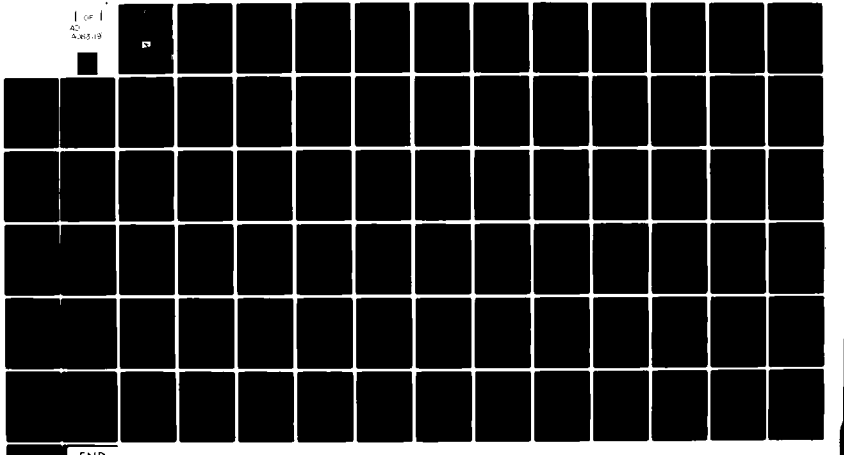
AD-A083 119 AIR FORCE AVIONICS LAB WRIGHT-PATTERSON AFB OH F/G 9/2
COMPUTER PROGRAM DEVELOPMENT SPECIFICATION FOR IDAMST ERROR HAN--ETC(U)
JUL 76
UNCLASSIFIED AFAL-TR-76-209-ADD-3 NL



END
DATE FILMED
5-80
DTIC

ADDENDUM #3

LEVEL III

SPECIFICATION NUMBER SD 2042
CODE IDENT
PART 1 OF TWO PARTS
(DATE) 30 JULY 1976

A047650
A045596

(6)

COMPUTER PROGRAM DEVELOPMENT SPECIFICATION FOR IDAMST ERROR HANDLING AND RECOVERY SYSTEM

SOFTWARE
TYPE B5 • Addendum 3.

(11) 30 Jul 76

(14) AFAL-TR-76-209-ADD-3, SPEC-SD-2042-PT-1

(12) 83

AIR FORCE AVIONICS LABORATORY
AFAL/AAA-1
WRIGHT-PATTERSON AFB, OHIO 45433

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

LIST OF FIGURES

LIST OF TABLES

1.0 SCOPE

1.1 Identification

This part of this specification establishes the requirements for performance, design, test and qualifications of a computer program identified as Operational Flight Program (OFP) IDAMST Error Handling and Recovery System (EHARS) Software.

1.2 Functional Summary

The EHARS Software System is concerned with control of the IDAMST System when system errors and terminal failures occur. In particular, EHARS shall:

a. Perform bus error handling.
b. Perform system failure analysis and modification of the BCIU list accordingly.
c. Halt processing to allow the monitor processor to assume control if a processor/BCIU fails.
d. To direct the reconfiguration scheme in case of processor failure.

2.0 APPLICABLE DOCUMENTS

The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this specification, the contents of this specification shall be considered a superseding requirements.

Specifications

1. OFP IDAMST Executive Software, SD2041

Other Publications

1. Specifications for IDAMST Software Technical Report

3.0 REQUIREMENTS

3.1 Program Definition

3.1.1 Hardware Interfaces

The IDAMST EHARS System interfaces with the following elements of hardware: a Bus Control Interface Unit (BCIU), Remote Terminals, Mass Memory, a Processor Control Panel (PCP), and Processors.

3.1.1.1 Bus Control Interface Unit (BCIU)

The Bus Control Interface Unit (BCIU) shall provide the interface control and data transfer function required to connect a Processor with two multiplexed data buses. The BCIU shall be directed to operate in a mode by its interfacing processor. The following are the modes in which the BCIU shall be capable of operating:

a. Remote Mode, providing transfer of data in both directions between the Processor and either of the two Buses, Providing status replies on the appropriate bus in response to commands, and special internal operations and interrupts to the associated processor upon receipt of certain special commands on the data bases.

b. Master Mode, providing control of the data bus based upon instructions fetched from the memory of the Processor through the Director Memory Access (DMA) Channel by the BCIU.

This Master Control mode shall result in:

1. The BCIU issuing Bus Commands to other devices on the Data Buses.
2. Participating in data transfers on the buses (when the instruction dictates it).
3. Checking status responses from devices on the data buses.
4. Checking formats of the data bus operation.
5. Reporting of error conditions to the processor.

At any time, there shall only be one BCIU in Master Mode.

3.1.1.1.1 Instruction Format

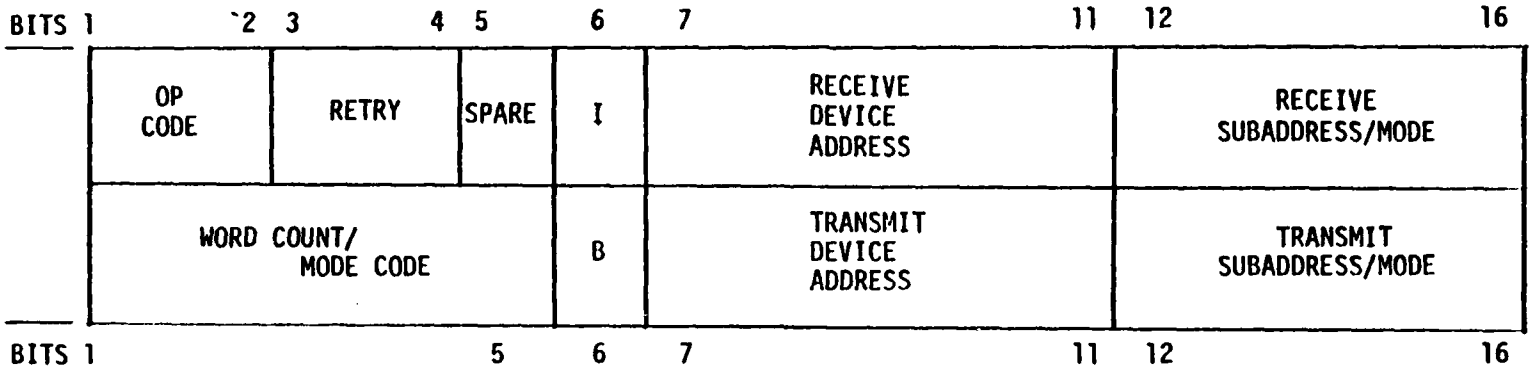
The BCIU instruction list is composed of pairs of instructions accessed by the BCIU using a DMA Channel. The BCIU sequentially interprets instruction pairs to determine the action required. The format of the instruction pair is shown in Figure 1.

Each of the fields in the two word instruction have the following uses:

a. OP CODE - These two bits determine the function of the command.

   00 = Halt the BCIU. This is always the last command in a list and denotes that no other command is to be performed. When the BCIU executes this instruction the Halt bit is set in the Internal Status Register and a BCIU level 1 interrupt will be generated.

   01 = Link. This OP code is used to link sections of the command list. Thus, the individual instructions of the command list need not occupy contiguous memory locations. The second word of the instruction is used as the address of the next two word



B = BIT TO DEFINE WHICH BUS THIS BUS OPERATION SHALL BE PERFORMED ON. (LOGIC 1 SELECTS BIM2)

I = BIT TO INDICATE WHETHER AN INTERRUPT TO THE PROCESSOR UPON SUCCESSFUL COMPLETION OF THE BUS OPERATION. (LOGIC 1 PRESENTS PROGRAMMED CONTROLLED INTERRUPT (PCI) TO PROCESSOR)

RETRY = INDICATOR TO SOFTWARE OF NUMBER OF RETRIES ALLOWED BY THIS 2 WORD INSTRUCTION (MAXIMUM OF THREE RETRIES PER INSTRUCTION)

FIGURE 1. BCIU INSTRUCTION FORMAT

instruction. The other fields of the instruction are ignored except for the interrupt (I) field.

10 = No Operation. This OP code has two uses. The first is to cancel commands which the Master Processor no longer wishes the Master BCIU to perform.

The second is to create a processor interrupt before the next BCIU instruction is generated. A typical use of the latter case is sending Mode Commands. The Mode Data Register must be set before the command is sent. Thus, the interrupt causes a BCIU pause which permits the Master Processor to set the MDR and then set the Continue Bit in the PCR to resume BCIU processing.

For this OP code only the interrupt field is examined. All other options are ignored.

11 = Bus Operation. For this operation the rest of the fields are interpreted as reception or transmission across the Bus.

b. RETRY - If the transmission attempt by this instruction was not successfully completed, and this field is not zero, then the transmission will be retried up to three times.

c. SPARE - This bit is not used.

d. I - If this bit is set, successful completion of this instruction will cause an interrupt. The PCI bit in the ISR will be set. The interrupt will be of level 1. The discussion accompanying the No Operation Code explains the use of this bit, although the bit may be used in any of the four instructions.

e. RECEIVE DEVICE ADDRESS - This field contains the address of the terminal to receive the message. This field is only used for BCIU instruction OP code "Bus Operation" (11). If the Receive Device Address is not the address of the Master BCIU (as contained in the BCIU address field of the PCR), then a Receive Command will be formed by concatenating the Receive Device Address Field, a bit denoting Receive, the Receive Subaddress/ Mode field, and the Word Count/Mode Code field. This receive command will then be transmitted across the Bus.

If the Receive Device Address field is the address of this BCIU and the Receive Subaddress/ Mode field is not zero (i.e., this is not a Mode Command), then the Receive Subaddress field will be used to load the Data Address Register (See Section 3.1.1.1.3.2.12) which will then determine where the received message will be stored.

f. RECEIVE SUBADDRESS/MODE - This field describes the message to be received. The use of this field is described in the Receive Device Address field. If this address were zero it would indicate that this is a Mode Command.

g. WORD COUNT/MODE CODE - For mode commands this field contains the number of the command. For Receive/ Transmit commands this field contains the number of data words to be transmitted.

h. B - This field indicates which Bus will be used for data transmission. If this bit is zero, Bus number one will be used. If this bit is one,

h. Cont'd

Bus number two will be used.

i. TRANSMIT DEVICE ADDRESS - This field is similar to the Receive Device Address except that it is the address of the terminal which will send the message.

If the address is not that of this Master BCIU, then Transmit Command will be formed by concentrating the Transmit Device Address field, the Transmit bit, the Transmit Subaddress/Mode field and the Word Count/Mode Code field.

If the Transmit Device Address field is the address of this terminal then the Data Address Register will be formed (See Section 3.1.1.1.3.2.12) and the data will be written into the Bus from that address.

For Mode Commands the Transmit Device Address field is the address of the terminal to receive the Mode Command and the Receive Device Address field is the address of the Master BCIU.
It is an error for the Receive Device Address field and the Transmit Device Address field to be the same device. This error will cause an interrupt of level 1 and the IVI bit will be set in the Internal Status Register.

j. TRANSMIT SUBADDRESS/MODE - The use of this field has been discussed in the description of the Transmit Device Address field.

For mode commands, both the Transmit Subaddress and Receive Subaddress will be zero.

h. SPARE - Set to logic 0

i. READY - Set to logic 1 by the BCIU after completing its power-on initialization.

j. BUSY/CONT - Set to logic 1 by the remote processor to indicate the BCIU is to enter BUSY state. It is set to logic 0 by the BCIU after having been directed to exit BUSY state.

In Master Mode, the bit is set to logic by master processor to indicate to the BCIU that an interrupt has been processed.

k. RUN - Set to logic 1 by BCIU after being directed to enter an operational mode or upon exiting a BUSY state. It is set to 0 by the BCIU after terminating an operational mode.

3.1.1.1.2 BCIU Registers

The registers of the BCIU control its mode of operation, provide information for the master processor and provide information to its local processor. There are sixteen, 16-bit registers accessible to the processor through the PIO.

These registers and their respective PIO addresses are listed in Table I. Their description follows:

3.1.1.1.2.1 Processor Control Register (PCR)

This register's format is illustrated in Figure 2. The description of this format follows:

a. MASTER - This bit is set to logic 1 by the processor, to direct the BCIU to operate in Master Mode.

b. GO - Set to logic 1 by the processor to indicate the BCIU is to enter an operational mode. A logic 0 indicates the termination of an operational mode. a HALT instruction in Master Mode will set it to logic 0.

c. FAIL - Set to logic 1 after detecting an error in self-test.

d. SPARE - Set to logic 0

e. SYSTEM RESET ACKNOWLEDGE - Set to logic 1 by the processor to indicate acknowledgment of the power-on-reset interrupt.

f. SELF-TEST BY-PASS - Set to logic 1 by the processor to indicate that the BCIU is out to perform self-test.

g. BCIU ADDRESS - These 5 bits shall be set by the processor to indicate the address of the BCIU.

h. SPARE - Set to logic 0

i. READY Set to logic 1 by the BCIU after completing its power-on intialization.

j. BUSY/CONT - Set to logic 1 by the remote processor to indicate the BCIU is to enter BUSY state.

