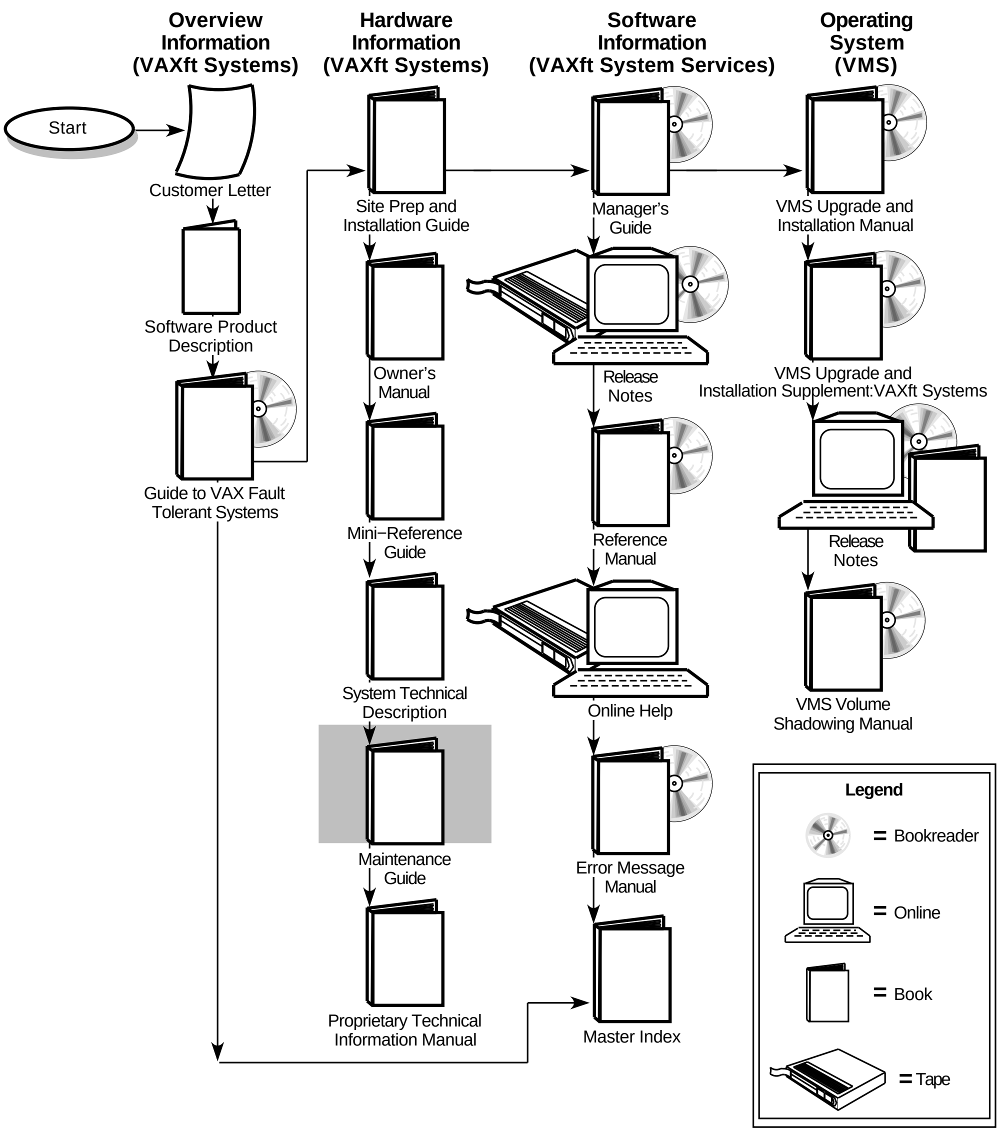
VAXft Systems
Maintenance Guide

EK-VXFT1-MG.003

Digital Equipment Corporation

May, 1992

VAXft Systems Documentation Road Map



Contents

2 Errors and Error Analysis

3 Troubleshooting

4 Model 110 Removal and Replacement Procedures

5 Model 310 and 410 Removal and Replacement Procedures

A Managing Integrated Storage Elements

Index

Examples

Figures

Tables

About This Manual

Intended Audience

This manual is intended for use by Digital Customer Services and other qualified personnel responsible for servicing the fault-tolerant VAXft system.

Fault-Tolerant Operation

The VAXft system achieves fault tolerance through a combination of redundancy and failover techniques. All critical functions of the VAXft hardware are duplicated.

The VAXft system has two zones. Each of the zones contains the hardware required to execute an application. The two zones are identical in configuration except in cases where the customer chooses not to have hardware redundancy. Each zone is housed in a cabinet called a system cabinet. The zones are physically and logically connected and simultaneously process the same instructions. When both zones operate in this synchronous manner, they perform as a single, fault-tolerant system. If a single hardware fault occurs in a component in either zone, the problem is communicated to the other zone.

Once the fault is “known” within the system, the system takes action to isolate the faulty component. This action can be:

- Disabling an I/O path
- Removing an element from service (for example, a memory module)
- Removing an entire zone from service

Despite the nature of the failure and recovery action, the system is able to remain in full operation.

System Architecture

All the memory, processing, and I/O facilities are provided in two interconnected system cabinets in a base system.

During normal operation, both zones operate in lockstep. While operating in lockstep, there is no single point of hardware failure. An error in one zone will not disable the VAXft system.

When a solid hardware failure occurs, the zone with the failing component is brought off-line for repair. When the repair is completed, the zone is powered on and the VAXft system resynchronizes with the operating zone, restoring redundancy. This process is transparent to applications running on the VAXft system.

Document Structure

This manual provides service personnel with operating, maintenance, and troubleshooting information for the VAXft systems.

This manual is made up of the following chapters and appendixes:

- **Chapter 1, Diagnostics** — Describes how to use the ROM-based diagnostics (RBDs) to verify the integrity of the hardware procedures, and to isolate failures.
- **Chapter 2, Errors and Error Analysis** — Describes how the VAXft system detects errors and how to use error logs to analyze them.
- **Chapter 3, Troubleshooting** — Describes the maintenance strategy and troubleshooting procedures for the VAXft system.
- **Chapter 4, Model 110 Removal and Replacement Procedures** — Describes how to remove and replace the model 110 field replaceable units (FRUs).
- **Chapter 5, Model 310 and 410 Removal and Replacement Procedures** — Describes how to remove and replace the model 310 and 410 field replaceable units (FRUs).
- **Chapter 6, Model 610 and 612 Removal and Replacement Procedures** — Describes how to remove and replace the model 610 and 612 field replaceable units (FRUs).
- **Appendix A, Managing Integrated Storage Elements** — Provides guidelines for managing integrated storage elements (ISEs).

Related Documentation

The VAXft documentation set includes the following manuals:

- *VAXft Systems Site Preparation and Installation Guide* (EK-VXFT1-IN) — Provides site preparation guidelines and the system specifications. Describes how to install, boot, and verify the system. Provides procedures for removing, handling, and replacing the logic modules, and for removing and replacing the system drives.
- *VAXft Systems Owner's Manual* (EK-VXFT1-OM) — Provides a functional description of the VAXft system. Describes the system controls and indicators, console commands, bootstrap functions, and tape drive operation. Provides procedures for removing and replacing the system drives and for removing, handling, and replacing the logic modules.
- *VAXft Systems Mini-Reference Guide* (EK-VXFT1-HR) — Provides summaries of the system controls and indicators, console operation, console commands, bootstrap functions, and system registers.

Additional Documentation

Other documents related to the VAXft system include:

- *VAXft Systems Guide to VAX Fault Tolerant Systems* — Describes the VAXft system and describes fault-tolerant computing.
- *VAX Wide Area Network Device Drivers* — Describes the software utilities used in wide area network communications.
- *VAXft System Services Installation Guide* — Provides step-by-step procedures for installing the VAXft system services software on your VAXft system.
- *VAXft System Services Manager's Guide* — Describes the VAXft system and the VAXft system services software. Provides information on managing a fault tolerant system that is running VAXft system services software.
- *VAXft System Services Release Notes* — Provides information related to the current version of VAXft system services. Provides additional information for installing and maintaining your VAXft system.
- *VAXft System Services Reference Manual* — Provides reference information on VAXft system services operation. Describes the DCL commands used on a VAXft system.

- *VAXft System Services Online Help* — Provides information about using the VAXft system services specific information and the DCL commands used on a VAXft system.
- *VAXft System Services Error Message Manual* — Provides descriptions of error messages that may be encountered in using VAXft system services. Provides a reference for fault tolerant and system error messages.
- *VAXft System Services Master Index* — Provides a complete index for the software documentation set.
- *VMS Upgrade and Installation Manual* — Describes the installation and upgrade procedures for the current release of the VMS operating system. Provides information on the user environmental test package (UETP).
- *VMS Upgrade and Installation Supplement: VAXft Systems* — Supplements the *VMS Upgrade and Installation Manual* with information specific to the VAXft computer including startup, shutdown, and backup procedures.
- *VMS Release Notes* — Provides notes on various aspects of the VMS operating system.
- *VMS Volume Shadowing Manual* — Provides an in-depth discussion of volume shadowing (phase II), shadow sets, the mount utility, and DCL commands used to mount, monitor, and dismount volume shadow sets.

1
Diagnostics

The VAXft diagnostics reside on the hardware modules. The diagnostic code is contained in the ROMs on the processor, system I/O controller, and WAN controller modules. ROM-based diagnostics (RBDs) execute automatically when you power on the VAXft system. The RBDs may also be invoked manually by an operator through the RBD monitor. RBD monitor access is through the console terminal.

The VAXft diagnostics exercise the basic functions of the system first, and then test additional functions until the entire system is verified. This type of testing is called *concentric circle* methodology. It is designed to detect solid failures in the VAXft hardware.

Some tests require manual intervention. The external loopback connector tests, for example, are invoked manually. These tests are called interactive tests.

1.1 Power-On Tests

There are three groups of power-on tests:

- Module self-tests
- Zone tests
- System tests

Except for the memory module, each logic module contains a diagnostic ROM. When you power on the system cabinet, the modules perform their self-test diagnostics concurrently. These tests perform functional verification of the module logic. If a self-test diagnostic detects a hardware failure, a magnetic fault indicator (MFI) on the module is set, and the device is removed from the system configuration while the rest of the system continues testing.

For example, if a KFE52 I/O controller module fails, examine the LED pack (Figure 1–1). It is located on the back of the module at the top. You may have to remove the disk drive module in the slot above the KFE52 I/O controller module to see the LED pack. Using Table 1–1, record the error codes and test groups for each error.

At the end of the module self-tests, the zone tests begin. The zone tests poll modules for the results of the self-tests and check system buses and trace RAMs. Then these tests determine the configuration of the zone. Finally, the information from the zone test is written into memory and reported to the console terminal.

At the end of the zone tests, system tests begin. The system tests check for the presence of the cross-link cables. Next, they verify that the other zone is powered on, is able to send and receive data, and is not running an operating system. If these conditions are met, the system tests check the function of the cross-link cables, the DMA-to-buffer RAM in the other zone, and the error decoders.

When all of the three test groups are finished, the results are reported to the console terminal and any failure information is written into the EEPROM on the failing module. Then control is returned to the console firmware, which may (depending on its setup) bring up the operating software.

Figure 1–1 LED Pack

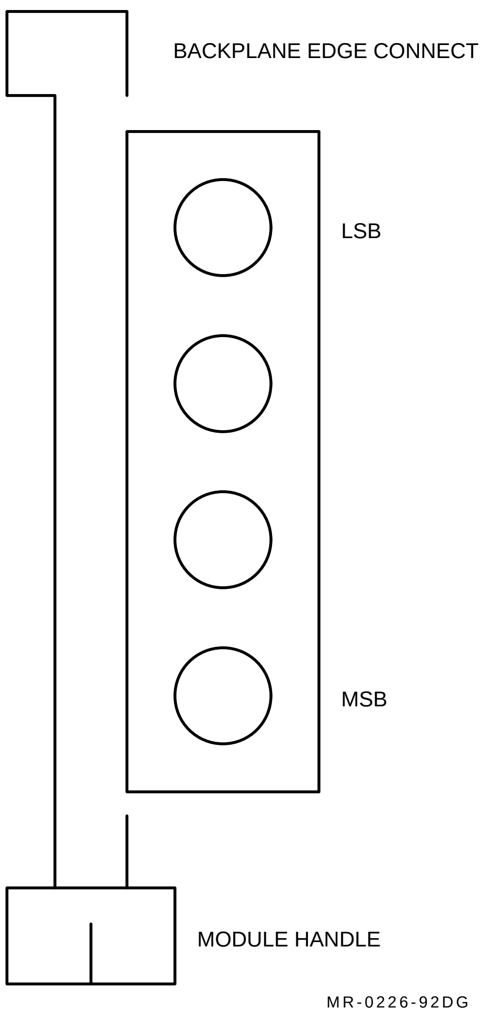


Table 1–1 LED Pack Error Codes

Error Code	Test Group	Tests Include
1	EEPROM	EEROM
2	ROM	ROM
3	ENET ROM	ENET ROM
4	SSC	LEDs
		TOY clock
		Bus timeout
		Interval timer
5	SSC COMM	Console UART
6	SSC COMM	Modem UART
7	SLIM	SLIM registers
8	Memory	Buffer RAM
		Buffer RAM mask
9	Firewall	FIREWALL registers
		Rail switching
		Interrupts
		Cross-check
		Force cross-check error
		Trace RAM write/read
A	PCM	PCM hardware loopback
		PCM software loopback
B	SWIFT	Swift HPDAL
		Swift initialization
		Swift CSR
		Swift internal loopback
C	LANCE	Lance LADAL
		Lance CSR
		Lance internal loopback without interrupts
		Lance internal loopback with interrupts
F	Completion Code	

1.2 Interactive Tests

Table 1–2 describes the loopback connectors required to execute the interactive tests. The interactive tests are described in Table 1–3.

NOTE

Do not run the interactive tests on a zone that is in duplex mode. You must first issue a STOP/ZONE command to bring the zone to a simplex state before you issue any RBD commands.

Table 1–2 Diagnostic Loopback Connectors

Module	Connector Part Number	Test	Mounting Location
I/O	12-29258-01	SWIFT external loopback test	J6 of I/O module
I/O	12-26318-01	LANCE external loopback test — ThinWire	J4 ThinWire
I/O	12-22196-02	LANCE external loopback test — thickwire	J5 thickwire
I/O	12-15336-08	Modem port external loopback test	Remote modem console port
WAN 620	12-33192-01	WAN diagnostic extended self-test	T3004 J4
WAN 620	12-33193-01	WAN diagnostic extended self-test	T3004 J3
WAN 620	H3199	WAN diagnostic extended self-test	Y-box

Table 1–3 Interactive Tests

Module	Test Type	Description
Processor	EEPROM test	Tests EEPROM in page mode and byte-write mode.
System I/O controller	SWIFT external loopback test	Tests DSSI control and data signals.
	LANCE external loopback test	Tests external drivers of the Ethernet circuitry.
	Modem external loopback test	Tests modem control signals.
	SWIFT to MicroVAX interrupt test	Tests SWIFT to MicroVAX interrupts. (This test is implemented in RBD 1, version 2.70 or later.)
	EEPROM test	Fully tests the EEPROM. This test takes 10 minutes to complete.
WAN	Communication test	Tests module drivers and receivers.

1.3 Running the RBDs Interactively

The RBDs reside in ROM on the processor, system I/O controller, and WAN modules. Each of the ROMs contains a diagnostic monitor used to execute the diagnostic tests. A single RBD test, a subtest, or a selected group of subtests can be invoked by the diagnostic monitor.

1.3.1 How to Invoke the RBD Monitor

You must invoke the RBD monitor before you can run interactive RBDs. The modules that support interactive RBDs are the CPU module, the CIO module, and the WAN module. The procedure to invoke the RBD monitor is different for each of these modules. See Examples 1–1, 1–2, and 1–3.

For the CPU module, you issue the TEST command from CIO mode to invoke the RBD monitor.

For the primary CIO module, you must issue the MIO command from CIO mode to enter MIO mode. Then, from MIO mode, you issue the TEST or RBD command to invoke the RBD monitor. The console returns the RBD*n*> prompt, where *n* is a slot ID number.

For the secondary CIO module, you must issue the Z command to invoke a system console communication mode. (The console returns the MIO> prompt **only** when you specify the secondary CIO module.) Then, from MIO mode, you issue the TEST or RBD command to invoke the RBD monitor.

For the WAN module, you must also issue the Z command before you invoke the RBD monitor. (The console returns the DSF_*n*> prompt, where *n* is a slot ID number, **only** when you specify the slot ID number.) Then you issue the T/R command.

See Figures 1–2 and 1–3 for valid CIO and WAN module slot ID numbers. For more information on how to access the different console modes and use the Z command, refer to the *VAXft Systems Owner's Manual*.

Example 1–1 How to Invoke the RBD Monitor on the CPU Module

```
>>>                    ! Begins your console session in CIO mode.
>>> T                  ! Invokes the RBD monitor on the CPU module.
RBD>
```

Example 1–2 How to Invoke the RBD Monitor on the Primary CIO Module

```
>>> MIO                ! Enters MIO mode from CIO mode.
MIO> T                 ! Invokes the RBD monitor on the primary CIO
RBD1>                  ! returns the RBD1> prompt.
```

Example 1–3 How to Invoke the RBD Monitor on the Secondary CIO Module

```
>>> Z 2                 ! Invokes the RBD monitor on the
CTA0: Z 2               ! secondary system I/O controller module
Return                  ! in slot 1 of the backplane. When the
MIO> T                  ! module responds, press Return again and
                        ! issue the TEST/RBD command.

VAXft RBD Monitor Vx.x

RBD2>                   ! Places you in the RBD monitor on the
                        ! secondary system I/O controller module
                        ! in slot 1. (Slot 1 has slot ID 2.)
                        ! You are able to run RBD tests.
RBD2> ^P                ! Returns you to the primary CIO.
```

Another console mode, identified by the DSF_## prompt, is used to run WAN module RBD tests. From this mode, the TEST/RBD command invokes the RBD monitor on the WAN module (Example 1–4).

Example 1–4 How to Invoke the RBD Monitor on the WAN Module

```
>>>Z_3                  ! Invokes the RBD monitor on the WAN
Return                  module.
DSF_03> TEST/RBD        ! Invokes the interactive RBD monitor.

VAXft RBD Monitor V3.1-562

RBD3> ^Z                ! Places you in DSF32 ROM console mode.
DSF_03> ^P              ! Returns you to the primary CIO.
```

Figure 1–2 Primary System I/O Controller Module/Slot Specifiers for Model 110 System

MODULE SLOTS IN SYSTEM BACKPLANE

	1	2	3	4	5	
	I/O	CPU	MEM			
I/O RBD PROMPT	1	–	–	5	4	BOTH ZONES
ZONE A	A	–	–	E	D	ZONE SLOT IDENTIFIERS FOR BOOT PROCEDURE
ZONE B	F	–	–	J	I	
ZONE A SLOT ID	–	–	–	5	4	USED WITH Z COMMAND
ZONE B SLOT ID	–	–	–	A	9	
MEMORY	–	–	1	2	3	MODULE EXPANSION SEQUENCE
I/O	1	–	–	–	–	
WAN	–	–	–	4	2	

CS–8844

Figure 1–3 Primary System I/O Controller Module/Slot Specifiers and Module Expansion Sequence for Model 310, 410, 610, and 612 Systems

MODULE SLOTS IN SYSTEM BACKPLANE

	1	2	3	4	5	6	7	
		I/O	CPU	MEM				
I/O RBD PROMPT	2	1	–	–	5	4	3	BOTH ZONES
ZONE A	B	A	–	–	E	D	C	ZONE SLOT IDENTIFIERS FOR BOOT PROCEDURE
ZONE B	G	F	–	–	J	I	H	
ZONE A SLOT ID	2	–	–	–	5	4	3	USED WITH Z COMMAND
ZONE B SLOT ID	7	–	–	–	A	9	8	
MEMORY	–	–	–	1	2	3	4	MODULE EXPANSION SEQUENCE
I/O	2	1	–	–	–	–	–	
WAN	1	–	–	–	4	2	2	

MR–0468–91RAGS

1.3.2 RBD Monitor

Diagnostics are run interactively through the RBD monitor. To access the RBD monitor, use the T[est] command at the local console prompt or use the RBD command. The console returns the RBD> prompt.[1]

Example 1–5 shows how to invoke external loopback tests.

Example 1–5 How to Invoke External Loopback Tests

```
RBD#> ST 1/T=0:2/C [Return]
```

When issued, test RBD 1 invokes the external loopback tests for SWIFT, LANCE, and the modem. The /C qualifier automatically confirms the presence of the loopback connectors. (See Table 1–2.)

NOTE

If you use the /C qualifier and the loopback connectors are *not* present, RBD 1 causes the RBD to fail and the EEPROM to be written.

Table 1–4 lists the RBD monitor commands in the format **command** *required-parameter [optional-parameter]*, where the command name is in **bold type**, and the parameters are in *italics*. Optional parameters are surrounded by square brackets [ ]. There may be several parameters for a command.

WARNING

Do not use DEPOSIT or EXAMINE commands while both zones are running the operating software. Doing so could cause a CPU/memory miscompare, and result in a zone fault. The system I/O controller module must be taken off-line before the RBD monitor is invoked.

To run diagnostics from the RBD monitor, use the **Start** command. The **Start** command syntax is:

```
ST RBD_number [/test=start_test_number:end_test_number] [parameters]
```

[1] Since CIO mode is the default console mode, the prompt does not specify a slot ID number.

Tables 1–12, 1–13, and 1–14 list the RBD numbers, test numbers, and test names. Brief descriptions of the tests follow the tables. Example 1–6 shows how to issue a command to run diagnostics from the RBD monitor.

Example 1–6 How to Issue an RBD Test Command

```
RBDn> ST 0/t=0:28 [Return]
```

Table 1–4 RBD Monitor Commands

Command	Description
Clear	Clears out RBD error frames in the EEPROM and asks for confirmation.
[Crtl/C]	Stops RBD, runs cleanup code and returns to the RBD monitor.
[Crtl/D]	Toggles delete from line printer style to video terminal style.
[Crtl/Q]	XON. Suspended terminal output is resumed.
[Crtl/R]	Redisplays current command line.
[Crtl/S]	XOFF. Terminal output is suspended.
[Crtl/U]	Ignores command line and issues new prompt.
[Crtl/Y]	Stops RBD without running cleanup code. Returns to the RBD monitor.
[Crtl/Z]	Same as [Crtl/C] when running RBD. Same as Quit command when at the monitor prompt.
Copy *length source_address destination_address*	Copies a number of bytes specified by the length parameter from the source address to the destination address.

Table 1–4 (Continued) RBD Monitor Commands

Command	Description
Deposit *address [qualifier] data*	Deposits the specified data at the specified address. Address may be: An address location (hex) IPR number (hex) (See /I qualifier.) GPR number (hex) (See /G qualifier.) * deposits to same address as last examine /deposit. + deposits to next address from last examine/deposit. - deposits to previous address from last examine/deposit. Qualifiers: /BYTE deposits byte-length data. /GPR deposits to a general purpose register. /IPR deposits to an internal processor register. /LONGWORD deposits longword-length data. /PHYSICAL deposits to a physical memory location. REPEAT=n repeats the command n (decimal) times. n=0 is used for infinity. /WORD deposits word-length data.
Dump	Prints out error frames from the EEPROM.
DUP *node [local_program]*	Invokes the DUP utility. This command is valid only on I/O modules. Refer to Section 1.4 for more information.

Table 1–4 (Continued) RBD Monitor Commands

Command	Description
Examine *[qualifier] [address]*	Examines the contents of the specified address. If no address is specified, the address location that follows the last address referenced in an examine or deposit command is examined. Address may be: An address location (hex) IPR number (hex) (See /I parameter.) GPR number (hex) (See /G parameter.) * examines same address as last examine /deposit. + examines next address from last examine /deposit. - examines previous address from last examine/deposit. Qualifiers: /BYTE examines byte-length data. /GPR examines a general purpose register. /IPR examines an internal processor register. /LONGWORD examines longword-length data. /PHYSICAL examines a physical memory location. /REPEAT=n repeats the command n (decimal) times. n=0 is used for infinity. /WORD examines word-length data.
Quit	Returns to console mode.
SHOW_DSSI	Uses the DUP firmware to show all devices connected to the DSSI cable. This command is valid only on I/O modules.

Table 1–4 (Continued) RBD Monitor Commands

Command	Description
Start *RBD_number [qualifier]*	Begins the interactive execution of the specified RBD test(s). The default for all qualifiers except for /P and /T is disabled. Qualifiers: /C — destructive test confirmation[1] /LE — loop on test on error /HE — halt on error /P=n — passcount = n /QV — quick verify /T=n [:m] — run only test n, or tests n to m inclusive /BE — bell on error /DS — disable status reports /IE — inhibit error reports /IS — inhibit summary reports /TR — enable test trace
SUMMARY	Outputs a summary report of the last diagnostic that was executed to the console terminal.
XFC *address*	Initiates a diagnostic that was down-line loaded into main memory at the specified address.

[1]See Section 1.3.3 for details about this parameter, including warning information.

1.3.3 Destructive Test Confirmation

Some RBD tests have the ability to destroy customer data. When any of these tests are specified to be run, the RBD issues a warning message in the form `Confirm [N]?` to avoid inadvertent destruction of data. To proceed with the diagnostic execution, type Y Return. Typing anything else prevents diagnostic execution, and the RBD prompt returns. None of the tests specified in the command string run if the user declines the confirmation. Examples 1–7, 1–8, and 1–9 show the commands used to execute, abort, and suppress confirmation of a destructive test. User input is shown underlined. The warnings in the first two examples are RBD test dependent and may not appear. No warning appears in the third example.

Example 1–7 How to Execute a Destructive Test

```
RBD2> ST 1/T=2:5     ! Runs RBD 1, tests 2 to 5.
Confirm [N]? Y       ! User chooses to run test anyway.
                     ! Tests 2 to 5 of RBD 1 begin execution.
```

Example 1–8 How to Abort a Destructive Test

```
RBD2> ST 1/T=2:5       ! Runs RBD 1, tests 2 to 5.
Confirm [N]? Return    ! User chooses to not run test.
RBD2>                  ! Monitor awaits next command.
```

Example 1–9 How to Suppress Destructive Test Confirmation

```
RBD2> ST 1/T=2:5/C   ! Runs RBD 1, tests 2 to 5. Does
                     ! not issue confirmation prompt.
                     ! Tests 2 to 5 of RBD 1 begin execution.
```

1.3.4 Console Readout

RBD console messages follow a standard output format summarized in Figure 1–4. The RBD messages are categorized into the following single-line formats.

- Level 1 error/status report — used to report system and device errors, status reports, and a diagnostic completion message.
- Level 2 error/status report — used to report system and device errors, and status report messages.
- Level 3 error report — used to report system and device error messages.
- Summary report — used as part of a diagnostic completion message, or in response to the RBD monitor SUMMARY command.

- Trace header — provides trace header information if the switch /TR is set.
- Test trace — provides trace information if the switch /TR is set.
- Extended level 3 information — is determined by the RBD being run.

An error message readout may not contain all seven lines. For example, when the RBD completes without errors, level 2 and level 3 messages are not displayed.

