Fuel cell start-up will commence directly on the connection of an external load.

Failure Modes, Detection and Action (Figure 3-27).

Heater Failure (Figure 3-27a). A heater failure will be noted by the pressure measurement in the storage vessel outlet line. Failure to observe an increase in pressure when the heater is activated will require isolation of the affected vessel and changeover to the redundant vessel.

Line or Vessel Leakage (Figure 3-27b). If the leakage is significant, it will be detected by excessive activation of the heaters and by more than normal rate of decrease in reactant quantity. This will require isolation of the affected vessel and changeover to the redundant vessel. Leakage between the vessel isolation valves and the fuel cell

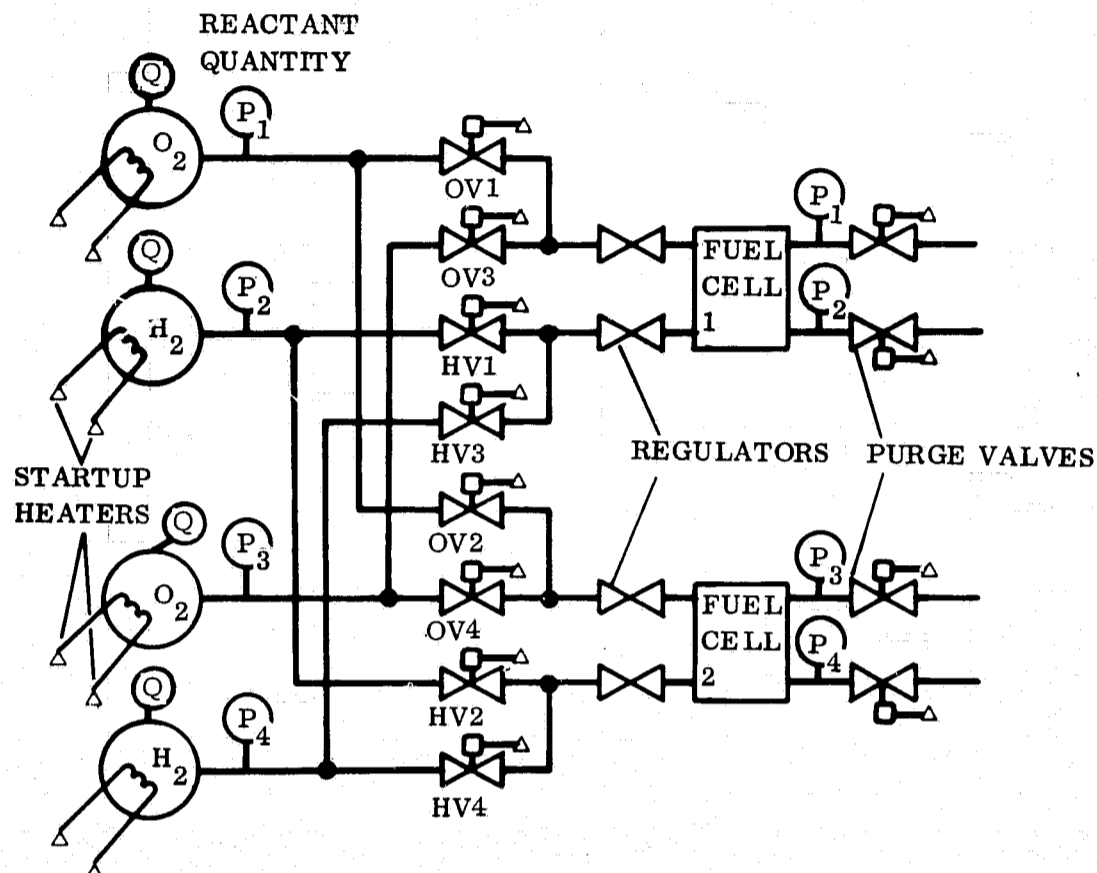
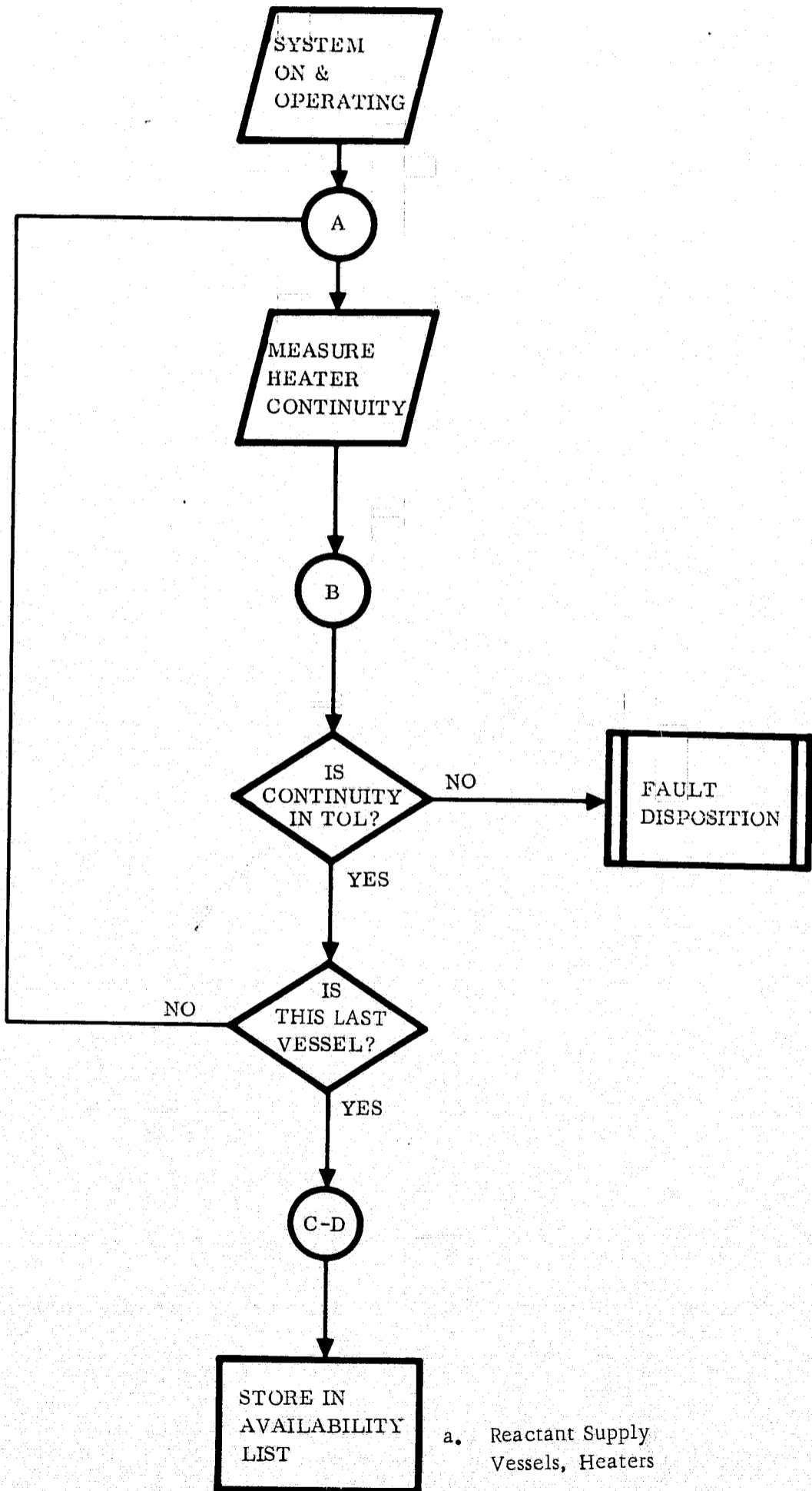