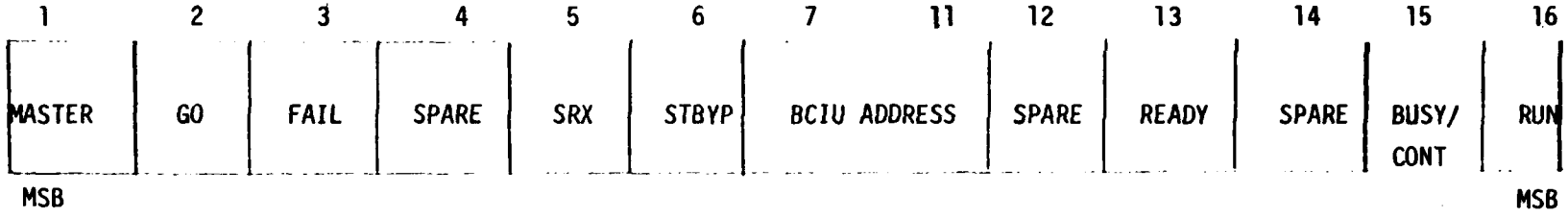
It is set to logic by the BCIU after having been directed to exit BUSY state.

In Master Mode, the BIT is set to logic by master processor to indicate to this BCIU that an interrupt has been processed.

k. RUN - Set to logic 1 by BCIU after being directed to enter an operational mode or upon upon exiting a BUSY state. It is set to 0 by the BCIU after terminating an operational mode.

TABLE I. BCIU REGISTERS

PIO ADDRESS	
0	PROCESSOR CONTROL REGISTER (PCR)
1	INTERNAL STATUS REGISTER (ISR)
2	BASE ADDRESS REGISTER (BAR)
3	INSTRUCTION ADDRESS REGISTER (IAR)
4	BUILT-IN-TEST REGISTER (BITR)
5	MODE DATA REGISTER (MDR)
6	LAST COMMAND REGISTER (LCR)
7	STATUS CODE REGISTER (SCR)
8	MASTER FUNCTION REGISTER (MFR)
9	POINTER REGISTER (PR)
10	DATA ADDRESS REGISTER (DAR)
11	WORD COUNT REGISTER (WCR)
12	XMIT STATUS WORD REGISTER (XSWR)
13	RECV STATUS WORD REGISTER (RSWR)
14	INSTRUCTION WORD REGISTER 1 (IWR1)
15	INSTRUCTION WORD REGISTER 2 (IWR2)



16

FIGURE 2. PROCESSOR CONTROL REGISTER (PCR)

3.1.1.1.2.2 Internal Status Register (ISR)

This register shall be set only by the BCIU. It contains indications of the cause of a BCIU generated interrupt. This register is cleared by the BCIU prior to processing a new instruction or command.

This register's format and the meaning of each bit is indicated in Figure 3. The interrupt levels generated by these bits are also indicated in this figure. A description of each bit follows:

a. HALT (H) - This bit shall be set to logic 1, in Master Mode only, to indicate that the BCM has processed a HALT instruction. The operational mode (Master) shall be terminated.

b. PROGRAM CONTROLLED INTERRUPT (PCI) - THis bit shall be set to logic 1, in Master Mode only, after completion of 2 word instruction operation in which PCI was requested (PCI=1)

c. INVALID INSTRUCTION (IVI) - In Master Mode only, this bit shall be set to logic 1 if the Device Address within the Receive field of the 2-word instruction is equal to the Device Address within the Transmit field.

d. SYSTEM INTERRUPT (SI) - In Remote Mode only, this bit shall be set to logic 1 upon receiving the System Interrupt Mode Command.

e. MODE DATA PRESENT (MDP) - This bit shall be set to logic 1, in Master Mode only, after successfully receiving the Data Word associated with Mode Operations (Interrupt results from mode operations 3,10,11, and 13 - Refer to Paragraph 3.2.1.1.1.).

f. ASYNCHRONOUS MESSAGE XMIT/RECV (AXR) - In Master or Remote MOdes, this bit shall be set in conjunction with Bit 6 (AM) to indicate whether the BCIU was the Receiver (AXR=0) or the Transmitter (AXR=1) of an asynchronous message (Sub-Address =31).

g. ASYNCHRONOUS MESSAGE (AM) - In Master or Remote Modes, this bit shall be set to logic 1 after successful completion of an asynchronous bus message operation (Sub-Address=31).

h. MASTER FUNCTION (MF) - This bit shall be set to logic 1, in Remote Mode only, after receiving the Master Function Mode Command.

i. TRANSMIT STATUS EXCEPTION (XSEX) - This bit shall be set to logic 1, in Master Mode only, after receiving and excepted, valid status word associated with a Remote device in Transmit Mode in which the Message Error, Terminal Failure, or Status Code is non-zero. The status word shall be placed intact within the Xmit Status Word Register.

j. RECEIVE STATUS EXCEPTION (RSEX) - This bit shall be set to logic 1, in Master Mode only, after receiving an expected, valid status word associated with a Remote device in Receive Mode in which the Message Error, Terminal Failure, or Status Code is non-zero. The status word shall be placed intact within the Received Status Word Register.

k. TRANSMIT STATUS ERROR (XSE) - This bit shall be set to logic 1, in Master Mode only, if an expected status word associated with a Remote device in Transmit Mode is not received, is received,

k. Cont'd

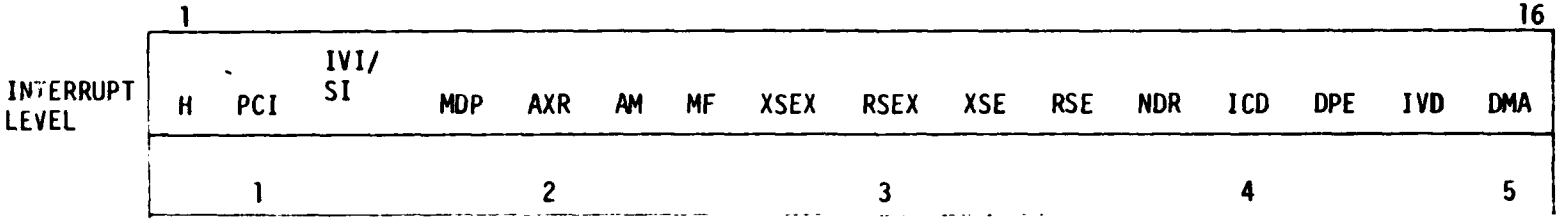
is received invalidly, is received validly with bad parity, or is received validly with good parity with a Device Address that does not match the Transmit Device Address within the 2-word instruction.

l. RECEIVE STATUS ERROR (RSE) - This bit shall be set to logic 1, in Master Mode only, if an expected status word associated with a Remote Device in Receive mode, is not received, is received invalidly, is received validly with bad parity, or is received validly with good parity with a Device Address that does not match the Receive Device Address within the 2-word instruction.

m. NO DATA RECEIVE (NDR) - This bit shall be set to logic 1, in Master Mode only, after commanding a Remote device to transmit one or more data words and the first such data word has not arrived within 60 microseconds after status word reception.

n. INCOMPLETE DATA (ICD) - This bit shall be set to logic 1, in Master Mode only, after receiving at least one expected data word and with further data words expected, the next data word is not received within 60 microseconds after reception of the last data word.

o. INVALID DATA (IVD) - This bit shall be set to logic 1, in Master Mode only, after an expected data word was received with Parity Error indicated. Data word reception continues.



	BIT	MEANING
1	1	H - HALT
	2	PCI - PROGRAM CONTROLLED INTERRUPT
	3	IVI/ - INVALID INSTRUCTION (MASTER MODE ONLY) SI - SYSTEM INTERRUPT (REMOTE MODE ONLY)
2	4	MDP - MODE DATA PRESENT
	5	AXR - A SYNC MSG INT. 0=RECV. 1=XMIT
	6	AM - A SYNC MSG INT.
3	7	MF - MASTER FUNCTION (REMOTE MODE ONLY)
	8	XSEX - XMIT STATUS EXCEPTION
	9	RSEX - RECV STATUS EXCEPTION
	10	XSE - XMIT STATUS ERROR
	11	RSE - RECV STATUS ERROR
4	12	NDR - NO DATA RECEIVED
	13	ICD - INCOMPLETE DATA
	14	DPE - DATA PARITY ERROR
	15	IVD - INVALID DATA
5	16	DMA - DIRECT MEMORY ACCESS (ERROR)

FIGURE 3. INTERNAL STATUS REGISTER (ISR)

p. DIRECT MEMORY ACCESS ERROR (DMA) - This bit shall be set to logic 1, in Master or Remote Mode, after an unrecoverable DMA Error is detected while attempting to fetch an instruction word, a pointer word, or a data word from main memory or while attempting to store a tag word or a data word into main memory.

3.1.1.1.2.3 Base Address Register (BAR)

This register shall be set only by a Processor for the associated BCIU (Master/Remote) and shall contain the most significant 10 bits of a pointer word address within main memory for a given data transfer operation. The addressed pointer word shall contain the true data block address.

3.1.1.1.2.4 Instruction Address Register (IAR)

This register shall be set only by a Processor whose associated BCIU is to operate a Master Mode. The register shall contain the main memory address of the initial 2-word instruction executed, the BCIU shall modify the register in order to reflect the address of the next instruction to be executed. The register shall be unused in Remote Mode.

3.1.1.1.2.5 Last Command Register (LCR)

This register shall be used only in support of the Transmit Last Command Mode Command. In Remote mode, the BCIU shall place commands which are received validly and directed to the particular BCIU into this register. Exceptions shall be Transmit Status Word, Transmit Bit Word, and the Transmit Last Command itself.

3.1.1.1.2.6 Build-In Test Word Register (BITR)

This register shall be used to either maintain the Built-In Test Word (Remote Mode), or to temporarily hold Terminal Failure or bus monitoring of own transmission information

3.1.1.1.2.6 Cont'd

(Master Mode). The format of a BCIU BIT word is shown in Figure 4 and described in the following paragraphs.

a. POWER-ON-RESET - This bit shall be set to logic 1 if the BCIU performs Power-on Initialization.

b. POWER SUPPLY FAILURE - This bit shall not be implemented for the BCIU (Set to Logic 0).

c. BIM 1 OUT - This bit shall be set to logic 1 by the Remote Mode BCIU after powering down BIM 1 as a result of receiving a Remove Power BIM 1 Mode Command. The BIT shall indicate that power has been removed from BIM 1.

d. BIM 2 OUT - This bit shall be set to logic 1 by the Remote mode BCIU after powering down BIM 2 as a result of receiving a Remove Power BIM 2 Mode Command. The bit shall indicate that power has been removed from BIM 2.

e. DMA ERROR - This bit shall be set to logic 1 by the Remote Mode BCIU after an unrecoverable direct memory access error is detected while fetching data words from or storing data words (excluding tag words) into main memory.

f. FAILURE CODE ERRORS - The failure code shall be set to indicate detected self-test failures as follows:

- o No failure 00000
- o BIM #1 failure 10001
- o BIM #2 failure 10010
- o MROM Parity Error 10011