Figure 1–4 RBD Message Fields

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Level 1	Status	Slot Number	Module ID	Pass Count				
Level 2	Error Type	Logic ID	Test Number	RBD Number	Unit Number			
Level 3	Error Code	Error Number	Expectd Data	Receivd Data	Error Data	Error Address	Error PC	
Summary	UUT Mask	Hard Errcnt	Soft Errcnt					
Trace Header	RBD ID	RBD Version						
Test Trace	Test ID	Test ID	Test ID	Test ID	Test ID	Test ID	Test ID	Test ID
Extended Level 3	Data	Data	Data	Data	Data	Data	Data	Data

MR−0671−90.RAGS

Example 1–10 uses the RBD formats described in Figure 1–4 to show a diagnostic failure. The Test Trace qualifier and Halt on Error qualifier are used.

NOTE

The failure shown in Example 1–10 is caused by *not* installing the modem loopback connector. *Never* run this test without a modem loopback connector. See Section 1.3.7 for more details.

Example 1–10 Readout Showing Diagnostic Failure and RBD Message Fields

```
RBD1>ST 1/TR/HE

;EXT CONN      2.70                                                   ! Trace Header
Confirm [N]: Y

;0..1..2..                                                            ! Test Trace

;        F XXXXXXXX      CIO 00000001                                 ! Level 1
;       HE MOD lpbk T0000002 RBD00001 XXXXXXXX                        ! Level 2
; 00000003 00000003 00000000 XXXXXXXX XXXXXXXX 00000000 2006B425  ! Level 3
;        F XXXXXXXX      CIO 00000001                                 ! Level 1
; XXXXXXXX 00000001 00000000                                          ! Summary
```

1.3.4.1 Level 1 Message Fields

Figures 1–5 to 1–11 focus on the individual fields in each of the seven message formats. Level 1 messages follow a standard output summarized in Figure 1–5.

Figure 1–5 Level 1 Messages

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Level 1	Status	Slot Number	Module ID	Pass Count				

MR−0678−90.RAGS

- Status — indicates the current status of the RBD.

  F = Failed
  P = Passed
  S = Status report

- Slot ID — identifies the logical slot ID number (hex) of the module under test. This field is xxx for the processor module, which has no logical slot ID.

- Module ID — identifies the type of module under test.

  CIO = I/O module
  COMM = WAN module
  SYS = System test
  ZONE = Zone test
  CPU = CPU/memory module

- Pass count — indicates the number of passes (decimal) through the RBD at the time of the message.

1.3.4.2 Level 2 Message Fields

Level 2 messages follow a standard output summarized in Figure 1–6.

Figure 1–6 Level 2 Messages

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Level 2	Error Type	Logic ID	Test Number	RBD Number	Unit Number			

MR−0677−90.RAGS

- Error type — specifies the type of error reported.

  FE = System fatal error
  HE = Hard device error
  SE = Soft device error
  XX = Not an error, a status message

- Logic ID — mnemonic of the logic being tested on module under test.
- Test number — a *T* followed by seven decimal numeric characters that specify the number of the test currently being executed. The cleanup code fills this field with xs.
- RBD number — contains the string RBD followed by five numeric decimal characters that specify the number of the RBD that is currently executing. The format is RBDxxxxx, where xxxxx is the RBD number in decimal.
- Unit number — the number of the unit under test, if appropriate. If the unit number is not a meaningful field, the RBD macros fill this field with xs.

1.3.4.3 Level 3 Message Fields

Level 3 messages follow a standard output summarized in Figure 1–7.

Figure 1–7 Level 3 Messages

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Level 3	Error Code	Error Number	Expected Data	Received Data	Error Data	Error Address	Error PC	

MR−0676−90RAGS

- Error code — a decimal error code that specifies the nature of the error detected by the RBD.
- Error number — a decimal error code that specifies the position of the error detected by the RBD. Used as an index into the RBD code, the error number allows a knowledgeable user to pinpoint the detection of an error in the RBD code.
- Expected data — a hex longword representing the expected data from the comparison that detected the error. If the RBD does not specify the expected data, this field is filled with xs.
- Received data — a hex longword representing the received data from the comparison that detected the error. If the RBD does not specify the received data, this field is filled with xs.
- Error data — a hex longword representing the data associated with an error. If no error is detected, this field is filled with xs.
- Error address — a hex longword representing the address associated with a detected error. If the RBD does not specify the error address, this field is filled with xs.
- Error PC — a hex longword representing the value of the PC at the time when the error occurred.

1.3.4.4 Summary Report Fields

Summary report messages follow a standard output summarized in Figure 1–8.

Figure 1–8 Summary Report Messages

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Summary	UUT Mask	Hard Errcnt	Soft Errcnt					

MR−0675−90.RAGS

- UUT mask — a byte-length hex mask that indicates which units are under test by the RBD. Each bit in the mask corresponds to a separate unit.
- Hard errcnt — the number (decimal) of hard errors detected by the RBD.
- Soft errcnt — the number (decimal) of soft errors detected by the RBD.

1.3.4.5 Trace Header Message Fields

Trace header messages follow a standard output summarized in Figure 1–9.

Figure 1–9 Trace Header Messages

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Trace Header	RBD ID	RBD Version						

MR−0674−90.RAGS

- RBD ID — a mnemonic that identifies the RBD.
- RBD version — identifies the major and minor revision values of the RBD in the format M.mm, where M = major revision level and mm = minor revision level.

1.3.4.6 Test Trace Message Fields

Test trace messages follow a standard output summarized in Figure 1–10.

Figure 1–10 Test Trace Messages

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Test Trace	Test ID	Test ID	Test ID	Test ID	Test ID	Test ID	Test ID	Test ID

MR−0673−90.RAGS

The test trace provides a variable number of fields of information that signify the identification number of the test being run (if the trace is enabled by the /TR switch when the RBD is started).

Each field contains a test ID that identifies the test being run in the format:

Tn

;0..1..2..3..4..5..6..7..8..9..10..11..12..13..

and so on, where n is the decimal test number.

As each new test begins, a new ID is added to the string of test ID numbers. When a line reaches the maximum number of characters (8 ID numbers), a new line is generated for the next test trace.

1.3.4.7 Extended Level 3 Message Fields

Extended level 3 messages follow a standard output summarized in Figure 1–11.

Figure 1–11 Extended Level 3 Messages

	Field 1	Field 2	Field 3	Field 4	Field 5	Field 6	Field 7	Field 8
Extended Level 3	Data	Data	Data	Data	Data	Data	Data	Data

MR−0672−90.RAGS

The extended level 3 message fields contain up to eight longwords (hex) of data per line, determined by the RBD being run. Tables 1–5 through 1–11 list the error codes and messages for the KFE52 I/O modules.

Table 1–5 Core Error Codes

Logic ID	Error Code	Description
EEROM TO	1	A timeout is encountered while writing to the EEROM power-on counter.
EEROM TO	2	A timeout is encountered while writing to the EEROM.
EEROM	3	A data miscompare occurs following a write/read to the EEROM.
EEROM TO	4	A timeout is encountered while writing original data back to the EEROM.
UPDATREG	5	A data miscompare occurs following a write/read to UPDATREG.
UPDATREG	6	The EEROM was written to, even with UPDATE REGISTER in “read” mode.
ROM CSEL	8	SSC generated an address allowing a write to EEROM. EEROMCSEL_L is probably stuck low. The EEROM was incorrectly enabled.
EEROMSEL	9	SSC generated an address allowing a write to EEROM. EEROMCSEL_L is probably stuck low. The EEROM was incorrectly enabled.
EEROMSEL	10	Should have gotten a machine check for trying to access unavailable EEROM.
TOY CLK	1	This error occurs if the time-of-year clock is not counting.
CON PORT	1	This error occurs when the SSC console transmitter does not show ready before the first write.
CON PORT	2	This error occurs when the SSC console transmitter does not show ready after the first write.
CON PORT	3	This error occurs when the SSC console receiver does not show that the data has been received.
CON PORT	4	This error occurs when the SSC console data read is not equal to the data written.
STO PORT	1	This error occurs when the SSC storage transmitter does not show ready before the first write.
STO PORT	2	This error occurs when the SSC storage transmitter does not show ready after the first write.

Table 1–5 (Continued) Core Error Codes

Logic ID	Error Code	Description
STO PORT	3	This error occurs when the SSC storage receiver does not show that the data has been received.
STO PORT	4	This error occurs when the SSC storage data read is not equal to the data written.
ROM TEST	1	This error occurs when the checksum of the ROMs does not match the data calculated.
ENET ROM	1	This error occurs when the ENET ROM data is inconsistent.

Table 1–6 SLIM Chip Error Codes

Logic ID	Error Code	Description
SLIM REG	0	A pattern of AA8 was written to the control register and a different value was read back.
SLIM REG	1	A pattern of 154 was written to the control register and a different value was read back.
SLIM REG	2	A pattern of 2AAA8 was written to the DMA pointer and a different value was read back.
SLIM REG	3	A pattern of 15554 was written to the DMA pointer and a different value was read back.
SLIM REG	4	The DMA select bit was not set after a write of the DMA pointer.
SLIM REG	5	The DMA select bit was cleared by a write of 0 to it.
SLIM REG	6	The DMA select bit was not cleared by a write of a 1 to it.

Table 1–6 (Continued) SLIM Chip Error Codes

Logic ID	Error Code	Description
MEM TEST	1	Memory was not 0 when read prior to the first write. This indicates that either the location cannot be written or a write to some other address has been written to this address also.
MEM TEST	2	Memory was written with As, but a different value was read back.
MEM TEST	3	Memory was written with 5s, but a different value was read back.
MEM TEST	4	The high-to-low direction of memory was not initialized to 5s during the first read in this direction. This indicates that a write command to some other address has been written to this address also.
MEM TEST	5	Memory was written with As, but a different value was read back.
MEM TEST	6	Memory was written with its own address, but a different value was read back.
MASK TST	1	The RAM mask test failed during byte-size writes. The expected data was not equal to the data received.
MASK TST	2	The RAM mask test failed during word-size writes. The expected data was not equal to the data received.
MASK TST	3	The RAM mask test failed during word-size writes when the write started on the third byte of the longword. The expected data was not equal to the data received.

Table 1–7 Firewall Chip Error Codes

Logic ID	Error Code	Description
FW REG	1	Expected data was not equal to the data received while testing the firewall registers.
INT TEST	1	The test did not service the required four interrupts.
INT TEST	2	The test serviced the interrupts, but not as expected.
F-XC_DAL	1	This error occurs when the machine check does not happen or happens in the wrong place.
BAD INT	2	This error occurs when an exception other than a machine check happens.
F-XC_BIT	2	This error occurs when no machine check happens.
F-XC_BIT	3	This error occurs when no machine check happens while resetting the CSR.
F-XC_BIT	4	This error occurs when a machine check happens at the wrong place.
BAD INT	5	This error occurs when an exception other than a machine check happens.
RAILID	1	The right rail cannot be selected as the master.
RAILID	2	The left rail cannot be selected as the master.
TR_L_A	2	The left rail trace RAM write/read of AAAA failed.
TR_R_A	3	The right rail trace RAM write/read of AAAA failed.
TR_L_5	5	The left rail trace RAM write/read of 5555 failed.
TR_R_5	6	The right rail trace RAM write/read of 5555 failed.
TR_L_U	7	The left rail trace RAM write/read of marching 1s failed.
TR_R_U	8	The right rail trace RAM write/read of marching 1s failed.
F_PCMHRD	2	This error occurs when the PCM register is not behaving properly. A bad loopback, or a bad bus or chip has occurred.
F_PCMHRD	3	This error occurs when the PCM register is not behaving properly. A bad loopback, or a bad bus or chip has occurred.

Table 1–7 (Continued) Firewall Chip Error Codes

Logic ID	Error Code	Description
WRT FAIL	1	This error indicates that the PCM has not signaled that it is ready to accept a command.
F_NOACK	2	This error indicates that the 8051 received the self-test command but never responded.
F_PCMSLF	3	This error indicates that the 8051 responded to the self-test command with a bad code (R5).
WRT FAIL	4	The 8051 does not signal that it is ready to accept another command after passing the self-test.
WRT FAIL	6	The 8051 never signals that it is ready to accept the next command after accepting the command to address itself.
F_NOACK	7	The 8051 does not acknowledge the loopback command after accepting it.
F_PCMLP	8	The 8051 acknowledges the loopback command with the wrong value after accepting it.
WRT FAIL	9	The 8051 never signals that it can take a date value after properly going into loopback mode.
F_NOACK	10	The 8051 never responds with a value after accepting the loopback data.
F_8051	11	The 8051 responds with loopback data but it is incorrect.
WRT FAIL	12	The 8051 never signals that it can take the command to get it out of loopback mode.
F_NOACK	16	The 8051 accepts the exit loopback command but never responds to it.
F_PCMEND	13	The 8051 responds to the exit loopback command with invalid data.
DEV INT	90	An unexpected device interrupt occurs from the firewall registers.
UNEXP	99	An unexpected interrupt or exception occurs.

Table 1–8 LANCE Chip Error Codes

Logic ID	Error Code	Description
S-LA_DAL	1	An error occurs when the received result from the latch is not valid.
S-LA_DAL	2	An error occurs when the received result from the latch is not valid.
BAD CSR0	1	LANCE did not transmit and/or receive data properly. The incorrect status is in CSR 0.
BAD CSR1	2	LANCE did not transmit and/or receive data properly. The incorrect status is in CSR 1.
BAD BUF	3	LANCE received bytes that do not match the transmitted bytes.
BAD CSR0	1	LANCE had an incorrect status in CSR 0.
NO IDON	2	LANCE did not initialize properly. IDON was not set.
NO INIT	3	LANCE did not initialize properly. INIT was not set.
NO INTR	4	LANCE did not initialize properly. INTR was not set.
NO INEA	5	LANCE did not initialize properly. INEA was not set.
OVER_INT	6	Too many interrupts have occurred during the LANCE test.
BAD INT	7	Another device interrupted during the LANCE test.
NO INTR	8	No LANCE interrupt occurred when interrupts were enabled.
ERR_CSR0	9	Error bit was set in CSR 0 during the LANCE test.
MISS_PKT	10	LANCE missed the packet bit set in CSR 0.
CERR SET	11	The LANCE collision error bit was set in CSR 0.
MERR SET	12	The LANCE memory error bit was set in CSR 0. A memory interface problem exists.
BABBLE	13	The LANCE babble error bit was set in CSR 0. A packet setup error has occurred in LANCE.
NO INIT	14	LANCE is incorrectly initialized. The INIT bit was not set in CSR 0.
NO INTR	15	LANCE is incorrectly initialized. The INIT bit was not set in CSR 0.

Table 1–8 (Continued) LANCE Chip Error Codes

Logic ID	Error Code	Description
NO INEA	16	LANCE is incorrectly initialized. The INEA bit was not set in CSR 0.
NO TXON	17	The LANCE transmitter is not on. TXON was not set.
NO RXON	18	The LANCE receiver is not on. TXON was not set.
NO STRT	19	The LANCE is incorrectly started. The STRT bit was not set.
TXCNT	20	The LANCE transmitted packet count is not as expected.
RXCNT	21	The LANCE packet count received is not as expected.
BAD CSR1	22	LANCE has an incorrect status in CSR 1.
BAD BUF	23	The received bytes do not match the transmitted bytes after a LANCE transfer.
BAD CRC	24	An incorrect CRC is detected during the LANCE test.
RXDESC0	25	The receive message descriptor 0 is not as expected during the LANCE test.
RXDESC1	26	The receive message descriptor 1 is not as expected during the LANCE test.
RXDESC2	27	The receive message descriptor 2 is not as expected during the LANCE test.
RXDESC3	28	The receive message descriptor 3 is not as expected during the LANCE test.
TXDESC0	29	The transmit message descriptor 0 is not as expected during the LANCE test.
TXDESC1	30	The transmit message descriptor 1 is not as expected during the LANCE test.
TXDESC2	31	The transmit message descriptor 2 is not as expected during the LANCE test.
TXDESC3	32	The transmit message descriptor 3 is not as expected during the LANCE test.
UNEXP	33	An unexpected interrupt occurs during the LANCE test with interrupts.

Table 1–9 SWIFT Chip Error Codes

Logic ID	Error Code	Description
S-SW_DAL	1	Error numbers 1 and 2 indicate that the HPDAL latch is not functioning correctly. The latch is resident on the SLIM chip at address offset 60.
S-SW_DAL	2	See above.
SW RESET	1	An error here indicates that the SWIFT CSRs do not reset correctly due to the SWIFT chip, the DSSI bus, or the interface to the SWIFT reset signals.
SW IAD	2	An error here indicates that an illegal access has been made to the SWIFT address space and that the SWIFT chip or external addressing may be at fault.
SW IREG	3	An illegal address error does not occur when forced. The SWIFT chip or external addressing may be the cause.
SW R-W	1	The register under test failed patterns of 5s. Possible stuck-at on the DAL bus or a bad SWIFT chip.
SW R-W	2	The register under test failed patterns of As. Possible stuck-at on the DAL bus or a bad SWIFT chip.
SW IACC	3	Illegal access to SWIFT register space occurs. Possible stuck-at on the HPDAL or a faulty SWIFT chip.
SW CSR	4	Special case testing on the DSSI bus registers. Areas to check include the DSSI cables and the output drivers on SWIFT.
SWIFT IL	0	The SWIFT transaction status does not show success. When the DSSI transaction/transfer is complete, the SWIFT returns a status word, stored in the first synchronous word of the first transmit buffer in RAM. This status is not as expected.
SWIFT IL	1	The SWIFT, though enabled and set up with good buffers, does not try to arbitrate for the use of the DSSI bus. The expected data is the bit corresponding to the DSSI node ID on the DSSI data bus.
SWIFT IL	4	The SWIFT does not try to select the CPU DSSI node, even though it arbitrated for it and should have won. The bits expected on the DSSI bus are those representing the SWIFT (initiator) and CPU (target) IDs.

Table 1–9 (Continued) SWIFT Chip Error Codes

Logic ID	Error Code	Description
SWIFT IL	8	XORing all command bytes and the command checksum does not give a 0 result. A transmit of some sumcheck error has occurred.
SWIFT IL	12	The TX and RX buffers in RAM do not match after the DSSI transfer.
SWIFT IL	13	Frame data checksum is not correct, or data is corrupt.
SWIFT IL	5	A timeout is encountered while waiting for the assertion of DSSI ACK.
SWIFT IL	9	See above.
SWIFT IL	11	See above.
SWIFT IL	7	A timeout is encountered while waiting for the deassertion of DSSI ACK.
SWIFT IL	2	A timeout is encountered while waiting for the assertion of DSSI SEL.
SWIFT IL	3	A parity error is detected on the DSSI data bus.
SWIFT IL	6	See above.
SWIFT IL	10	See above.
BAD INT	1	Unexpected interrupt or exception.
SWIFT INT	1	A timeout is encountered while waiting for the SWIFT to MicroVAX interrupt, or the wrong interrupt is received.
SWIFT INT	2	The test hangs in a continuous SWIFT to MicroVAX interrupt loop.

Table 1–10 External Loopback Error Codes

Logic ID	Error Code	Description
SW_DDB5	1	The DSSI data bus is incorrect. (Missing terminator, bad drivers, or bad SWIFT chip.)
SW_DDBA	2	The DSSI data bus is incorrect. (Missing terminator, bad drivers, or bad SWIFT chip.)
SW_DCS5	3	The DSSI control signals are incorrect. (Missing terminator, bad drivers, or bad SWIFT chip.)
SW_DCSA	4	The DSSI control signals are incorrect. (Missing terminator, bad drivers, or bad SWIFT chip.)
BAD CSR0	1	An incorrect status in CSR 0 is detected during the LANCE external loopback test.
BAD CSR1	2	An incorrect status in CSR 1 is detected during the LANCE external loopback test.
BAD BUF	3	The received bytes do not match the transmitted bytes during LANCE external loopback test.
BAD CRC	4	An incorrect CRC is detected during LANCE external loopback test.
RXDESC0	5	The receive message descriptor 0 is not as expected during LANCE external loopback test.
RXDESC1	6	The receive message descriptor 1 is not as expected during LANCE external loopback test.
RXDESC2	7	The receive message descriptor 2 is not as expected during LANCE external loopback test.
RXDESC3	8	The receive message descriptor 3 is not as expected during LANCE external loopback test.
TXDESC0	9	The transmit message descriptor 0 is not as expected during LANCE external loopback test.

Table 1–10 (Continued) External Loopback Error Codes

Logic ID	Error Code	Description
TXDESC1	10	The transmit message descriptor 1 is not as expected during LANCE external loopback test.
TXDESC2	11	The transmit message descriptor 2 is not as expected during LANCE external loopback test.
TXDESC3	12	The transmit message descriptor 3 is not as expected during LANCE external loopback test.
MOD LPBK	1	This error indicates that the SSC is never clear to send.
MOD LPBK	2	This error indicates that the SSC is never clear to receive.
MOD LPBK	3	This error indicates that a character is sent, but the receiver is never signaled done.
MOD LPBK	4	This error indicates that the data sent is not equal to the data read.
MOD LPBK	5	This error indicates that the modem control register in the firewall does not loopback properly.

Table 1–11 Manufacturing EEROM Error Codes

Logic ID	Error Code	Description
EEROM	1	This error occurs if a timeout occurs during a write.
EEROM	2	This error occurs if the data written is not equal to the data read.
EEROM	3	Two locations in EEROM were written with one write.
EEROM	4	Write timeout occurs during the second write.
EEROM	5	A bad write occurs during the second write.
EEROM	6	A timeout error occurs during an EEROM write.
EEROM	7	An error that restores data occurs.
UPDATREG	8	A data miscompare occurs following a write/read to UPDATREG.

Table 1–11 (Continued) Manufacturing EEROM Error Codes

Logic ID	Error Code	Description
UPDATREG	9	The EEROM is written when UPDATREG is in “read” mode.
ROM CSEL	11	The SSC generated an address that allowed a write to EEROM when ROM space was specified.
EEROMSEL	12	The SSC generated an address that allowed a write to EEROM. EEROMCSEL_L is probably stuck low. EEROM is incorrectly enabled.
EEROMSEL	13	A machine check should have been received when trying to access unavailable EEROM.

1.3.5 CPU Module RBD Tests

The diagnostic ROM on the processor module contains three RBDs. All three are run as part of the power-up self-test. RBD 0 is the CPU/memory module test, RBD 1 is the zone test, and RBD 2 is the system test.

The diagnostic ROM on the I/O module contains three RBDs. RBD 0 tests the logic on the I/O module and is run as part of the power-up self-test. RBD 1 is the external loopback test, and RBD 2 is the full EEPROM test.

The diagnostic ROM on the WAN module contains two RBDs. RBD 0 tests the logic on the WAN module, and is run as part of the power-up self-test. RBD 1 is the external loopback test.

The following sections contain tables that list the CPU module, I/O module, and WAN module RBDs. Brief descriptions of the tests follow the tables.

1.3.6 CPU Module RBDs

Table 1–12 CPU Module RBDs

RBD Number	Test Number	Test Name
RBD 0		Module self-test
RBD 0	Test 0	CVAX/CFPA hardcore test
RBD 0	Test 1	Scratchpad RAM test
RBD 0	Test 2	Short CPU EEPROM test
RBD 0	Test 3	External cache with no memory interaction test
RBD 0	Test 4	MCTL MEMERR interrupt test
RBD 0	Test 5	MCTL bus timeout control register test
RBD 0	Test 6	MCTL control and status register test
RBD 0	Test 7	MCTL error registers test
RBD 0	Test 8	DMA engine with no memory interaction test
RBD 0	Test 9	Memory array(s) test
RBD 0	Test 10	External cache with memory interaction test
RBD 0	Test 11	Parallel cross-link logic test
RBD 0	Test 12	Serial cross-link logic test
RBD 0	Test 13	DMA engine with memory interaction test
RBD 0	Test 14	MCTL bus comparators test
RBD 0	Test 15	Programmable internal timer test
RBD 0	Test 16	Memory array(s) march test and bitmap generator
RBD 0	Test 17	CPU module EEPROM rail symmetry test
RBD 0	Test 18	CPU module interrupt test
RBD 0	Test 19	CPU module reset test
RBD 1		Zone test

Table 1–12 (Continued) CPU Module RBDs

RBD Number	Test Number	Test Name
RBD 1	Test 0	I/O module(s) access using CVAX test
RBD 1	Test 1	I/O module(s) access using DMA test
RBD 1	Test 2	I/O module(s) firewall cross-check test
RBD 1	Test 3	Programmable divider test
RBD 1	Test 4	I/O module(s) selection test
RBD 1	Test 5	Firewall to CVAX interrupt test
RBD 1	Test 6	SWIFT to CVAX interrupt test
RBD 1	Test 7	LANCE to CVAX interrupt test
RBD 1	Test 8	Trace RAM test
RBD 1	Test 9	Halt arbitration test
RBD 2		System test
RBD 2	Test 0	Cross-link modes test
RBD 2	Test 1	Master/slave - I/O module(s) access using CVAX test
RBD 2	Test 2	Resync. master/slave - I/O module(s) access using CVAX test
RBD 2	Test 3	On (duplex) mode - I/O module(s) access using CVAX test
RBD 2	Test 4	Master/slave - I/O module(s) access using DMA test
RBD 2	Test 5	Resync. master/slave - I/O module(s) access using DMA test
RBD 2	Test 6	On (duplex) mode - I/O module(s) access using DMA test
RBD 2	Test 7	Master/slave - I/O module select test
RBD 2	Test 8	Resync. master/slave - I/O module select test
RBD 2	Test 9	On (duplex) mode - I/O module select test
RBD 2	Test 10	Master/slave - System interrupt test

Table 1–12 (Continued) CPU Module RBDs

RBD Number	Test Number	Test Name
RBD 2	Test 11	Resync. master/slave - System interrupt test
RBD 2	Test 12	On (duplex) mode - System interrupt test
RBD 2	Test 13	Reset test
RBD 2	Test 14	Automatic failover test
RBD 3		Extended manufacturing test
RBD 3	Test 0	CPU module EEPROM page mode test
RBD 3	Test 1	CPU module EEPROM byte write test

CPU RBD 0, **Module self-test —** verifies the logic on the CPU module. When run interactively, this test executes CPU RBD 0 tests 0 through 19.

CPU RBD 0 - Test 0, **CVAX/CFPA hardcore test —** verifies the operational status of the CVAX and the CFPA.

CPU RBD 0 - Test 1, **Scratchpad RAM test —** verifies the addressing and data integrity of the scratchpad RAM by performing a nondestructive march test on the entire scratchpad RAM.

CPU RBD 0 - Test 2, **Short CPU EEPROM test —** performs a nondestructive write/read test of the CPU EEPROM.

CPU RBD 0 - Test 3, **External cache with no memory interaction test —** verifies the ability of the external caches to function correctly. Tests that are run when test 3 is selected include:

- Control and status tests
- Cacheable transaction tests
- Noncacheable transaction tests
- Wrap tests
- Word-mask tests
- Data/index tests
- Data/tag RAM tests

CPU RBD 0 - Test 4, **MCTL MEMERR interrupt test —** verifies the MCTL error reporting logic by forcing nonexistent memory (NXM) and nonexistent I/O (NXIO) conditions, and checking that MEMERR interrupts are detected and recoverable.

CPU RBD 0 - Test 5, **MCTL bus timeout control register test —** verifies the data integrity and the functional operation of the MCTL bus timeout control register.