Figure 3-26. Fuel Cell Reactant Supply

module will be detected by charging the fuel cell to regulated pressure and then closing the isolation valves and observing the pressure decay. Leakage may or may not be sufficient to warrant changeover to the redundant system. Operational standards can be defined to regulate the appropriate response to a leakage indication.

Valve Malfunction (Figure 3-27 c and d). Following the leakage check, opening and closing the manifold solenoids and the purge valves and observing the step change in pressure will verify normal valve operation. Action in the event of purge valve malfunction would depend on the malfunction. If the valve will not open, operation can be continued, and fuel cell performance will degrade as a function of the impurities collected in the cells. Eventual changeover to the redundant module will be required when module load sharing becomes out of tolerance. If the valve will not close, the fuel cell module would be isolated and operation continued on the second module.

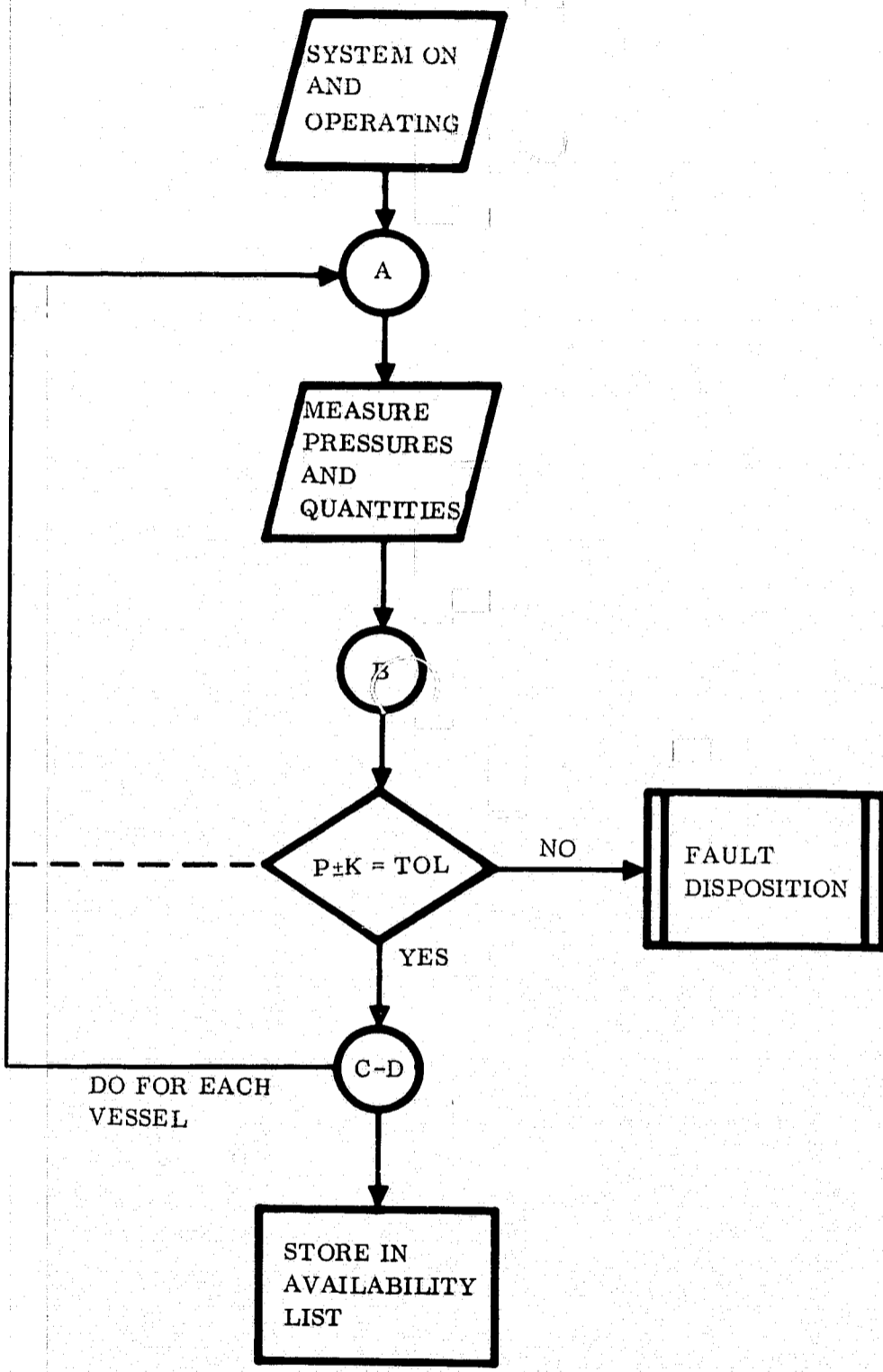
Regulators (Figure 3-27e). A regulator malfunction will be indicated by inability to maintain fuel cell pressure, maintenance of improper fuel cell pressure or inability to pressurize the module. Operation may be continued if fuel cell pressure is off specification but within a limited (possibly emergency mode) band. Otherwise operation will be continued with only the second module.