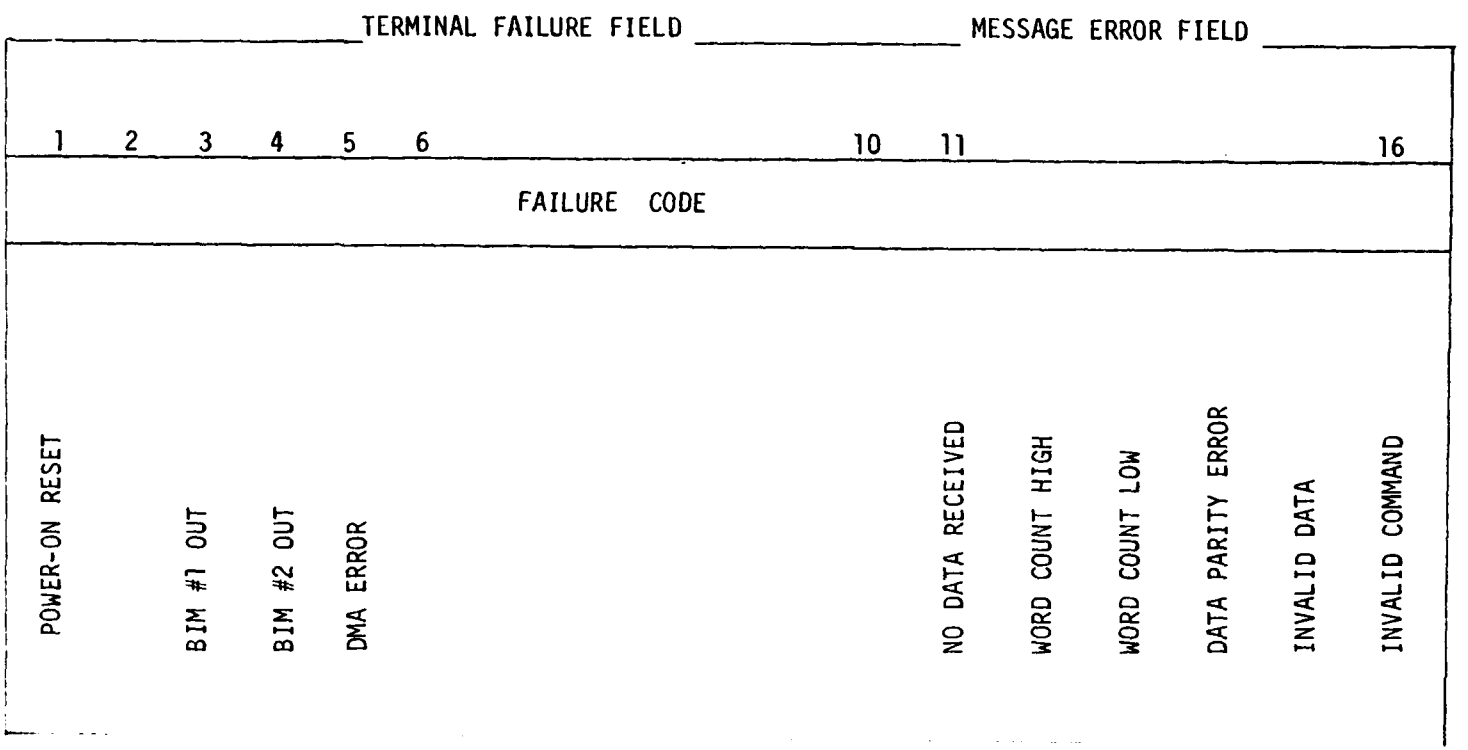


FIGURE 4. BCIU BUILT-IN-TEST (BIT) WORD FORMAT

f. Cont'd

- o BCM Data Flow Error 10100
- o BCM DROM Error 10101
- o BCM SEQ Error 10110
- o PIM DMA Data Flow Error 10111

g. NO DATA RECEIVED - This bit shall be set to logic 1 by the Remote BCIU after having been directed to receive one or more data words and the first such data word has not arrived within 75 microseconds after command word reception.

h. WORD COUNT LOW - This bit shall be set to logic 1 by the Remote Mode BCIU after having been directed to receive two or more data words, at least one such data word has arrived, but the next expected data word does not arrive within 60 microseconds of last data word reception.

i. WORD COUNT HIGH - This bit shall be set to a logic 1 by the Remote Mode BCIU after detecting another Data Word after the word count is zero.

j. DATA PARITY ERROR - This bit shall be set to logic 1 by the Remote BCIU after an expected data word was received with Parity Error indicated. Data word reception continues.

k. INVALID DATA - This bit shall be set to logic 1 by the Remote Mode BCIU after an expected data word was received with RECV WORD INVALID indicated. Data word reception continues.

l. INVALID COMMAND - This bit shall be set to logic 1 by the Remote BCIU after receiving a mode command in which the mode code designates an invalid operation for the BCIU.

3.1.1.1.2.7 Status Code Register (SCR)

This register shall be used in Remote Mode only and shall be set and reset by the Remote Mode Processor. The actual status code shall be the nine (9) least significant bits of the register and shall be merged into any status word prior to status word bus transmittal by the Remote BCIU.

3.1.1.1.2.8 Master Function Register (MFR)

This register shall be used only in support of the Master Function Mode Command. In Master Mode and in accordance with Master Function processing, the contents of the register shall be transmitted to the Remote device as a data word immediately following the command word. It shall be the Master Processor's responsibility to set the register. In Remote Mode, the Remote Mode BCIU shall place the received data word, in response to the Master Function mode command, into the Master Function Register. It shall be the Remote Processor's responsibility to then interpret the contents of the register.

3.1.1.1.2.9 Instruction Word Register 1 (IWR1)

This register shall be used in Master Mode only to hold the first half of the current 32-bit instruction.

3.1.1.1.2.10 Instruction Word Register 2 (IWR2)

This register shall be used in Master Mode only to hold the second half of the current 32-bit instruction.

3.1.1.1.2.11 Xmit Status Word Register (XSWR)

This register shall be used in Master Mode only to hold any status word received from a Remote Device in Transmit Mode, in which the Message Error, Terminal Failure, or Status Code fields were non-zero.

3.1.1.1.2.12 Received Status Word Register (RSWR)

This register shall be used in Master Mode only to hold any status word received from a Remote device in Receive Mode, in which the Message Error, Terminal Failure, or Status Code fields were non-zero.

3.1.1.1.2.13 Mode Data Register (MDR)

In Master Mode, and only in accordance with performing a certain class of mode commands, the contents of this register shall be transmitted to the Remote device as a data word immediately following the command word. The Master Processor shall be responsible for setting the register.

In Remote Mode, the MDR shall be undefined for the Mode Operations defined.

3.1.1.1.2.14 Pointer Register (PR)

This register shall be set by a BCIU operating in either Master or remote mode and shall contain the initial data area address for a given data bus operation involving main memory data transfers. The register shall be use in Tag Word Operations.

3.1.1.1.2.15 Data Address Register (DAR)

This register shall be set by a BCIU operating in either Master or Remote mode and shall be used to indicate the main memory address of the next data word to be fetched/ stored in support of a given bus operation. The register shall be derived from the Pointer Register and in all cases (Receive or Transmit) that value shall be initially incremented by 1 to get over the Tag Word. This value then becomes the address to fetch/store the first data word. As each word is fetched/stored, the BCIU shall increment the register value by 1 to affect sequential data word

3.1.1.1.2.15 Cont'd

fetch/stores.

3.1.1.1.2.16 Word Count Register WCR)

This register shall be derived from the Bus Command and set by the BCIU in either Master or Remote Mode. In Bus Operations involving data word transfers, it shall indicate the remaining number of data words to be transferred. The register shall be decremented by 1, by the BCIU, as each data word transfer is performed.

3.1.1.1.3 Interrupt Generation

The BCIU shall examine the Program Controlled Interrupt Indicator within the Instruction Word One Register (IWR1). If set to logic 1, the BCIU shall set the PCI indicator within the ISR to logic 1. (See Figure 4).
The BCIU shall begin to examine the contents of the ISR from right to left, one field at a time. If any field is found to be non-zero, the BCIU shall discontinue the examination and present the corresponding level interrupt as indicated in Figure 4.

3.1.1.2 Remote Terminals

3.1.1.2.1 Basic Characteristics

The Remote Terminal (RT) provides the interface between the IDAMST Multiplex System and an Aircraft Subsystem.

The RTs provide for Bus communication with the IDAMST processors (as described in Section 3.1.1.12).
The subaddress field of each Transmit or Receive Command acts as a message identifier. The message is formatted by the RT for correct interface with the Interface Modules (IM) which relay (or accept from) the signals to the

3.1.1.2.1 Cont'd

aircraft subsystems.
The RT also acts as a buffer, holding the message until correct transmission has occurred.

The RT performs all the error checking and setting or error and status bits of a remote BCIU.

3.1.1.2.2 RT Functions

The RT shall contain the registers, logic, decoders, buffers, comparators and control sequences required to perform the following functions:

a. Receive Command Words from the Bus.
b. Detect Command Words directed to this RT.
c. Receive Data Words from the Bus (one at a time) if directed to do so by the received Command Word.
d. Transmit Data Words through the Bus to the data bus (one at a time) if directed to do so by the received command Word.
e. Transmit Status Words through the Bus to the data bus as directed by the received Command Word.
f. Perform Mode Operations when and as directed by received Command Words.
g. Distribute received Data Words to the proper channels of the proper IMs.
h. Input Data Words from the proper channels of the proper IMs for transmission to the data bus.
i. Maintain the Status Word of the RT by performing continuous and periodic self test functions within the RT.
j. Maintain an Activity Word and Error Word for monitoring status of serial digital IM's.
k. Maintain a Last Command Register for verification of command receipt in the event of an invalid response.

3.1.1.2.2 Cont'd

1. Perform Bit and Word Masking.

3.1.1.3 Processor Control Panel (PCP)

The IDAMST Processor Control Panel is illustrated in Figure 5 and its description as follows.

3.1.1.3.1 IDAMST Bus Power Switch

The function of these switches is to provide the required signal to the power control unit to turn on and off the power supplied to the multiplex elements (Remote Terminal side A and B, and the Bus Control Interface Units). Those switches shall also control power to all other processor control panel functions. These switches shall be push-on, push-off, and backlighted to indicate the "on" condition.

3.1.1.3.2 Processor Power Switches

The function of these switches is to provide the control signal to the power control unit to turn on or off each IDAMST processor. One switch shall be supplied for each processor. The processor "power on" signal shall also be supplied to the advisory caution panel circuitry to control the processor failure indication. The switches shall be push-on, push-off and backlighted as described below.

3.1.1.3.3 Processor Interrupt - Startup/Restart

This switch, when depressed, shall enable the startup/restart interrupt to each IDAMST Processor. The processor shall enter the Startup/Loader program and perform complete system restart as defined in the IDAMST System Control Procedures. This switch shall be a momentary switch and backlighted while depressed.

3.1.1.3.4 Processor Interrupt - Reconfiguration

This switch, when depressed, shall enable the reconfigure to interrupt to each IDAMST Processor and cause the Master Executive performing system control either Master Executive in Master Processor or Monitor PROCESSOR) to initiate reconfiguration. Reconfiguration is performed after one or more processors have failed; the system is in either the recovery or backup mode; and the pilot manually initiates reconfiguration.

3.1.1.3.5 Press to Test

The function of this switch shall be to test all lights on the PCP.

3.1.1.3.6 Switch Indicators

3.1.1.3.6.1 IDAMST BUS Power and Processor Interrupts

These switches shall be backlighted to indicate the "on" condition.

3.1.1.3.6.2 Processor Power

These switches shall be backlighted as follows:

a. White - Indicates the switches have been depressed
b. Green - Indicates ("GO") that power has been supplied to the processor and the "Processor GO/NO-GO" signal has been set to the "GO" state within the previous 40 msec.
c. Red - Indicates ("Fail") processor power is "on" and the absence of the "GO" signal for more than 40 msec.

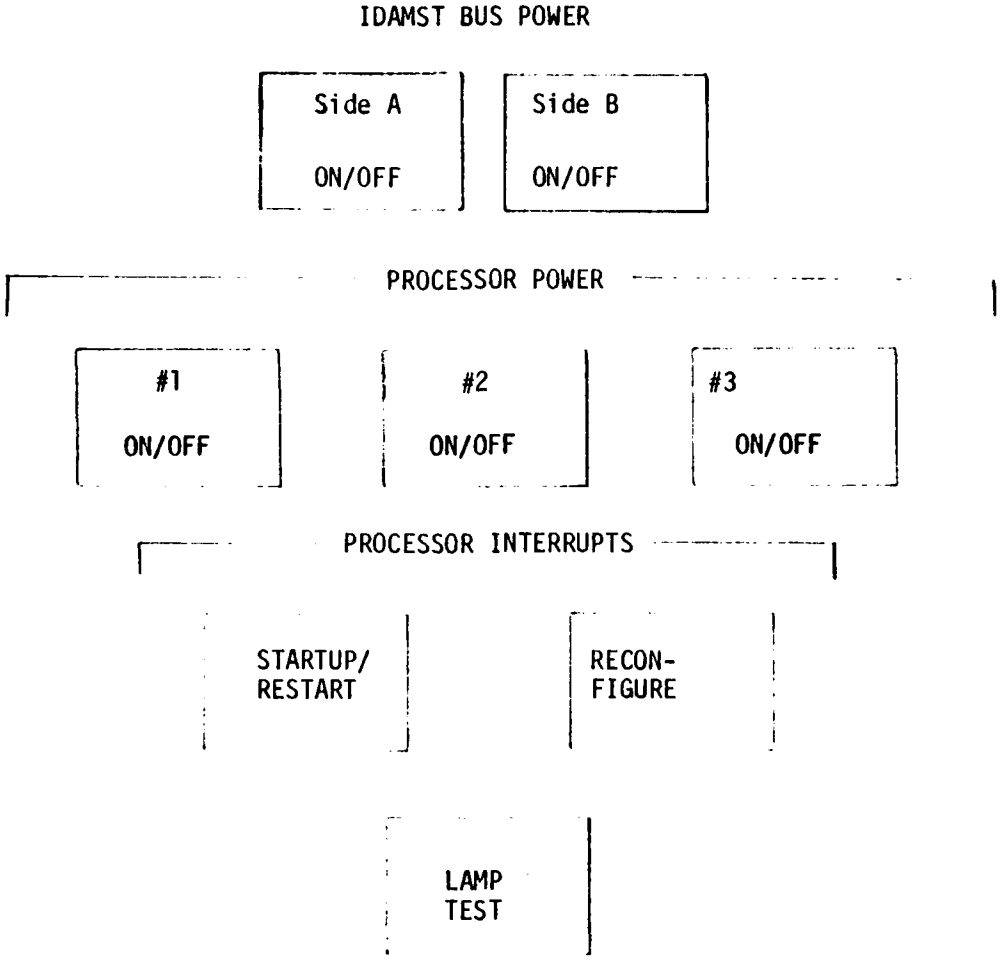


FIGURE 5. IDAMST Processor Control Panel (PCP)

3.1.2 Software Interfaces

The IDAMST EHARS software interfaces directly with the IDAMST Executive Software. The Executive Software, as described in Document SD 2041, controls all interactions with the application software, the Remote Terminals, Processors and BCIU's under normal conditions. Under abnormal conditions detected by the Executive System control will be transferred to EHARS. EHARS will exercise control until the system error or failure is resolved.

