

PRECEDING PAGE BLANK NOT FILMED

SELF-TEST TECHNIQUES FOR REDUNDANT DATA MANAGEMENT SYSTEMS

Myron Kayton and H. S. E. Tsou

TRW Systems Group
Redondo Beach, California

N71-35065

DESCRIPTION OF DATA MANAGEMENT SYSTEM

The function of the data management system for the Phase B Space Shuttle is to provide a data transmission and data processing service for the avionics equipment and for other vehicle subsystems. It performs all the on-board data processing except that assigned to special processors for engine control, and for analog stability augmentation.

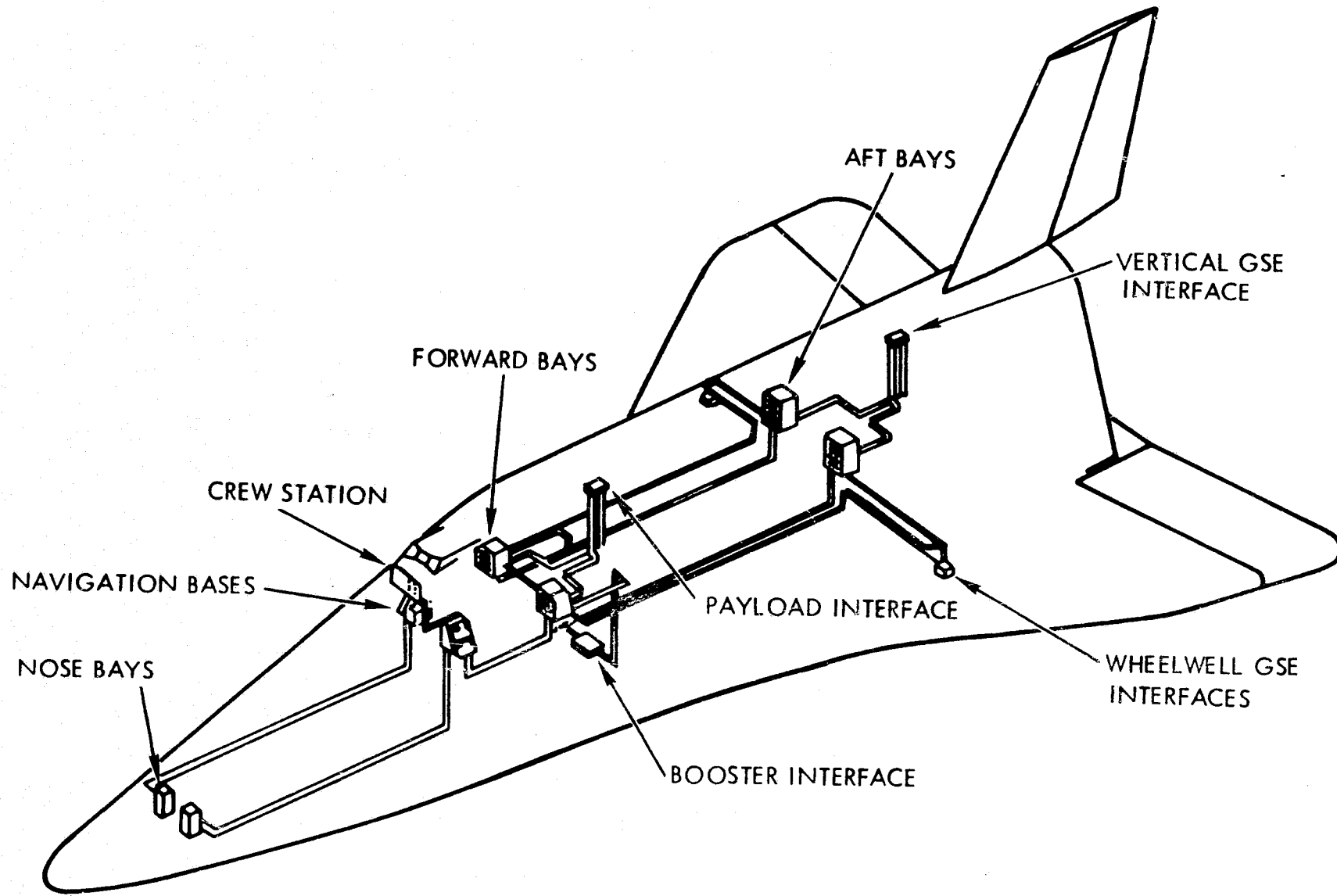
The system consists of quadruply-redundant data buses and computers, and associated equipment. An Input-Output Control Unit (IOCU) is dedicated to each computer. It can operate or monitor all four data buses under software control. It has direct access to a portion of the computer's memory. The System Control Unit (SCU) designates the computer-IOCU that is in control of the data bus and compares status information from redundant computers.

Digital interface units (DIU) in each bay connect the line replaceable units (LRU) to the data bus. The DIU receives and transmits bus messages, multiplex and demultiplex data, performs the analog-digital conversion, applies excitation and stimuli to some of the sensors, and collects status information.

The Bulk Memory stores a copy of the flight program for use if a reload is necessary. It also stores alternate landing site constants and provides a means for loading maintenance tapes in the hangar for subsystem checkout.

The data management system monitors and displays checkout parameters of the LRUs, performs signal switching in case of failure, and performs power switching.

DATA MANAGEMENT SYSTEM



DATA MANAGEMENT DESIGN AND SELF-TEST

The data management system is required to process engine control, autopilot, navigation, and subsystem monitoring signals, of which most are essential for crew safety. As a result, the principal consideration in the system design has been to provide means of detecting failures, and of switching the elements of the data management system. The design utilizes a hierarchy of control:

Crew controls computers via SCU panel, keyboard, and cathode ray tubes.