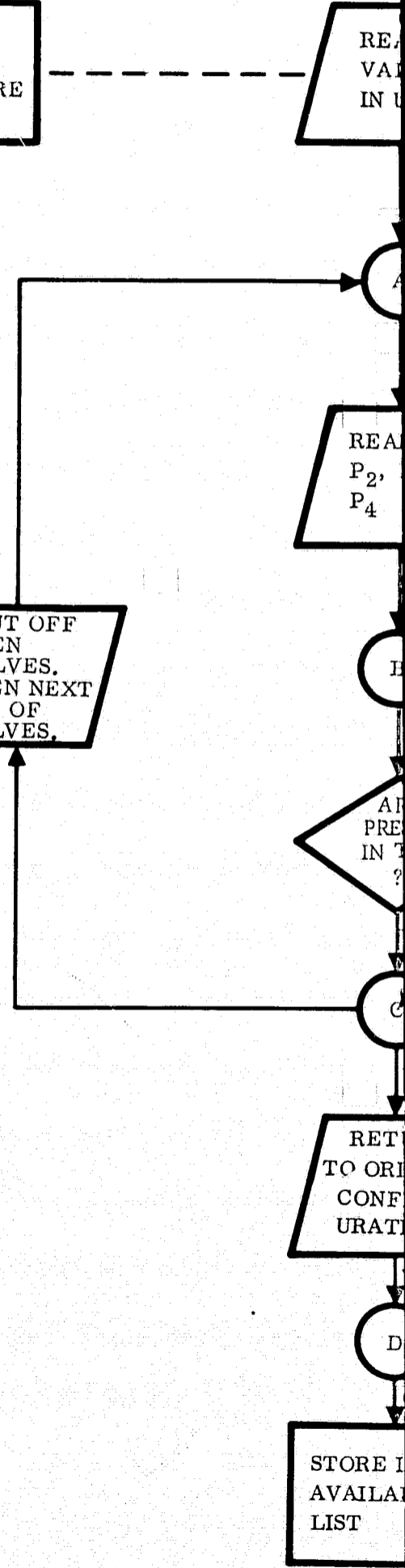
QUANTITY OF FUEL CONSUMPTION. ALSO EVALUATE FOR LEAKAGE

a. Reactant Supply Vessels, Heaters

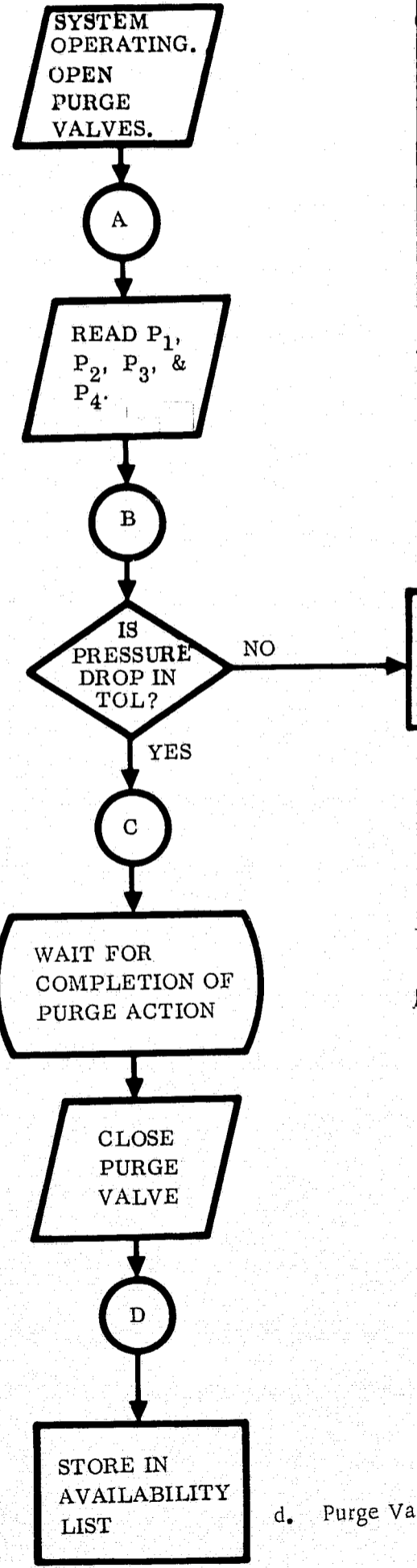
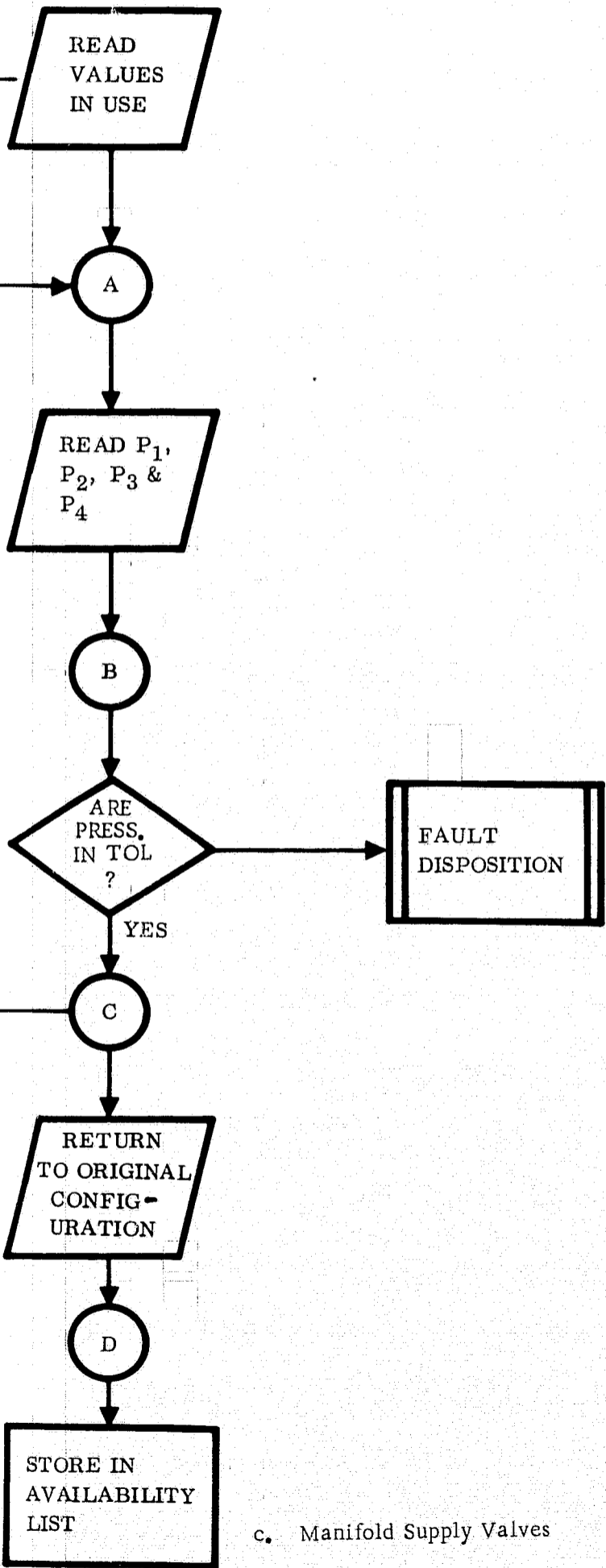
FOLDOUT FRAME /