Figure 6 illustrates the interface between the Executive and EHARS Software.

3.2 Detailed Functional Requirements

The EHARS software shall perform system error/failure management by:

a. Acknowledging the reception of an unsuccessful transmission.

b. Reporting the messages first, in the same bus, and then on the alternate has if message retry is indicated.

c. Analyzing detected message error, terminal failure status information; and message sequence history to detect and isolate failure to the core elements.

d. Request self-test be performed wehen core element is suspected as failed, and declare core element as failed if self-test is not successful.

e. Report declare failures, establish configuration management and direct a reconfiguration as directed by the pilot.

Figure 7 illustrates the lop level functional flow of the Error Handling and Recovery System (EHARS) Software.

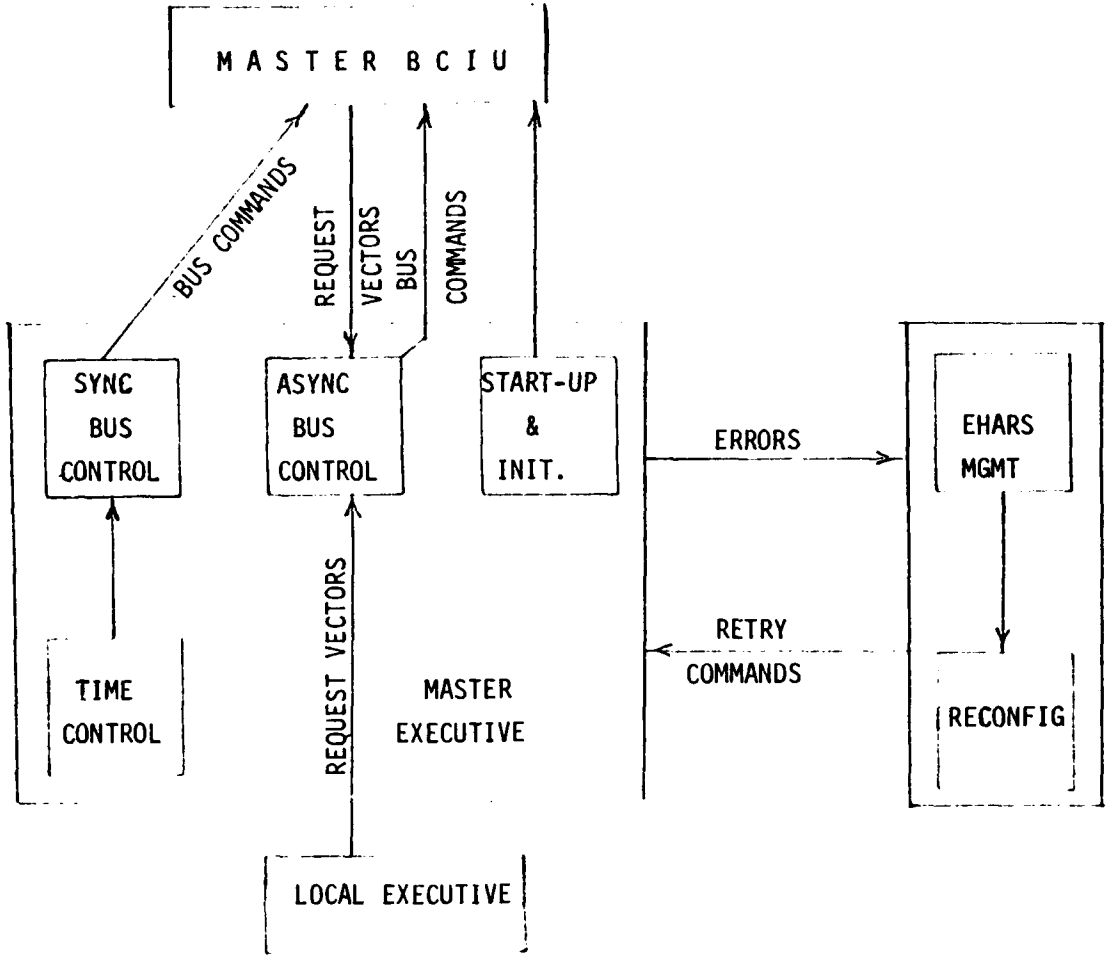


FIGURE 6. EHARS AND EXECUTIVE INTERFACE

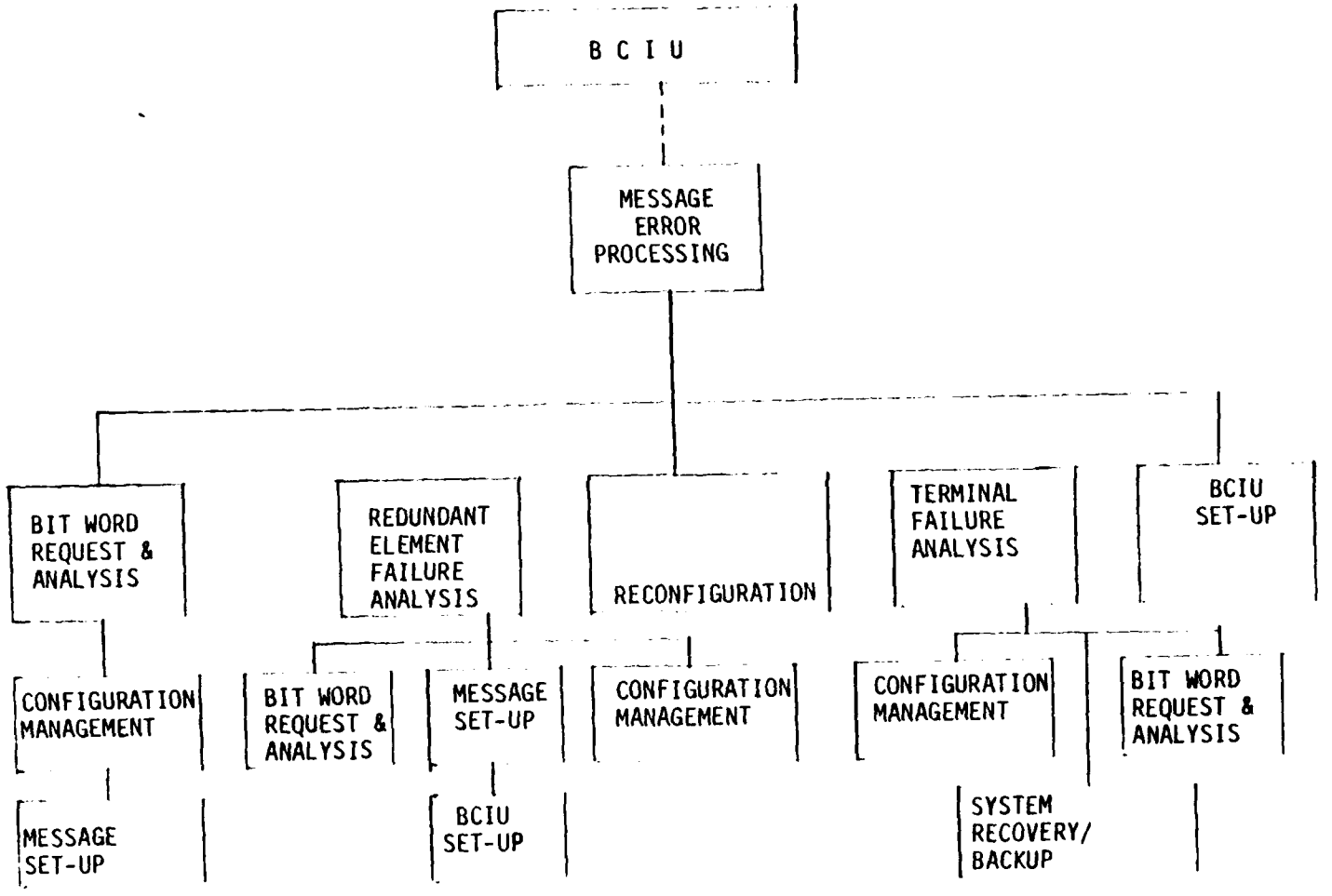


FIGURE 7. EHARS FUNCTIONAL FLOW

3.2.1 Function One - Message Error Processing

This function will be entered upon recognizing the occurrence of a core element error or, if already in an error processing mode, the reception of a successful error handling message transmission. This function serves as a traffic control toward the rest of the functions listed in this document.

Six levels of interrupts are recognized that can indicate the presence of an error:

Interrupt level 1: Invalid instruction at BCIU
Interrupt level 2: Successful asynch. message
Interrupt level 3: Status word with error or no status word received

Interrupt level 4: Data word has error
Interrupt level 5: DMA error
Interrupt level 6: Terminal failure

3.2.1.1 Inputs to Message Error Processing Function

Inputs to this function are listed in Table II

3.2.1.2 Processing for Function One

The processing exercised by this function is illustrated in Figure 8.

3.2.1.3 Outputs from Message Error Processing

The outputs are listed in Table III

TABLE II. INPUTS TO MESSAGE ERROR PROCESSING

DATA NAME	SYMBOL	SOURCE	REFERENCE
Interrupt Level		BCIU	
BIT Word		BCIU	
Status Word		BCIU	
Internal Status Register (ISR)		BCIU	
BCIU Status		BCIU PCP	
Error Processing Indicator			
Retry Counter			