Crew may select the manual or automatic mode of reconfiguration after a failure.

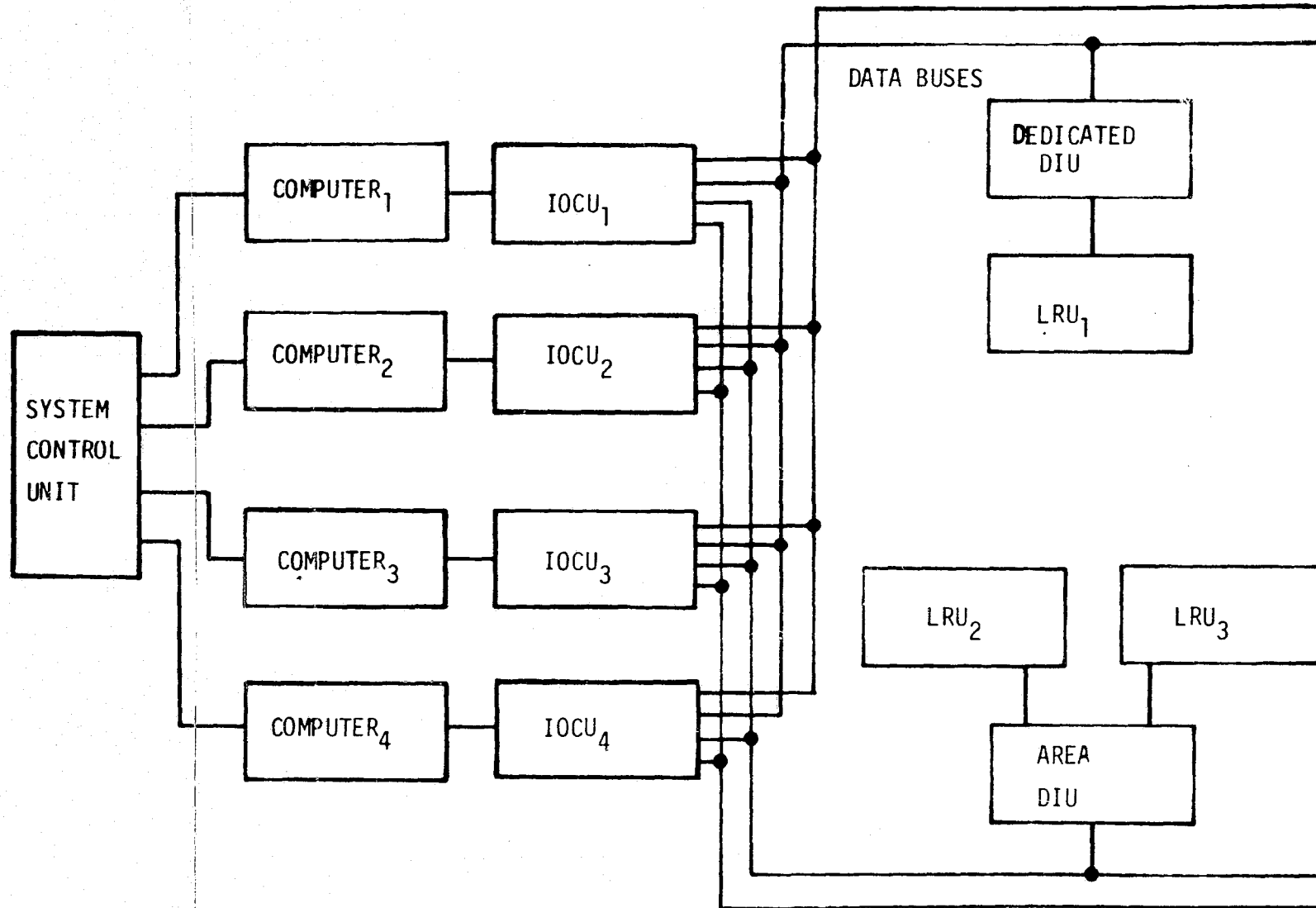
Computer controls testing of IOCU and data buses.

DIU controls its own self-test and also generates stimuli for testing LRUs.

LRUs may test themselves and may vote multiple bus inputs.

The avionic system is designed in two physically separate halves, such that mechanical damage to one half will not affect the other. Replicative redundancy is used in order to meet the "fail-operational, fail-operational, fail-safe" requirement within the two-bay constraint, without excessive equipment. No cross-strapping among the four redundant sheets is used except at the computer complex and at those LRUs that require voters.

DATA MANAGEMENT DESIGN AND SELF-TEST



TEST OF COMPUTER AND IOCU

The controlling computer and the monitoring computers perform the same computations and receive the same inputs. However, only the controlling computer-IOCU issues commands and data to the subsystems. The monitoring IOCU receives the commands and data generated by its own computer in addition to receiving the information on the buses. A discompare will result in switching of the controlling computer or elimination of a monitoring computer-IOCU.

All input data from four (or fewer) data buses are received by all operating computers. These redundant data are compared by software, using the same algorithm in each computer. The end results of the computations are transferred to the IOCU's for transmission on the buses.

Thus, errors in the IOCU and computer are detected by discompares in the IOCU that are sent to the SCU for logical evaluation. A software self-test problem in the computers, and self-test circuitry in the computers and IOCU's assist in evaluating the nature of the failure.