CPU RBD 0 - Test 6, **MCTL control and status register test —** verifies the data integrity of the MCTL control and status register.

CPU RBD 0 - Test 7, **MCTL error registers test —** verifies the operational status of the MCTL diagnostic error register, system fault register, and system fault address register.

CPU RBD 0 - Test 8, **DMA engine with no memory interaction test —** verifies the following functions of the DMA logic in the memory controller chip without communicating with any memory arrays.

- Interrupt
- Register access
- Address decode
- Interlock access

CPU RBD 0 - Test 9, **Memory array(s) test —** verifies the function of all available memory array modules, one at a time. The following logic is tested on the memory array as it interfaces with the memory controller:

- Write/read/control register
- Address registers
- Error detection and correction code (EDCC)
- Addressing
- EEPROM

CPU RBD 0 - Test 10, **External cache with memory interaction test —** verifies the function of the external caches by running a memory array test and a DMA data invalidate test.

CPU RBD 0 - Test 11, **Parallel cross-link logic test —** verifies the path in the parallel cross-link logic by gaining access to the parallel cross-link registers. It also checks power-up and stuck-at conditions of the parallel cross-link registers and the CROME bus.

CPU RBD 0 - Test 12, **Serial cross-link logic test —** accesses all of the serial cross-link registers and verifies the serial cross-link logic. The following functions are tested:

- Register access
- Register data integrity
- Zone ID
- Query and loopback continuity
- Query and reply register overflow
- Status read continuity

CPU RBD 0 - Test 13, **DMA engine with memory interaction test —** uses diagnostic DMA mode to verify the function of the DMA logic in the memory controller chip. The following functions are tested:

- Queue processing
- Subtransfer length
- I/O byte alignment
- Memory byte alignment
- Maximum length transfer
- CVAX/DMA arbitration
- CRC generation/checking

CPU RBD 0 - Test 14, **MCTL bus comparators test —** forces a miscompare on each data line to verify the function of the MCTL bus comparators.

CPU RBD 0 - Test 15, **Programmable internal timer test —** verifies the data integrity and the interrupt logic of the programmable internal timer.

CPU RBD 0 - Test 16, **Memory array(s) march test and bitmap generator —** performs a march test on all available memory arrays, and produces the memory bitmap used by the operating system.

CPU RBD 0 - Test 17, **CPU module EEPROM rail symmetry test —** verifies that the contents of the CPU module EEPROM is symmetric and nondivergent.

CPU RBD 0 - Test 18, **CPU module interrupt test —** verifies the cross-link interrupt logic. Interrupt delivery is checked on each of the four request lines at the four interrupt levels.

CPU RBD 0 - Test 19, **CPU module reset test —** verifies the function of hard and soft resets on the CPU module.

CPU RBD 1, **Zone test —** verifies the ability of the logic modules in the zone to communicate. When run interactively, this test executes CPU RBD 1 tests 0 through 9.

CPU RBD 1 - Test 0, **I/O module(s) access using CVAX test —** verifies the path to all I/O modules through the firewall chip. The path to all major gate arrays and the accessibility of the I/O module DMA register is checked. The test also verifies the function of the interlock instruction logic in the cross-link registers.

CPU RBD 1 - Test 1, **I/O module(s) access using DMA test —** verifies DMA transactions between main memory and local RAM on all I/O modules. The following functions are tested:

- Queue processing
- Subtransfer length
- I/O byte alignment
- Memory byte alignment

CPU RBD 1 - Test 2, **I/O module(s) firewall cross checkers test —** verifies the operation of the firewall cross checkers by forcing and verifying firewall miscompares for all 32 bits, with each rail as the primary controller.

CPU RBD 1 - Test 3, **Programmable divider test —** verifies the programmable divider logic.

CPU RBD 1 - Test 4, **I/O module(s) selection test —** verifies the I/O module selection. The DMA byte count register is written into an I/O module firewall, setting the selection bit in the firewall DMA status register for this module and leaving it clear for other modules. This test is repeated for all “good” I/O modules in the zone.

CPU RBD 1 - Test 5, **Firewall to CVAX interrupt test —** verifies the delivery of firewall interrupts to the CPU through the MI bus. This test generates and verifies an interrupt at each IPL. Next, all four interrupt lines are asserted and dismissed, one at a time.

CPU RBD 1 - Test 6, **SWIFT to CVAX interrupt test —** verifies interrupt delivery from the SWIFT chip on all I/O modules to the CVAX.

CPU RBD 1 - Test 7, **LANCE to CVAX interrupt test —** verifies interrupt delivery from the LANCE chip on all I/O modules to the CVAX by forcing an interrupt using the LANCE initialization sequence.

CPU RBD 1 - Test 8, **Trace RAM test —** verifies the integrity of the trace RAMs by writing, then reading the contents of the RAMs. Trace freeze and mismatch capture is verified by a forced error during an I/O interrupt cycle.

CPU RBD 1 - Test 9, **Halt arbitration test —** verifies the ability to halt the CPU module.

CPU RBD 2, **System test —** verifies the interaction of the zones.

CPU RBD 2 - Test 0, **Cross-link modes test —** verifies the functional operation of the cross-link and memory controller for all cross-link modes. This test verifies the following registers:

- Cross-link error register
- MCTL diagnostic error register
- Serial cross-link CSR
- Parallel cross-link CSR

CPU RBD 2 - Test 1, **Master/slave - I/O module(s) access using CVAX test —** verifies the path to all I/O modules through the firewall chip. The function is the same as in the zone tests, except the I/O modules are tested in the master/slave mode.

CPU RBD 2 - Test 2, **Resync. master/slave - I/O module(s) access using CVAX test —** verifies the path to all I/O modules through the firewall chip. The function is the same as in the zone tests, except the I/O modules in both zones are tested in the resync. master/slave mode.

CPU RBD 2 - Test 3, **On (duplex) mode - I/O module(s) access using CVAX test —** verifies the path to all I/O modules through the firewall chip. The function is the same as in the zone tests, except the I/O modules in both zones are tested in the on, or duplex, mode.

CPU RBD 2 - Test 4, **Master/slave - I/O module(s) access using DMA test —** verifies the function of the DMA transactions between the main memory and the local RAM on all I/O modules. The function is the same as in the zone tests, except the I/O modules in both zones are tested in the master/slave mode.

CPU RBD 2 - Test 5, **Resync. master/slave - I/O module(s) access using DMA test —** verifies the function of the DMA transactions between the main memory and the local RAM on all I/O modules. The function is the same as in the zone tests, except the I/O modules in both zones are tested in the resync. master/slave mode.

CPU RBD 2 - Test 6, **On (duplex) mode - I/O module(s) access using DMA test —** verifies the function of the DMA transactions between the main memory and the local RAM on all I/O modules. The function is the same as in the zone tests, except the I/O modules in both zones are tested in the on, or duplex, mode.

CPU RBD 2 - Test 7, **Master/slave - I/O module select test —** verifies the I/O module selection by writing the DMA byte count register into an I/O module firewall chip. The test sets the selection bit in the firewall DMA status register for the I/O module and clears the bit for other I/O modules. The test is repeated for all “good” I/O modules in a zone using the master/slave mode.

CPU RBD 2 - Test 8, **Resync. master/slave - I/O module select test —** verifies the I/O module selection by writing the DMA byte count register into an I/O module firewall chip. The test sets the selection bit in the firewall DMA status register for the I/O module and clears the bit for other I/O modules. The test is repeated for all “good” I/O modules in a zone using the resync. master/slave mode.

CPU RBD 2 - Test 9, **On (duplex) mode - I/O module select test —** verifies the I/O module selection by writing the DMA byte count register into an I/O module firewall chip. The test sets the selection bit in the firewall DMA status register for the I/O module and clears the bit for other I/O modules. The test is repeated for all “good” I/O modules in a zone using the on, or duplex, mode.

CPU RBD 2 - Test 10, **Master/slave - system interrupt test —** verifies the delivery of FW interrupts from either zone to the CPU module through the MI bus and cross-link register. The test is repeated for all “good” I/O modules in a zone using the master/slave mode.

CPU RBD 2 - Test 11, **Resync. master/slave - system interrupt test —** verifies the delivery of FW interrupts from either zone to the CPU module through the MI bus and cross-link register. The test is repeated for all “good” I/O modules in a zone using the resync. master/slave mode.

CPU RBD 2 - Test 12, **On (duplex) mode - system interrupt test —** verifies the delivery of FW interrupts from either zone to the CPU module through the MI bus and cross-link register. The test is repeated for all “good” I/O modules in a zone using the on, or duplex, mode.

CPU RBD 2 - Test 13, **Reset test —** verifies the function of the CPU module for the following cross-link modes:

- Master/slave
- Duplex

CPU RBD 2 - Test 14, **Automatic failover test —** verifies the ability of the system to automatically failover from the duplex mode to the nonduplex mode on zone miscompares and CPU/MEM faults.

CPU RBD 3, **Extended manufacturing test**.

CPU RBD 3 - Test 0, **CPU module EEPROM page mode test —** verifies that the EEPROM is addressable and read/writeable. This test also verifies that the update register functions correctly. This test performs a nondestructive test of the EEPROM. Writes to the EEPROM are performed by page-mode writes.

CPU RBD 3 - Test 1, **CPU module EEPROM byte write test —** verifies that the EEPROM is addressable and read/writeable. This test also verifies that the update register functions correctly. This test performs a nondestructive test of the EEPROM. Writes to the EEPROM are performed by single-byte writes.

1.3.7 I/O Module RBDs

Table 1–13 I/O Module RBDs

RBD Number	Test Number	Test Name
RBD 0		Module self-test
RBD 0	Test 0	Short EEPROM test
RBD 0	Test 1	ROM checksum test
RBD 0	Test 2	ENET ROM test
RBD 0	Test 3	SSC LEDs test
RBD 0	Test 4	SSC console UART test
RBD 0	Test 5	SSC TOY clock test
RBD 0	Test 6	SSC storage UART test
RBD 0	Test 7	SSC bus timeout test
RBD 0	Test 8	SSC interval timer test
RBD 0	Test 9	SLIM register toggle test
RBD 0	Test 10	Buffer RAM memory test
RBD 0	Test 11	Buffer RAM mask test
RBD 0	Test 12	Firewall register toggle test

Table 1–13 (Continued) I/O Module RBDs

RBD Number	Test Number	Test Name
RBD 0	Test 13	Rail switching test
RBD 0	Test 14	Firewall interrupt test
RBD 0	Test 15	Firewall cross-check/diagnostic bit test
RBD 0	Test 16	Firewall cross-check - forced error test
RBD 0	Test 17	Firewall trace RAM test
RBD 0	Test 18	PCM hardware loopback test
RBD 0	Test 19	PCM software loopback test
RBD 0	Test 20	SWIFT special case CSR test
RBD 0	Test 21	SWIFT CSR initialization test
RBD 0	Test 22	SWIFT CSR read/write test
RBD 0	Test 23	SWIFT initiator internal loopback test
RBD 0	Test 24	SWIFT target internal loopback test
RBD 0	Test 25	LANCE CSR read latch test
RBD 0	Test 26	LANCE CSR read/write test
RBD 0	Test 27	LANCE internal loopback test
RBD 0	Test 28	LANCE internal loopback test with interrupts
RBD 1		External loopback test
RBD 1	Test 0	SWIFT external loopback test
RBD 1	Test 1	LANCE thin/thickwire external loopback test
RBD 1	Test 2	MODEM port external loopback test
RBD 1	Test 3	SWIFT to MicroVAX interrupt test (RBD 1 version 2.70 or later)
RBD 2		Full EEPROM test

I/O RBD 0, **Module self-test —** verifies the logic on the I/O module. When run interactively, this test executes I/O RBD 0 tests 0 through 28.

I/O RBD 0 - Test 0, **Short EEPROM test —** performs a nondestructive write/read verification of EEPROM. This test runs the first 10 times RBD 0 is executed.

I/O RBD 0 - Test 1, **ROM checksum test —** performs a read of the ROM and verifies that the calculated checksum equals the checksum stored in the last longword in ROM.

I/O RBD 0 - Test 2, **ENET ROM test —** verifies the format and the checksums of the ENET ROM.

I/O RBD 0 - Test 3, **SSC LEDs test —** flashes the LEDs on the I/O module to verify their operation.

I/O RBD 0 - Test 4, **SSC console UART test —** performs an internal loopback of the SSC console UART. All baud rates are checked using the patterns 55 and AA as data.

I/O RBD 0 - Test 5, **SSC TOY clock test —** performs a test of the SSC TOY clock. If set, this test verifies that the clock is counting. If not set, this tests sets the clock and then verifies that the clock is running.

I/O RBD 0 - Test 6, **SSC storage UART test —** performs an internal loopback of the SSC storage UART. All baud rates are checked using the patterns 55 and AA as data.

I/O RBD 0 - Test 7, **SSC bus timeout test —** verifies that the SSC initiates a machine check when a read or write access is attempted to a nonexistent location.

I/O RBD 0 - Test 8, **SSC interval timer test —** verifies that the interval timer counts down and interrupts the CVAX when the time expires.

I/O RBD 0 - Test 9, **SLIM register toggle test —** verifies the accessibility and data integrity of the registers in the SLIM gate array.

I/O RBD 0 - Test 10, **Buffer RAM memory test —** verifies the accessibility, data integrity, and data uniqueness of the buffer RAM by writing a pattern of 5s and As to the RAM, then writing the location address into each location and reading it back.

I/O RBD 0 - Test 11, **Buffer RAM mask test —** verifies the byte mask function by writing a unique byte into a longword, and checking that only that single byte was written. The test is repeated for all byte positions.

I/O RBD 0 - Test 12, **Firewall register toggle test —** verifies the accessibility and data integrity of the registers in the firewall gate arrays. Right, left, and both addresses are checked.

I/O RBD 0 - Test 13, **Rail switching test —** verifies that either rail can be selected as master. Rail switching is accomplished by toggling bit 5 of FW_CSR. Then unique data is written to the left and right rails of the FW_INTVEC0 register, and the contents of the register is read back through a dual rail address.

I/O RBD 0 - Test 14, **Firewall interrupt test —** verifies the operation of the firewall interrupts with the CVAX. All four IRQ lines are tested at all four IPLs.

I/O RBD 0 - Test 15, **Firewall cross-check/diagnostic bit test —** verifies that all 32 address/data lines miscompare. Each line is checked individually.

I/O RBD 0 - Test 16, **Firewall cross-check - forced error test —** sets the force miscompare bit in the firewall to force a miscompare on the next firewall access.

I/O RBD 0 - Test 17, **Firewall trace RAM test —** verifies the operation of the trace RAM by writing data into the trace RAM and then reading it back. The test is repeated for both firewalls.

I/O RBD 0 - Test 18, **PCM hardware loopback test —** verifies the operation of the PCM logic in the firewall and the external drivers by putting the external drivers into the loopback mode and looping information through them.

I/O RBD 0 - Test 19, **PCM software loopback test —** verifies the functional communication with the 8051 by putting the 8051 in a mode where it returns the complement of whatever has been sent to it.

I/O RBD 0 - Test 20, **SWIFT special case CSR test —** verifies the integrity of the HPDAL latch residing on the HPDAL bus.

I/O RBD 0 - Test 21, **SWIFT CSR initialization test —** verifies the accessibility of the SWIFT CSRs. This test also verifies that the SWIFT chip has correctly reset.

I/O RBD 0 - Test 22, **SWIFT CSR read/write test —** verifies the accessibility and data integrity of all nondriver-related registers on the SWIFT chip.

I/O RBD 0 - Test 23, **SWIFT initiator internal loopback test —** performs an internal loopback with the SWIFT chip. The SWIFT is acting as an initiator and transferring one packet of data from the buffer RAM.

I/O RBD 0 - Test 24, **SWIFT target internal loopback test —** performs an internal loopback with the SWIFT chip. The SWIFT is acting as a target and transferring one packet into buffer RAM.

I/O RBD 0 - Test 25, **LANCE CSR read latch test —** verifies the integrity of the LADAL latch residing on the LADAL bus.

I/O RBD 0 - Test 26, **LANCE CSR read/write test —** verifies the accessibility of the LANCE CSRs and checks the reset state of the LANCE chip.

I/O RBD 0 - Test 27, **LANCE internal loopback test —** verifies the ability of the LANCE chip to transmit and receive data while in internal loopback mode with interrupts disabled. Initialization, transmit and receive rings, and buffers are verified. The test also checks that the CRC for the transmit packet agrees with the CRC of the received packet.

I/O RBD 0 - Test 28, **LANCE internal loopback test with interrupts —** verifies the ability of the LANCE chip to transmit and receive data while in internal loopback mode with interrupts enabled. Initialization, transmit and receive rings, and buffers are verified. The test also checks that the CRC for the transmit packet agrees with the CRC of the received packet.

I/O RBD 1, **External loopback test —** verifies the external drivers and port logic on the I/O module. Each of the I/O RBD 1 tests requires a loopback connector. When run interactively, this test executes I/O RBD 1 tests 0 through 3. (Test 3 is implemented only in RBD 1 version 2.70 or later.)

I/O RBD 1 - Test 0, **SWIFT external loopback test —** verifies the integrity of the external drivers on the host port. With the addition of a DSSI terminator, the test proves data integrity of the DSSI control and data signals. This test requires a loopback connector (PN 12-29258-01, minimum rev. B01).

I/O RBD 1 - Test 1, **LANCE thin/thickwire external loopback test —** verifies the integrity of the external drivers for the LANCE chip. The required loopback connector depends on the configuration of the Ethernet select switch on the I/O module (ThinWire or thickwire). If the switch is set for ThinWire, use a T-connector with two 50-Ω terminators. If the switch is set for thickwire, use an H4080 turnaround connector.

I/O RBD 1 - Test 2, **Modem port external loopback test —** determines the slot identification for the CIO module under test. If it is not in slot 2, the rest of the test is ignored and the following message is displayed:

```
Non-primary CIO, modem loopback test skipped.
```

This test then verifies the integrity of the modem port of the I/O module by writing, then reading back data to a turnaround connector at the modem port. All baud rates are tested. This test requires a loopback connector (PN 12-15336-08). (The check and message for slot identification is implemented only in RBD 1 version 2.70 or later.)

I/O RBD 1 - Test 3, **SWIFT to MicroVAX interrupt test —** verifies the correct delivery of an interrupt from the SWIFT on a CIO module to the MicroVAX by the firewall. (This test is implemented in RBD 1 version 2.70 or later.)

I/O RBD 2, **Full EEPROM test —** provides a full nondestructive write/read test on EEPROM. This is the only test in RBD 2. Once started, the test cannot be aborted. Any error that occurs during this test may cause the entire content of the EEPROM to be lost. To protect the system from being shut down and causing loss of EEPROM integrity, the following messages are displayed:

```
Test will run up to ten minutes. Control C will be ignored.

Power cycling the system or interrupting this test in any way prior
to completion may cause irretrievable loss of EEPROM data.
```

The full EEPROM test is implemented in RBD2 version 2.70, or later.

1.3.8 WAN Module RBDs

Table 1–14 WAN Module RBDs

RBD Number	Test Number	Test Name
RBD 0	Test 1	ROM checksum test
RBD 0	Test 2	ROM byte pack test
RBD 0	Test 3	SSC timer test
RBD 0	Test 4	SSC bus timeout test
RBD 0	Test 5	SSC interval timer test
RBD 0	Test 6	SSC UART loopback test
RBD 0	Test 7	Local RAM access test
RBD 0	Test 8	Local RAM addressing test
RBD 0	Test 9	Local RAM data integrity test
RBD 0	Test 10	Local RAM byte mask test
RBD 0	Test 11	VIC access test
RBD 0	Test 12	VIC registers test
RBD 0	Test 13	VIC interrupt test
RBD 0	Test 14	Shared RAM access test
RBD 0	Test 15	Shared RAM addressing test
RBD 0	Test 16	Shared RAM data integrity test
RBD 0	Test 17	Shared RAM byte mask test
RBD 0	Test 18	Firewall access test
RBD 0	Test 19	Firewall registers test
RBD 0	Test 20	Firewall master/slave test
RBD 0	Test 21	Firewall cross-check test
RBD 0	Test 22	Firewall interrupt test
RBD 0	Test 23	Firewall trace RAM test

Table 1–14 (Continued) WAN Module RBDs

RBD Number	Test Number	Test Name
RBD 0	Test 24	Turbo counter access test
RBD 0	Test 25	Turbo counter test
RBD 0	Test 26	Micro DMA access test
RBD 0	Test 27	Micro DMA registers test
RBD 0	Test 28	DUSCC access test
RBD 0	Test 29	DUSCC registers test
RBD 0	Test 30	DUSCC receiver baud rate generator test
RBD 0	Test 31	DUSCC transmitter baud rate generator test
RBD 0	Test 32	FIFO access test
RBD 0	Test 33	Drive –5 V check test
RBD 0	Test 34	Drive to Y-box current limiter test
RBD 0	Test 35	On-board data loop test
RBD 0	Test 36	DUSCC interrupt test
RBD 0	Test 37	FIFO DCD logic test
RBD 1	Test 0	EEPROM write/read test
RBD 1	Test 1	Off-board data loop test
RBD 1	Test 2	Modem signal loop test
RBD 1	Test 3	Driver enable/disable test
RBD 1	Test 4	UART loopback test
RBD 2	Test 1	EEPROM exhaustive test
RBD 2	Test 2	HDLC loopback test
RBD 2	Test 3	On-board synchronous communication test

DSF RBD 0 - Test 1, **ROM checksum test —** verifies that the ROM can be accessed longword by longword without error.

DSF RBD 0 - Test 2, **ROM byte pack test —** verifies that the ROM can be accessed by bytes, words, or longwords on any alignment.

DSF RBD 0 - Test 3, **SSC timer test —** verifies that the two programmable SSC timers keep time within ± 5% of programmed values.

DSF RBD 0 - Test 4, **SSC bus timeout test —** verifies that the microprocessor ERR line is asserted when a bus timeout occurs. The timing of the bus timeout is also verified.

DSF RBD 0 - Test 5, **SSC interval timer test —** verifies the SSC /microprocessor interval timer logic and that the TOY/INTIM increments occur every 10 milliseconds ± 5%.

DSF RBD 0 - Test 6, **SSC UART loopback test —** verifies both SSC UARTs in the loopback mode.

DSF RBD 0 - Test 7, **Local RAM access test —** attempts to access the local RAM.

DSF RBD 0 - Test 8, **Local RAM addressing test —** accesses the local RAM and performs simple tests.

DSF RBD 0 - Test 9, **Local RAM data integrity test —** performs complete testing of the local RAM using longword-aligned longword accesses only.

DSF RBD 0 - Test 10, **Local RAM byte mask test —** verifies that bytes, words, and longwords on different alignments can be written to and read from local RAM.

DSF RBD 0 - Test 11, **VIC access test —** attempts to access the VIC.

DSF RBD 0 - Test 12, **VIC registers test —** performs a duplicate addressing and data test on selected VIC registers.

DSF RBD 0 - Test 13, **VIC interrupt test —** verifies that the VIC can interrupt the microprocessor using all four IRQs and that the VIC can operate with different types of inputs (level/edge, high/low). This is accomplished by using the PIRQ 15 and PIRQ 14 diagnostic inputs to test the VIC.

DSF RBD 0 - Test 14, **Shared RAM access test —** attempts to access the shared RAM.

DSF RBD 0 - Test 15, **Shared RAM addressing test —** searches for duplicate addressing errors in shared RAM.

DSF RBD 0 - Test 16, **Shared RAM data integrity test —** performs complete testing of the shared RAM using longword-aligned longword accesses only.

DSF RBD 0 - Test 17, **Shared RAM byte mask test —** verifies that bytes, words, and longwords on different alignments can be written to and read from shared RAM.

DSF RBD 0 - Test 18, **Firewall access test —** attempts to access the firewalls.

DSF RBD 0 - Test 19, **Firewall registers test —** performs a duplicate addressing and data test on selected firewall registers.

DSF RBD 0 - Test 20, **Firewall master/slave test —** verifies that the microprocessor can change which firewall chip is the master.

DSF RBD 0 - Test 21, **Firewall cross-check test —** verifies that the firewalls can detect a miscompare error between them.

DSF RBD 0 - Test 22, **Firewall interrupt test —** verifies that the firewall can interrupt the microprocessor through the VIC.

DSF RBD 0 - Test 23, **Firewall trace RAM test —** performs writes of three different data patterns (AAAA, 5555, and marching 1s) to a trace RAM in the firewall and reads the firewall status register to determine the rail ID. The trace RAM is in the diagnostic mode.

DSF RBD 0 - Test 24, **Turbo counter access test —** attempts to access the turbo counter.

DSF RBD 0 - Test 25, **Turbo counter test —** performs a fake turbo DMA transfer to test the firewall interface without the use of the firewall interface or the CPU module.

DSF RBD 0 - Test 26, **Micro DMA access test —** attempts to access the micro DMA.

DSF RBD 0 - Test 27, **Micro DMA registers test —** performs a duplicate addressing and data test on selected micro DMA registers.

DSF RBD 0 - Test 28, **DUSCC access test —** attempts to access the DUSCC.

DSF RBD 0 - Test 29, **DUSCC registers test —** performs a duplicate addressing and data test on selected DUSCC registers.

DSF RBD 0 - Test 30, **DUSCC receiver baud rate generator test —** verifies the operation of the DUSCC receiver baud rate generator.

DSF RBD 0 - Test 31, **DUSCC transmitter baud rate generator test —** verifies the operation of the DUSCC transmitter baud rate generator.

DSF RBD 0 - Test 32, **FIFO access test —** attempts to access the FIFO control bits.

DSF RBD 0 - Test 33, **Drive –5 V check test —** verifies that the –5 V is between –3.9 V and –6.2 V.

DSF RBD 0 - Test 34, **Drive to Y-box current limiter test —** verifies that the current limiter circuit, which limits the +5 V going to the Y-box by the 100-pin cable, has not detected a short.

DSF RBD 0 - Test 35, **On-board data loop test —** verifies the on-board data paths.

DSF RBD 0 - Test 36, **DUSCC interrupt test —** verifies that the DUSCC can interrupt the microprocessor.

DSF RBD 0 - Test 37, **FIFO DCD logic test —** verifies the DCD through the FIFO logic.

DSF RBD 1 - Test 0, **EEPROM write/read test —** verifies that the EEPROM can be written to and read from, and that no duplicate addressing or retention errors have occurred.

DSF RBD 1 - Test 1, **Off-board data loop test —** verifies the off-board data paths. This test can be run with an H3199 loopback cable or any personality loopback cable, with one connector on either of the two channels, or without connectors on the channels.

DSF RBD 1 - Test 2, **Modem signal loop test —** verifies all modem signal loops in the loopback connectors currently in place on each channel. All of the DSF32 modem signals are tested if an H3199 loopback cable is used.

DSF RBD 1 - Test 3, **Driver enable/disable test —** verifies that the logic enables and disables the drivers.

DSF RBD 1 - Test 4, **UART loopback test —** verifies the path from the SCC out and back by the 20-pin loopback cable for both UART ports.

DSF RBD 2 - Test 1, **EEPROM exhaustive test —** verifies the EEPROM completely.

DSF RBD 2 - Test 2, **HDLC loopback test —** allows the user to pass a parameter directly to the HDLC subroutine SUB$_HDLC_DLP.