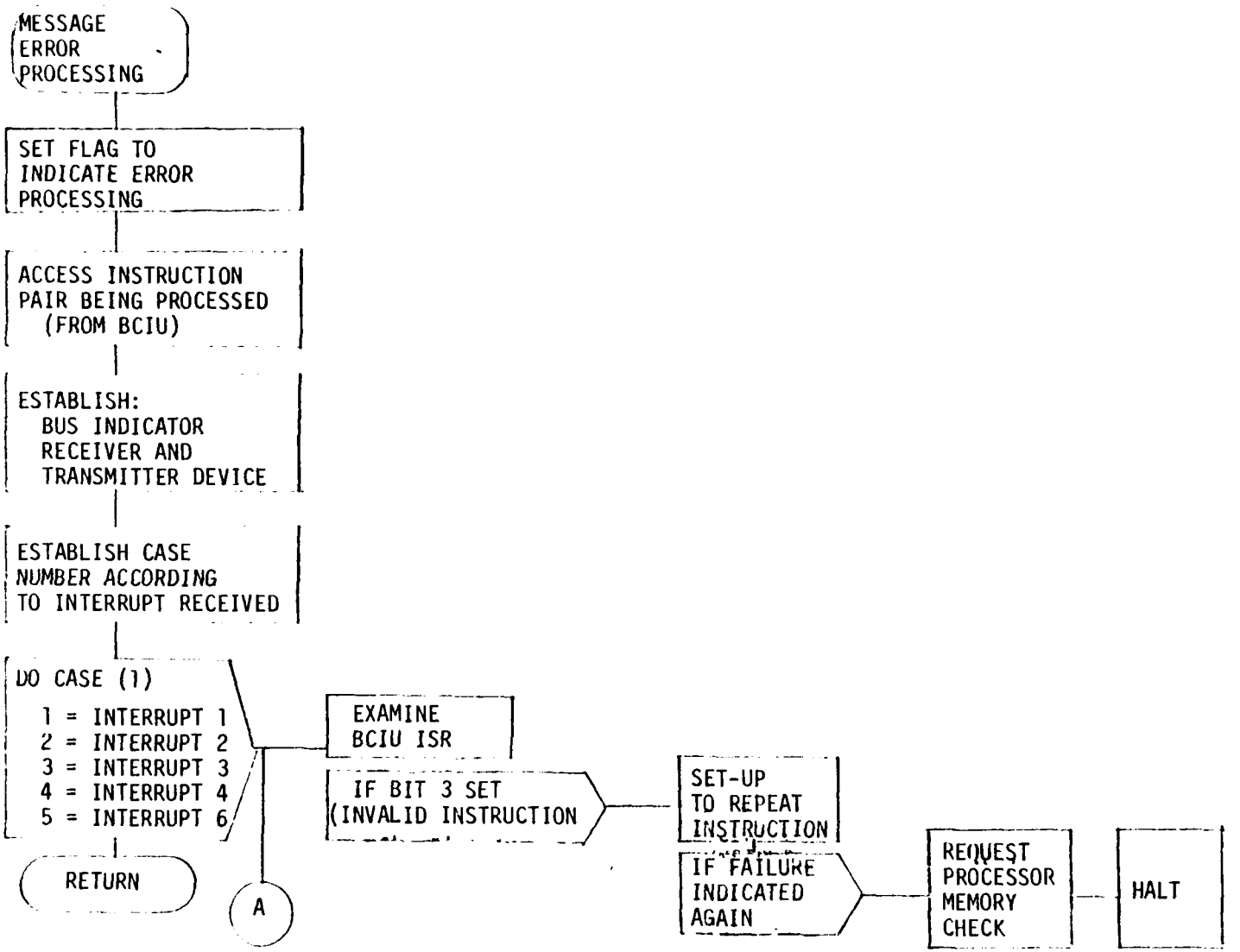


FIGURE 8. MESSAGE ERROR PROCESSING

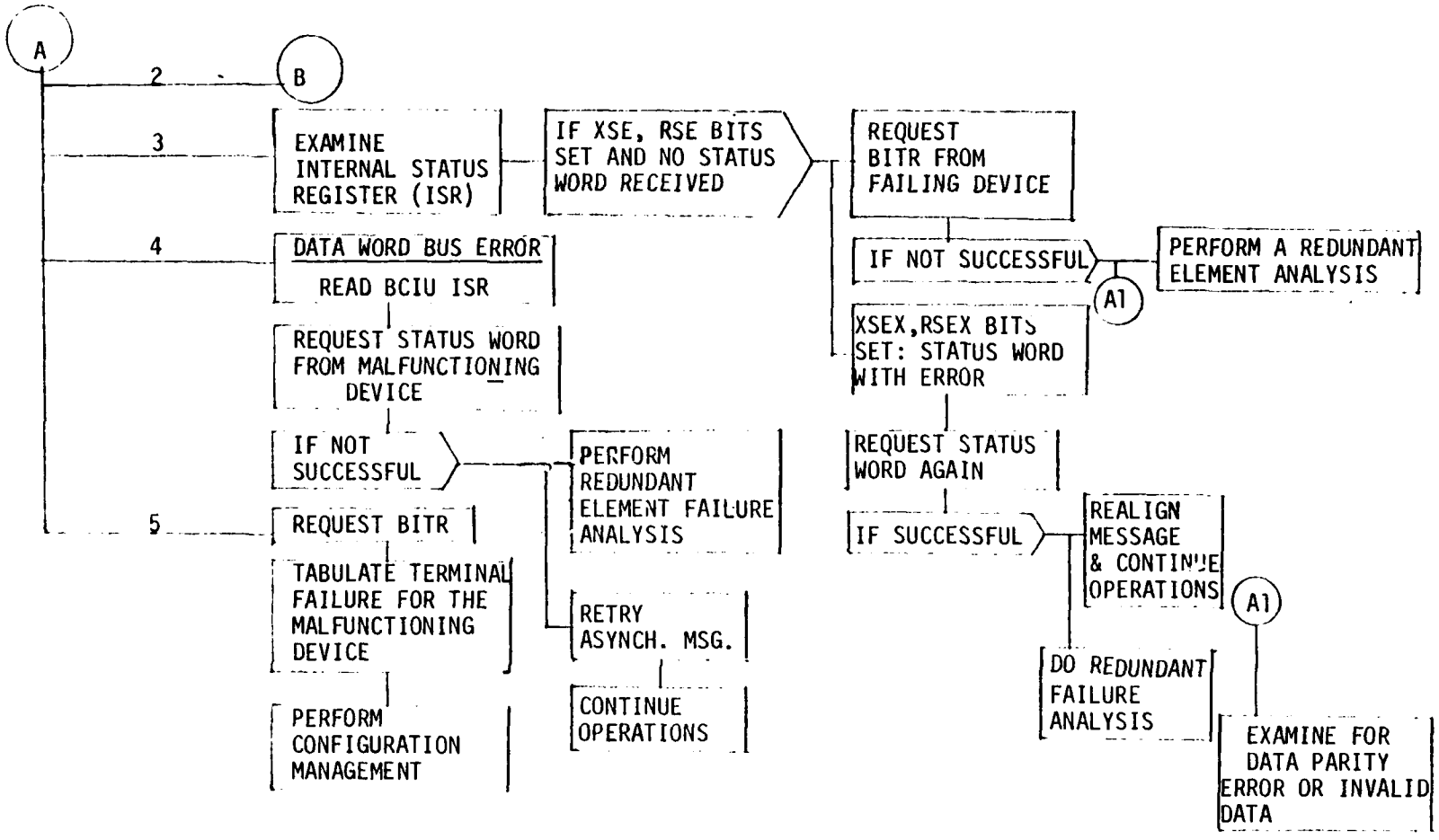


FIGURE 8. MESSAGE ERROR PROCESSING (Sheet 2 of 3)

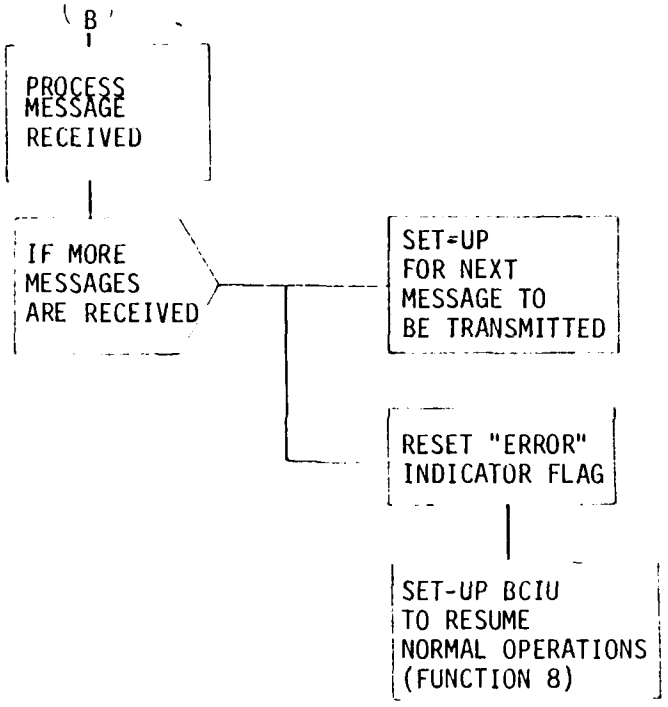


FIGURE 8. MESSAGE ERROR PROCESSING (Sheet 3 of 3)

TABLE III. OUTPUTS FROM MESSAGE ERROR PROCESSING

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Failed Terminal Indicator		Function Two	
Redundant Element Failure Counter		Function Three	
"Suspected" Device Address		Function Three	
Repeat Message Indicator		Function Eight	

3.2.2 Function Two - Terminal Failure Analysis Function

This function shall be invoked as a result of a failure to successfully complete a bus message due to a "BUSY" condition received or no status word response or the failed element or device doe not have a redundant element.

3.2.2.1 Inputs to Terminal Failure Analysis Function

The inputs to this function are indicated in Table IV.

3.2.2.2 Terminal Failure Analysis Processing

The processing to this function is illustrated in Figure 9.

If the function was invoked as a result of a "busy" condition encountered during the master transmission, a *busy override operation* is immediately executed.

As indicated in Figure 9 , if no status word was received another status word request is formulated for a different terminal in order to isolate the failure from the master terminal.

If on the other hand, a status word was received indicating a failure, a self-test command is set to the "suspect" failed terminal. If this command was not successful the remote terminal or processor is considered failed and the configuration management procedure is exercised. If the self-test was performed, the "suspect" failed terminal BIT register is requested and analyzed through Function 6 in Paragraph 3.2.6.

3.2.2.3 Outputs from Terminal Failure Analysis Function

The output from this function and listed in Table V.

TABLE IV. INPUTS TO TERMINAL FAILURE ANALYSIS

DATA NAME	SYMBOL	SOURCE	REFERENCE
Status Word		Remote Terminal	
Message Type Indicator		Message Error Processing Function (Function 1)	
Malfunctioning Device Address		Failed Terminal	
BIT Word			

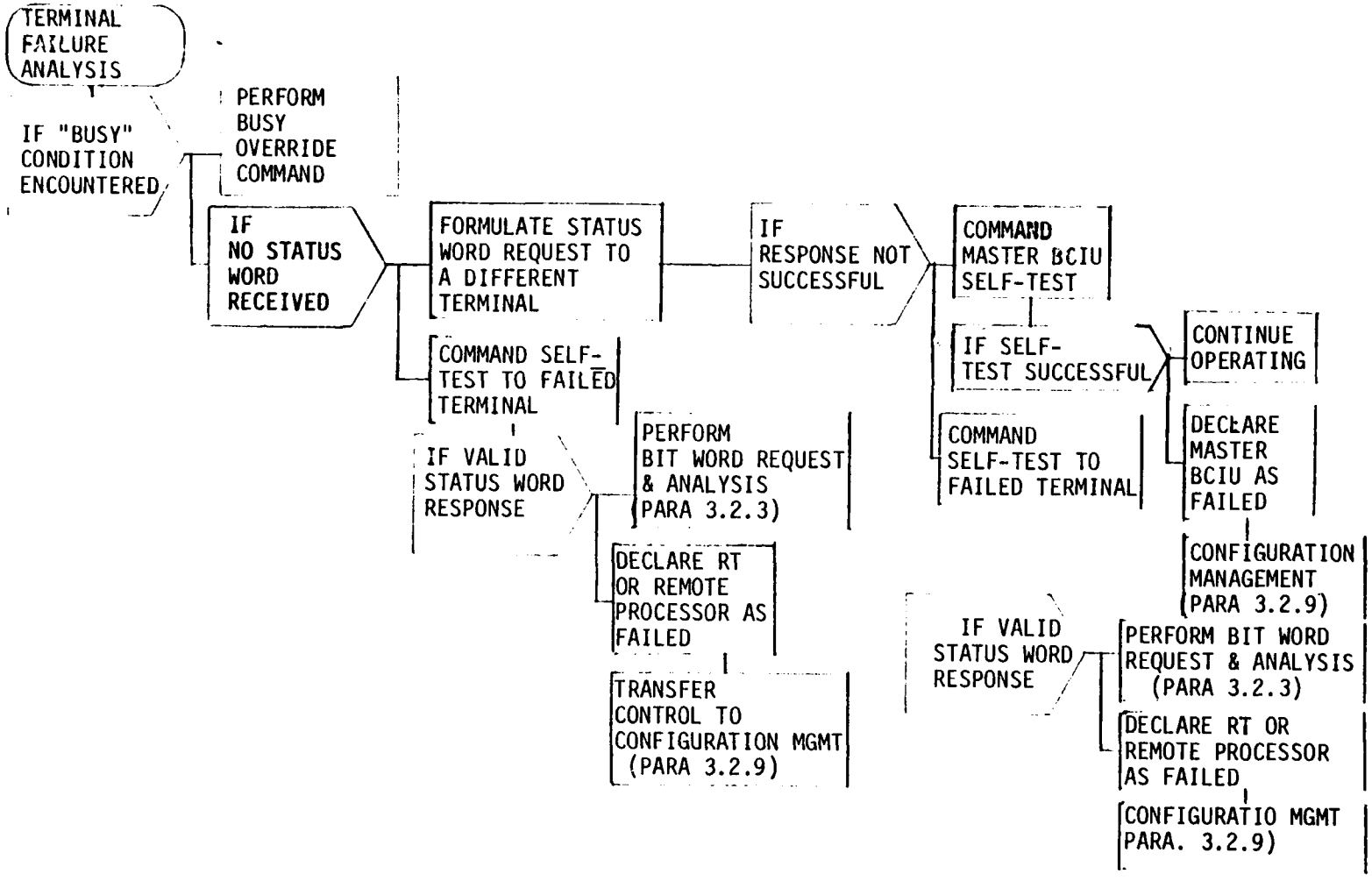


FIGURE TERMINAL FAILURE ANALYSIS PROCESSING

TABLE V. OUTPUTS FROM TERMINAL FAILURE ANALYSIS

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Self-Test Command Failed Terminal Indicator		Master/Remote Terminal Message Error Processing	

3.2.3 Function Three - Redundant Element Failure Analysis

The main purpose of this function is to record suspected redundant element failures and, in the process, determine whether the "suspect" failed element is the BCIU itself or a redundant element in a terminal. This function also commands self-test procedures on the suspected redundant element. If a failure is declared, configuration management is performed.