FAILURE DETECTION BY THE SYSTEM CONTROL UNIT

The function of the System Control Unit (SCU) and Panel is to apply power to the computers, to display status of the data management system, and to designate the controlling computer.

The SCU monitors the following computer parameters at all times:

Built-in test discretes from computer and IOCU

power

clocks

IOCU status words

Software self-test

20 millisecond time-ticks

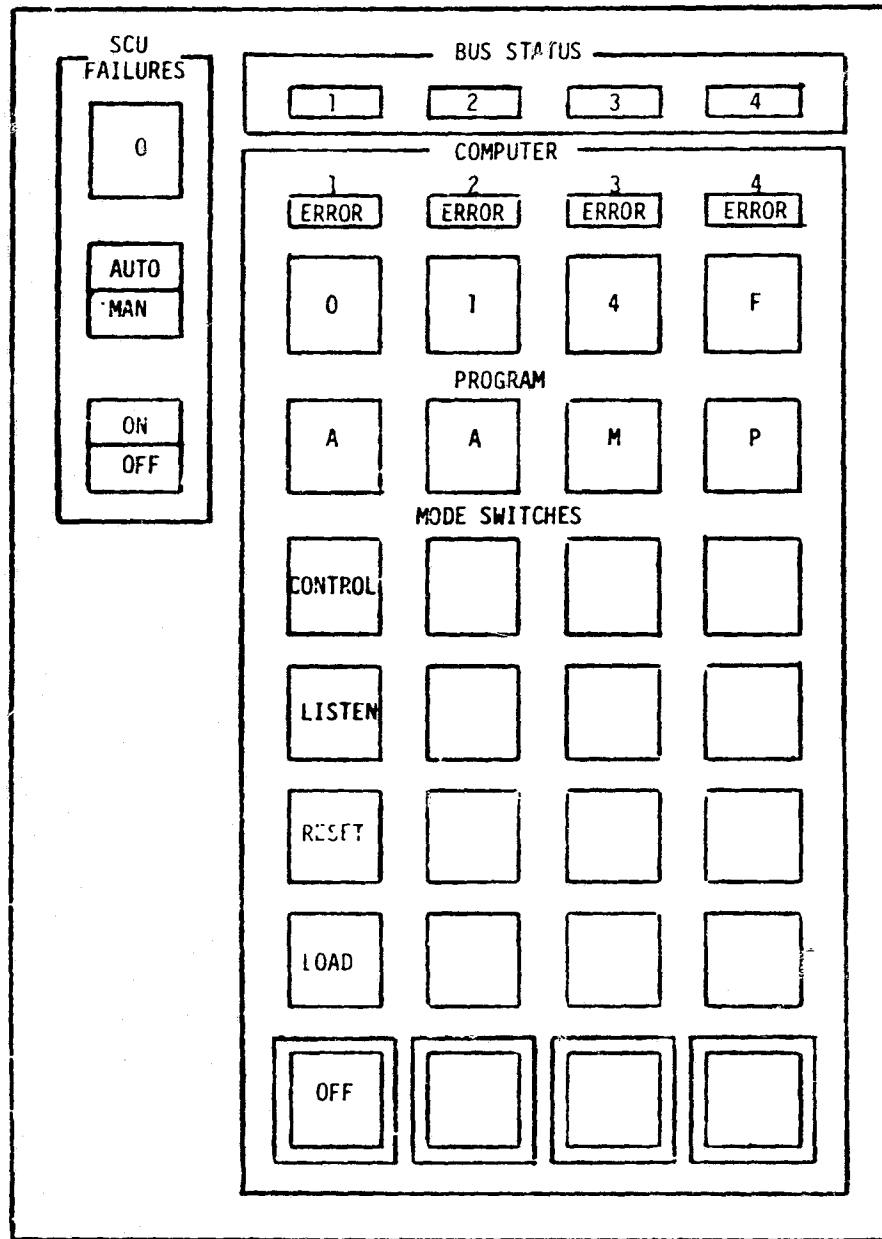
Row and column checks of the reconfiguration tables

The panel allows the computers to be reset after a transient error, and controls the loading of programs into the core memories.

In the manual mode, the crew selects the computer-in-control using the interlocked command switches. In the automatic mode, the SCU chooses the computer-in-control based on the monitored data.

The SCU also displays the bus and DIU status. The crew can monitor failures on the caution-and-warning panel and can perform detailed diagnosis using formats displayed on the cathode ray tubes.