DSF RBD 2 - Test 3, **On-board synchronous communication test —** verifies all on-board synchronous communication data loops.

1.4 DUP

The diagnostic/utility protocol (DUP) RBD provides a means to exercise the mass storage device, erase user data, or alter configuration data on DSSI mass storage devices. The DUP uses local programs that reside on the ROM in the mass storage controllers. Each mass storage device in the VAXft system has a dedicated controller mounted in the cannister or carrier module. The DUP RBD may be started by the RBD monitor.

1.4.1 Local Programs

The following list includes the local programs for RF-series devices. Refer to the *RF31/RF72 Integrated Storage Element User Guide* for detailed information about the RF31 local programs.

Program	Description
DIRECT	Provides a directory of local programs resident in the ISE.
DRVEXR	Exercises the RF-series subsystem.
DRVTST	A comprehensive verification of the ISE hardware.
HISTRY	Displays information about the ISE.
ERASE	Utility that completely writes over data on the ISE.
VERIFY	A read check of the ISE. Also checks the remaining margin on the disk.
DKUTIL	Displays disk structures and disk data.
PARAMS	Allows the examination and edit of device status and internal parameters.

The following list includes the local programs for the TF70 tape drive. Refer to the *TF70 Cartridge Tape Drive Subsystem Service Manual* for detailed information about the TF70 local programs.

Program	**Description**
DIRECT	Provides a directory of local programs resident in the drive.
DRVEXR	Exercises the TF70 subsystem.
DRVTST	A comprehensive verification of the TF70 subsystem hardware.
HISTRY	Displays information about the TF70 drive.
PARAMS	Allows the examination and edit of device status and internal parameters.

1.5 Accessing the DUP Utility from VMS Operating System

To access a local program, you need to know the node name of the device you wish to test. To get this information, use the SHO DEV command. To access a local program while the VMS operating system is running, use the following DCL commands.

```
SYSGEN>CONN FYA0/NOADAPT
```

```
$ Set Host/DUP/SERVER=MSCP$DUP/TASK=local_program_name node_name
```

Where:

local_program_name	=	name of the requested local program
node_name	=	node name of the device

Example 1–11 shows how to invoke DUP from the VMS operating system. User input is shown underlined.

Example 1–11 How to Invoke DUP from the VMS Operating System

```
$ Set Host/DUP/SERVER=MSCP$DUP/TASK=params DIAGS0
Starting DUP server...

DSSI Node 1 (DIAGS1)
Copyright © 1988 Digital Equipment Corporation

PARAMS> help
  EXIT
  HELP
  SET {parameter | .} value
  SHOW {parameter | . | /class}
    /ALL     /CONST   /DRIVE
    /SERVO   /SCS     /MSCP
    /DUP
  STATUS [type]
    CONFIG   LOG      DATALINK
    PATHS
  WRITE

PARAMS>
```

1.5.1 Accessing the DUP Utility While in Console Mode

To access the DUP utility with a console command, you must be in MIO mode. Use the Z n command to get to the correct RBD. You also need to know the node number of the device you wish to test. Use the SHOW_DSSI command to find this information.

Example 1–12 shows how to issue the SHOW_DSSI command from the primary system I/O controller module. User input is shown underlined.

NOTE

You must issue a STOP/ZONE command to bring the zone to a simplex state before you issue any RBD commands.

Example 1–12 How to Issue the SHOW_DSSI Command

```
>>> MIO             ! Goes to primary system I/O controller
                    ! module I/O mode.

MIO> Test           ! Invokes RBD monitor.

VAXft RBD Monitor V2.0    30-JAN-1990 09:13:01.12

RBD1> SHOW_DSSI

DSSI Node 0 (DIAGS0)             ! Node_name (volume_id)
-DIA0   (RF31)                   ! Device_name   (device_type)
DSSI Node 1 (DIAGS1)             ! Node_name (volume_id)
-DIA1   (RF31)                   ! Device_name   (device_type)
DSSI Node 2 (BACKUP)             ! Node_name (volume_id)
-MIA2   (TF70)                   ! Device_name   (device_type)
DSSI Node 6 (*)                  ! Node_name (volume_id)
                                 ! (Node 6 is the I/O module.)

VAXft RBD Monitor V2.0    30-JAN-1990 09:13:01.12

RBD1>
```

To access the DUP utility, use the following command.

DUP *node_number local_program_name*

Where:

node_number	=	node number of the device to be tested
local_program_name	=	name of the requested local program

Remember to use the Z n command first, if necessary. Example 1–13 shows the console output from the local program DRVTST. User input is shown underlined.

Example 1–13 How to Invoke DUP from the Console

```
RBD2> DUP 0 drvtst
Starting DUP server...

DSSI Node 0 (DIAGS0)
Copyright © 1988 Digital Equipment Corporation
Write/read anywhere on medium [1=Yes/(0=No)] 0
  5 minutes to complete.
Test passed.

Stopping DUP server...

VAXft RBD Monitor V2.0    30-JAN-1990 09:13:01.12
```

2
Errors and Error Analysis

2.1 Error Detection

The VAXft system detects errors by comparing the control and data information at various points in the hardware with the corresponding information in the other zone. The comparison takes place in trace RAMs. Figure 2–1 shows the locations of the trace RAMs in an expanded system. The following list provides an overview of system error types, and shows where they are detected. Some errors may be detected in more than one place.

Errors detected at the CLINK

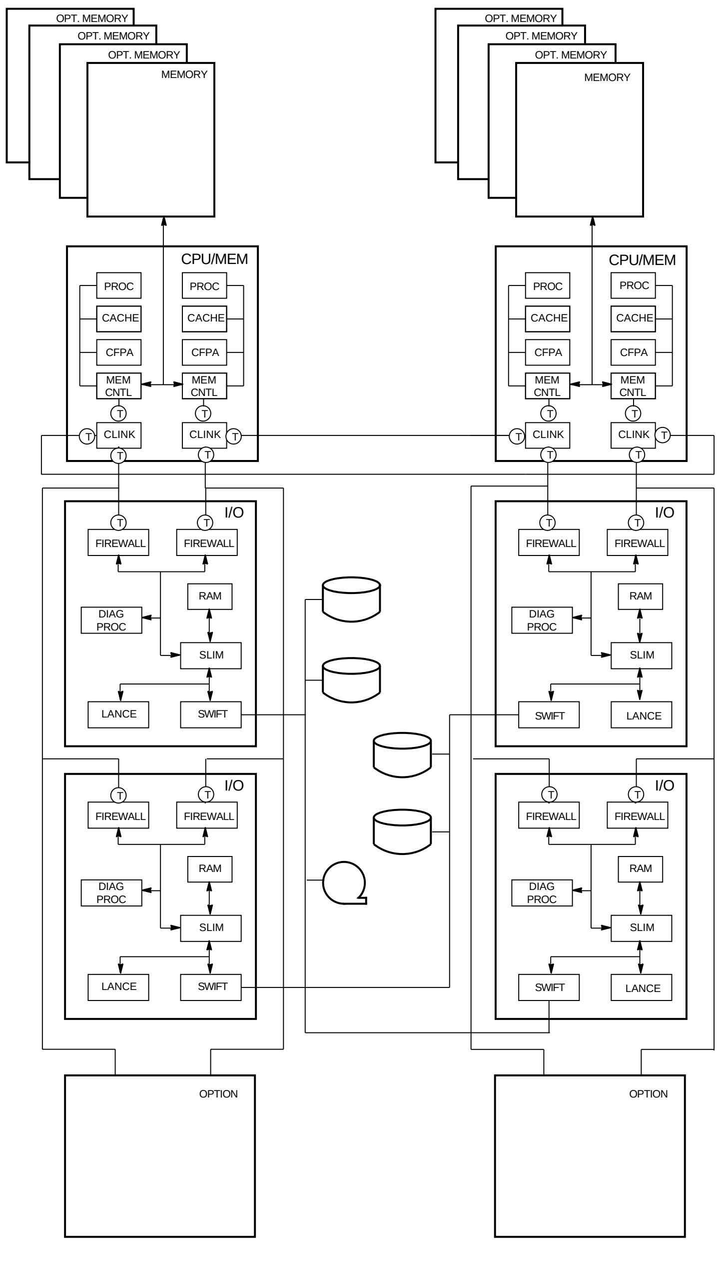
Clock error
CS_UP miscompare error
CVAX I/O miscompare
DMA error miscompare

Errors detected at the firewall

CVAX I/O miscompare
DMA error miscompare
DMA error CRC/EDC error

Errors detected at the WAN module (Section 2.4)

Figure 2–1 Location of Trace RAMs



2.2 Error Handling

The following list shows how a solid system error is handled.

1. A solid error is detected on a system module. IPL 29 error processing begins. The user is notified by an opcom message, and an entry is made to the error log.
2. The FRU is marked bad, a reset command is issued to the module, and self-test diagnostics are run. An entry is made into the module EEPROM, the MFI is set, and the module is removed from the system configuration.
3. System service is initiated. Additional data is written to the error log, and VAXsimPLUS is used to troubleshoot.
4. The event is reported to the operating system software.
5. The system initiates an automatic dial-out, usually to the customer or Customer Services, to notify them of the problem.
6. When the Customer Services engineer arrives, the customer must shut down the appropriate zone. This requires CMKRNL privileges.
7. Repairs are made (with other zone still running).
8. Device/Zone is powered on. The power-on tests verify the repair.
9. Customer starts up the zone.
10. System synchronizes clocks with the other zone, and restores I/O.
11. System synchronizes processors.
12. System reports completion of synchronization to the error log, and to the user by an opcom message.

2.3 Error Log Analysis

The error log for the VAXft system contains some entries that may not be familiar to you. The following types of error log entries are shown in examples that follow.

- EF driver entries (Example 2–1)
- EP driver entries (Example 2–2)
- PW driver entries (Example 2–3 and Example 2–4)
- CM driver entries (Example 2–5)
- MEMERR entries (Example 2–6)

2.3.1 EF Driver Entries

An EF driver entry is shown in Example 2–1.

Example 2–1 EF Driver Entries

```
******************************* ENTRY   40613. *******************************
ERROR SEQUENCE 585.                          LOGGED ON:        SID 14000006
DATE/TIME 6-MAR-1992 22:30:13.58                           SYS_TYPE 07200001
SYSTEM UPTIME: 1 DAYS 06:12:35
SCS NODE: FTCSSE                                            VAX/VMS V5.5

DEVICE ATTENTION  KA550-AA  CPU FW REV# 6.  CONSOLE FW REV# 2.0

FT_NI SUB-SYSTEM, UNIT _FTCSSE$EFB0:
```

Example 2–1 Cont'd on next page

Example 2–1 (Continued) EF Driver Entries

```
        ERROR TYPE       00000003
                                        PHYSICAL ADAPTER VERIFICATION FAILED
        DEVICE NAME      20425045
                                        EPB
        FAILURE CODE     00000001
                                        PORT DEVICE ERROR
        LOOP DATA        00000000
        UCB$B_ERTCNT           01
                                        1. RETRIES REMAINING
        UCB$B_ERTMAX           40
                                        64. RETRIES ALLOWABLE
        ORB$L_OWNER      00000000
                                        OWNER UIC [000,000]
        UCB$L_CHAR       0C442000
                                        NETWORK
                                        AVAILABLE
                                        ERROR LOGGING
                                        CAPABLE OF INPUT
                                        CAPABLE OF OUTPUT
        UCB$W_STS            2010
                                        ONLINE
        UCB$L_OPCNT      00000000
                                        0. QIO'S THIS UNIT
        UCB$W_ERRCNT         0001
                                        49. ERRORS THIS UNIT
        IRP$W_BCNT           0000
                                        TRANSFER SIZE 0. BYTE(S)
        IRP$W_BOFF           0000
                                        TRANSFER PAGE ALIGNED
        IRP$L_PID        00000000
                                        REQUESTOR "PID"
        IRP$Q_IOSB       00000000
                         00000000       IOSB, 0. BYTE(S) TRANSFERRED
        IRP$W_FUNC       460A0000
****************************************************************************
```

The failed device is located by checking two fields in the EF driver entry:

```
FT_NI SUB-SYSTEM, UNIT_FTCSSE$EFB0:
  ^                       ^
  |                       |
  |                       +- The FTCSSE is the node name of
  |                       the system in this example. The EF
  |                       means that the EF driver is reporting
  |                       the error. The B means that this is
  |                       the second set of EP devices. Secondary
  |                       I/O adapters are in physical slot 1
  |                       in both zones. Each EF device has
  |                       two EP devices as a failover set.
  |                       The failover set for EFB0 is EPB0 and
  |                       EPG0. If a problem occurs within the
  |                       EP that is running (e.g. EPB0), the EF
  |                       driver selects and starts using the
  |                       backup device (EPG0). EFA0 is the
  |                       failover set of EPA0 and EPF0. See the
  |                       EP driver entry example for more detail.
  |
  +- This message means that an Ethernet error has occurred.
     The subsystem is located on the I/O module. The subsystem
     includes the LANCE chip, part of the I/O memory, and the
     Ethernet drivers and receivers. One subsystem is present
     on all VAXft I/O modules.
```

The device name field identifies the device and module in question.

```
       DEVICE NAME     20425045
                                       EPB
```

The EPB defines the physical device. The EP defines the EP driver. The B denotes zone A, and the I/O module in slot 1. EPA denotes zone A, and slot 2. EPF would be zone B, and slot 2. EPG would be zone B, and slot 1.

The next field contains the actual error information reported by the driver. The following error type is one of many that can be reported by the driver. The error in the example indicates that a device running the physical adapter verification test has failed that test.

```
ERROR TYPE      00000003
                                PHYSICAL ADAPTER VERIFICATION FAILED
```

The following list includes the possible entry type codes:

1 = Failover successful
2 = Failover unsuccessful
3 = Physical adapter verification failed
4 = Physical adapter verification succeeded
5 = Inter-adapter test failed, previously passed
6 = Inter-adapter test failed, first attempt
7 = Inter-adapter test failed, both directions
8 = Inter-adapter test succeeded
B = Operator requested failover
C = Operator removed failover set member
D = Operator added a failover set member
E = Operator changed the test interval

Sometimes this failure code provides a failure reason (code contains a 3 or 5). If the failure code does not contain a 3 or 5, the field is filled with 0s.

```
FAILURE CODE    00000001
                                PORT DEVICE ERROR
```

The following list defines failure reason codes for entry types 3 or 5:

1 = Port device error
2 = Timeout
3 = Bad received data

The output indicates that the EF driver has detected an error while running the physical adapter verification test on the EPB device. The other parts of the entry contain status information provided for all VMS device entries.

2.3.2 EP Driver Entries

An EP driver entry is shown in Example 2–2.

Example 2–2 EP Driver Entries

```
******************************* ENTRY    1409. *******************************
 ERROR SEQUENCE 50.                            LOGGED ON:        SID 0A000005
 DATE/TIME 19-NOV-1991 03:18:22.22                          SYS_TYPE 07100001
 SYSTEM UPTIME: 0 DAYS 00:41:00
 SCS NODE: FTCSSE                                            VAX/VMS V5.4

 DEVICE ATTENTION  KA520-AA  CPU FW REV# 6.  CONSOLE FW REV# 1.0
                   CPU ID # 0.

 NI SUB-SYSTEM, UNIT _EPG0:

       ERROR CODE      00000005
                                       DMA EDC ERROR
       PORT MODE       0000007A
                                       MAINTENANCE MODE
                                       FATAL ERROR
                                       DEVICE INITIALIZED
                                       CONTROLLER TIMER RUNNING
                                       FINIT HAS BEEN DONE
                                       LIB/ERCB LADRF = MASK
                                       NO SQUEEZE REQUIRED
       UCB$B_ERTCNT          01
                                       1. RETRIES REMAINING
       UCB$B_ERTMAX          38
                                       56. RETRIES ALLOWABLE
       ORB$L_OWNER     00000000
                                       OWNER UIC [000,000]
       UCB$L_CHAR      0C442000
                                       NETWORK
                                       AVAILABLE
                                       ERROR LOGGING
                                       CAPABLE OF INPUT
                                       CAPABLE OF OUTPUT
       UCB$W_STS           0010
                                       ONLINE
       UCB$L_OPCNT     00000000
                                       0. QIO'S THIS UNIT
       UCB$W_ERRCNT        0001
                                       1. ERRORS THIS UNIT
       IRP$W_BCNT          0000
                                       TRANSFER SIZE 0. BYTE(S)
       IRP$W_BOFF          0000
                                       TRANSFER PAGE ALIGNED
       IRP$L_PID       00000000
                                       REQUESTOR "PID"
       IRP$Q_IOSB      00000000
                       00000000        IOSB, 0. BYTE(S) TRANSFERRED
       IRP$W_FUNC      45030000
*******************************************************************
```

The failed device is located by checking two fields in the EP driver entry:

```
NI SUB-SYSTEM, UNIT _FTCSSE$EPG0:
      ^                   ^
      |                   |
      |                   +- The FTCSSE is the node name of
      |                      the system in this example. The EP
      |                      means that the EP driver is reporting
      |                      the error. The G denotes the physical
      |                      device in error is in zone B, and is
      |                      the I/O module in slot 1. EPA denotes
      |                      zone A, and slot 2. EPB denotes zone A,
      |                      and slot 1. EPF denotes zone B, and
      |                      slot 2.
      |
      +- This field indicates an Ethernet error. The subsystem is
         located on the I/O module. The subsystem includes the LANCE
         chip, part of the I/O memory, and the Ethernet drivers and
         receivers. One of these subsystems is present on all VAXft
         I/O modules.
```

The next field contains the error code. This code indicates an Ethernet transmit timeout, detected by the LANCE chip, from an active node.

```
       ERROR CODE      00000005
                                      DMA EDC ERROR
```

The following are the possible active Ethernet error codes:

1 = Collision detect error
2 = Babbling transmitter
3 = Initialization timeout
4 = Transmit timeout
5 = DMA EDC error
6 = Memory error
7 = Fatal DMA error
8 = I/O module is invalid

The port mode provides the status of the LANCE subsystem. The bits can be further defined (see the *VAXft Systems Proprietary Technical Information Manual*).

```
PORT MODE       0000007A
                                MAINTENANCE MODE
                                FATAL ERROR
                                DEVICE INITIALIZED
                                CONTROLLER TIMER RUNNING
                                FINIT HAS BEEN DONE
                                LIB/ERCB LADRF = MASK
                                NO SQUEEZE REQUIRED
```

The other parts of the entry contain status information provided for all VMS device entries.

2.3.3 PW Driver Entries

A PW driver entry is shown in Example 2–3.

Example 2–3 PW Driver Entries

```
******************************* ENTRY   40606. *******************************
ERROR SEQUENCE 578.                           LOGGED ON:        SID 14000006
DATE/TIME 6-MAR-1992 22:30:13.03                             SYS_TYPE 07200001
SYSTEM UPTIME: 1 DAYS 06:12:34
SCS NODE: FTCSSE                                              VAX/VMS V5.5

DEVICE ATTENTION  KA550-AA  CPU FW REV# 6.  CONSOLE FW REV# 2.0

DSSI SUB-SYSTEM, UNIT _FTCSSE$PWF0:
```

Example 2–3 Cont'd on next page

Example 2–3 (Continued) PW Driver Entries

```
ERROR REG       32008102
                                ERROR SUB-TYPE = 2.
                                ERROR TYPE = 129.
                                RETRY CNT = 0.
                                MAX RETRY CNT = 50.
CSR                 0000
                                NON HP MODE ARBITRATION
ID                  0000
                                BUS ID = 0.
                                SWIFT ID DETERMINED VIA BUS ID
DSTMO               0000
BUFFER SIZE         0000
                                SWIFT BUFFER SIZE = 0000(X)
TLP                 0800
                                INCOMING BUFFER ADR
ILP                 0000
                                OUTGOING BUFFER ADR
DSCTRL              0000
                                OUTBOUND PACKETS DISABLED
                                INCOMING PACKETS DISABLED
DICTRL              0000
DATA BUS PARITY     0000
                                SP DATA = 00(X)
                                PARITY BIT = 0(X)
CNTRL SIGNALS       0000
DIAG CNTRL          0000
OVERHEAD SIZE       0000
                                OTHER OVERHEAD SIZE = 0(X)
ERROR CODE          0001
                                MODULE IS "INVALID"
LOTC                0000
BC                  0000
SAVED DSCTRL        C042
                                INITIATOR POINTER ZERO SET
                                MICROPROCESSOR OUTPUT ENABLED
                                MICROPROCESSOR INPUT ENABLED
                                INCOMING PACKETS DISABLED
                                OUTBOUND PACKETS DISABLED

SAVED ISTAT         2001
                                LIST DONE
                                INPUT DONE
UCB$B_ERTCNT          07
                                7. RETRIES REMAINING
UCB$B_ERTMAX          00
                                0. RETRIES ALLOWABLE
```

Example 2–3 Cont’d on next page

Example 2–3 (Continued) PW Driver Entries

```
       ORB$L_OWNER     00000000
                                       OWNER UIC [000,000]
       UCB$L_CHAR      0C450000
                                       SHARABLE
                                       AVAILABLE
                                       ERROR LOGGING
                                       CAPABLE OF INPUT
                                       CAPABLE OF OUTPUT
       UCB$W_STS           0810
                                       ONLINE
                                       SOFTWARE VALID
       UCB$L_OPCNT     00000000
                                       0. QIO'S THIS UNIT
       UCB$W_ERRCNT        001A
                                       26. ERRORS THIS UNIT
       IRP$W_BCNT          0000
                                       TRANSFER SIZE 0. BYTE(S)
       IRP$W_BOFF          0000
                                       TRANSFER PAGE ALIGNED
       IRP$L_PID       00000000
                                       REQUESTOR "PID"
       IRP$Q_IOSB      00000000
                       00000000        IOSB, 0. BYTE(S) TRANSFERRED
       IRP$W_FUNC      4F0A0000
*****************************************************************************
```

The failed device is located by checking two fields in the PW driver entry:

```
DSSI SUB-SYSTEM, UNIT _FTCSSE$PWF0:
 ^                          ^
 |                          |
 |                          +- The FTCSSE is the node name of
 |                             the system in this example. The PW
 |                             means that the PW driver is reporting
 |                             the error. The F indicates that the
 |                             module in error is the I/O module in
 |                             zone B, and slot 2. A denotes zone A,
 |                             and slot 2. B denotes zone A, and
 |                             slot 1. G denotes zone B, and slot 1.
 |
 +- This field indicates a DSSI subsystem error. The subsystem is
    located on the I/O module. The DSSI subsystem includes the SWIFT
    chip, part of the I/O memory, the DSSI tranceivers, the DSSI bus,
    and the disks and tapes on that bus. One of these subsystems is
    present on all VAXft I/O modules.
```

The next field defines the DSSI node associated with this module.

```
ID                  0000
                                BUS ID = 0.
```

The next field defines the error code for this entry.

```
ERROR CODE          0001
                                MODULE IS "INVALID"
```

The following list defines the error codes:

0 = Software timeout detected by driver
1 = Module is "invalid"
2 = SWIFT detected "illegal access"
3 = SWIFT detected "bad first buffer"
4 = SWIFT/PWDRIVER detected "SYNC not found"
5 = DMA related error (non EDC related)
6 = DMA EDC error threshold exceeded
7 = SWIFT EDC error threshold exceeded

A further explanation of the register logged by this entry is given in the *VAXft Systems Proprietary Technical Information Manual*.

The rest of the entry contains status information provided for all VMS device entries.

The following example is a traditional cluster entry logged by the PW device. Pay close attention to the local and remote station addresses. They are DSSI node addresses. The local station is the module in zone A, slot 2. The DSSI node address is 6. The remote node is the disk drive in the expander cabinet in DSSI slot 4. The cluster software is closing the virtual circuit to the software located in the integrated storage element (ISE). To the software, this event is the same as one occurring in a CI cluster, with all the same actions taken. The only difference is that the transport is the DSSI. This information is for those with experience with CI clusters.

A PW driver entry, DSSI cluster special case is shown in Example 2–4. It is the entry resulting from loss of connection to an RF-series disk drive.

Example 2–4 PW Driver Entry, DSSI Cluster Special Case

```
******************************* ENTRY    2453. *******************************
ERROR SEQUENCE 150.                             LOGGED ON:        SID 14000006
DATE/TIME 26-MAR-1992 15:04:10.80                            SYS_TYPE 07200001
SYSTEM UPTIME: 0 DAYS 00:28:00
SCS NODE: FTCSSE                                              VAX/VMS V5.5

ERL$LOGMESSAGE  KA550-AA  CPU FW REV# 6.  CONSOLE FW REV# 2.0

UNKNOWN SUB-SYSTEM, _FTCSSE$PWA0:

      SOFTWARE IS CLOSING VIRTUAL CIRCUIT

      LOCAL STATION ADDRESS, 000000000006(X)
      LOCAL SYSTEM ID, 00000000FA7B(X)

      REMOTE STATION ADDRESS, 000000000004(X)
      REMOTE SYSTEM ID, 405104304931(X)

      UCB$B_ERTCNT          32
                                    50. RETRIES REMAINING
      UCB$B_ERTMAX          32
                                    50. RETRIES ALLOWABLE
      UCB$W_ERRCNT        0001
                                    1. ERRORS THIS UNIT
      PPD$B_PORT            04
                                    REMOTE NODE # 4.
      PPD$B_STATUS          00
      PPD$B_OPC             00
                                    UNKNOWN OPCODE
      PPD$B_FLAGS           00

PORT RESPONSE

      BYTE <3:0>      00050504      /..../
      BYTE <7:4>      00080001      /..../
      BYTE <11:8>     00000000      /..../
      BYTE <15:12>    00000000      /..../
      BYTE <19:16>    00000000      /..../
      BYTE <23:20>    00000000      /..../
      BYTE <27:24>    00000000      /..../
      BYTE <31:28>    00000000      /..../
      BYTE <35:32>    00000000      /..../
      BYTE <39:36>    00000000      /..../
      BYTE <43:40>    00000000      /..../
      BYTE <47:44>    00000000      /..../
      BYTE <51:48>    00000000      /..../
      BYTE <55:52>    00000000      /..../
      BYTE <59:56>    00000000      /..../
      BYTE <63:60>    00000000      /..../
      BYTE <67:64>    00000000      /..../
******************************************************************************
```

2.3.4 CM Driver Entries

A CM driver entry is shown in Example 2–5.

Example 2–5 CM Driver Entries

```
******************************* ENTRY    2149. *******************************
 ERROR SEQUENCE 5.                               LOGGED ON:        SID 14000006
 DATE/TIME 26-MAR-1992 14:16:48.56                             SYS_TYPE 07200001
 SYSTEM UPTIME: 0 DAYS 00:01:25
 SCS NODE: FTCSSE                                               VAX/VMS V5.5

 EMM ENTRY  KA550-AA  CPU FW REV# 6.  CONSOLE FW REV# 2.0

       ERROR ID        00410000
                                       CABINET ID = SYSTEM CAB
                                       ZONE ID = A
                                       TEMPERATURE IN NORMAL ZONE
       COOLING MONITOR 0000005F
                                       PCM DATA = 5F(X)
******************************************************************************
```

Use the following field to define the device. The event occurs from a PCIM in zone A to a PCM in zone B and is reported by the CM driver.

```
 EMM ENTRY  KA550-AA  CPU FW REV# 6  CONSOLE FW REV# 2.0
```

To further define the location where the event occurred, examine the following entry:

```
ERROR ID        00410000
                  ^ ^ ^
                  | | |
                  | | |
                  | | +---- CABINET ID = SYSTEM CAB (1 = expander)
                  | +------ ZONE ID = A (1 = zone B)
                  +-------- TEMPERATURE IN NORMAL ZONE
```

The ERROR ID field in the previous example identifies a zone A system cabinet as the location of the error. The error message reports that the temperature is in the normal operating zone. This is not really an error, but is reported after the temperature has been outside the normal limit and returned to normal, when the fault-tolerant system services layered product is started, or when a zone is started.