3.2.3.1 Inputs to Redundant Element Failure Analysis

The inputs to this function shall be as specified in Table VI.

3.2.3.2 Redundant Element Failure Analysis Function Processing

The processing performed by this function is illustrated in Figure 10.

Upon entering, this function shall increment a "suspect" failure counter for the indicated redundant element of the device. If the "suspect" involves a different terminal and different device from the previous failure, the Master redundant element is flagged as "suspect". The Master redundant element shall be considered as failed if it has received two "suspect" counts within the minor cycle

If the same device has been involved in three "suspect" counts, a self-test of the device in question is commanded. If, as a result, its BIT word indicates a failure, the device shall be declared failed and configuration Management performed. If the BIT word shows as failure, then the "suspect" count for this device shall be cleaned and operations continued.

TABLE VI. INPUTS TO REDUNDANT ELEMENT FAILURE ANALYSIS

DATA NAME	SYMBOL	SOURCE	REFERENCE
Redundant Element Failure Counter		Message Error Processing	
"Suspect" Device Address		Suspected Device	
Status Word			

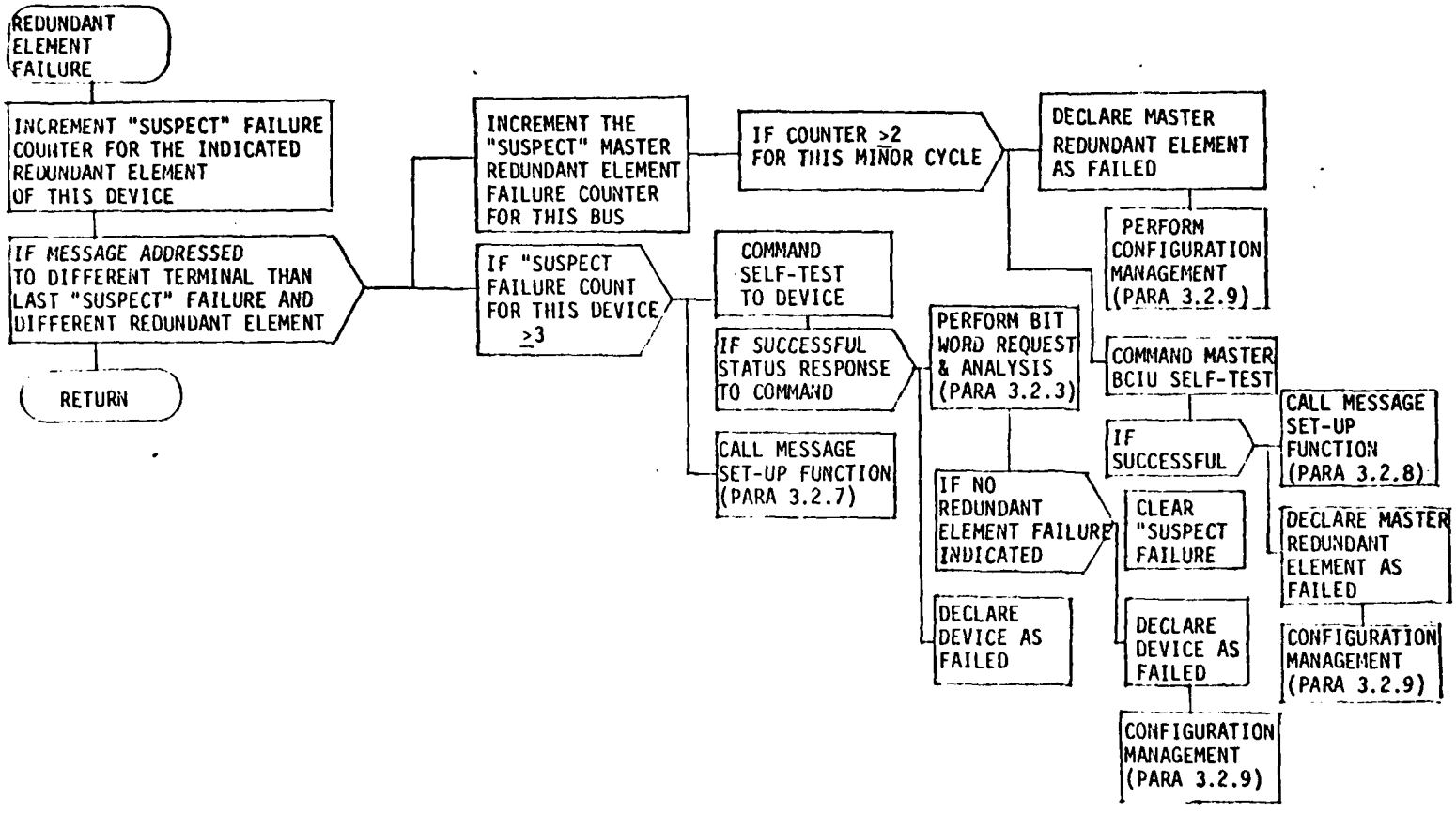


FIGURE 10. REDUNDANT ELEMENT FAILURE PROCESSING

3.2.3.3 Outputs from Redundant Element Failure Analysis

The outputs from this function are listed in Table VII.

3.2.4 Function Four - Configuration Management

The objectives of this function are to:

a. Modify the bus command list to delete bus messages to the failed terminal or redundant element.

b. Update the system status and configuration based on declared failures of core elements.

c. Communicate system status and configuration information to the monitor processor.

d. Initiate system backup/recovery operations *(Function 10) if required.*

e. Inform the Applications Software Configurator of any core element failure.

3.2.4.1 Inputs to the Configuration Management Function

Inputs to this function are shown in Table VIII.

TABLE VII. OUTPUT FROM REDUNDANT ELEMENT FAILURE ANALYSIS

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Redundant Element Failed Address Self-Test Command Failure Indicator		Message Error Processing Suspected Device Configuration Management	

TABLE VIII. INPUTS TO CONFIGURATION MANAGEMENT

DATA NAME	SYMBOL	SOURCE	REFERENCE
Failure Indicator		Function Three	
Bus Instruction List		Master Executive	

3.2.4.2 Configuration Management Processing

The processing exercised by this function is illustrated in Figure 11.

3.2.4.3 Outputs from Configuration Management

The outputs from this function are listed in Table IX.

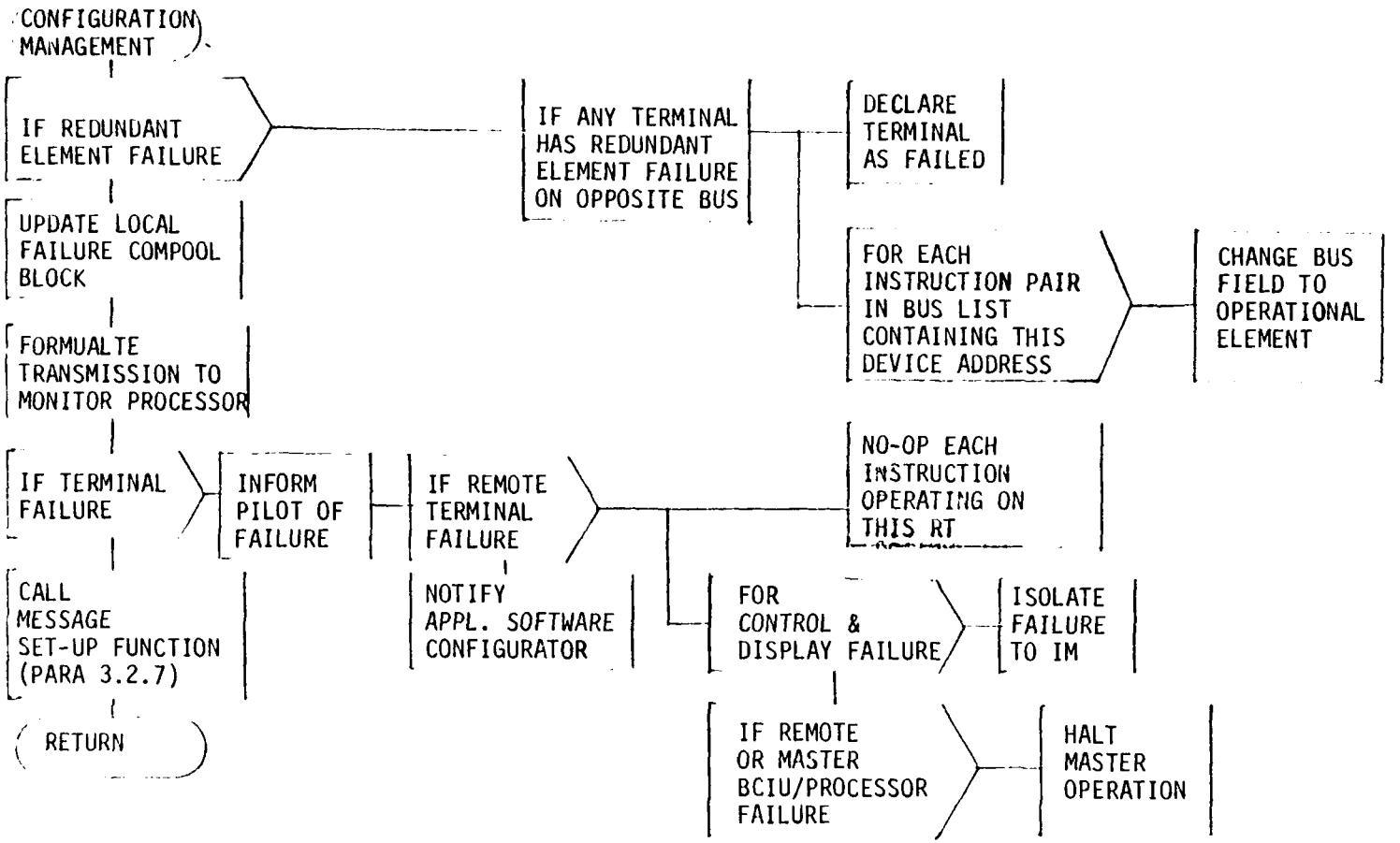


FIGURE 11. CONFIGURATION MANAGEMETN PROCESSING

TABLE IX. OUTPUTS FROM CONFIGURATION MANAGEMENT

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Failure Compool Black		Monitor Executive	
Bus Instruction List		Master Executive	

3.2.5 Function Five - System Recovery/Backup Function

This function shall be invoked upon the recognition of a terminal failure on the master processor/BCIU or a remote processor/BCIU. Its purpose is to ultimately assume control over the master executive functions and subsequently control the reconfiguration process directed by the pilot.

If the terminal failure occurs on the monitor processor/BCIU, the master executive in the master processor shall execute its copy of this function and proceed to control reconfiguration when and if directed by the pilot.

3.2.5.1 Inputs to System Recovery/Backup Function

The inputs to this function are shown in Table X.

TABLE X. INPUTS TO SYSTEM RECOVERY/BACKUP FUNCTION

DATA NAME		SOURCE	
BCIU PCR		BCIU	
BUS COMMUNICATION LIST		MASTER EXECUTIVE	
FAILURE DESCRETE		PROCESSOR CONTROL PANEL	

3.2.5.2 System Recovery/Backup Processing

The processing performed by this function is illustrated in Figure 12.

If the monitor processor is executing this function, then either the master or remote processor/BCIU has failed. Therefore, upon assuming bus communication control, the monitor processor shall command a signal to indicate the proper processor as failed. It shall also notify the pilot of its master function and recommend reconfiguration. The monitor shall initialize its minor cycle synchronization to start at the beginning of the last commanded minor cycle.

If this function is executed in the master processor as a result of a failure on the monitor/BCIU, the bus command instruction list shall be altered by deleting all communications with the monitor processor. The master executive shall command a discrete to the PCP indicating failure of the monitor processor, advise on reconfiguration. Normal operations shall be continued until the pilot decides to initiate reconfiguration process.

3.2.5.3 Outputs from Recovery/Backup Function

The outputs are listed in Table XI.