FAILURE DETECTION BY THE SYSTEM CONTROL UNIT



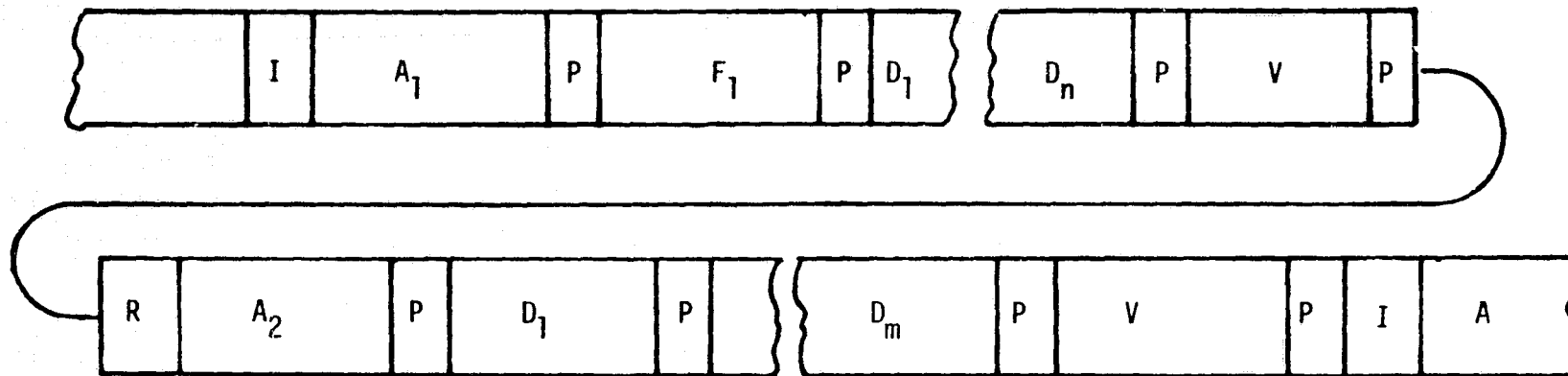
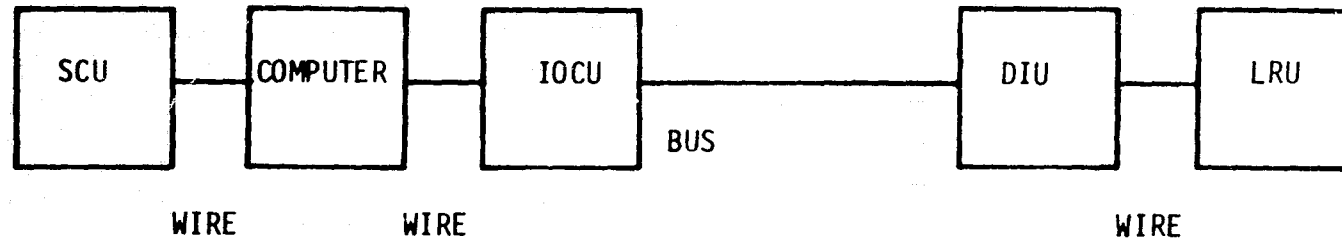
SELF-TEST OF IOCU AND DATA BUS

The input/output control unit incorporates a number of tests to help detect failures in the transmission system. It detects parity errors resulting from accessing the computer's memory. It uses parity checks, an echo check, and a time-out check for data bus operation.

A typical subsystem message format is shown in the figure. It contains a DIU address, a Function Code, a variable number of data bytes, and a message parity byte. The first field contains the address of the DIU being interrogated. The IOCU stores this address and compares it with the responding DIU address. The IOCU monitors the input/output functions and the word count of the data to be transferred. Each 8-bit data byte in the message is checked by use of a horizontal parity bit, and each message is checked by a vertical parity byte. The IOCU also performs a time-out check of the data bus operation to ensure that a response is received within a preset time. This check prevents a non-responding DIU from halting data bus traffic. The modem in the IOCU receives the data which is being transmitted and performs bit-by-bit comparison checks on some of the data. Commands that constitute potential flight hazards are transmitted several times and compared by the DIU before execution to guard against burst errors of long duration.

The probability of an undetected error is 1 in 10^{15} bits for a single-bit error rate of 10^{-5} .

SELF-TEST OF IOCU AND DATA BUS



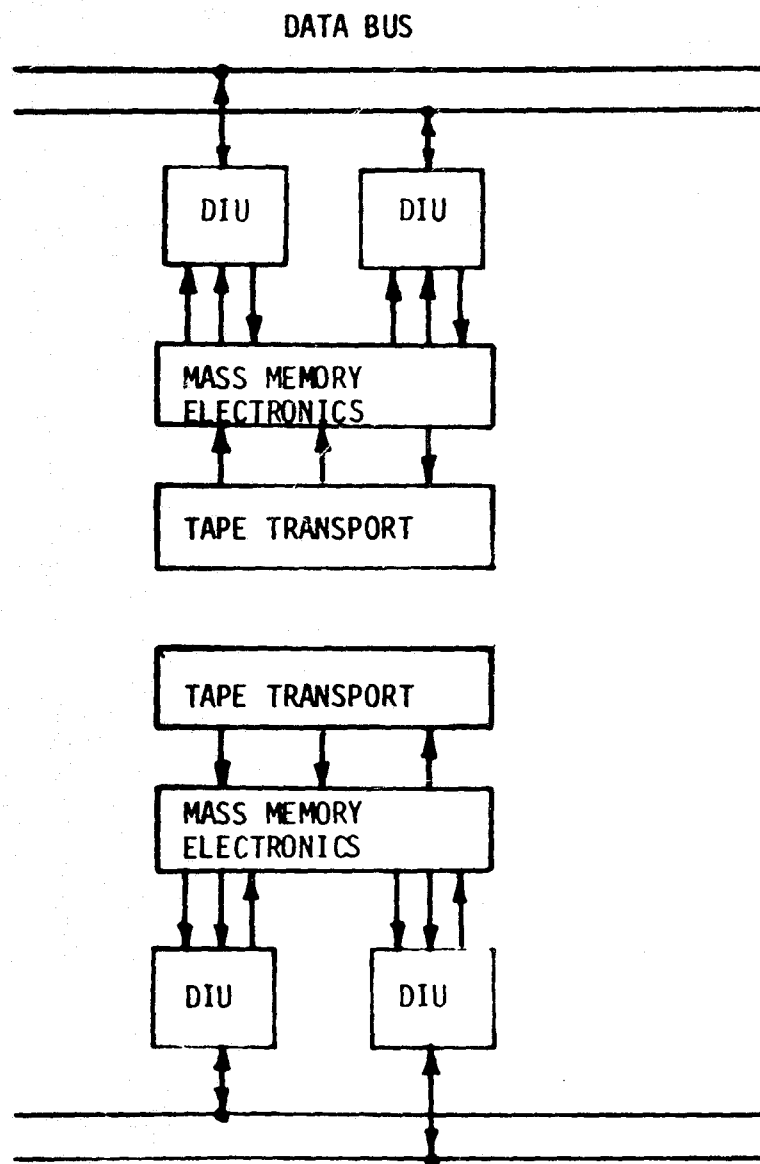
- I : Inter-message gap: minimum 2-bit time
- A₁ : Address of the polled DIU
- F₁ : Function Code
- P : Horizontal (or byte) parity bit
- D : Data bytes
- V : Vertical (or message) parity byte
- R : DIU response gap: 2-bit time