The following are the possible error codes:[1]

22 = self-test failure
41 = temperature in normal zone
42 = temperature in yellow zone
43 = temperature in red zone
44 = on battery backup
45 = off battery backup
46 = battery voltage low
47 = battery voltage OK
48 = dc box fault
49 = left fan fault
4A = right fan fault
4B = power input box fault
4C = no battery present
4D = battery fully charged
4E = battery charging
4F = right fan or dc box fault
50 = left fan or dc box fault
51 = summary panel or dc box fault
52 = dc box or power input box fault
54 = lost communication between PCM/PCIM
55 = battery or power input box fault
56 = no right fan present
57 = dc front end present
58 = fans set to maximum speed
59 = battery test failed

The following are the possible zone ID values:

0 = zone A
1 = zone B

The following are the possible cabinet ID values:

0 = system cabinet
1 = expander cabinet
2 = second expander cabinet (model 610 only)

[1] Codes are hexadecimal.

2.3.5 MEMERR Entries

A MEMERR entry is shown in Example 2–6.

Example 2–6 MEMERR Entries

```
******************************* ENTRY   29521. *******************************
ERROR SEQUENCE 1053.                          LOGGED ON:        SID 14000006
DATE/TIME  15-MAR-1992 07:37:13.90                         SYS_TYPE 07200001
SYSTEM UPTIME: 1 DAYS 15:10:08
SCS NODE: FTCSSE                                            VAX/VMS V5.4-3

INT60 ERROR  KA550-AA  CPU FW REV# 6.  CONSOLE FW REV# 42.0

      SYSTEM FAULT    00000001
                                      TRANSIENT FAULT
      SYSTEM FLT ADDR 7AC00052
                                      _CVAX PHYSICAL ADDR = 3AC00052(X)
                                      _CVAX ACCESS TYPE = LONGWORD
      MCTL_DIAG_REG_P FFFFFFFF
      MCTL_DIAG_REG_M FFFFFFFF
      CACHE_FAULT_P   FFFFFFFF
      CACHE_FAULT_M   FFFFFFFF
      MEM CNTRL CSR   FFFFFFFF
      P_XLINK_E_STAT  000000D0
                                      _MEMERR INTERRUPT
                                      _TRACE RAMS FROZEN
                                      ZONE B ERROR = CPU/MEM FAULT
                                      ZONE A ERROR = CVAX I/O ERROR
                                      CLINK MODE = MASTER
      PL_XLINK_CSR_A  00000042
                                      OPERATING SYS RUNNING
                                      CLNK MODE BITS = CLNK MASTER
                                      BUS OPERATION = NORMAL BUS OPERATION
      PL_XLINK_CSR_B  00000001
                                      CLNK MODE BITS = CLNK SLAVE
                                      BUS OPERATION = NORMAL BUS OPERATION
```

Example 2–6 Cont'd on next page

Example 2–6 (Continued) MEMERR Entries

```
SER_CSR_A        4D000802
                                ENABLE QUERY INTERRUPT
                                OS RUN BIT SET
                                CLOCK FAULT ENABLED
                                CLOCK SELECT = SLAVE
                                MAGNETIC INDICATOR ENABLED
                                ZONE_ID  =  A
                                RESYNC MODE = NORMAL BUS OPERATION
                                CLINK_MODE = MASTER
                                SERIAL CMD =  LOOPBACK RQST
SER_CSR_B        98000801
                                ENABLE QUERY INTERRUPT
                                CLOCK FAULT ENABLED
                                SYSTEM FAULT
                                ZONE_ID  =  B
                                MAGNETIC INDICATOR ENABLED
                                MAGNETIC INDICATOR SET
                                CLOCK SELECT   =  MASTER
                                RESYNC MODE = NORMAL BUS OPERATION
                                CLINK_MODE = SLAVE
                                SERIAL CMD =  LOOPBACK RQST

DMA ADDRESS      FFFFFFFF
DMA STATUS_A     FFFFFFFF
DMA STATUS_B     FFFFFFFF
DMA ERROR ADDR   FFFFFFFF
FIREWALL DMA     FFFFFFFF
TRACE RAM SIG_B  FFFFFFFF
FAULT_ID         00000003
                                CPU/MEM FAULT
FT_FLAGS_BEFORE 33003301
                                ACT SET - SYSTEM RUNNING IN DUPLEX MODE
                                ZONE A CPU PRESENT
                                ZONE B CPU PRESENT
                                ZONE A IO PRESENT
                                ZONE B IO PRESENT
                                ZONE A CPU IN USE
                                ZONE B CPU IN USE
                                ZONE A IO IN USE
                                ZONE B IO IN USE

FT_FLAGS_AFTER 31003300
                                ZONE A CPU PRESENT
                                ZONE B CPU PRESENT
                                ZONE A IO PRESENT
                                ZONE B IO PRESENT
                                ZONE A CPU IN USE
                                ZONE B CPU IN USE
                                ZONE A IO IN USE
                                ZONE B IO IN USE
```

Example 2–6 Cont’d on next page

Example 2–6 (Continued) MEMERR Entries

```
       ERROR_SUM       00000001
                                       CPU OR MEM ZONE B
                                       TRANSIENT ERROR
       MODULE_SUM      00000000
       SAVED PC        FFFFFFFF
       SAVED PCL       FFFFFFFF
       THRESHOLD TIME PER  00000000
                                       12. HRS, 0. MINS, 0. SECS
       THRESHOLD VALUE  00030001
                                       ERRORS SEEN IN TIME PERIOD = 1.
                                       THRESHOLD LIMIT = 3.
       CONSOLE STATUS FFFFFFFF
       DIAGNOSTIC STATUS FFFFFFFF

 ******************************* ENTRY   29513. *******************************
 ERROR SEQUENCE 1054                           LOGGED ON:        SID 14000006
 DATE/TIME  15-MAR-1992 07:37:13.92                          SYS_TYPE 07200001
 SYSTEM UPTIME: 1 DAYS 15:10:08
 SCS NODE: FTCSSE                                             VAX/VMS V5.4-3

 $SNDERR MESSAGE  KA550-AA  CPU FW REV# 6.  CONSOLE FW REV# 4.2

 MESSAGE TEXT

       FTSS-I-SYNCLOSSIO, Synchronization lost: zone B has I/O only
********************************************************************************
```

SAVED PC is valid only for CPU MEM fault end action entries (10). All other entries contain Fs. THRESHOLD TIME PERIOD is the length of time an intermittent module has to exceed the threshold count. THRESHOLD VALUES is broken down into two word fields. The low order word contains the number of errors seen in the time period and is displayed as **n** ERRORS SEEN IN TIME PERIOD (**n** = the value in this word). The high order word contains the number of errors that will be allowed for the time period and is displayed as THRESHOLD LIMIT is **n** (**n** = the value in this word). All thresholds are rate-based. The fields indicate how many of the allowable errors have been seen in the time period.

The following procedure shows how to analyze the contents of the memory error shown in Example 2–6. Additional information on register contents may be found in the *VAXft Systems Proprietary Technical Information Manual*.

1. Look at the contents of the FAULT_ID register to find the fault ID code and its meaning. The following table shows the possible contents of this register:

ID Code	Error Type	Meaning
0	NONSI	Nonsense MEMERR interrupt
1	NXM	Nonexistent memory
2	NXIO	Nonexistent I/O address
3	CPUMEM	CPU/MEM fault
4	DMA	DMA fault (not CRC)
5	CLOCK	Clock synchronization fault
6	CABLE_GONE	CLINK cable absent
7	PWR_GONE	No power in other zone
8	CVAXIO	CVAX I/O error
9	ZONE_FAULT	Unspecified zone fault
10	END_ACTION	CPU/MEM fault end action
11	MOD_FAULT	Software detected module fault
12	NO_SYNC	Zone or CPU is not synchable

2. Look at the contents of the MODULE_SUM register. Bits 1 through 15 of this register correspond to module slots within the system. Any bit that is set to 1 indicates that the corresponding module is suspect. If only one bit is set and the fault is solid, the module has been marked as bad. If more than one bit is set the corresponding modules are suspect, but further isolation is not possible.

The following list shows the bit assignments for the MODULE_SUM register:

Bit 0 = unused
Bit 1 = zone A, slot 1
Bit 2 = zone A, slot 2
Bit 3 = zone A, slot 3
Bit 4 = zone A, slot 4
Bit 5 = zone A, slot 5
Bit 6 = zone A, slot 6
Bit 7 = zone A, slot 7
Bit 8 = zone B, slot 1
Bit 9 = zone B, slot 2
Bit 10 = zone B, slot 3
Bit 11 = zone B, slot 4
Bit 12 = zone B, slot 5
Bit 13 = zone B, slot 6
Bit 14 = zone B, slot 7
Bit 15 = zone B, slot 8
Bit 16 to 31 = unused

3. Look at the contents of the ERROR_SUM register to further define the fault. The following list shows the definition of the register bits:

Bit 0: 1 = zone B CPU/MEM fault
Bit 1: 1 = zone A CPU/MEM fault
Bit 2: 1 = entire zone B has been removed
Bit 3: 1 = entire zone A has been removed
Bit 4: 1 = CLINK error
Bit 5: 1 = zone B had a nonisolated fault
Bit 6: 1 = zone A had a nonisolated fault
Bit 7: 1 = module isolated as FRU
Bit 8: 1 = unexpected trace RAM signature
Bit 29: 1 = dial-out requested
Bit 30: 1 = zones have been split as a result of the fault
Bit 31: 1 = solid error, 0 = transient error

4. Look at the FT_FLAGS before and after registers to see the results of the fault-tolerant system services error handling routine. The contents of the register is reported before the error handling routine is entered, and after it has completed. The FT_FLAGS longword gives the state of the CPU CIO system.

5. Look at the RAM_SIGNATURE registers. Each of these registers corresponds to a zone. (Signature_A is for zone A; and signature_B is for zone B.) Bits 2 to 9 in the register correspond to trace RAMs in the zone. If a bit is set to 1, the information from the two zones did not agree at the indicated trace RAM.

   The following list shows the bit assignments and locations of the trace RAMs. This information is useful for analyzing MI and CHROME bus failures.

   Bit 0 = unused
   Bit 1 = unused
   Bit 2 = trace RAM # 2, CPU CLINK
   Bit 3 = trace RAM # 3, CPU CLINK
   Bit 4 = trace RAM # 4, CPU CLINK
   Bit 5 = trace RAM # 5, slot 2
   Bit 6 = trace RAM # 6, slot 1
   Bit 7 = trace RAM # 7, slot 7
   Bit 8 = trace RAM # 8, slot 6
   Bit 9 = trace RAM # 9, slot 5
   Bit 16 to 31 = reserved for future use

6. More bit definitions may be found in the register descriptions in the *VAXft Systems Proprietary Technical Information Manual*. The other fields should be approached based on the type of fault in the FAULT_ID field.

   If the fault is a CPU/MEM fault, use the MCTL_DIAG_REG_P and MCTL_DIAG_REG_M diagnostics to define the problem as a CPU or memory problem. They are also used to define the point of detection.

   If the problem occurs in a bus, the MEM fault or system fault address register contains the address being accessed and the data size.

   If a DMA problem occurs, access the DMA fields and look for address and error bits being set.

Example 2–7 shows the deassignment error log entry noting the deassignment of the processor module.

Example 2–7 Deassignment

```
******************************* ENTRY   38616. *******************************
ERROR SEQUENCE 1836.                            LOGGED ON:        SID 14000006
DATE/TIME  1-APR-1992 16:07:50.37                           SYS_TYPE 07200001
SYSTEM UPTIME: 0 DAYS 04:53:00
SCS NODE: FTCSSE                                              VAX/VMS V5.4-3

$SNDERR MESSAGE  KA550-AA  CPU FW REV# 6.  CONSOLE FW REV# 2.0

MESSAGE TEXT

  %FTSS-E-MODULEBROKEN, CPU Module in Slot 03 has been removed from service.
********************************************************************************
```

Example 2–8 includes some sample opcom messages you might see on your console terminal. They are from fault-tolerant system services and they explain what is happening. These two opcom messages will be printed out as a result of the deassignment of a CPU module because of CVAX I/O errors.

Example 2–8 Opcom Messages

```
%%%%%%%%%%%  OPCOM   4-MAY-1990 10:25:28.11  %%%%%%%%%%%
Message from user FTSS$CORE on FT3000
FTSS-I-FAULTID Fault ID: CVAX IO  has been detected.

%%%%%%%%%%%  OPCOM   4-MAY-1990 10:25:28.12  %%%%%%%%%%%
Message from user FTSS$CORE on FT3000
FTSS-I-MODULEBROKEN CPU Module in Slot 03 has been marked BROKEN.
```

2.4 Errors Detected at the WAN Module

This section describes how to interpret WAN module errors. An error is logged whenever a fatal error occurs on an SM device.

Figure 2–2 illustrates the VMS error log buffer format. Table 2–1 describes the VMS error log buffer format. Use Table 2–2 and Table 2–3 to interpret the error codes and subcodes. Section 2.4.1 is a sample WAN module error log.

Figure 2–2 VMS Error Log Buffer Format

<table>
<tr><td colspan="2">ERROR CODE</td><td colspan="2">SUB CODE</td></tr>
<tr><td colspan="2">ERROR CODE</td><td colspan="2">SUB CODE</td></tr>
<tr><td colspan="4">CSL</td></tr>
<tr><td colspan="4">XUB</td></tr>
<tr><td>DSTATE</td><td>STANDBY</td><td>ACTIVE</td><td>CONFIG</td></tr>
<tr><td>CABLE</td><td>XCB_FLAGS</td><td colspan="2">XUB_FLAGS</td></tr>
<tr><td colspan="4">ADAPTOR_REF</td></tr>
<tr><td colspan="2">ROLLOVER_COUNT</td><td colspan="2">FAILOVER_COUNT</td></tr>
<tr><td colspan="4">TX_CUR</td></tr>
<tr><td colspan="4">NOT USED</td></tr>
<tr><td colspan="2">FW_KERNEL</td><td colspan="2">FW_REVISION</td></tr>
<tr><td colspan="2">FW_TRANSMIT</td><td colspan="2">FW_RECEIVE</td></tr>
</table>

MR−0397−91PIC

Table 2–1 VMS Error Log Buffer Format

Field	Size	Description
FAILURE_REASON	Longword[1]	Used for failover reasons. See Table 2–2 and Table 2–3.
ROLLOVER_ REASON	Longword[1]	Used for rollover reasons. See Table 2–2 and Table 2–3.
CSL	Longword unsigned	Bit definitions for the CSL are: <2> - DSF$X_CSL_ADAPTER_ READY <3> - DSF$X_CSL_ED_0 <4> - DSF$X_CSL_ED_1 <5> - DSF$X_CSL_SIMPLEX <6> - DSF$X_CSL_STANDBY_0 <7> - DSF$X_CSL_STANDBY_1 <8> - DSF$X_CSL_Y_5V_SHORTED <11> - DSF$X_CSL_WHICH_ BOARD <31> - DSF$X_CSL_LOCK
XUB	Longword	XUB address.
CONFIG_STATE	Byte	Codes for CONFIG_STATE are: 0 - Null 1 - Single 2 - Partnered 3 - Partnered same zone 4 - Invalid
ACTIVE_STATE	Byte	Codes for ACTIVE_STATE are: 1 - Standby 2 - Active 3 - Failed 4 - Suspect

[1]The FAILURE_REASON and ROLLOVER_REASON fields are made up of two word fields: a high word and a low word. The high word defines the error code (type) and the low word defines the subcode (place). Together they identify the point where the failure was detected in SFDRIVER.EXE.

Table 2–1 (Continued) VMS Error Log Buffer Format

Field	Size	Description
STANDBY_STATE	Byte	Codes for STANDBY_STATE are: 1 - Standby 2 - Active 3 - Failed 4 - Suspect
DSTATE	Byte	Controller state codes are: 1 - Init 2 - Load 3 - Ignore 4 - Wait 5 - Run 6 - Dumping 7 - Load_failed 8 - Failed
XUB_FLAGS	Word	Datalink related flags are: <1> - DSF_DATALINK_HOLDOFF_SENT <2> - DSF_FLUSH_IN_PROGRESS <3> - DSF_LINE_IN_USE <4> - DSF_LOOPBACK <5> - DSF_DRIVER_LOOPBACK <6> - DSF_DISABLE_PENDING <7> - DSF_RX_BUFFER_CHANGE <8> - DSF_TX_POSSIBLE <9> - DSF_RX_POSSIBLE <10> - DSF_FW_RELOAD <11> - DSF_BAD <12> - DSF_X21_MODE

Table 2–1 (Continued) VMS Error Log Buffer Format

Field	Size	Description
XCB_FLAGS	Byte	Controller state flags are: <1> - Init <2> - Load <3> - Ignore <4> - Wait <5> - Run <6> - Dumping <7> - Load_failed <8> - Failed
CABLE	Byte	Personality cable type codes: 0 - NO_CABLE 1 - CABLE_V35 2 - CABLE_V24 3 - CABLE_X21 4 - CABLE_RS422 5 - TOTAL_LOOPBACK
ADAPTER_REF	Longword	Sync to DSF. Monitors the number of commands done.
FAILOVER_COUNT	Word	Number of failovers on this controller.
ROLLOVER_COUNT	Word	Number of rollovers on this controller.
TX_CUR	Longword	Transmits current at time error was logged.
ERRORLOG_CODE	Longword	Not used.
FW_REVISION	Word	Firmware revision.
FW_KERNEL	Word	Firmware kernel revision.
FW_RECEIVE	Word	Firmware receive revision.
FW_TRANSMIT	Word	Firmware transmit revision.

Table 2–1 (Continued) VMS Error Log Buffer Format

Field	Size	Description
SUCCESS	Longword	Number of successful DSF commands.
BADCMD	Longword	Number of commands returned with BADCMD status.
BAD	Longword	Number of commands returned with BADP1, BADP2, BADP3, or BADP4 status.
BAD_REF	Longword	Number of commands returned with a bad reference count.
NOCMD	Longword	Number of times there has been no space to insert a command in a command ring.
BUFFOVRFLW	Longword	Number of commands returned with buffer overflow status.
DATACRC	Longword	Number of commands returned with RX data CRC status.
HDRCRC	Longword	Number of commands returned with RX header CRC status.
MDMERR	Longword	Number of commands returned with modem error status.
PARITY	Longword	Number of commands returned with RX parity error status.
RX_ABORT	Longword	Number of commands returned with RX abort status.
RX_OVERRUN	Longword	Number of commands returned with RX overrun status.
RESPONSE_MIA	Longword	Not used.
MISC	Longword	Miscellaneous errors.
YSHORT	Longword	Number of commands returned with Y connector 5 V short status.
DMA_FAIL	Longword	Number of DMA failures.
INACCESS	Longword	Not used.

Table 2–1 (Continued) VMS Error Log Buffer Format

Field	Size	Description
TIMEOUT	Longword	Not used.
TX_UNDERRUN	Longword	Number of transmits returned with TX underrun status.
TX_CRC	Longword	Not used.
UNEXPECTED	Longword	Number of unexpected events that have occurred.
NO_RESP	Longword	Number of times there has been no response slot available.
NO_BUFF	Longword	Number of times no RX buffer slots have been available.
FATAL_HW	Longword	Number of commands returned with fatal hardware status.
FATAL_FW	Longword	Number of commands returned with fatal firmware status.

Table 2–2 WAN Module Error Codes

Error Name	Code	Description
NO_ERROR	01	
TRANSFER_TIMEOUT	02	Transfer timeout on load of firmware block.
SELFTEST_FAILURE	03	Firmware self-test failure.
SELFTEST_TIMEOUT	04	Firmware self-test timeout.
DEVICE_INIT_FAIL	05	Unable to initialize firmware after soft load.
FW_INTERFACE_ERROR	06	Firmware interface error.
RESPONSE_ERROR	07	Firmware returned response with “odd” error.
DRIVER_ERROR	08	Driver interface error.
FIRMWARE_NOT_VALID	09	Firmware revision is below expected revision.

Table 2–2 (Continued) WAN Module Error Codes

Error Name	Code	Description
FW_DUMP_FAILURE	0A	Unable to dump firmware.
FAULT_BIT	0B	Adapter indicated firmware error.
SOFTLOAD_FAILURE	0C	Load failure notified by driver.
DEV_SOFTLOAD_FAILURE	0D	Load failure notified by device.
THRESHOLD_ERROR	0E	Count threshold exceeded.
LOCK_TIMEOUT	0F	Could not take out a lock.
ADAPTER_FAILED	10	WAN module considered “dead.”
FAILOVER	11	Not used.
ROLLOVER	12	Not used.
BOARD_DATACRC	13	Data CRC detected by board — threshold reached.
BUS_DATACHECK	14	Header CRC detected by board — threshold reached.
BOARD_HDRCRC	15	Fatal error due to board header CRC.
YCON_SHORT	16	Short on Y-box. Corresponds to YSHORT status returned by firmware.
STRUCTURE_HEADER	17	Bad structure header seen by driver.
STANDBY_ERROR	18	Standby error.
RXDATA_HEADER	19	Error in received data header.
RESPONSE_HEADER	1A	Invalid response header.
NO_RESPONSE	1B	No response returned by firmware.
NO_RX_RESPONSE	1C	No RX data buffer returned by firmware.
REFERROR	1D	Command reference number sequence error.

Table 2–2 (Continued) WAN Module Error Codes

Error Name	Code	Description
CTL_QUEUE_EMPTY	1E	Control command queue empty.
CIR_NOT_VALID	1F	ADP valid flag clear.
TX_INSERT_FAIL	20	Failed to insert a transmit on the appropriate ring.
CMD_INSERT_FAIL	21	Failed to insert a command on the appropriate ring.
NO_100_PIN	22	Rollover due to cable pull on active channel.
BAD_CMD_STATUS	23	Command block came back with bad status.
DRIVER_RELOAD	24	
FATAL_FW_ERR	25	WAN module returned fatal firmware error status in a response block.
FATAL_HW_ERR	26	WAN module returned fatal hardware error status in a response block.
RING_CHECK	27	Command/response ring corrupt (debug only).
ALREADY_FAILED	28	DSF$VERIFY_FAILSET detected a good board as the standby and a board without functional firmware as the active board. Failover occurred on the good board.

Table 2–3 WAN Module Error Subcodes

Error Name	Code	Description
UNKNOWN_CMD	00	Unknown CMD type processed.
UNKNOWN_ERR_CODE	01	Unknown error code returned by firmware.
UNKNOWN_CABLE_TYPE	02	Unknown cable type.
FW_REQUEST_TIMEOUT	03	Transfer timeout on firmware request.
SEQUENCE_ERROR	04	Softload or command block sequence error.
INVALID_CONTROLLER_ID	05	Invalid controller ID provided by device PPI.
CONTROLLER_IN_USE	06	Attempted to “create” same controller more than once.
BROKE_BIT	07	WAN module broke bit set.
RX_BUFFER_OVFL	08	Received buffer larger than supplied LPD buffer.
P1_GETSTS_RANGE	09	Undefined value returned in P1 field of GETSTS CMD.
FREE_QUEUE_EMPTY	0A	Free command queue empty.
DEALL_RX_LPDS_FAIL	0B	Unable to deallocate RX LPDs.
INVALID_DSTATE	0C	Invalid XCB$B_DSTATE.
INVALID_PORT_STATE	0D	Invalid XUB$B_DSF_PORT_STATE (UP).
RESPONSE_BUFFER_ERROR	0E	Response not within host CMD buffer.
INVALID_STATE	0F	Invalid state, impossible action.
SANITY_TIMER_TICK	10	Sanity timer ticked without board activity.
NO_STATE_TIMER	11	Unable to start a board sanity timer.
TX_LPD_FAIL	12	No matching LPD for a completed transmit.
LNKSTR_LPD_FAIL	13	No startup link LPD present.

Table 2–3 (Continued) WAN Module Error Subcodes

Error Name	Code	Description
FLUSH_ERROR	14	Flushing failed.
LOOPBACK_FAIL	15	Unable to set up requested loopback mode.
INV_LOOP_MODE	16	Invalid loopback mode.
INV_UNIT_STATE	17	Invalid unit state.
FWTIMER_ACTIVE	18	Firmware request timer already active.
FWTIMER_NOSPACE	19	Unable to allocate firmware request timer.
LPTIMER_ACTIVE	1A	Loopback timer already active.
LPTIMER_NOSPACE	1B	Unable to allocate loopback timer.
FSTIMER_NOSPACE	1C	Unable to allocate failset watchdog timer.
TIMER_STOPPED	1D	Timer already stopped.
NONEXISTANT_TIMER	1E	Timer does not exist.
RX_BUFFER_FAIL	1F	Unable to allocate receive buffers.
CHANNEL_ERROR	20	Invalid channel number in CMD block.
MANUAL_FAILOVER	21	Software initiated failover.
MANUAL_ROLLOVER	22	Software initiated rollover.
FSM_SET_CUR	23	FSM set current command.
FAILED_HOST	24	Host machine “dead.” Clear valid flag.
NO_ACTIVE_XCB	25	Could not find an active XCB on a device unit create.
SINGLE_BADREF	26	Bad reference count.
UNEXP_CMD	27	Unsolicited command returned.
NO_CONSOLE_SYNC	28	Could not get in sync with WAN module.
BAD_DSRT	29	Did not get correct header for DSRT from firmware.

Table 2–3 (Continued) WAN Module Error Subcodes

Error Name	Code	Description
INIT_CHANNEL	2A	Failure occurred in DSF$$INIT_CHANNEL.
ABORT_CHANNEL	2B	Failure occurred in DSF$$ABORT_CHANNEL.
ABORT_QUEUE	2C	Failure occurred in DSF$$ABORT_QUEUE.
ABORT_TRANSMIT	2D	Failure occurred in DSF$$ABORT_TRANSMIT.
ADAPTER_STATUS	2E	Failure occurred in DSF$$ADAPTER_STATUS.
QUEUE_MODEM	2F	Failure occurred in DSF$$QUEUE_MODEM.
REPORT_MODEM_ENABLE	30	Failure occurred in DSF$$REPORT_MODEM_ENABLE.
QUEUE_TRANSMIT	31	Failure occurred in DSF$QUEUE_TRANSMIT (first place).
QUEUE_TRANSMIT1	32	Failure occurred in DSF$QUEUE_TRANSMIT (second place).
QUEUE_TRANSMIT2	33	Failure occurred in DSF$QUEUE_TRANSMIT (third place).
QUEUE_TRANSMIT3	34	Failure occurred in DSF$QUEUE_TRANSMIT (fourth place).
QUEUE_TRANSMIT4	35	Failure occurred in DSF$QUEUE_TRANSMIT (fifth place).
TRANSMIT_COMPLETION	36	Failure occurred in DSF$TRANSMIT_COMPLETION.
RECEIVE_COMPLETION_NODATA	37	Failure occurred in DSF$RECEIVE_COMPLETION_NODATA.