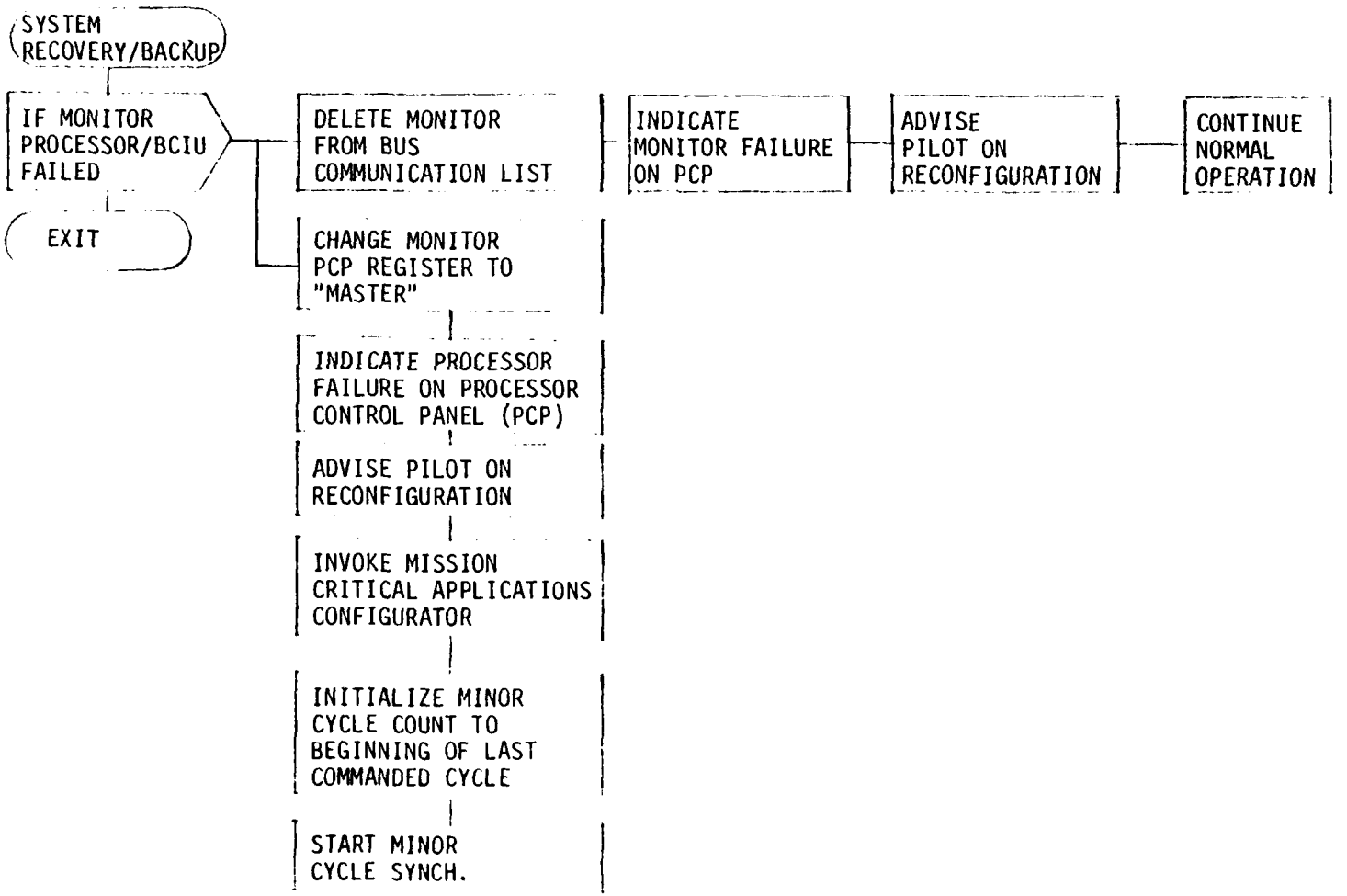


FIGURE 12. SYSTEM RECOVERY/BACKUP PROCESSING

TABLE XI. OUTPUTS FROM SYSTEM RECOVERY/BACKUP FUNCTION

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Bus Communication List		Master Executive	
Master Function Reg.		BCIU	

3.2.6 Function Six - BIT Word Request and Analysis Function

This function shall be invoked upon encountering a "suspect" terminal failure in status word, a level 6 interrupt has been received and/or a self-test request has been commanded to the terminal. The Built-In-Test (BIT) word received in response to the request shall contain information regarding results obtained from the terminal self-test.

The terminal Built-In-Test Word format is illustrated in Figure 13.

Once the BIT word is received successfully, its bit configuration shall be analyzed and proper action taken.

3.2.6.1 Inputs to BIT Word Request and Analysis Function

The inputs to this function shall be as listed in Table XII.

3.2.6.2 Processing

The processing exercised by this function is illustrated in Figure 14.

3.2.6.3 Outputs from BIT Word Request and Analysis Function

The outputs from this function are lsited in Table XIII.

1 2 3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
SYNC	POWER ON RESET	POWER SUPPLY FAILURE	MTU 1 OUT	MTU 2 OUT	SPARE	SELF TEST FAILURE	SELF TEST FAILURE	SELF TEST FAILURE	SELF TEST FAILURE	SELF TEST FAILURE	NO DATA RECEIVED	WORD COUNT HIGH	WORD COUNT LOW	DATA PARITY ERROR	INVALID DATA	INVALID COMMAND	BIT WORD PARITY

FIGURE 13. TERMINAL BUILT-IN-TEST (BIT) WORD FORMAT

TABLE XII. INPUTS TO BIT WORD REQUEST AND ANALYSIS FUNCTION

DATA NAME	SYMBOL	SOURCE	REFERENCE
BIT Word		Suspected Failed Device	

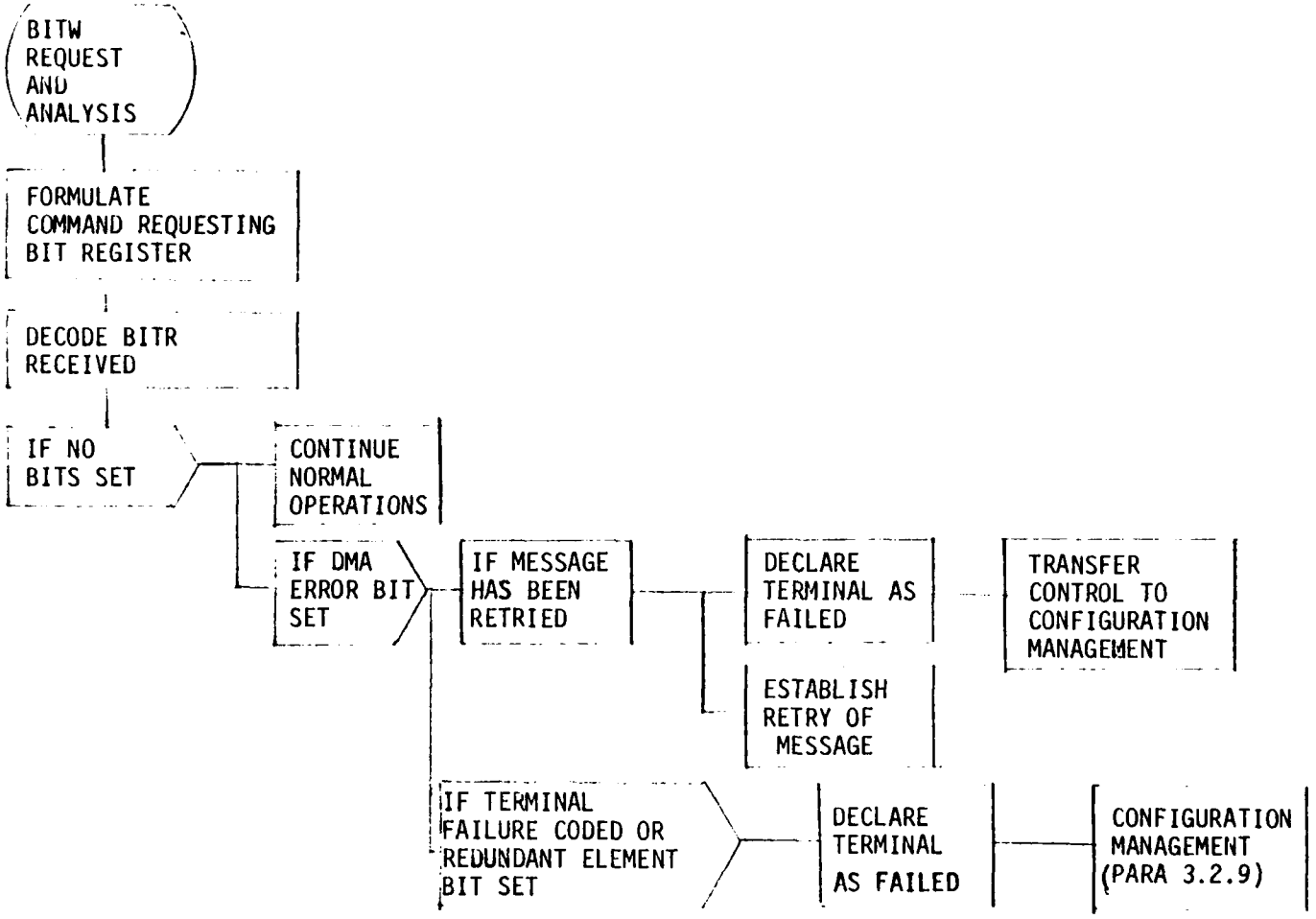


FIGURE 14. PROCESSING FOR BIT WORD REQUEST AND ANALYSIS FUNCTION

TABLE XIII OUTPUT FROM FUNCTION SIX

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Failure Indicator		Configuration Management	
Retry Message Indicator		Message Set-Up Function	

3.2.7 Function Seven - Message Set-Up Function

The Message Set-Up Function is responsible for the arrangement of the data base in the establishment of the communication sequence during an error process.

3.2.7.1 Inputs to Message Set-Up Function

Inputs to this function shall be as listed in Table XIV.

3.2.7.2 Message Set-Up Function Processing

This function shall be invoked by the Redundant Element Failure Function (Function 3) upon determining that a message must be retransmitted and by the Configuration Management Function (Function 4) after changing the Bus list configuration.

It shall set the BCIU Instruction Address Register (IAR) pointing to the message to be repeated or resumed when continuing operations.

3.2.7.3 Outputs from Message Set-Up Function

The outputs are listed in Table XV.

TABLE XIV. INPUTS TO MESSAGE SET-UP FUNCTION

DATA NAME	SYMBOL	SOURCE	REFERENCE
Repeat Message Indicator		Redundant Element Failure (Function 3)	
Indicator		Configuration Management (Function 4)	

TABLE XV. Outputs From Message Set-Up Function

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Instruction Address Register (IAR)		BCIU	

3.2.8 Function Eight BCIU Set-Up Function

This function shall be invoked by the Message Error Processing Function (Function One) with the purpose of making the Bus Control Interface Unit (BCIU) ready for the next message transmission. The BCIU shall be set-up for transmission of a required repeat message, a failure analysis message or the resumption of non-error related messages.

3.2.8.1 Inputs to the BCIU Set-Up Function

Inputs to this function are listed in Table XVI

3.2.8.2 BCIU Set-Up Function Processing

The processing performed by this function is illustrated in Figure 15 . In particular, it shall load the BCIU Instruction Address Register (IAR) with the address of the instruction accomplishing the linkage to continue operations.

3.2.8.3 Outputs from the BCIU Set-Up Function are listed in Table XVII.

TABLE XVI. INPUTS TO FUNCTION 8

DATA NAME	SYMBOL	SOURCE	REFERENCE
Failure Indicator		Message Error Processing	
Repeat Message Indicator		Message Error Processing	

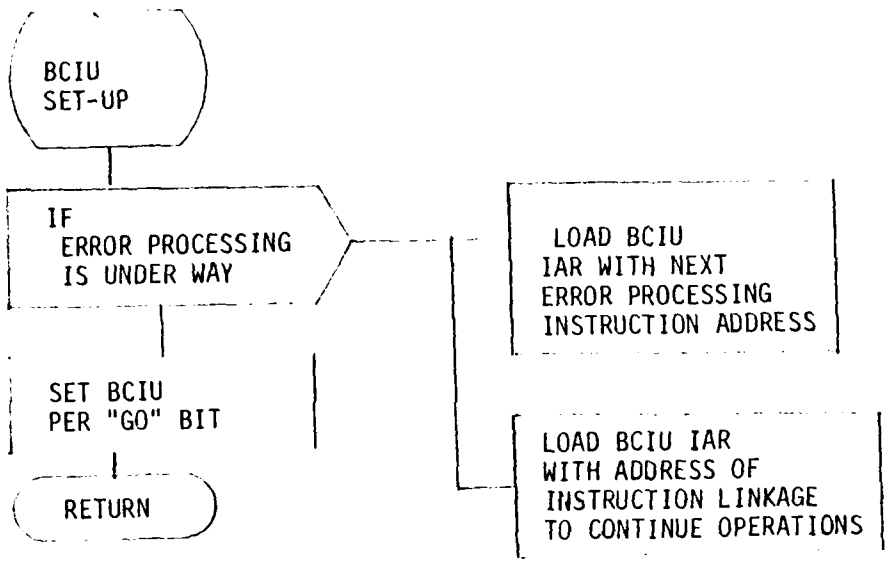


FIGURE 15. BCIU SET-UP FUNCTION PROCESSING

TABLE XVII. OUTPUTS FROM BCIU SET-UP FUNCTION

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Instruction Address Register (IAR)		bciu	
Processor Control Register (PCR)		BCIU	

3.2.9 Function Nine - System Reconfiguration Function

System reconfiguration is invoked by the pilot through the Processor Control Panel (PCP) upon being informed of a processor failure and configuration advised.