SELF-TEST OF MASS MEMORY UNIT

The mass memory is not required for mission success or for crew safety. Therefore, the degree of in-flight self-test is not as encompassing as for other data management equipment. Because the two mass memories operate in the read-only mode, the self-test is concerned only with reading from the tapes. The information on the tape is stored in block form - each block containing 128, 32-bit words and a sum check. In order to ensure the accuracy of information read from the tape, the data read into core are compared to the data read from a separate track of the same tape unit via a separate DIU and data bus.

The mass memory units have built-in test monitors to assist self-test. These include motor rotation, temperature, pressure, tape movement, operational mode, and power status.

SELF-TEST OF MASS MEMORY UNIT



DIU issues commands and checks BIT.

Memory Electronics controls tape and generates BIT.

DIU-LRU FAILURE DETECTION

Redundant sensors are connected as in Figure (a). The sensor outputs are compared in the central computers. This method of connection permits each LRU to be placed into an independent state. Common actuators such as landing gear, drag brake, chute, engines, control surfaces, and attitude control jets are actuated as in Figure (b). Commands are delivered to these devices by one to four paths. The actuators have the option of comparing the redundant signals in order to protect against faults in the DIU and in the wiring harness from DIU to LRU.

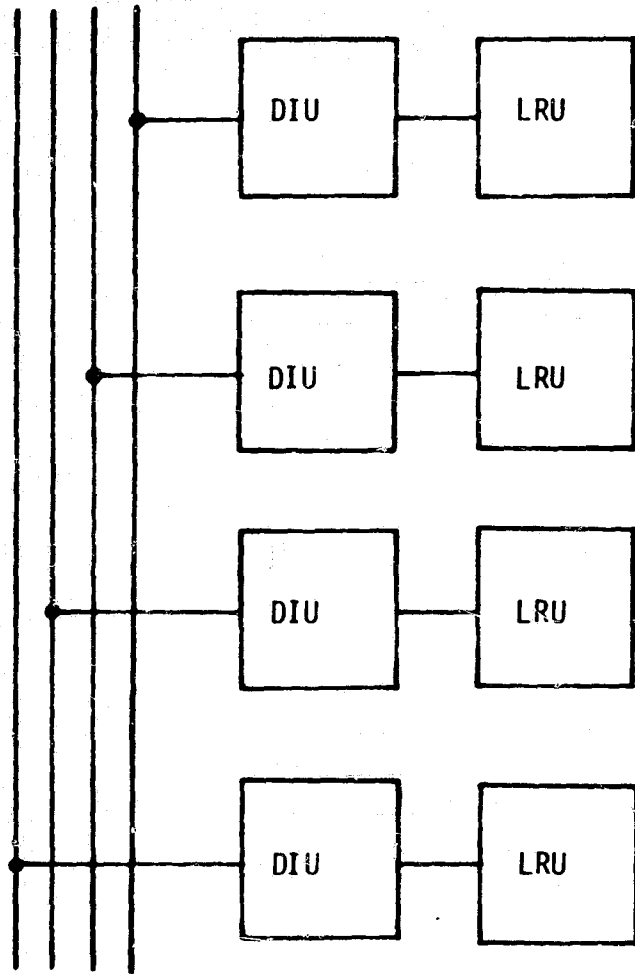
Actuators that incorporate voters must be designed to vote one to four signals depending on the power-on and failure status of each bus. "Data-good" discretes go from each DIU to the voter, and voter status is sent to the DIU for re-transmission to the control computers.

A further test of the DIU itself is provided by built-in test circuits that monitor the power supply and clock, and check the DIU memory. Analog-digital encoders and digital-analog encoders are checked by sending a test signal down the bus once per second to be decoded, recoded, and sent back to the computer. The test also verifies a portion of the multiplexer in the DIU.