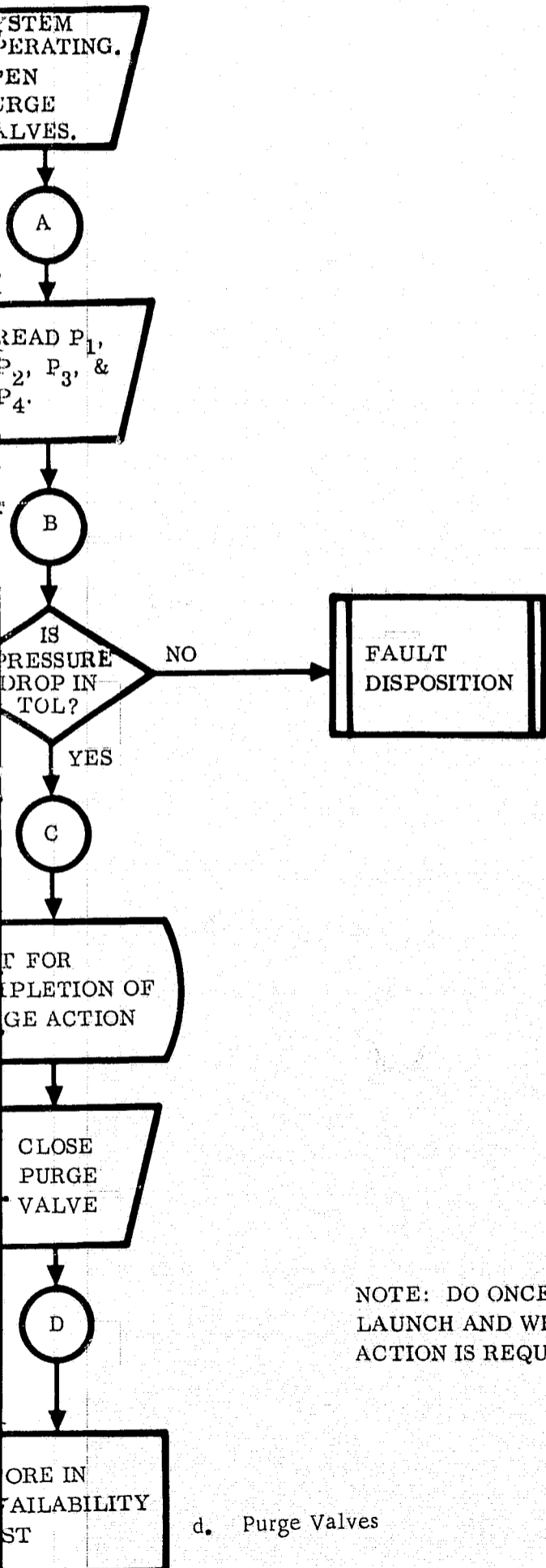


REGULATORS
MUST BE
EVALUATED BEFORE
THIS ROUTINE



b. Manifold and Supply Vessel





NOTE: DO ONCE AT PRE
LAUNCH AND WHEN PURGE
ACTION IS REQUIRED.