Table 2–3 (Continued) WAN Module Error Subcodes

Error Name	Code	Description
RECEIVE_COMPLETION	38	Failure occurred in DSF$RECEIVE_COMPLETION.
FORK_PROCESSING	39	Failure occurred in DSF$FORK_PROCESSING (first place).
FORK_PROCESSING2	3A	Failure occurred in DSF$FORK_PROCESSING (second place).
COMMAND_COMPLETION	3B	Failure occurred in DSF$COMMAND_COMPLETION.
INIT_COMPLETION	3C	Failure occurred in DSF$INIT_COMPLETION.
START_UNIT	3D	Failure occurred in DSF$START_UNIT.
STATE_TIMEOUT	3E	Failure occurred in DSF$STATE_TIMEOUT.
TRANSMIT_NOW	3F	Failure occurred in DSF$TRANSMIT_NOW (macro).
EMPTY_TX_PENDINGQ	40	Failure occurred in DSF$EMPTY_TX_PENDINGQ (macro).
EMPTY_TX_PENDINGQ2	41	Failure occurred in DSF$EMPTY_TX_PENDINGQ2 (macro).
TX_CMD_AVAILABLE	42	Failure occurred in DSF$TX_CMD_AVAILABLE (macro).
CMD_AVAILABLE	43	Failure occurred in DSF$CMD_AVAILABLE (macro).
RAISE_ABORT	44	Failure occurred in DSF$RAISE_ABORT (macro).
RUTHERE	45	Board did not respond to “are you there” poll.
RESPONSE_MIA	46	Used only when thresholding enabled.

Table 2–3 (Continued) WAN Module Error Subcodes

Error Name	Code	Description
INACCESS	47	Used only when thresholding enabled.
BADREF	48	Used only when thresholding enabled.
MISC	49	Used only when thresholding enabled.
NOCMD	4A	Used only when thresholding enabled.
OUTOFSEQ	4B	Used only when thresholding enabled.
NO_BUFFER	4C	Used only when thresholding enabled.
BUFFOVRFLW	4D	Used only when thresholding enabled.
TX_CRC	4E	Used only when thresholding enabled.
BADPARAM	4F	Used only when thresholding enabled.
DMA_FAIL	50	Used only when thresholding enabled.
NO_FREE_CMD	51	Used only when thresholding enabled.
TIMEOUT	52	Used only when thresholding enabled.
RX_SHORT	53	Used only when thresholding enabled.
NO_XCB	54	Not used in error logs.
DOWNLOAD_FAILURE	55	Not used in error logs.
UNEXPECTED	56	Used only when thresholding enabled.
CABLE_INFO_ERROR	57	Driver found inconsistent cable information. Not yet used.

Table 2–3 (Continued) WAN Module Error Subcodes

Error Name	Code	Description
SLOT_NOT_FREE	58	Status returned by DSF$INSERT_COMMAND. Not used in error log.
ADP_INVALID	59	Not used.
STRUCTURE_HEADER_ CORRUPT	5A	Not used.
INSFCMD_ENTRIES	5B	Not used.
RING_ERROR0	5C	Ring corruption detected (debug only).
RING_ERROR1	5D	Ring corruption detected (debug only).
RING_ERROR2	5E	Ring corruption detected (debug only).
RING_ERROR3	5F	Ring corruption detected (debug only).
FAILSET_ADD1	60	Failure occurred in DSF$FAILSET_ADD
FAILSET_ADD2	61	Failure occurred in DSF$FAILSET_ADD2.
VERIFY_FAILSET	62	Failure occurred in DSF$VERIFY_FAILSET.

2.4.1 Sample WAN Module Error Log

```
VAX/VMS SYSTEM ERROR REPORT  COMPILED 21-MAR-1991 19:19:33
                                                          PAGE 5.

******************************* ENTRY    3475. ********************
ERROR SEQUENCE 104.                       LOGGED ON:  SID 0A000005
DATE/TIME 21-MAR-1991 19:16:52.67         SYS_TYPE 07100001
SYSTEM UPTIME: 0 DAYS 00:51:29
SCS NODE: FTCSSE                           VAX/VMS V5.4-1A

DEVICE ATTENTION  KA520-AA  CPU FW REV# 6.  CONSOLE FW REV# 1.0
                  CPU ID # 0.

DSF32 SUB-SYSTEM, UNIT _FTCSSE$SMH0:

      ERROR CODE      001F003E   1F = CIR_NOT_VALID
                                 3E = STATE_TIMEOUT
      ERR SUBCODE     00120023   12 = ROLLOVER

      CSL             00000000   23 = FSM_SET_CUR
      CSR1            808C6660
      CSR2            08030202
      CSR3            02180304
      SYNC_TO_DSF     00000B40
      DSF_TO_SYNC     0011000B
      AT_DSF          00000002
      FAILURE CODE    00000000
      BOARD_P1        016B03D4
                                      CODE = D4(X)
                                      FW REVISION = 03(X)
                                      LINES = 6B(X)
                                      HW REVISION = 01(X)
      BOARD_P2        012A013F
                                      EXPECTED HW REV = 3F(X)
                                      ROM VERSION = 01(X)
                                      DLL EXPECTED HW REV = 2A(X)
                                      DLL FW REVISION = 01(X)
      SUCCESS         00001B0A
      BADCMD          00000000
      BADP            00000000
      BAD_REF         00000000
      NOCMD           00000000
      BUFFOVRFLW      00000000
      DATACRC         00000000
      HDRCRC          00000000
      MDMERR          00000000
      PARITY          00000000
      RX_ABORT        00000000
      RX_OVERRUN      00000000
      RESPONSE_MIA    00000000
      MISC            00000000
      YSHORT          00000000
      DMA_FAIL        00000000
      INACCESS        00000000
      TIMEOUT         00000000
      TX_UNDERRUN     00000000
      TX_CRC          00000000
      UNEXPECTED      00000000
      NO_RESP         00000000
      NO_BUFF         00000000
      FATAL_HW        00000000
      FATAL_FW        00000000
```

```
VAX/VMS SYSTEM ERROR REPORT  COMPILED 21-MAR-1991 19:19:33
                                                      PAGE 6.

      UCB$B_ERTCNT          10
                                        16. RETRIES REMAINING
      UCB$B_ERTMAX          00
                                        0. RETRIES ALLOWABLE
      ORB$L_OWNER     00000000
                                        OWNER UIC [000,000]
      UCB$L_CHAR      0C442000
                                        NETWORK
                                        AVAILABLE
                                        ERROR LOGGING
                                        CAPABLE OF INPUT
                                        CAPABLE OF OUTPUT
      UCB$W_STS           0000
      UCB$L_OPCNT     00000000
                                        0. QIO'S THIS UNIT
      UCB$W_ERRCNT        000C
                                        12. ERRORS THIS UNIT
      IRP$W_BCNT          0000
                                        TRANSFER SIZE 0. BYTE(S)
      IRP$W_BOFF          0000
                                        TRANSFER PAGE ALIGNED
      IRP$L_PID       00000000
                                        REQUESTOR "PID"
      IRP$Q_IOSB      00000000
                      00000000          IOSB, 0. BYTE(S) TRANSFERRED
      IRP$W_FUNC      590A0000
      UCB$B_ERTCNT          10
                                        16. RETRIES REMAINING
      UCB$B_ERTMAX          00
                                        0. RETRIES ALLOWABLE
      ORB$L_OWNER     00000000
                                        OWNER UIC [000,000]
      UCB$L_CHAR      0C442000
                                        NETWORK
                                        AVAILABLE
                                        ERROR LOGGING
                                        CAPABLE OF INPUT
                                        CAPABLE OF OUTPUT
      UCB$W_STS           0000
      UCB$L_OPCNT     00000000
                                        0. QIO'S THIS UNIT
      UCB$W_ERRCNT        000C
                                        12. ERRORS THIS UNIT
      IRP$W_BCNT          0000
                                        TRANSFER SIZE 0. BYTE(S)
      IRP$W_BOFF          0000
                                        TRANSFER PAGE ALIGNED
      IRP$L_PID       00000000
                                        REQUESTOR "PID"
      IRP$Q_IOSB      00000000
                      00000000          IOSB, 0. BYTE(S) TRANSFERRED
      IRP$W_FUNC      590A0000
```

3 Troubleshooting

This chapter describes the maintenance strategy and troubleshooting procedures for the VAXft system.

NOTE

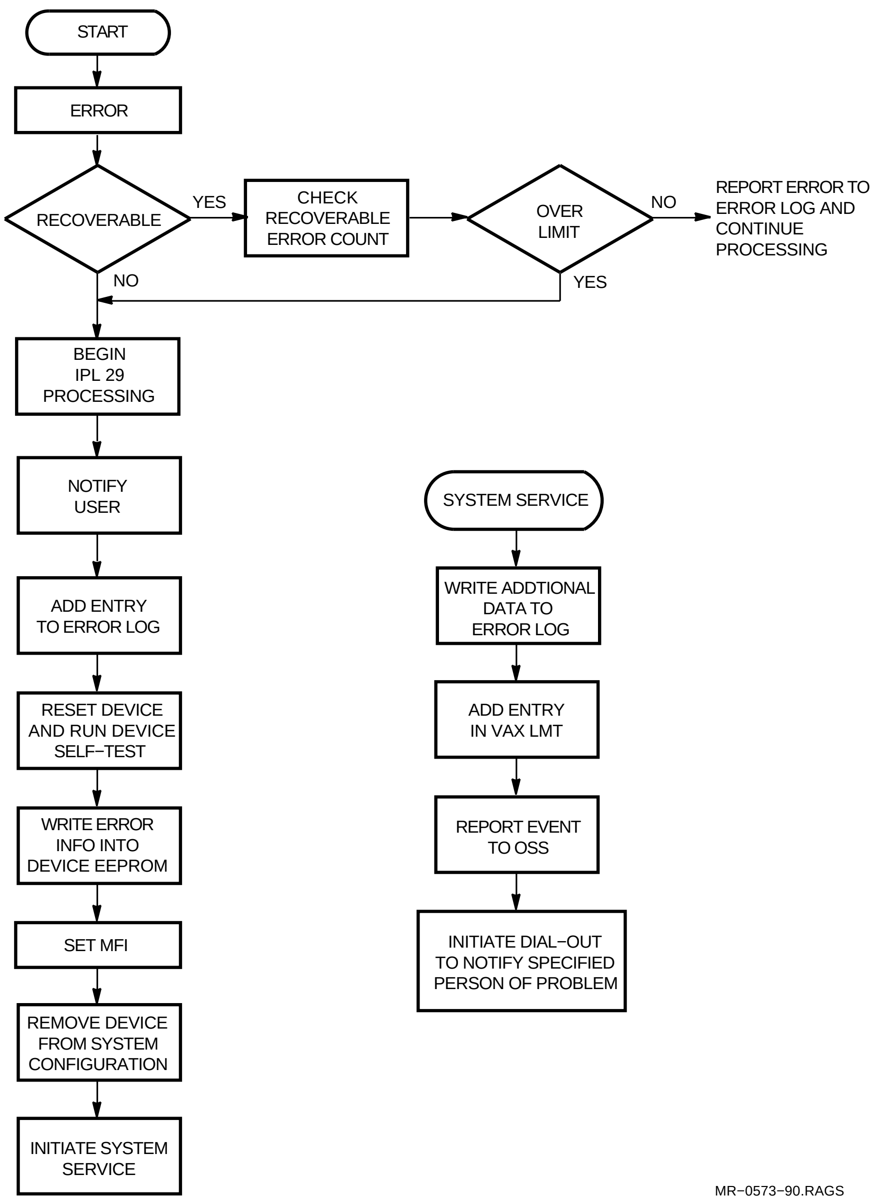
Throughout this chapter, the DSF32 module is referred to as the WAN module.

3.1 Maintenance Strategy

When a hardware component fails on a VAXft system, the system uses self-diagnostics to locate the failing FRU. If a solid fault occurs, the system automatically puts the suspect FRU off-line, reports the error, and identifies the suspect FRU to the console terminal. The strategy for a transient error is to log the error and then recover. A magnetic fault indicator (MFI) is set on the suspect FRU to make identification easy, and a red Fault LED blinks on the system or expander cabinet summary panel to identify the zone where the failure occurred.

If the VAXft system is under a Digital service contract, it will dial out to the remote diagnostic center using SICL/SDD. (A Customer Services engineer must install SICL/SDD since it is not shipped with the VAXft system.) Thus, in a dial-out situation the Customer Services engineer already knows the probable cause of failure and can bring the correct field replaceable unit (FRU) to the site. Figure 3–1 illustrates VAXft fault handling.

Figure 3–1 Fault Handling Flowchart



3.1.1 MFIs

Most FRUs in the VAXft system have a MFI to “flag” a failure within the FRU. An MFI is an electromagnetic switch. The normal state of an MFI is dark (reset). When the MFI is yellow (set), it indicates a failure within the device.

All MFIs are visible from the front of the VAXft cabinet when the front doors are open. The state of the MFI is visible with or without power applied to the device. Figures 3–2 through 3–7 show the locations of the switches and MFIs in the VAXft cabinets.

Figure 3–2 Model 110 MFI Locations

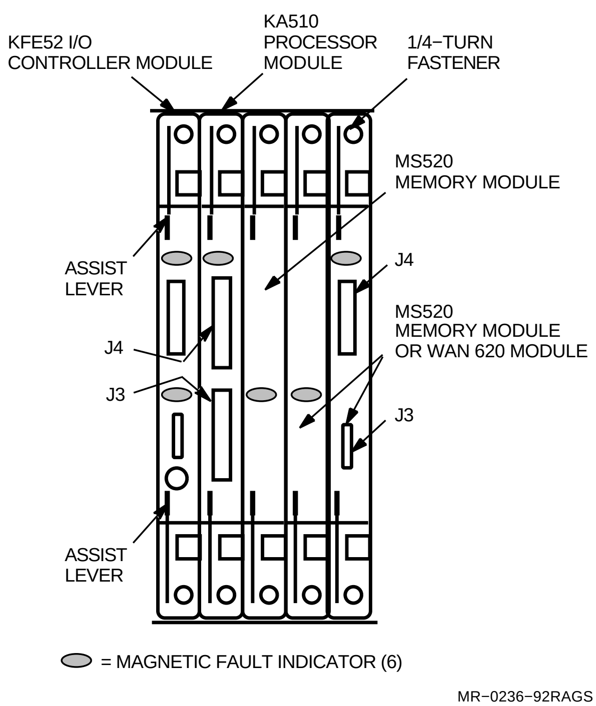


Figure 3–3 Model 310 and 410 System Cabinet MFI Locations

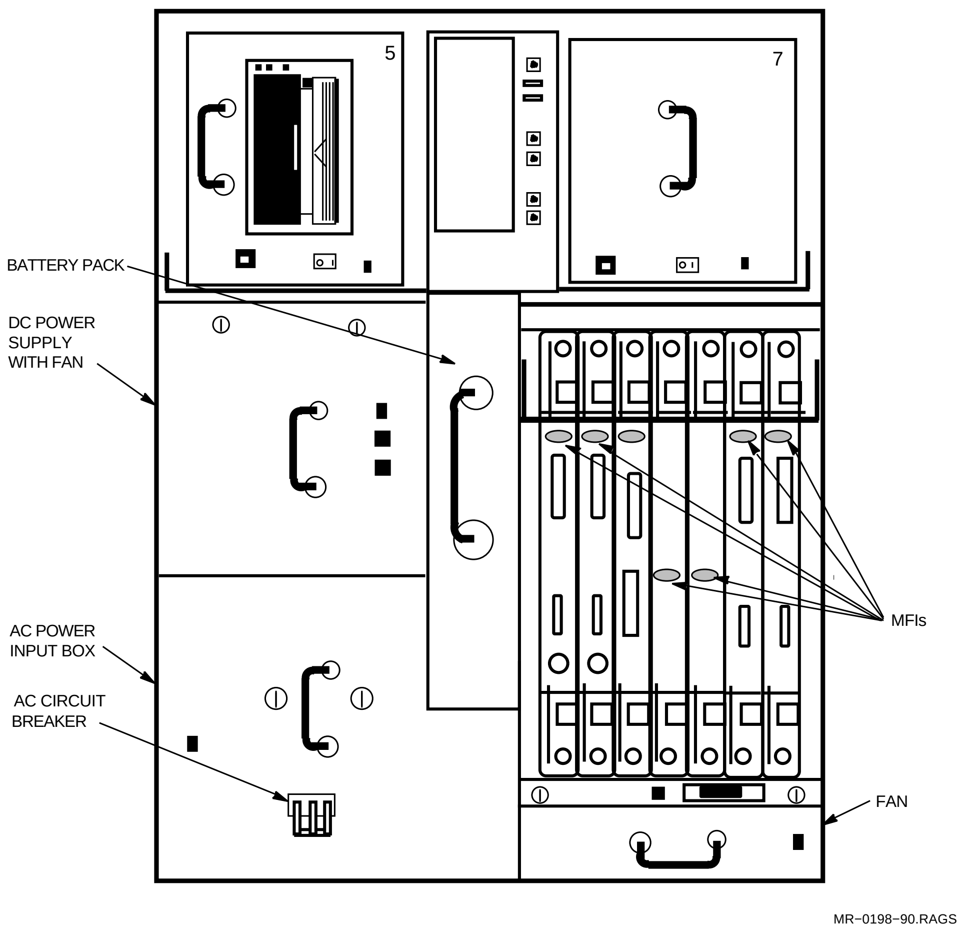


Figure 3–4 Model 310 and 410 Expander Cabinet MFI Locations

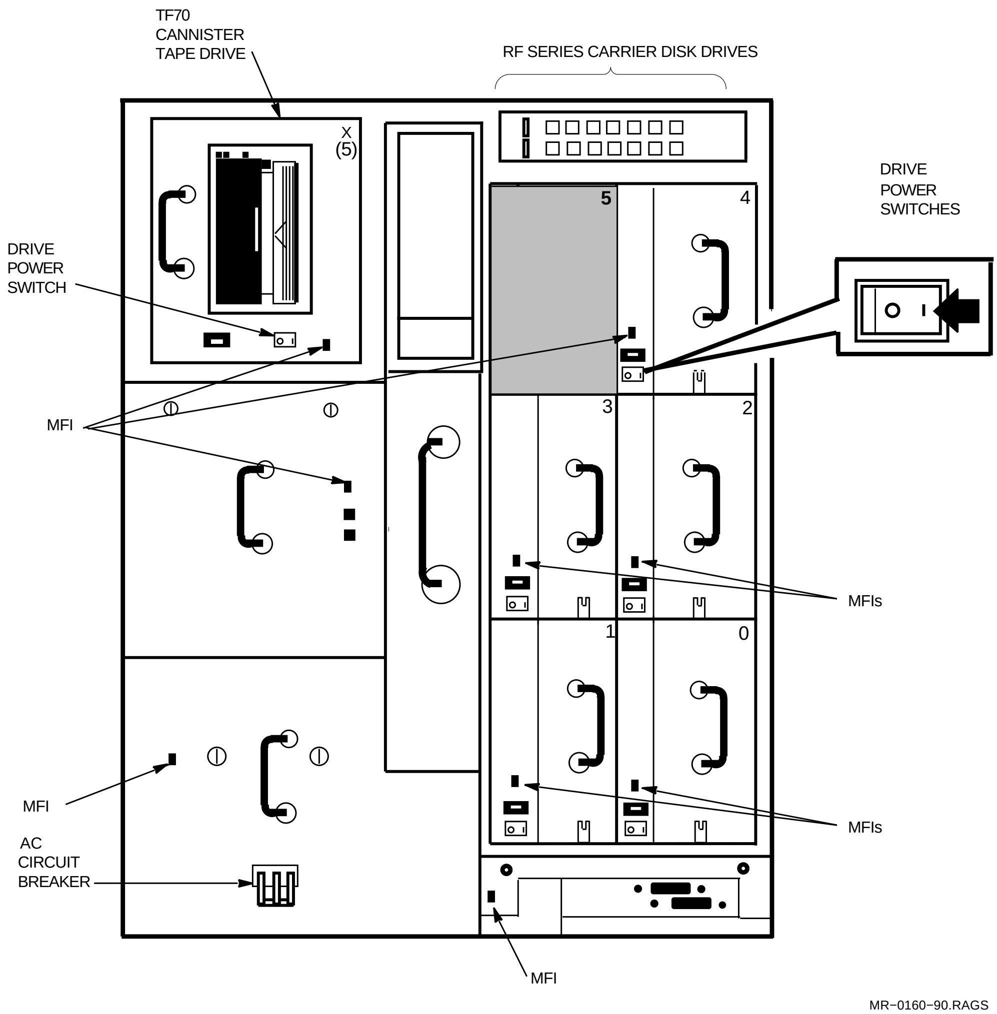


Figure 3–5 Model 610 and 612 System Cabinet Switches and MFIs

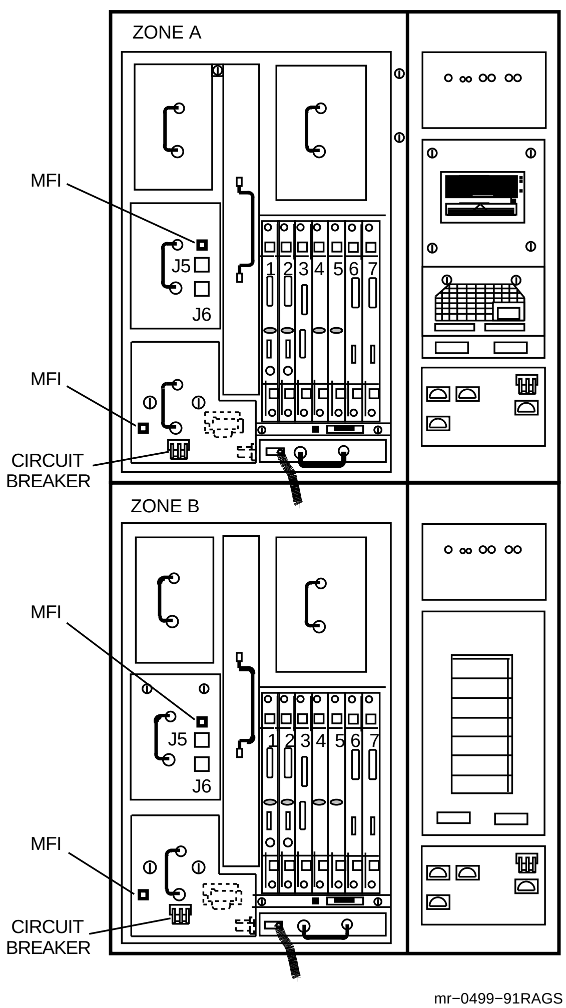


Figure 3–6 Model 610 and 612 Logic Module LED Indicators and MFIs

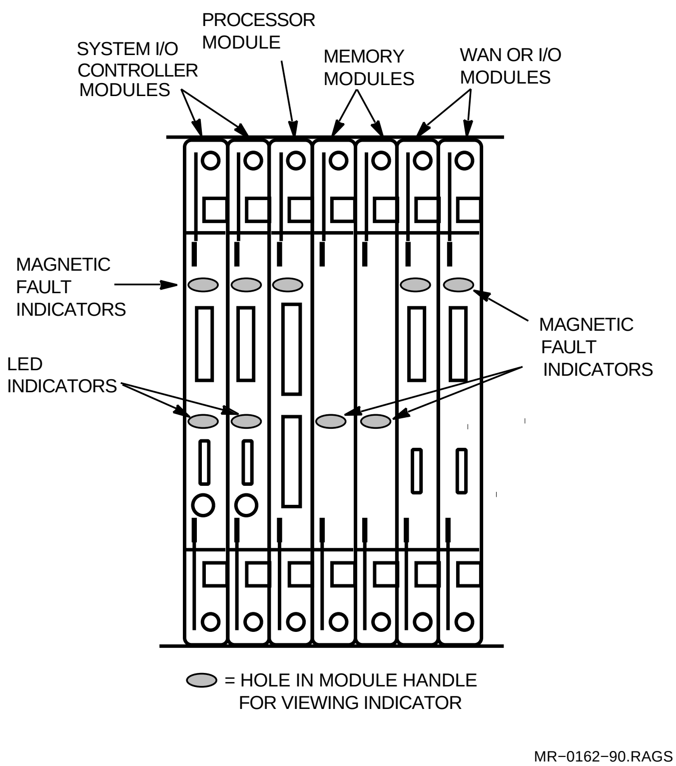
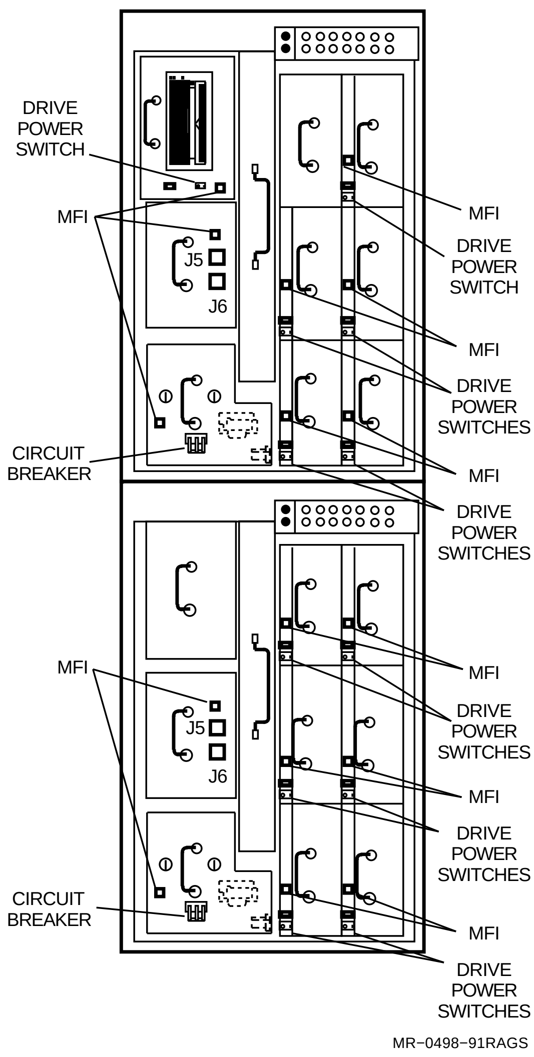


Figure 3–7 Model 610 and 612 Expander Cabinet Switches and MFIs



3.1.2 Repair Procedure

In most cases, the system automatically isolates the failure and determines the cause. When a call is logged with Customer Services, problem information (including the suspect FRU) is provided. The information may come from the customer or directly from the system, depending on the notification arrangement for the customer.

Use the following procedure to locate the failing FRU and repair the problem. While the repair is being performed, the customer application continues to run.

1. Locate the zone where the failure occurred by checking the red Fault indicators on the summary panels. When an indicator is blinking, a fault is present in the zone.
2. Open the cabinet door(s) and look for an MFI that is yellow (set). This identifies the faulty FRU.
3. If no MFIs are set, you must interpret the system error log using one of the following tools:
   - VAXsimPLUS
   - SPEAR
   - ERF
4. Replace the suspect FRU.
5. Verify the repair by checking the results of the power-on test.
6. If you performed a cold swap procedure, ask the operator or system manager to start up the zone.

3.1.3 How to Clear a Module Broke Bit

You should clear the broke bit in the module EEPROM **only** when the module has been set inadvertently to the broke state. This may occur due to incorrect use of the diagnostics. Never clear the broke bit when an actual fault condition is present.