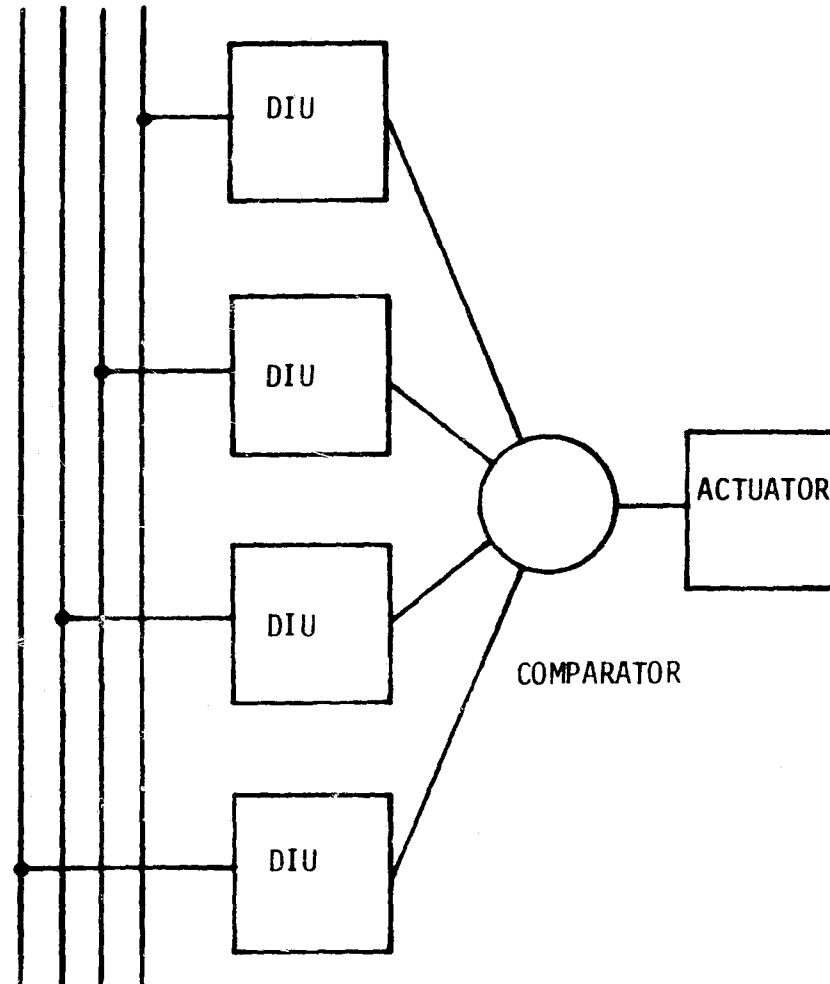
Design of the DIU circuits that apply stimuli to the LRU and measure LRU response is subsystem-peculiar.

DIU-LRU FAILURE DETECTION

a. SENSORS AND INDEPENDENT ACTUATORS



b. COMMON ACTUATORS



SUMMARY OF DATA MANAGEMENT SELF-TEST

Computer Receives Data (Figure a)

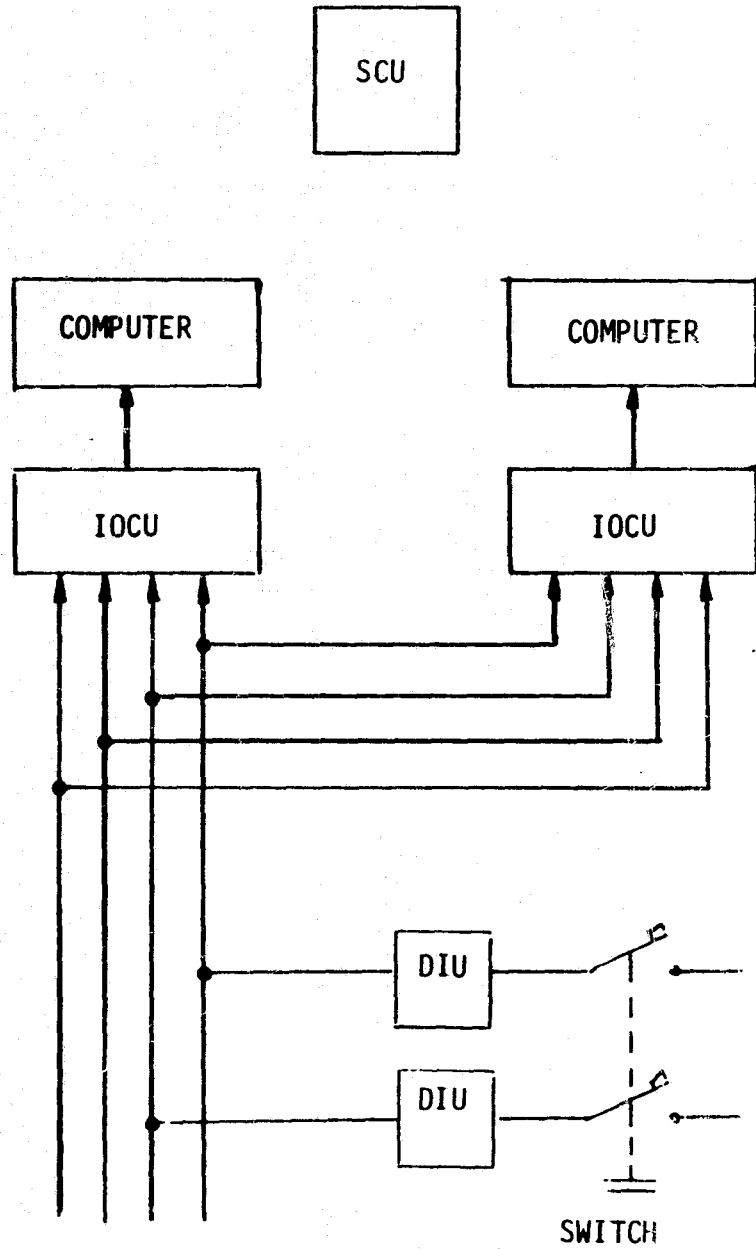
1. The controlling IOCU interrogates DIUs.
2. Each IOCU receives all data from LRUs.
3. Each IOCU transfers data to its computer.
4. Each computer compares redundant data.
 - a. Reasonability test on each signal
variable limit test
change from last measurement
 - b. Comparisons among redundant information
averaging
deviation from mean
 - c. Algorithms are subsystem-dependent

Computer Sends Commands (Figure b)