d. Purge Valves

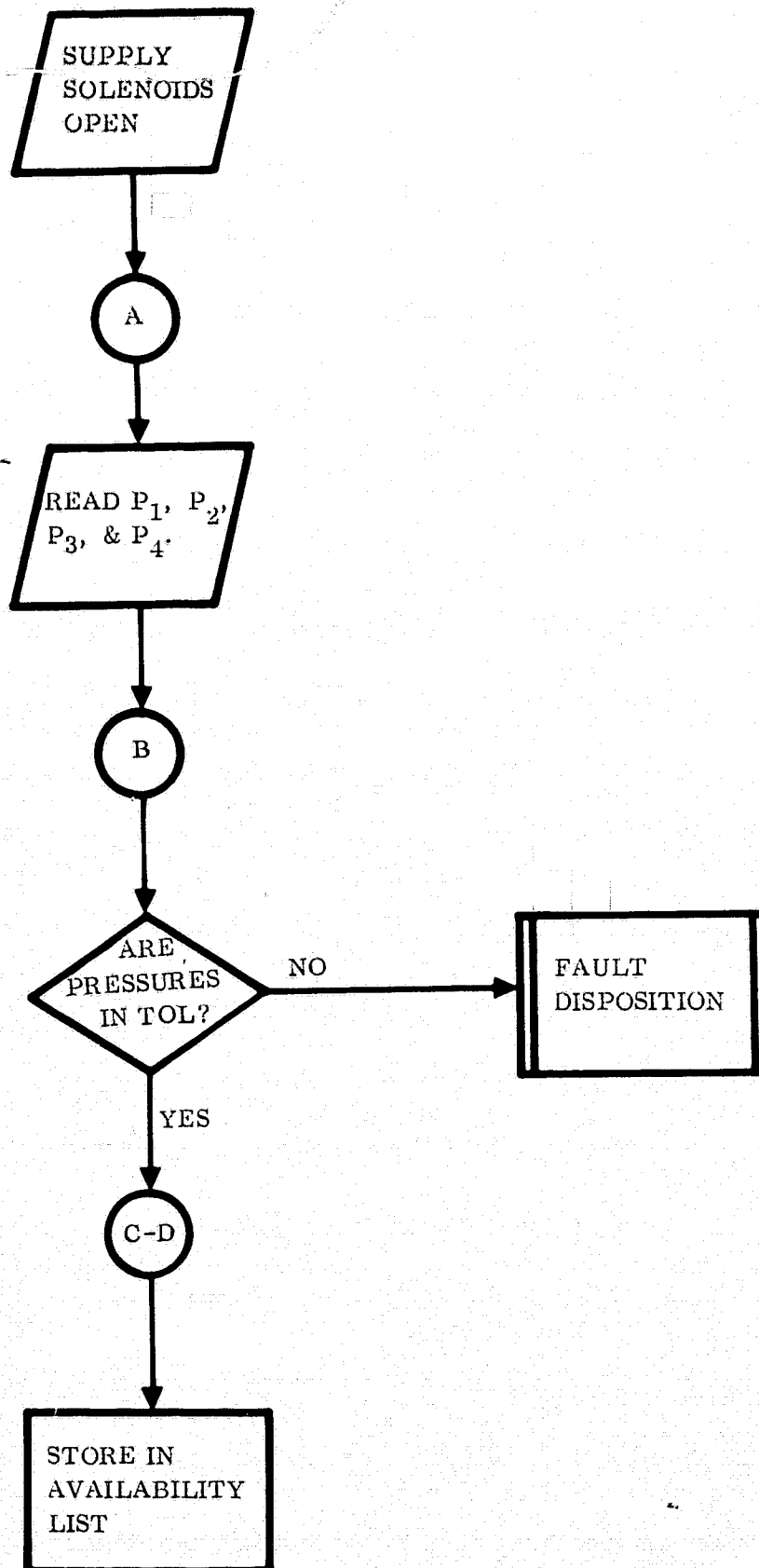
SUPPLY
SOLE
OPEN

READ
P3, &

A
PRES
IN

STORE
AVAILA
LIST

Figure 3-27. Fuel Cell Reactant S



e. Regulators

Figure 3-27. Fuel Cell Reactant Supply Fault Detection Routine

Fuel Cell Module. Cell integrity and membrane permeability will be verified by the leakage check of 1.2.2 if no leakage is observed.

3.9.2.3 Product Water Removal.

Description and Operation. (Flow charts are similar to atmosphere purification loop, Figure 3-16.) Figure 3-28 shows the major components in this accessory system.

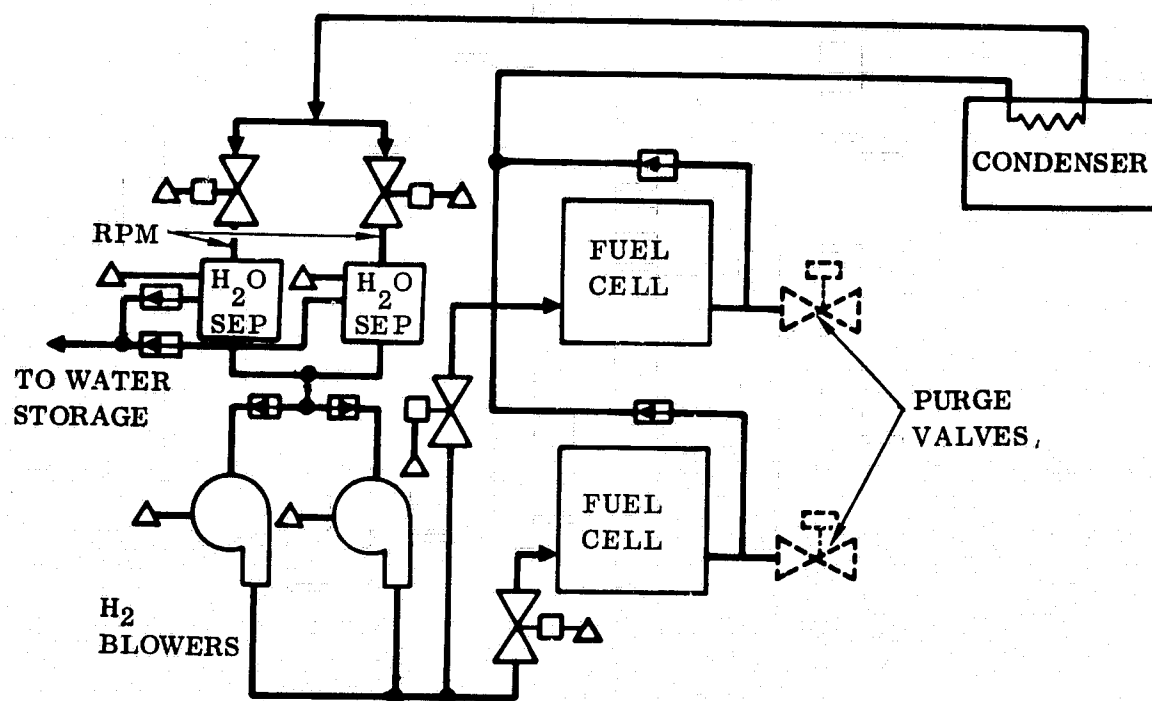


Figure 3-28. Fuel Cell Water Removal

Although other methods can be used to remove product water, this example provides insight into a typical checkout. In this system, water vapor produced from the electrochemical reaction is swept from the cell by circulating excess hydrogen through the module. The H_2 and water vapor then pass through a condensing heat exchanger where most of the water vapor is condensed. The resultant liquid is then centrifugally separated from the gas stream and can be either dumped or stored. The saturated gas stream then returns to the fuel cell to complete the loop. Single redundancies are provided for both the water separator and H_2 blower circuit. Each circuit is capable of servicing either or both fuel cell modules. The condenser is a two-loop configuration to satisfy the failure criteria.