The System Recovery/Backup Function (Paragraph 3.2.5) describes the procedure followed by the EHARS upon recognizing a processor failure. These procedures are:

a. If a master or remote processor has been declared failed the monitor processor shall take control as master and resume all mission critical operations allocated in the monitor processor.

b. If the monitor processor has failed, the monitor processor shall be deleted form all bus communication list and normal operations continued.

The pilot shall initiate the reconfiguration process by depressing the configuration button at the PCP. This discrete shall be recognized by the Error Handling and Recovery System (EHARS) and initiate processing as explained in Paragraph 3.2.9.2

3.2.9.1 Inputs to the System Reconfiguration Function

The input to this func ion are listed in Table XVIII.

3.2.9.2 System Reconfiguration Processing

The processing exercised by this function is illustrated in Figure 16.

This function shall be responsible for loading the mission software (monitor and local executives and application software) into the remaining good processor and perform memory load and check sum verification.

The reconfiguration scheme shall produce a one-processor back-up software mode.

TABLE XVIII. INPUTS TO SYSTEM RECONFIGURATION FUNCTION

DATA NAME	SYMBOL	SOURCE	REFERENCE
"Reconfiguration" Discrete		PCP	
Processor Failed Discrete		PCP	

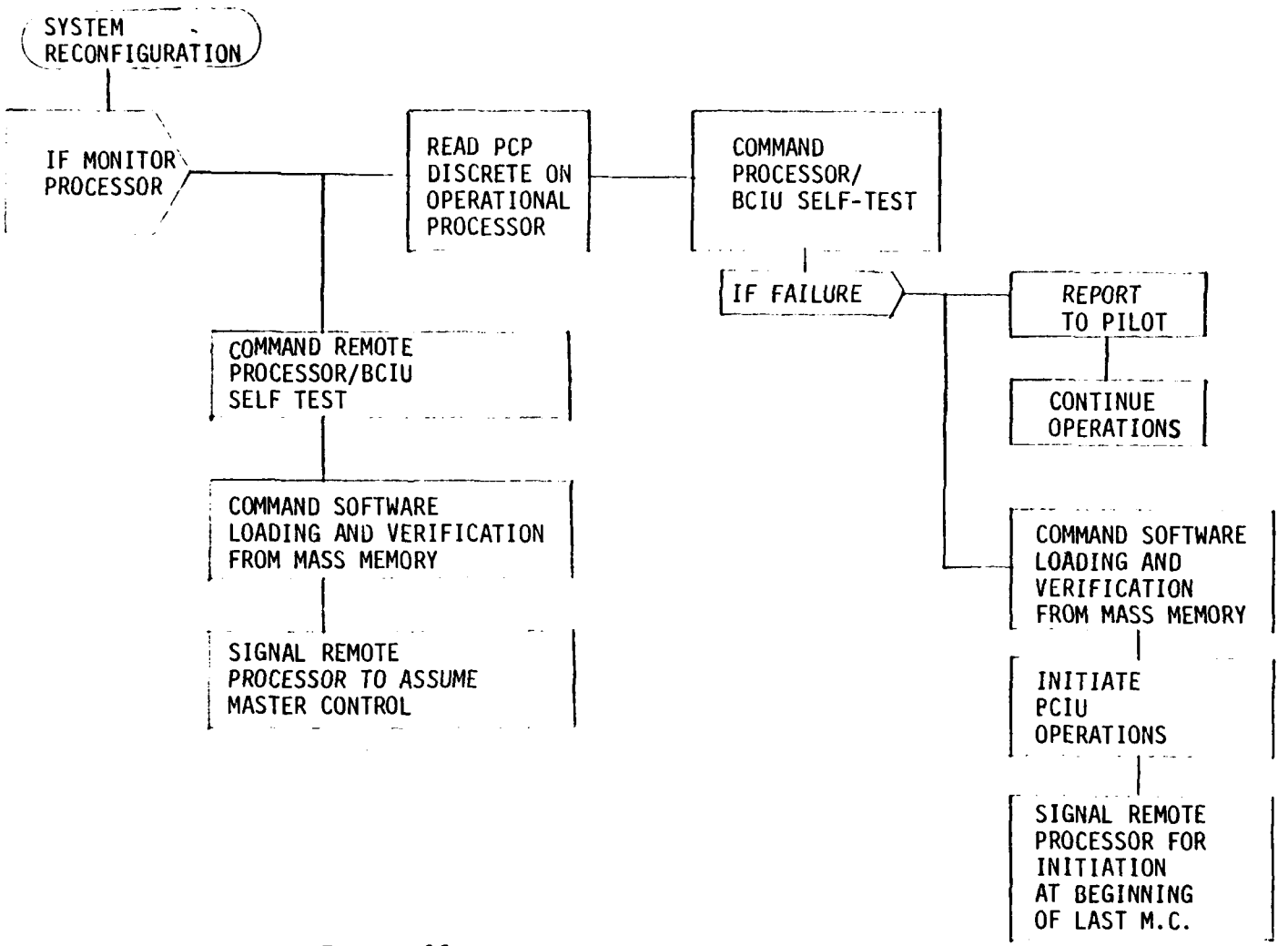


FIGURE 16. RECONFIGURATION PROCESSING

3.2.9.2 Cont'd

If the master or remote processor has failed, the monitor processor shall control the reconfiguration process by loading a copy of the monitor processor software from mass memory into the remaining good processor.

If the monitor processor has failed and reconfiguration is commanded, the master processor shall control the loading of the remote processor from mass memory with software similar to that contained in the original monitor processor. That is to say, this software shall contain monitoring functions and mission essential functions in its application software. Upon successful loading and verification; the just loaded processor shall assume control and direct the loading and verification of similar software from mass memory into the other processor.

As a result, in the final configuration, one processor shall control the integrated avionics system software while the second processor monitors the master's operation.

3.2.9.3 Outputs from System Reconfiguration Function

The outputs from this function are listed in Table XIX.

TABLE XIX. OUTPUTS TO SYSTEM RECONFIGURATION FUNCTION

DATA NAME	SYMBOL	DESTINATION	REFERENCE
Request Command for Mass Memory Loading		Mass Memory	

4.0 QUALITY ASSURANCE PROVISIONS

4.1 Introduction

Tests and evaluations shall be conducted to verify that the performance and design of the OFP-EHARS shall meet or exceed the requirements specified in Section 3.0. The test category, verification method, and test requirements for performance/design requirements are specified in the Verification Cross-Reference Index (VCRI), Table XX The requirements delineated shall be the basis for the test plan and test procedure which shall be written. The four methods given in Table XX of verifying individual requirements are explained as follows:

a. Inspection - Formal verification of a performance of a design requirement by examination of the assembled CPCI at the time and place of qualification testing. Inspection is not often specified as a formal means of verification for a requirement. One set of requirements that might be verified by inspection are the data base requirements, which can be verified by comparing the data base documentation with a system tape listing.

b. Analysis - Formal verification of a performance or design requirement by examination of the constituent elements of a CPCI component. For example, a weapons guidance equation or a coordinate conversion equation might be verified by analysis.

c. Demonstration - Formal verification of a performance or design requirement by observation of a demonstration test. For example, visual demonstration might be used to verify that the displays generated by the CPCI are in the format necessary to satisfy human performance requirements.

TABLE XX. VERIFICATION CROSS REFERENCE INDEX

METHOD LEGEND: NA Not Applicable

1 - Inspection
2 - Analysis
3 - Demonstration
4 - Review of Test Data

A - Computer Program Test and Evaluation
B - Preliminary Qualification Test
C - Formal Qualification Test
II - Category II Test

SECTION 3 REQUIREMENT REFERENCE	METHOD					TEST CATEGORY				VERIFICATION REQUIREMENT
	NA	1	2	3	4	A	B	C	II	
3.2.1		x			x	x	x			4.2.2, 4.2.3, 4.2.4
3.2.2		x			x	x	x			4.2.2, 4.2.3, 4.2.4
3.2.3		x			x	x	x			4.2.2, 4.2.3, 4.2.4
3.2.4		x		x	x	x	x			4.2.2, 4.2.3, 4.2.4
3.2.5		x			x	x	x			4.2.2, 4.2.3, 4.2.4
3.2.6		x			x	x	x			4.2.2, 4.2.3, 4.2.4
3.2.7		x			x	x	x			4.2.2, 4.2.3, 4.2.4
3.2.8		x		x	x	x	x			4.2.2, 4.2.3, 4.2.4

4.1 Cont'd

d. Review of Test Data - Formal verification of a performance or design requirement by examining the data output after operation of a CPCI component when selected input data are processed. For example, a review of hardcopy printout test data might be used to verify that the content of a specific told-in message is correctly processed. This method is the one likely to be used for the majority of qualification testing.

Narrative data pertaining to test categories, amplifying the tabular content of the VCRI are specified in subparagraphs below. Test requirements referenced in the VCRI are specified in 4.2 and subparagraphs thereto.

4.1.1 Category I Test

Category I testing is subdivided into the following broad types:

a. Computer program test and evaluation - Tests conducted prior to and in parallel with preliminary or formal qualification tests. These tests are oriented primarily to support the design and development process.

b. Preliminary qualification tests - Formal tests oriented primarily towards verifying portions of the CPCI prior to integrated testing/formal qualification tests of the complete CPCI (see paragraph 4.1.3 below). These tests will typically be conducted at the contractor's design and development facilities.

c. Formal qualification tests - Formal tests oriented primarily towards testing of the integrated CPCI, normally using operationally configured equipment at the category II site prior to the beginning of category II testing.

4.1.1 Cont'd

This testing will emphasize those aspects of the CPCI performance which were not verified by preliminary tests. The testing requirements which cannot be verified during category I test shall be specified in paragraph 4.1.5.

Qualification of this CPCI shall be accomplished during qualification testing to the maximum extent possible, as a result of preliminary qualification tests (PQT) and formal qualification test (FQP) conducted by the contractor and witnessed/verified by the procuring activity.

4.1.2 Computer Programming Test and Evaluation

Programming test and evaluation which apply satisfy one or both of the following criteria:

(1) They are intended to be the only source of data to qualify specific requirements in Section 3.

(2) They must be accomplished as part of an integrated test program involving other systems/equipment/computer programs.

4.1.3 Preliminary Qualification Tests

These tests will directly support the top-down implementation and verification. Method of verification shall be as specified in Table XX. The following three levels of qualification shall be performed.

a. Unit Design Qualifications shall apply to each module. At this level the characteristics which are of primary interest are the internal workings of the module; logical flow control, numerical results, convergence, scaling, and range.

4.1.3 Cont'd

b. Module Design Qualifications shall apply to each module after it is interfaced with its environment. These tests are basically interface tests; correct internal operations are assumed. The object is to verify that two or more modules work together. To comply with the top-down approach the interfacing tests shall be sequenced from the top to the bottom.

c. System Design Qualifications shall apply to the completely assembled CPCI. This level requires a totally integrated computer program. Such testin discloses errors due to conflicts introduced by data sharing convention violations, improper range of input values, sequencing requirements and communications and control. The internal working of the CPCI is of primary concern with the interfaces of the CPCI with the external environment deferred to the Formal Qualification Tests.

4.1.4 Formal Qualification Tests (Specified in the Part II Specifications)

4.1.5 Category II Tests (Specified in Part II Specifications)

4.2 Verification Requirements - This paragraph specified in greater detail the method used to verify the individual requirements given in Table 4.2-1. (This table cross-references the sub-paragraphs of 4.2 which apply).

4.2.1 Performance

The specified function shall be verified with respect to one of the following perforamnce and criteria:

a. Accuracy which may be affected by input precision, input frequency, input accuracy, or number of derations.

b. Execution Time

c. Storage used

d. Response time

e. Long Term degradation

f. Stability

4.2.2 Priority/Timing

The specified function shall be verified with respect to one of the following priority/timing criteria:

a. Interrupt and return

b. Frequency

c. Consistency in events

d. Order of processing

e. Scheduling/Canceling consistency

f. Job stocking

4.2.3 Interfaces

The specified function shall be verified with respect to one of the following interface parameters:

a. Data locks

b. Range

c. Consistency

d. Initialization

4.2.3 Cont'd

e. Data organization

f. Human command/response

g. External procedures

4.2.4 Logic Paths

The specified function shall be verified with respect to the correctness of the logic paths by exercising the computer program in operation.

4.2.5 Off-Nominal Conditions

The specified function shall be verified with respect to off-nominal conditions such as:

a. Error detection

b. Error recovery

c. Limitations