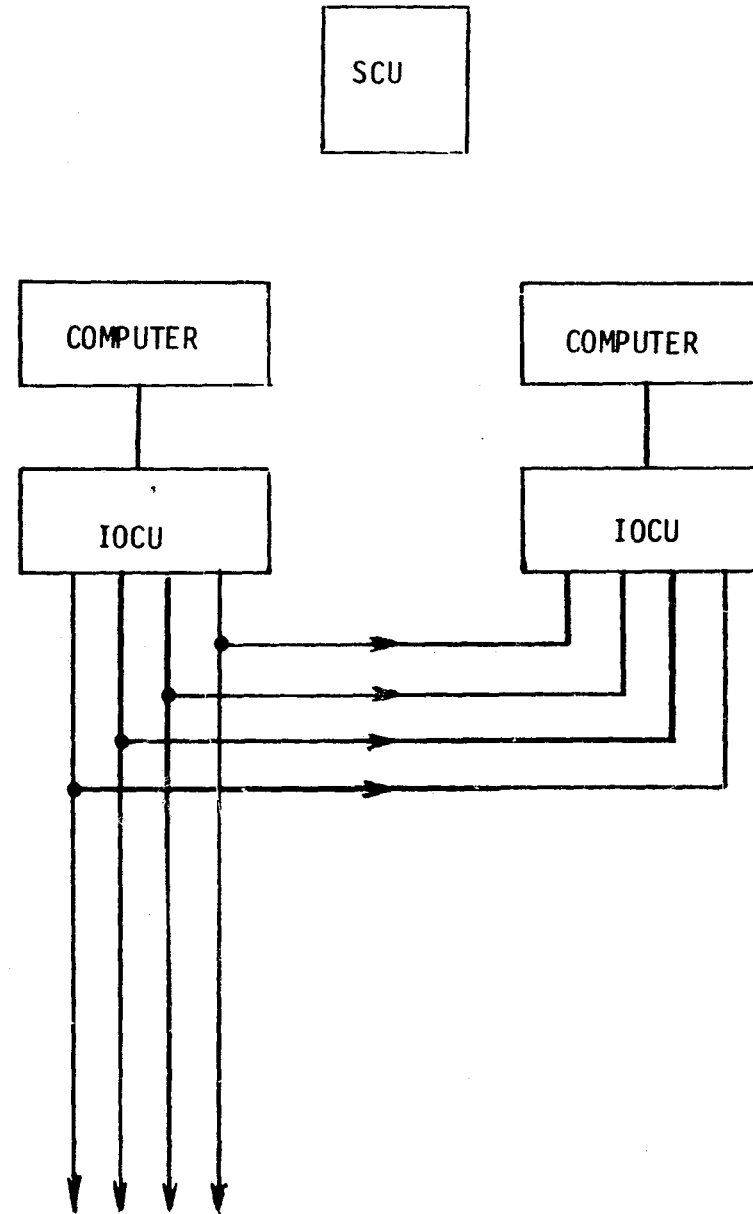
1. Each computer performs identical calculations.
2. Controlling IOCU interrogates panel switches and transmits commands on the bus.
3. Each computer sends commands to its IOCU.
4. Controlling IOCU transmits on four buses (or fewer if some are powered-down).
5. Monitoring IOCUs compare output commands.

SUMMARY OF DATA MANAGEMENT SELF-TEST

(a)



(b)



SUMMARY OF DATA MANAGEMENT SELF-TEST (Continued)

DIU Receives Commands (Figure c)

1. Parity check on each bus.
2. Address echo check on each bus.
3. IOCU repeats critical commands; DIU stores and compares repeated commands.
4. DIU performs closed-loop test and built-in tests.

LRU Receives Commands (Figure d)

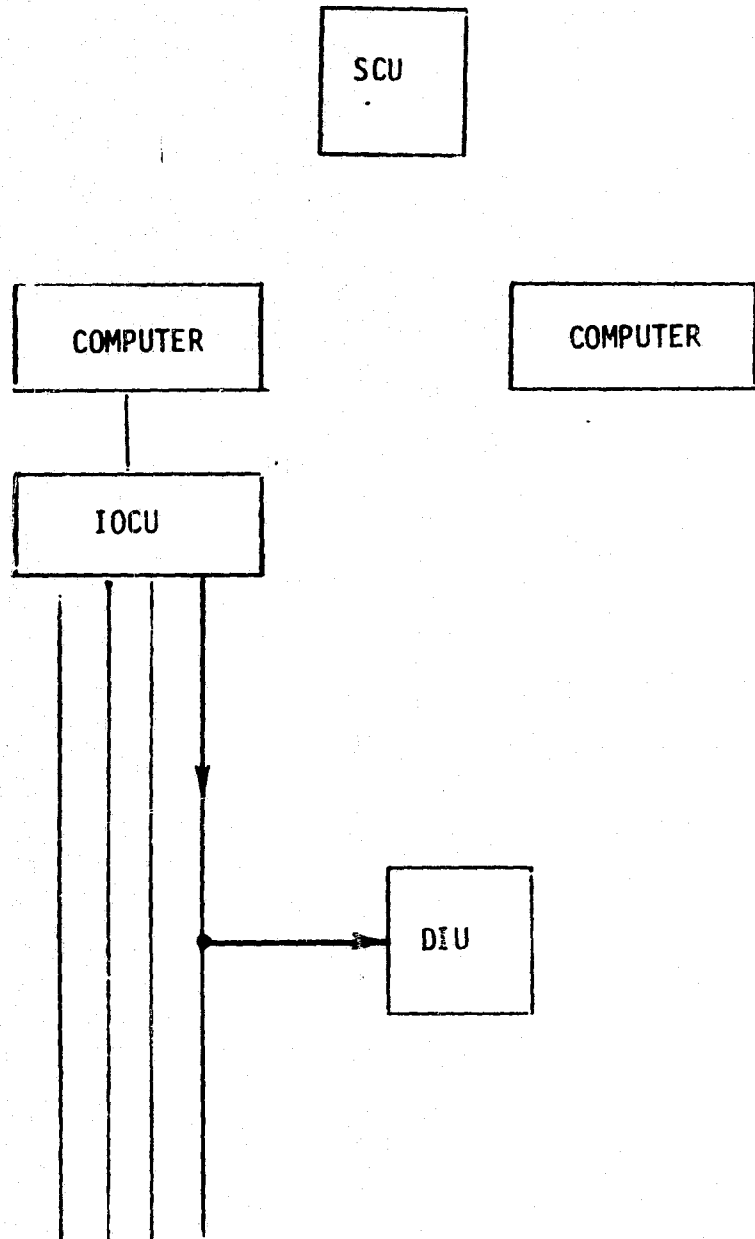
1. LRU votes multiple transmissions.
2. LRU responds to DIU stimuli.