Failure Modes, Detection and Action. Failure of any of the components that causes water not to be removed from the cells will cause an immediate degradation in electrical output. This will be detected by load-sharing being out of tolerance and a drop in module voltage.

Water Separator. Each water separator can be started in turn and operation verified by observing that rpm rises to proper value. Water separator rpm is also sensed to verify continued operation. Failure of the separator water pump will be reflected in a decrease or cycling in separator rotational speed. The faulty separator is then isolated, and the stand-by separator operated.

Water Separator Isolation Valves. With the recirculated loop activated, each valve can be opened and closed in a sequence that cause the operation to be detected by a change in blower output pressure. Either valve can be detected if faulty.

Blowers. Each blower can be checked by observing blower discharge pressure after starting. Continued monitoring of this pressure will detect incipient or actual failure. If failure occurs, the blower is turned off and the second blower is started. Check valves ahead of each blower prevent short-circuiting.

Module Isolation Valves. With the recirculation system operating, these valves may be sequentially operated and the response detected by change in blower discharge pressure. A failed-closed condition of either valve will require operation on the remaining module. A failed-open condition will permit continued operation, even if either fuel cell requires shutdown for other reasons.

Condenser. Condenser failure will be detected as an inability to remove product water from the cells. Voltage of both modules will decrease. Load sharing may or may not go out of tolerance.

3.9.2.4 Thermal Control.

Description and Operation. (Diagnostic flow charts are similar to the ECS/LS thermal control loop.) A typical thermal control system is shown in Figure 3-29. The proposed system interfaces with the spacecraft environmental control system and rejects heat in an intermediate heat exchanger in the ECS loop. The ECS ultimately rejects the heat to the main vehicle heat sink. Since the ECS loop is already temperature controlled, no additional temperature control is required for the fuel cell product water condenser. A liquid pump circulates coolant through the ECS heat exchanger and the product water condenser to a three-way modulating valve. The valve modulates to maintain the fuel cell module coolant discharge temperature to a preselected value. Excess coolant bypasses the module and is returned to the pump inlet. A start-up heater located in the coolant circuit permits rapid heating of the fuel cell to reduce start-up time.

Failure Modes, Detection, and Action.

Liquid Pumps. Operation of either pump is verified by sequentially activating each pump and observing the resultant coolant flow. A redundant pump is activated in the event of pump failure. Check valves at the pump discharge prevents fluid from