A specific sequence of commands must be used to clear the broke bit. The command sequences are notably different, depending on which module is affected. See Examples 3–1 through 3–4 for details. Use extreme care when entering the commands.

The following steps summarize how to clear the broke bit in EEPROM.

1. Use the STOP/ZONE command to shut down the the affected zone.
2. If necessary, use the Z command to move to the affected module. (The *VAXft Systems Owner's Manual* contains information on the Z command.)
3. Use the SHOW MAN command to display manufacturing data. Record this information.
   - The CPU module requires that you issue the escape sequence of Ctrl/[<x and immediately type the SHOW MAN command.
   - The CIO module requires that you enter DEV mode by issuing the Ctrl/[<x DEV command. You then enter the SHOW MAN command. Note the differences between the primary CIO and secondary CIO escape sequences.
   - The WAN module requires that you use the Z command (see step 2) and issue the SHOW MAN command.
4. Clear the broke bit, restore the manufacturing data, and update the EEPROM:
   - For the CPU module, issue the escape sequence of Ctrl/[<x DEV and immediately type the SET MAN command. Then enter the manufacturing data that you have recorded and update the EEPROM.
   - For the CIO module, enter DEV mode by issuing the Ctrl/[<x DEV command. Then issue the SET MAN command and update the EEPROM. Note the differences between the primary and secondary escape sequences.
   - For the WAN module, use the Z command (see step 2) and issue the SET FACTORY command. Note that this command is required **only** for the WAN module. **Never** use it for the CIO or CPU modules. Once you issue the SET FACTORY command, issue the SET MAN command to restore the manufacturing information.
5. If the Z command was used in step 2 above, use Ctrl/P to return to the primary CIO module.
6. Initialize the zone. Note that under certain circumstances, the broke bit still may be set. If so, power cycle the zone after completing steps 1 through 5.

Example 3–1 shows how to clear the broke bit in the CPU module.

Example 3–1 How to Clear the CPU Broke Bit

```
>>> [Ctrl/[] [<x] SHOW MAN      ! Record the manufacturing data.
>>> [Ctrl/[] [<x] SET MAN       ! This clears the broke bit.
                                ! Restore the data from SHOW MAN.
>>> INIT                        ! Initialize the zone.
```

Example 3–2 shows how to clear the broke bit in the primary CIO module. The Z command is not required to access the primary CIO module.

Example 3–2 How to Clear the Primary CIO Broke Bit

```
>>> MIO                         ! Enter MIO mode.
MIO> [Ctrl/[] [<x] DEV          ! Enter DEV mode.
DEV> SHOW MAN                   ! Record the manufacturing data.
DEV> SET MAN                    ! This clears the broke bit.
                                ! Restore the data from SHOW MAN.
DEV> CIO                        ! Return to CIO mode.
>>> INIT                        ! Initialize the zone.
```

Example 3–3 shows how to clear the broke bit in the secondary CIO module in zone A. The Z command is required. Notice also that the command syntax to enter DEV mode is different.

Example 3–3 How to Clear the Secondary CIO Broke Bit in Zone A

```
>>> Z 2                         ! "Z" to the secondary CIO module.
>>> MIO                         ! Enter MIO mode.
MIO> [Ctrl/[] [Ctrl/[] [<x] DEV ! Note: Press [Ctrl/[] twice!
DEV> SHOW MAN                   ! Record the manufacturing data.
DEV> SET MAN                    ! This clears the broke bit.
                                ! Restore the data from SHOW MAN.
DEV> INIT                       ! Initialize the module.
     [Return]                   ! Wait 10 seconds. Press [Return].
MIO> [Crtl/P]                   ! Return to the primary CIO module.
>>> INIT                        ! Initialize the zone.
```

Example 3–4 shows how to clear the broke bit in a WAN module located in slot 7 of zone A.

Example 3–4 How to Clear the WAN Broke Bit in Zone A

```
>>> Z 3                      ! "Z" to the WAN module.
DSF_03> SHOW MAN             ! Record the manufacturing data.
DSF_03> SET FACTORY          ! This clears the broke bit. Enter Y
                             ! to update EEPROM with factory defaults.
DSF_03> SET MAN              ! Restore the data from SHOW MAN
                             ! and update EEPROM.
DSF_03> Ctrl/P               ! Return to CIO mode.
>>>INIT                      ! Initialize the zone.
```

3.2 Troubleshooting Overview

The VAXft system design simplifies diagnosis and parts replacement. When an FRU fails the MFI located on that FRU is tripped, identifying it as the failed module. FTSS makes a special error log entry when a module is marked broken. This is how the MFI “flags” the problem FRU.

First, you should examine the error log for data supporting the diagnosis of the failed FRU. As a second verification, diagnostics can be invoked from the console. Refer to Chapter 1 for a complete description of the on-board diagnostics. Keep in mind that if diagnostics are run, you must shut down the zone they are to run in. This is because the VMS operating system and the diagnostics cannot run concurrently. Specific tests are available for self-test, zone test, and system test.

If the problem persists, further analysis of the error log is required. Refer to Chapter 2 for this information. As with any VAX computer, standard crash dump analysis is also a viable approach to troubleshooting the VAXft system. This tool, though, is likely to require a skill level beyond that of an SDU engineer.

Physical problems must never be overlooked. Be sure to examine cabling for the correct paths, especially the DSSI cables. If a logic module was replaced, it is possible that the DSSI cables were reconnected improperly. Also, even though the CPU cables cannot be connected incorrectly, they might not be seated correctly. Always check the module seating and cable connection seating.

Ethernet cables must also be connected properly. Incorrect connections can cause DECnet circuit or system errors.

Console messages should always be analyzed. For the message “PWA0 going off line, attempting reconnection of a virtual circuit,” you should understand that PWA0 represents the DSSI port in the primary slot of zone A. Investigate why this is happening. Perhaps a drive just went off line. Maybe there is a loose cable. Maybe there was a loss of power to the zone, or the zone may have left the configuration.

Keep in mind that the VAXft system design includes hardware redundancy and that what appears in the left half of the system should always appear in the right half of the system, except for disks.

In expanded systems, disks are connected to zone A and zone B, which extends the left-right symmetry.

When you debug boot problems, you should check boot paths. If zone A does not boot the system disk, there is an alternate path from zone B. If the problem persists on either path, it is possible that a fatal disk problem exists. Use the RF-series disk diagnostics via DUP from the console to further isolate the problem. If you succeed in booting from the alternate path, then all indications point to the primary KFE52 I/O module in zone A.

Disks on VAXft systems should be treated as other DSSI devices. A good resource document for these devices is the *RF31/72 Integrated Storage Element User’s Guide* (EK-RF72D-UG).

Your overall approach is to segment the system by zone and then pursue the problem logically from point to point, starting with MFIs, using error log data, console output, and crash dump analysis where appropriate.

3.3 WAN Module Diagnostics

This section describes how to use the following WAN module diagnostics for fault isolation:

- WAN self-test
- WAN extended self-tests:

  WAN module test
  Y-box and 100-pin cable test
  Personality/adapter and extension cable test

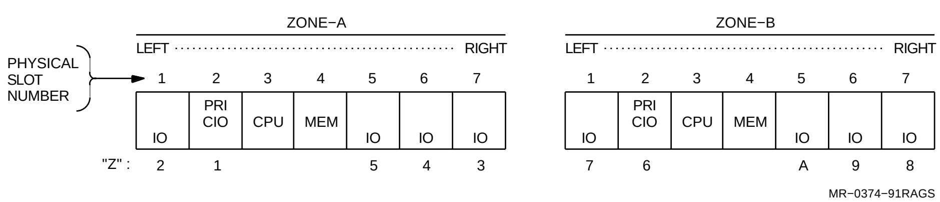
Figure 3–8 shows the physical slot numbers used with the WAN and RBD prompts. It also shows the Z command slot numbers used to select the module RBDs. Refer to Figure 1–2 and Figure 1–3 for additional information about using the Z command.

NOTE

The logical slot numbers for the model 110 are the same as in Figure 3–8 even though physical slots 1 and 7 are not present. If slot 1 or 7 is accessed, a not present message comes back.

The SHO CONFIG console command renumbers the slots to be 1 through 5.

Figure 3–8 Slot Numbers Used with the WAN and RBD Prompts and the Z Command



3.3.1 WAN Self-Test

A WAN self-test does not always use all the fields in the error report. XXXXXXXX indicates a field that is not meaningful. If the WAN self-test fails, replace the WAN module.

NOTE

The WAN self-test does not test the line drivers. Run the WAN extended self-test to test the WAN module completely.

The following sample shows how to run the WAN self-test. In the sample, the suspect WAN module is in physical slot 7 of zone A, a CPU module is in slot 3, and a CIO module is in slot 2.

Assumption: The zone containing the suspect WAN module (zone A) was shut down using the DCL command STOP/ZONE.

```
>>> Z 3            ! "Z" to the WAN module in slot 7 of zone A.
DSF_03>

DSF_03> T/R        ! Get to the WAN RBD monitor.
RBD3>

RBD3> ST 0/TR/HE   ! Run WAN self-test.

*If test passes:*

;selftest 1.00
;0..1..2..3..20
;21..22..23..37
;       P 00000003      DSF 00000001
;XXXXXXXX 00000000 00000000

*If test fails:*

;selftest 1.00
;0.1..2..3..20
;21..22..23..n(failing test number)
;       F 0000000N      DSF 00000001
;      HE Testname T00000## RBD00000
;ERRCODE  ERRNUMB  EXPDATA  RCVDATA  SCBOFF   ERRADDR  ERRORPC
;XXXXXXXX 00000001 00000000

RBD3> Quit         ! To return to DSF console.

DSF_03> ^P         ! To return to console.

>>>
```

3.3.2 WAN Extended Self-Tests

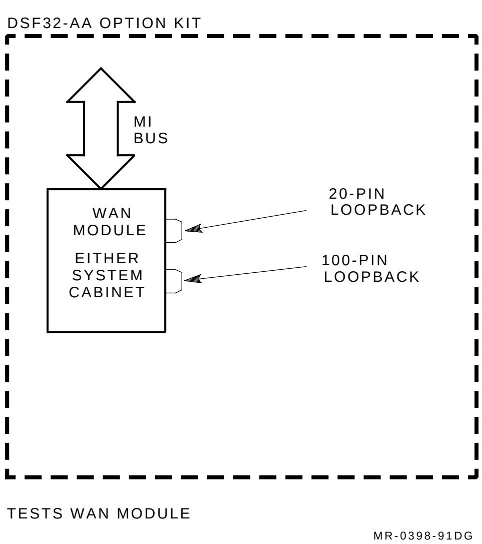
NOTE

Always power down the affected zone before you remove and replace the terminators and cables.

The WAN extended self-tests include three procedures:

1. Test the WAN module.
   a. Disconnect the 20-pin and 100-pin connectors from the suspect WAN module.
   b. Connect the 20-pin and 100-pin loopback connectors as shown in Figure 3–9.
   c. Test as a nonredundant configuration, starting with the suspect WAN module.

Figure 3–9 WAN Module Loopback Connectors



A WAN extended self-test does not always use all the fields in the error report. XXXXXXXX indicates a field that is not meaningful. If the WAN extended self-test fails (and the 20-pin and 100-pin loopbacks are known good), replace the WAN module.

The following sample shows the output of an extended WAN self-test during module testing. In the sample, ignore the CHAN = X REQUIRES LOOPBACK = H3199 messages. They are not meaningful in this configuration.

```
RBD3> ST 1/TR/HE    ! Run WAN extended self-test.
```

if test passes:

```
;extended 1.00
;0..1..2..

CHAN = 0 REQUIRES LOOPBACK=H3199
CHAN = 1 REQUIRES LOOPBACK=H3199
;3..4
;       P 00000003      DSF 00000001
;XXXXXXXX 00000000 00000000
RBD3>
```

if test fails:

```
;extended 1.00
;0..1..n
;       F 0000000N      DSF 00000001
;ERRCODE  ERRNUMB  EXPDATA  RCVDATA  SCBOFF   ERRADDR  ERRORPC
;XXXXXXXX 00000001 00000000
RBD3>
```

N = failing test number

2. Test the Y-box and 100-pin cable. See Figure 3–10.

NOTE

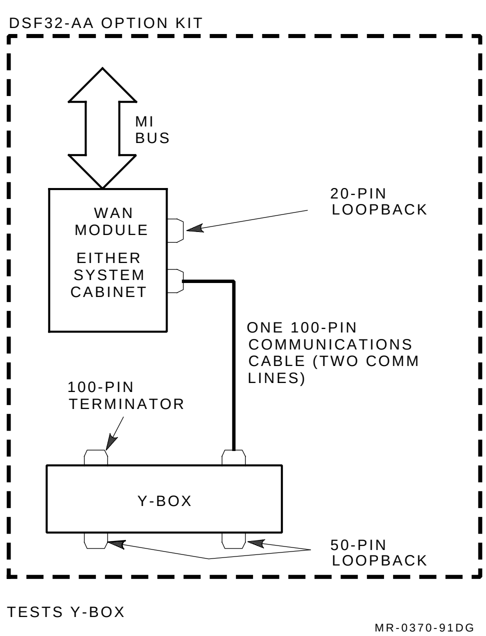
For a redundant configuration, you must test the two WAN modules that are connected to the Y-box separately. Test each as a nonredundant configuration. Start with the suspect WAN module.

a. Install the 100-pin cable, Y-box, and terminator.

b. Remove the personality/adapter cables.

c. Install two H3199 loopback connectors on the Y-box.

Figure 3–10 100-Pin Cable, Y-box, and Terminator



A WAN extended self-test does not always use all the fields in the error report. XXXXXXXX indicates a field that is not meaningful. If the WAN extended self-test fails (and the 50-pin loopbacks are known good), replace the 100-pin cable and/or the Y-box and/or the terminator.

The following sample shows the output of an extended WAN self-test during Y-box and 100-pin cable testing. In the sample (case 2), notice that an informational message is displayed when the diagnostic does not find one or both loopback connectors.

```
RBD3> ST 1/TR/HE    ! Run WAN extended self-test.
```

Case 1 - Two H3199 loopback connectors.

if test passes:

```
;extended 1.00
;0..1..2..
CHAN = 0 REQUIRES LOOPBACK=H3199
CHAN = 1 REQUIRES LOOPBACK=H3199
;3..4..
;       P 00000003      DSF 00000001
;XXXXXXXX 00000000 00000000
RBD3>
```

Case 2 - Channel 0: H3199, Channel 1: not terminated.

if test passes:

```
;extended 1.00
;0..1..2..

CHAN = 0 REQUIRES LOOPBACK=H3199
CHAN = 1 REQUIRES LOOPBACK=NONE
;3..4
;       P 00000003      DSF 00000001
;XXXXXXXX 00000000 00000000
RBD3>
```

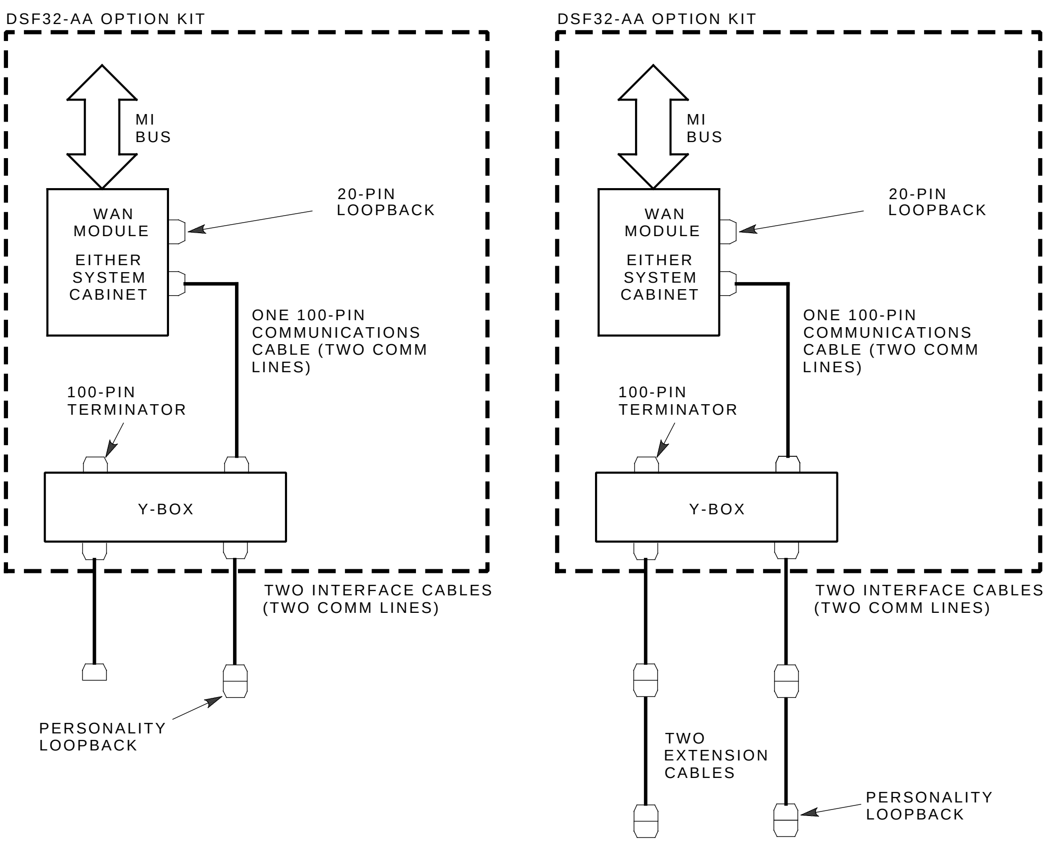
if test fails:

```
;extended 1.00
;0..1..n
;       F 0000000N      DSF 00000001
;ERRCODE  ERRNUMB  EXPDATA  RCVDATA  SCBOFF   ERRADDR  ERRORPC
;XXXXXXXX 00000001 00000000
RBD3>
```

N = failing test number

3. Test the personality/adapter and extension cables. See Figure 3–11.
   a. Install the personality/adapter and extension cables.
   b. Install a personality loopback connector at the end of each of the two personality/extension cables.
   c. Install an H3199 loopback connector on any port without a personality cable.

Figure 3–11 Personality Cables



If the WAN extended self-test fails, replace the personality/adapter or the extension cable for the failing port. If the WAN extended self-test finishes without a failure, check the customer's modem.

The following sample shows the output of an extended WAN self-test during personality/adapter and extension cable testing. In the sample, notice that test 1 asks for confirmation when it detects a cable plugged into either port. This prevents the destruction caused by running extended tests on a module that is connected through the Y-box to an active module.

```
RBD3> ST 1/TR/HE    ! Run WAN extended self-test.

Case - Channel 0: H3199, Channel 1: BC19D

*if test passes:*

;extended 1.00
;0..1..
CHAN 0, CABLE = H3199
CHAN 1, CABLE = BC19D/E
? 60 - CONFIRM [N]:

;2..3..4
;       P 00000001      DSF 00000001
;XXXXXXXX 00000000 00000000
RBD3>

*if test fails:*

;extended 1.00
;0..1..2..n
;       *Failure information*
;       F 0000000N      DSF 00000001
;ERRCODE  ERRNUMB  EXPDATA  RCVDATA  SCBOFF   ERRADDR  ERRORPC
;XXXXXXXX 00000001 00000000
RBD3>

N = failing test number
```

3.3.3 Reconfiguring a Failover Set

The initial state of a failover set is assumed to indicate good cable status. Bad cable status requires isolation of the bad cable prior to reconfiguring the failover set. When you remove a WAN module for repair, follow these steps:

1. If you are removing the active module, use WANDD$FSM to modify the failover set.
2. Use WANDD$FSM to remove the module from the failover set.
3. Use the command STOP/ZONE/POWER to remove the zone containing the module from the VAXft system configuration.
4. Remove the 20-pin and 100-pin cables from the module.
5. Replace the module.
6. Install the 20-pin and 100-pin cables on the module.
7. Power up the zone and verify that the power-up tests pass.
8. Use the command START/ZONE to restart the stopped zone.
9. Use the command SHOW DEVICE S to verify that the module is on-line. Then use WANDD$FSM to add the new module to the failover set.
10. To verify the function of the new module, use WANDD$FSM to make the new module active in the failover set.

3.4 Shutting Down the VAXft System

A total system shutdown **may** be required when you install additional memory or upgrade the system software. In this case, the VAXft system requires that the FTSS shutdown command file be invoked by the site-specific system shutdown procedure in SYS$MANAGER:SYSHUTDWN.COM. The FTSS shutdown command file is in SYS$MANAGER:FTSS$SHUTDOWN.COM. This file is created during the installation of the FTSS software. See the *VAXft System Services Installation Guide* for details.

The following shows how to start the system shutdown:

```
$! This site-specific system shutdown procedure includes
$! the FTSS specific system shutdown command file.
$!
$@SYS$MANAGER:FTSS$SHUTDOWN.COM
$exit
```

3.4.1 Powering Off a Zone After System Shutdown

After you run the system shutdown procedure and **before** you power off the zone, you must put the system console in the SIMPLEX state. This ensures that the other system console is operational.

The following shows when you can power off a zone.

```
$@SYS$SYSTEM:SHUTDOWN.COM
    .
    .   Shutdown messages appear...
    .
>>> HALT      ! Halt the CPU.
>>> INIT      ! Force the console to SIMPLEX state.
              ! At this point, you can power off
              ! one or both zones.
```

3.5 Recommended Console Terminals

Communication with the VAXft console subsystem is an integral part of the fault-tolerant system. Because of the unique characteristics of the VAXft console subsystem, Digital recommends use of independent video or hardcopy terminals. VT320 and VT420 terminals, for example, are recommended. Use of dual session video terminals (VT330 or non-Digital terminals) is not recommended. Also, video terminals should use jump scroll, not smooth scroll.

4 Model 110 Removal and Replacement Procedures

This chapter describes how to remove and replace the model 110 field replaceable units (FRUs). When specific installation/replacement procedures are not given, replace or install an FRU by reversing the steps in the removal procedure.

NOTE

Throughout this chapter, the DSF32 module is referred to as the WAN module.

A complete list of the model 110 FRUs is given in Table 4–1. A list of the WAN module diagnostic tools is given in Table 4–2.

Table 4–1 Model 110 FRUs

FRU	Part Number
KA510 processor module	T3005-BA
KFE52 I/O controller module	T3001-AA
MS520 memory module (32 MB)	T3003-AA
RF31 DSSI controller	54-18329-01
RF72 DSSI controller	54-19091-01
RF31 HDA assembly	70-24697-01
RF72 HDA assembly	70-25972-01
Cable, DSSI to disk with terminator	17-03333-01

Table 4–1 (Continued) Model 110 FRUs

FRU	Part Number
WAN 620 module (DSF32)	T3004-AA
TK70 tape drive	TK70-EA
TK70 DSSI controller	54-19085-01
Cable, tape control to tape drive	17-03199-01
Cable, DSSI to tape drive extension with terminator	17-03334-01
Power harness, disk/tape drive	17-03200-01
Console protection module	54-19491-01
Cable, console protection module	17-02258-02
Cable, console modem assembly to console protection module	17-03297-01
DSSI panel, system	54-21059-01
Cable, DSSI panel to backplane	17-01964-01
Cable, DSSI panel to disk	17-01936-01
Backplane	54-20251-01
–10 V converter	54-20074-01
Cable, –10 V converter to backplane	17-03296-01
TOY battery, 3 cell, 3.75 V	12-19245-02
Fan assembly, 120 V	70-28962-01
Fan assembly, 220 V	70-28962-02
Power supply, 120 V	H7868-A
Power supply, 220 V	H7868-B
AC power cord, 47–63 Hz, 120 Vac	17-00083-43
AC power cord, 47–63 Hz, 220 Vac	(Country Kits)
Y-Box	70-27483-01
100-pin terminator	12-33191-01

Table 4–1 (Continued) Model 110 FRUs

FRU	Part Number
Cable, synchronous communication	17-02390-01
Cable, synchronous communication	17-02740-01
Personality cable type RS-422, V.11	17-01108-01
Personality cable	17-01109-01
Personality cable type RS-232, V.24	17-01110-01
Personality cable type RS-423, V1.0	17-01111-01
Personality cable type V.35	17-01112-01
DSSI terminator	12-29258-01
Cable, cross-link	17-02194-01

Table 4–2 WAN Module Diagnostic Tools

Tool	Part Number
100-pin loopback	12-33192-01[1]
20-pin loopback	12-33193-01[1]
Universal loopback	12-25852-01 (H3199)
Personality loopback V.35	H3250
Personality loopback RS-232, V.24	H3248
Personality loopback RS-422, 423, 449, V.11	12-26259-01 (H3198)
Personality loopback X.21	12-26811-01 (H3047)

[1]A 100-pin and a 20-pin loopback ships with every WAN option.

4.1 Before You Begin

WARNING

Hazadous voltages exist within the system. Bodily injury or equipment damage can result when service procedures are performed incorrectly.

NOTE

FRUs should be removed/replaced only by qualified maintenance personnel. They must be familiar with the electrostatic discharge (ESD) procedures and power procedures for the VAXft system. Excessive shock or incorrect handling can damage the logic modules.

Before you use any of these procedures on a system that is running, you must first contact the responsible customer representative, system manager, or application manager to shut down the zone and power off the zone. The *VAXft System Services Manager's Guide* (AA-NL35A-TE) describes how to shut down the zone.

You do not need to shut down the entire VAXft system to remove and replace an option or FRU. In most cases, you can shut down the zone that houses the failing FRU while the other zone continues to operate. (Section 4.1.2 explains how to shut down a zone.)

4.1.1 Model 110 FRU Handling

Static electricity can damage the FRUs. Use an ESD wrist strap and a grounded ESD workmat whenever you perform removal and replacement procedures. Wear the wrist strap and attach both the wrist strap and the grounded workmat to the system chassis.

Spare FRUs are shipped in an antistatic ESD box. Before you open the ESD box, attach a ground strap from the ESD box to the system chassis.

Use great care when handling the FRUs. Do not drop them or bump them.

4.1.2 Shutting Down a Zone

Typically, the shutdown is performed by the system manager or the operator because it requires CMKRNL privileges. Before shutting down the zone, use the SHOW ZONE command to see the status of each zone. The system lists one of the following status messages for each zone.

- Active — The zone is running.
- Stopped — The zone is not running the system software. It may be running diagnostics or is available for synchronizing.
- Absent — The zone is not running.
- Synchronizing — The zone is in the process of synchronizing with the other zone.
- Providing I/O only — The zone has detected a CPU/MEM fault, and has placed the CPU and memory off-line.

The DCL command STOP/ZONE *zone-id* shuts down the zone. Example 4–1 shows how to shut down a zone. User input is underlined.

Example 4–1 How to Shut Down a Zone

```
$ SHOW ZONE                          ! Displays the status of each zone.
  Zone A is ACTIVE                  ! Zone A is running.
  Zone B is PROVIDING I/O ONLY      ! Zone B has a faulty component.

$ STOP/ZONE B                       ! Shuts down zone B.
```

At the console terminal of the zone that continues to run (in this case, zone A), the OPCOM messages show that synchronization has been lost with the other zone, and that virtual circuits are closed.

The SHOW ZONE command may be used to verify that the STOP/ZONE *zone-id* command executed correctly. Example 4–2 shows how to verify the zone is shut down. User input is underlined.