LRU Replies (Figure d)

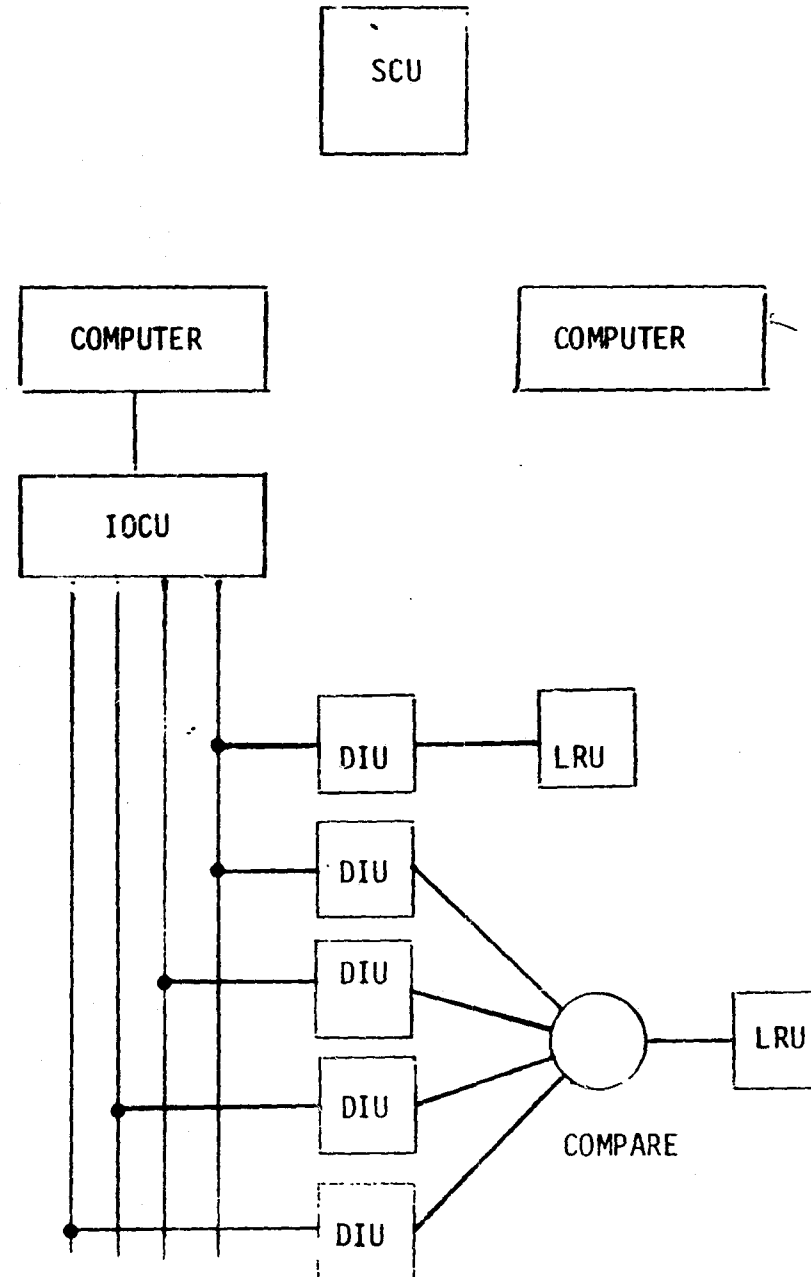
1. DIU samples LRU data.
2. LRU responds to DIU test signal.
3. Bus protection for LRU reply.
 parity
 data word count
4. Return to Figure (a) and repeat.

SUMMARY OF DATA MANAGEMENT SELF-TEST (Continued)

(c)



(d)



CONCLUSIONS

Proposed Method of Self-Test

1. Simplest solution to Phase B requirements.
2. Protects all data paths.
3. Adapts to crew participation in testing and to crew switching of computers and buses.
4. Well-defined hierarchy of control for operation and for self-test.
5. Does not change if subsystems are modified or added.

Problem Areas

1. Voter is potential single-point failure.
2. Internally redundant design of SCU.
3. Form of power transients and dropout, and of noise bursts is unknown. Affects data bus.
4. Redundancy implementation and interlocking of panel switches.

Recommendations

1. Early breadboard to identify hardware and software problems.
2. Early flight test to gain experience with real equipment.