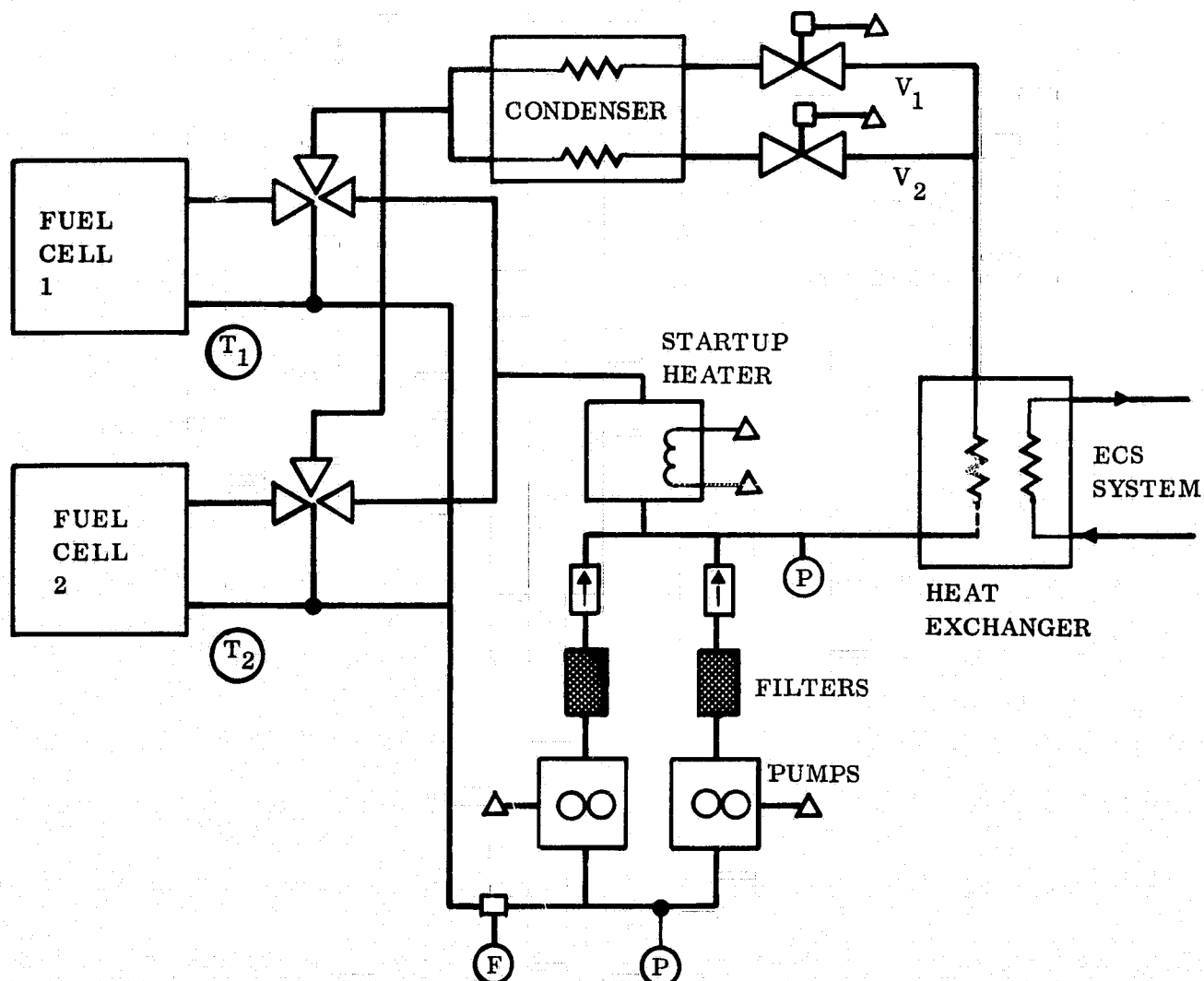


Figure 3-29. Fuel Cell Thermal Control

short-circuiting around the defective pump. System blockage may also be observed by monitoring pump inlet and discharge pressures.

Filters. Blocked or loaded filters will be detected by activating each pump in turn and observing pump inlet and outlet pressure, and also by a low flow indication. This may also indicate stuck or blocked check valves. Operation may be continued, if necessary, until a further fault is observed either in inadequate control of module temperature or lack of water removal.

Startup Heater. The heater may be tested for continuity and warm up time may be observed to determine that the heater is operational. The use of the heater is optional, because the module is capable of boot-strapping to operational temperature.

Thermal Control Valves. Improper operation of the thermal control valves will be evidenced by inability to maintain a preselected coolant discharge temperature from the module. This may be the result of a faulty temperature sensor and/or control, or could be caused by blockage in the valve. The latter fault would be detected as a low flow indication in the coolant loop.

3.9.2.5 Fuel Cell Fault Summary. Table 3-11 summarizes the fuel cell electrical generation and reactant supply fault detection process. This table lists the components (replaceable units) evaluated in preflight as well as the fault isolation process. The performance monitor portion outlines the instruments monitored during the fault detection program and the instruments used during fault disposition routines. The performance monitor section also includes the corrective action control necessary to make a failed portion of the system operational.

Subsystem	Components Evaluated During Startup	Performance Monitoring	
		Instruments Monitored	Failure Mode Instruments
Fuel cell thermal control	<ol style="list-style-type: none"> 1. Modulation valves 2. Coolant solenoids 3. Heat exchanger 4. Start up heater 5. Pump/filters 	<ol style="list-style-type: none"> 1. Cell output temps. 	<ol style="list-style-type: none"> 1. Cell output temps 2. Flow meter 3. Manifold pressures
Reactant supply	<ol style="list-style-type: none"> 1. O₂ supply valves 2. H₂ supply valves 3. Regulator valves 4. Reactant supply man. 5. Quantity gauges 6. Purge valves 7. Supply tank regulator 8. Tank heaters 	<ol style="list-style-type: none"> 1. Cell pressures 2. Manifold pressures 	<ol style="list-style-type: none"> 1. Cell pressures 2. Manifold pressures
Water removal	<ol style="list-style-type: none"> 1. H₂ solenoid 2. H₂ blowers 3. H₂O separators 4. H₂O removal solenoids 5. Condenser 	<ol style="list-style-type: none"> 1. Blower pressure 2. Separator RPM 3. Condenser temp 	<ol style="list-style-type: none"> 1. Blower pressure 2. Separator RPM
Electrical output	<ol style="list-style-type: none"> 1. Fuel cell 2. Battery 	<ol style="list-style-type: none"> 1. Cell current 2. Bus voltage 3. Bus current 	<ol style="list-style-type: none"> 1. Cell current 2. Bus voltage 3. Bus current

FOLDOUT FRAME /

Table 3-11. Fuel Cell Onboard Checkout Removable Unit Fault Summary

Performance Monitoring		Fault Isolation	
Failure Mode Instruments	Corrective Action Control	Components (LRU)	Fault Isolation Method
Cell output temps. Flow meter Manifold pressure	1. Coolant solenoid 2. Pump/filter	1. Modulation valves 2. Solenoids 3. Heat exchanger 4. Start up heater 5. Pump/filters 6. Condenser	Functional Functional Functional Instrument Instrument Correlation
Cell pressures Manifold pressures	1. Purge action 2. Supply valve control	1. O ₂ supply valves 2. H ₂ supply valves 3. Regulator valves 4. Reactant supply man. 5. Quantity gauges 6. Purge valves 7. Supply regulators 8. Tank heaters	Functional Functional Instrument Instrument Correlation Instrument Instrument Instrument/functional
Blower pressure Separator RPM	1. Separator solenoids 2. H ₂ O separator 3. H ₂ blowers 4. H ₂ solenoid	1. H ₂ solenoid 2. H ₂ blowers 3. H ₂ O separators 4. H ₂ O removal solenoids 5. Condenser	Functional Instrument Instrument Instrument
Cell current Bus voltage Bus current	1. Activate battery	1. Fuel cell 2. Battery	Instrument/correlation

FOLDOUT FRAME 2