Example 4–2 How to Verify the Zone is Shut Down

```
$ SHOW ZONE                       ! Displays the status of each zone.
  Zone A is ACTIVE                 ! Zone A is running.
  Zone B is ABSENT                 ! Zone B has been shut down.
```

4.1.3 Starting Up a Zone

NOTE

The zone to be started must be in the stopped state prior to the START/ZONE command being issued for successful execution.

Typically, the startup is performed by the system manager or the operator because it requires CMKRNL privileges. The DCL command START /ZONE *zone-id* starts up the zone after a shutdown.

4.1.4 Accessing the Model 110 FRUs

Refer to Figure 4–1 and Table 4–3. Use the following procedure to remove the front cover.

1. Insert the key (supplied with each cabinet) in the keyhole on the front cover.
2. Turn the key to the right to unlock the front cover window.
3. Slide the window down.
4. Pull out the release latch to unlock the front cover.
5. Grasp the front cover by its sides and lift up and out to free the cover brackets from the notches in the cabinet frame.
6. Remove the cover.

Use the following procedure to install the front cover.

1. Insert the key (supplied with each cabinet) in the keyhole on the front cover.
2. Turn the key to the right to unlock the front cover window.
3. Slide the window down.
4. Pull out the release latch to unlock the front cover.
5. Position the front cover so that its brackets slide into and rest in the notches in the cabinet frame.
6. Push in the release latch.
7. Slide the front cover window up.
8. Turn the key to the left to lock the front cover window.
9. Remove the key.

Figure 4–1 Removing the Model 110 Front Cover

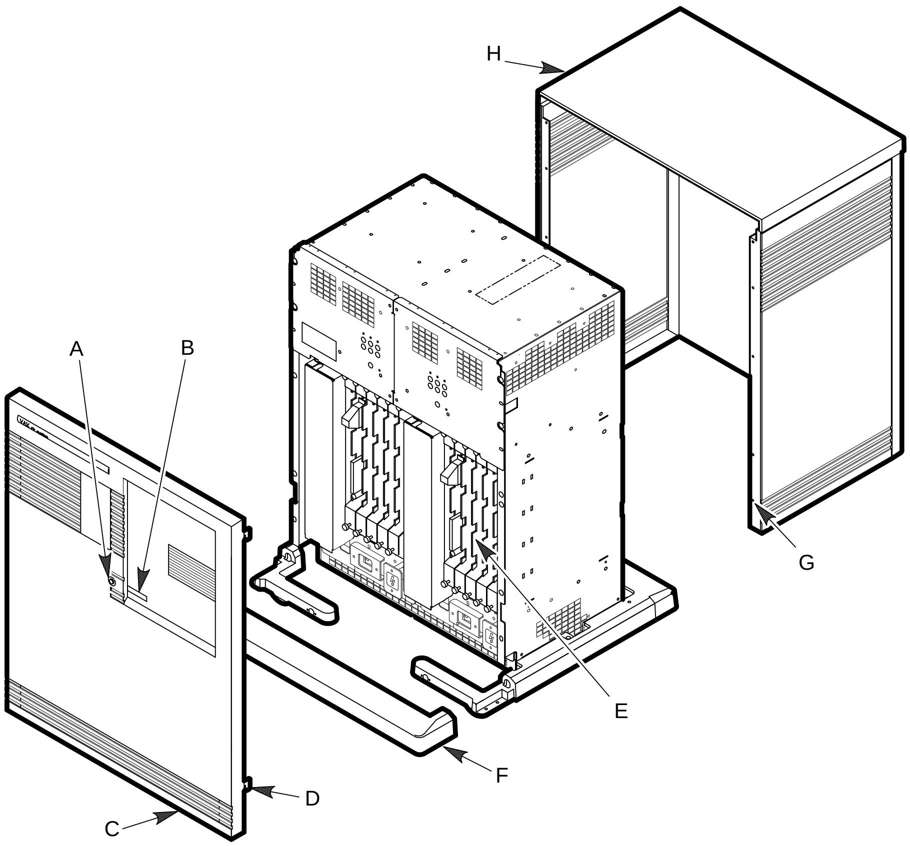


Table 4–3 Key to Figure 4–1 Callouts

Callout	Item
A	Front cover key
B	Front cover release latch
C	Front cover
D	Front cover notches (4)
E	Logic modules
F	Base cap
G	Cabinet cover screw holes (10)
H	Cabinet cover

4.2 Logic Modules

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 4.2.1 whenever you handle the logic modules.

4.2.1 Module Handling and ESD Procedures

T3000-series modules are fragile and static sensitive. Observe the following precautions when handling logic modules.

- Always put on a grounded ESD wrist strap *before* handling a logic module.
- Be sure that nothing touches the module or the components on the module because leads can be damaged. Avoid contact with the wrist strap, clothing, jewelry, cables, or other modules.
- Minimize any potential for physical or ESD damage as follows:
  - Remove all unnecessary materials in the service area (tools, documents, paper, plastics, polystyrene).
  - Avoid clothing that contains more than 80% nonconductive materials (silk or synthetic fiber).
  - Do not wear a jacket. Wear a short-sleeve shirt or roll up the sleeves on a long-sleeve shirt.
  - Do not wear jewelry.
  - Loose clothing, such as a necktie, must be fastened in place.

- Before removing a module from an ESD box, place the box on a clean surface. Do not allow the box to fall.

NOTE

Never place an ESD box on the floor.

- Keep the module in the antistatic ESD box until you are ready to install it.
- Before removing a module from an ESD box, attach the grounding clip to the ESD box.
- If you are replacing a module, put the module you just removed on a grounded ESD workmat on a clean surface in the service area. Put the module side 2 down on the ESD workmat.
- Save the ESD box for future use. Store a module in the ESD box until you are ready to install it.
- When removing or installing a module, be sure the module does not come into contact with a cable or another module. And be sure that nothing else touches the module or any module components.
- Hold a module **only** by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.
- Do not slide the module across any surface because the leads are fragile and can be damaged.
- An ESD sensitive module may come into contact with the following items **only**:
  - — An approved ESD workmat
  - — Antistatic packaging on the ESD workmat
  - — Tools and test equipment on the ESD workmat
  - — The chassis being serviced
  - — The hands of someone wearing an ESD wrist strap

4.2.2 Filler Modules

Each system cabinet contains two zones. Each zone contains a card cage with five slots. A module **must** be present in each of the ten slots to maintain cooling airflow. When a configuration does not use all the card cage slots, T3999 filler modules are placed in the unused slots.

4.2.3 KA510 Processor Module, MS520 Memory Module, WAN 620 Module, or KFE52 I/O Controller Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 4.2.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

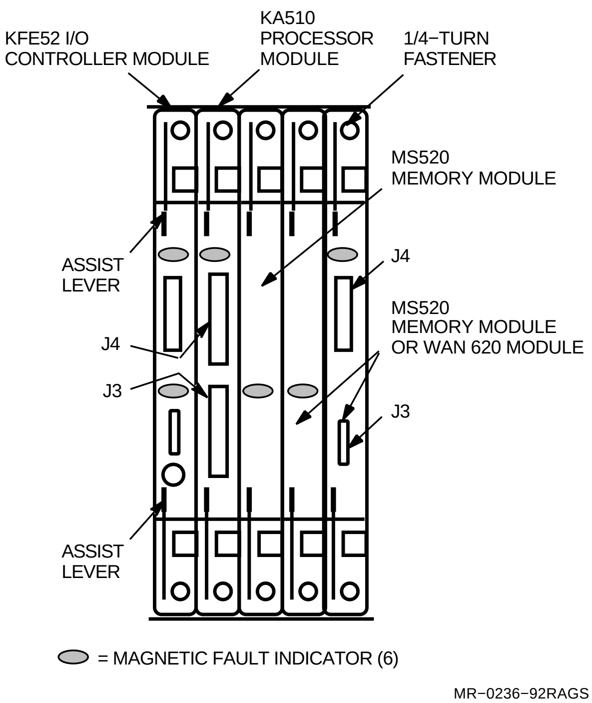
Use the following procedure to remove a module from the card cage. Remember to observe all FRU handling procedures (Section 4.1.1). Figure 4–2 shows the logic modules in the model 110 system.

1. Ask the system manager or the operator to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 4.1.2.)

2. Remove the cabinet front cover. (This procedure is described in Section 4.1.4.)

3. To power off the zone, set the main circuit breaker on the power supply in the affected zone to the OFF position.

Figure 4–2 Model 110 Logic Modules



4. If you are removing the KA510 processor module, disconnect the cross-link cables connected to J3 and J4 on the module. (See Figure 4–4.)

NOTE

After you replace a KA510 processor module, connect the lower cable to J3 on the new module and secure the spring clips. Then connect the upper cable to J4 on the new module and secure its spring clips.

If you are removing a WAN 620 module, disconnect the cables connected to J3 and J4 on the module. (See Figure 4–2.)

NOTE

After you replace the WAN 620 module, connect the cables to J3 and J4 on the new module.

If you are removing the KFE52 I/O controller module, remove the DSSI terminator and disconnect any Ethernet cables connected to the module. (See Figure 4–3.)

CAUTION

Make sure that the cable clip is unlocked before disconnecting the thickwire cable. Failure to do so may result in damage to the cable and/or connector.

NOTE

After you replace the KFE52 I/O controller module, connect the DSSI terminator and any Ethernet cables you removed from the old module to the new module. Set the Ethernet SWITCH on the new module to match the module you removed. Ensure that the DSSI jumper plugs are installed.

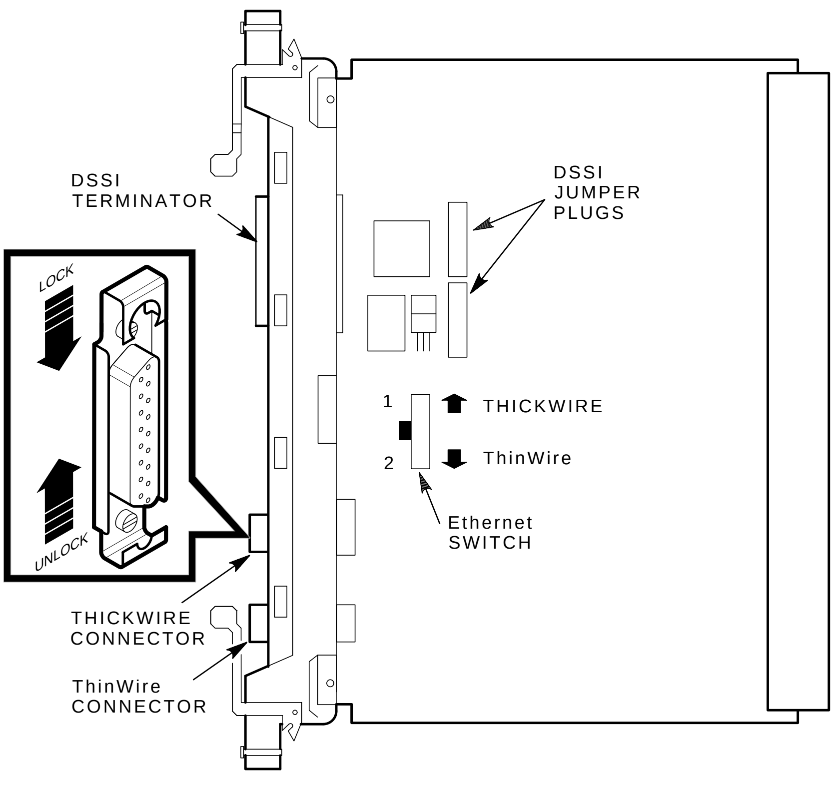
5. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

CAUTION

Use care when handling the module. A sudden shock to the module could cause component damage.

6. Use both hands to remove the module. Pull on the module assist levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
7. Grasp the module handle and slide the module out of the card cage slot.

Figure 4–3 Removing a KFE52 I/O Controller Module



4.3 Cross-Link Cables

Two cross-link cables connect between the processor modules in slot 2 of zone A and slot 2 of zone B.

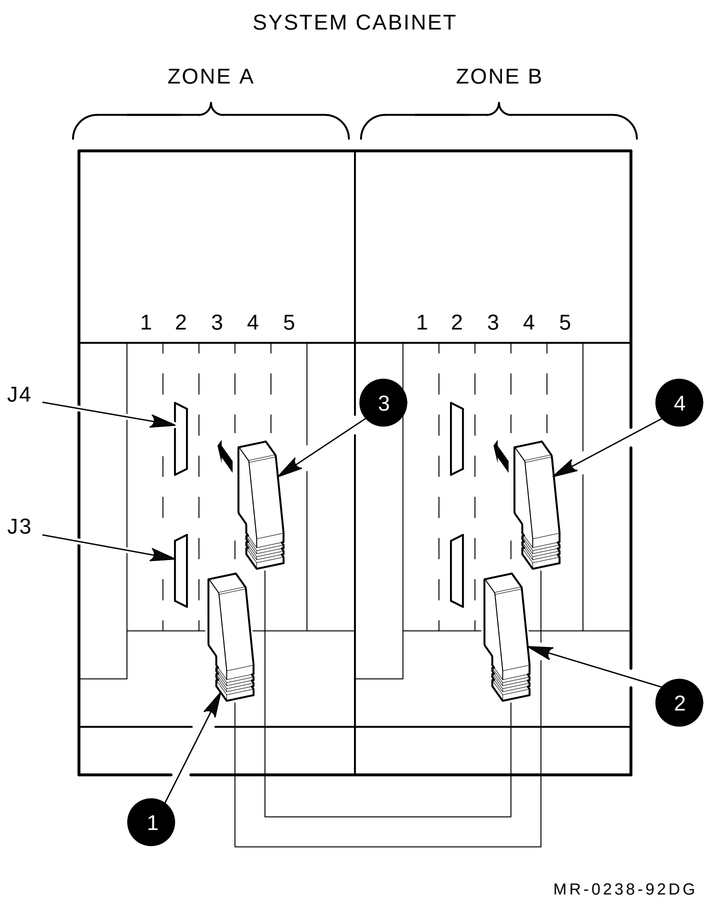
NOTE

The upper and lower connectors on the processor modules are arranged so the cables cannot be installed incorrectly. The connectors must be plugged in with the cable routed downward as shown in Figure 4–4.

The first two steps of the following procedure apply to the pedestal model only. Refer to Figure 4–4 as you remove and replace the cross-link cables.

1. Remove the cabinet front cover (Section 4.1.4).
2. Grasp the base cap at its center and pull it straight out.
3. Remove the faulty cross-link cables (Figure 4–4).
4. Plug one end of the first cross-link cable into the lower connector of the processor module in zone A (slot 2) and secure the spring clips. See Figure 4–4, callout ❶. Do not connect the other end of the cable at this time.
5. Plug one end of the second cross-link cable into the lower connector of the processor module in zone B (slot 2) and secure the spring clips. See Figure 4–4, callout ❷.
6. Plug the other end of the second cable into the upper connector of the processor module in zone A and secure the spring clips. See Figure 4–4, callout ❸.
7. Plug the other end of the first cable into the upper connector of the processor module in zone B and secure the spring clips. See Figure 4–4, callout ❹.

Figure 4–4 Model 110 Cross-Link Cable Connections



4.4 Model 110 System FRUs

Figures 4–5, 4–6, and 4–7 will help you during the removal and replacement of system FRUs.

Figure 4–5 is a front view of the model 110 system cabinet with the front cover removed. It identifies FRUs, cabinet switches, connectors, and zones. Table 4–4 is a key to the callouts.

Figure 4–6 is an exploded view of the model 110 system cabinet. It identifies FRUs, cover plates, and other hardware. Table 4–5 is a key to the callouts.

Figure 4–7 is a cabling diagram of zone B in the model 110 system cabinet. The cabling for zone A is the same except that zone A has no TK70 tape drive or TK70 DSSI controller. Figure 4–7 identifies the cables that must be disconnected when you remove a FRU. The cable part numbers are also given.

Figure 4–5 Model 110 Pedestal System, Front Cover Open

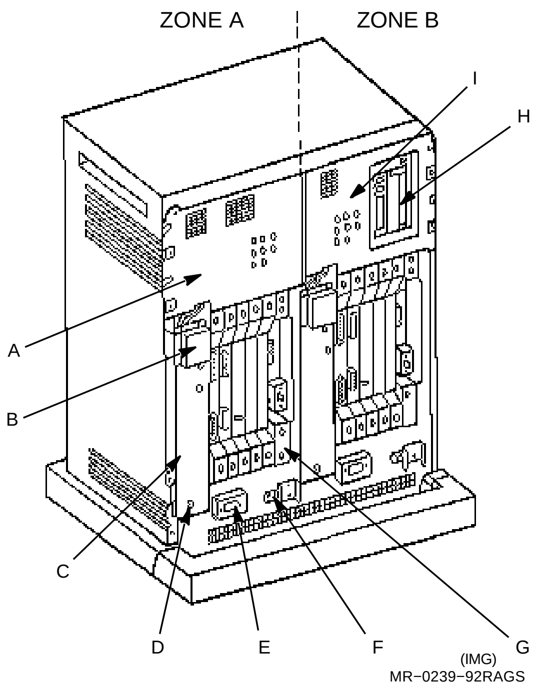


Table 4–4 Key to Figure 4–5 Callouts

Callout	Item
A	Drive cover plate, zone A
B	Power supply cable cover
C	Power supply
D	Main circuit breaker
E	Input power switch
F	Input power connector
G	I/O bulkhead
H	TK70 tape drive
I	Drive cover plate, zone B

Figure 4–6 Model 110 System, Exploded View

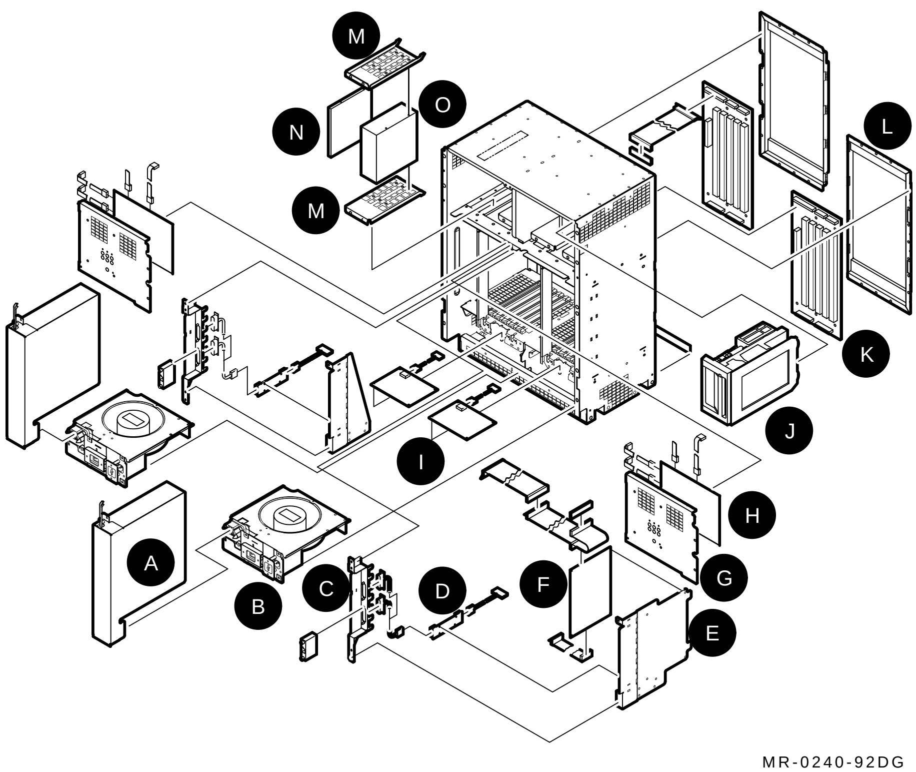
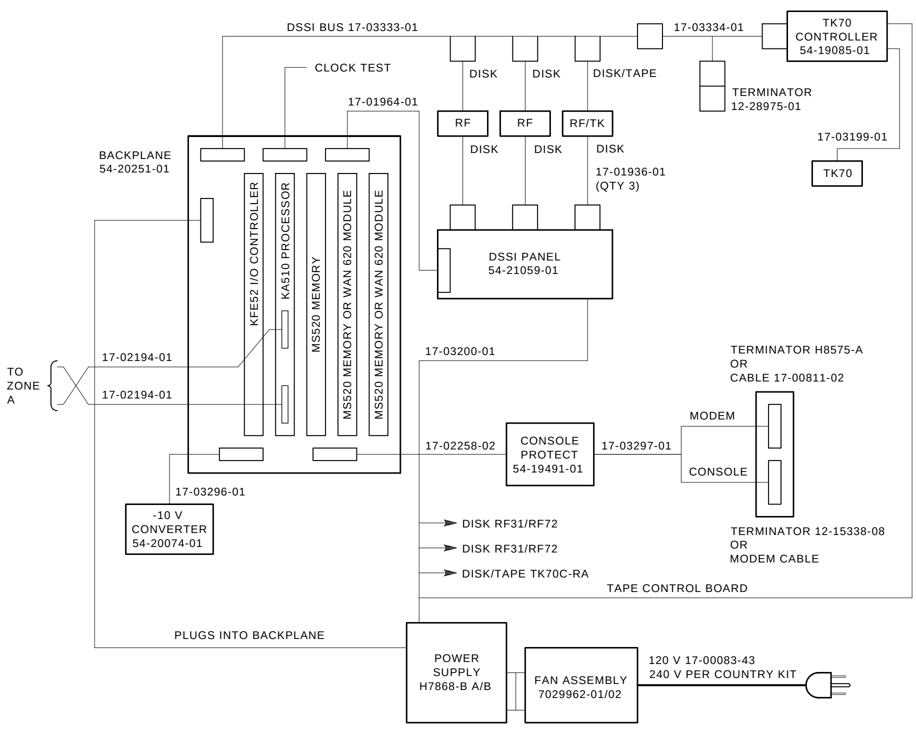


Table 4–5 Key to Figure 4–6 Callouts

Callout	Item
A	Power supply
B	Fan tray assembly
C	I/O bulkhead
D	Console protection module
E	Mounting plate
F	TK70 DSSI controller
G	Drive cover plate
H	DSSI panel
I	–10 V converter
J	TK70 tape drive
K	Backplane
L	Rear cover
M	Skid plates (upper and lower)
N	DSSI controller
O	Disk drive

Figure 4–7 Model 110 System, Zone B Cabling



4.5 Power Supply

The power supply is located to the left of the modules in each zone. Each power supply is fastened to the chassis with two screws.

Use the following procedure to remove the power supply. Refer to the figures in Section 4.4.

1. Remove the front cover (pedestal model only). Refer to Section 4.1.4.
2. Remove and save the Phillips screw that fastens the small cable cover at the top of the power supply. Then remove the cable cover.

NOTE

The lower lip of the cable cover fits inside the power supply chassis.

3. Using the finger strap, unplug the P4 cable connector.
4. Slide the cable assembly out of the grommet at the top of the power supply. Move the cable to the right to expose the captive screw at the top of the power supply.
5. Release the two captive screws (top and bottom) on the power supply.
6. Pull the power supply out of the cabinet.

NOTE

When you install the new power supply, push it in firmly to seat the connector at the rear of the module.

CAUTION

Make sure the new power supply is 120 V (H7868-A) or 220 V (H7868-B), as required.

4.6 Fan Assembly

The fan assembly is located under the card cage in each zone. Each fan assembly is fastened to the front of the chassis with four screws (two to the right of the ac connector and two to the left of the ac switch).

The first two steps of the following procedure apply to the pedestal model only. Refer to the figures in Section 4.4 as you remove and replace the fan assembly.

1. Remove the cabinet front cover (Section 4.1.4).
2. Grasp the base cap at its center and pull it straight out.
3. Remove the power supply (Section 4.5).
4. Remove the two screws that secure the power cord cover to the power supply. Remove the power cord.
5. Remove and save the four screws that fasten the front of the fan assembly to the chassis.
6. Pull the fan assembly out of the chassis.

4.7 –10 V Converter or TOY Battery

The –10 V converter is located under the fan assembly in each zone. The –10 V converter is pressed onto four split pegs on the bottom of the chassis. The TOY battery is clip mounted on the –10 V converter chassis.

Use the following procedure to remove the –10 V converter or TOY battery. Refer to the figures in Section 4.4.

1. Remove the front cover (pedestal model only). Refer to Section 4.1.4.
2. Remove the power supply (Section 4.5).
3. Remove the fan assembly (Section 4.6).
4. From the front of the chassis, unplug the backplane cable connector from the –10 V converter.
5. Lift the –10 V converter away from the four split pegs on the bottom of the chassis.

NOTE

When you install the new –10 V converter, make sure the backplane cable is positioned to avoid damage by the fan blade.

6. To remove the TOY battery, disconnect the TOY battery cable from the –10 V converter and remove the battery from the retaining clip.

4.8 TK70 DSSI Controller or Console Protection Module

The TK70 DSSI controller is located behind the I/O bulkhead in zone B. It is attached to a mounting plate that is connected to the I/O bulkhead. The zone B console protection module is also attached to the mounting plate, just below the TK70 DSSI controller.

There is no TK70 DSSI controller in zone A. The mounting plate that is connected to the I/O bulkhead in zone A is smaller than that in zone B. The zone A console protection module is attached to this smaller mounting plate.

Use the following procedure to remove the TK70 DSSI controller or the console protection module. Refer to the figures in Section 4.4.

1. Remove the front cover (pedestal model only). Refer to Section 4.1.4.
2. Remove all logic modules from slots 1 through 5 in the affected zone if replacing the console protection module, or in zone B if replacing the DSSI controller. Refer to Section 4.2 for information on handling and removing logic modules.
3. Locate the TK70 DSSI controller attached to the mounting plate behind the I/O bulkhead.
4. Disconnect the three cables connected to the TK70 DSSI controller. They are:
   - Power cable at top right of the TK70 DSSI controller.
   - DSSI bus cable at top left of the TK70 DSSI controller.
   - Tape drive cable at the bottom of the TK70 DSSI controller. Notice that the tape drive cable routes in back of the controller.
5. Disconnect the rear cable from the console protection module.
6. Remove the two screws (top and bottom) that secure the I/O bulkhead to the chassis.

7. Slide the I/O bulkhead and the mounting plate toward you.
8. To replace the console protection module, disconnect the cable at the front of the module.
9. Remove and save the four retaining screws that secure the FRU (DSSI controller or console protection module) to the mounting plate and remove the FRU.

4.9 DSSI Panel or TK70 Tape Drive

NOTE

When replacing the TK70 DSSI controller, set the address switches on the new controller to match the switch settings on the controller being removed. The switches should be set to an address of 2. Use the DUP to set the drive parameters. See Section 1.5.

The DSSI panel is located behind the drive cover plate in the upper part of each zone. The DSSI panel is pressed onto four split pegs that are attached to the drive cover plate.

The TK70 tape drive is located in the top right corner of zone B behind the drive cover plate and the DSSI panel. The TK70 tape drive slides into a retaining bracket that is attached to the right wall of the chassis.

Use the following procedure to replace the DSSI panel or the TK70 tape drive. Refer to the figures in Section 4.4.

1. Remove the front cover (pedestal model only). Refer to Section 4.1.4.
2. While holding the drive cover plate in place, remove and save the four retaining screws (one in each corner of the plate).
3. Tilt the plate toward you to gain access to the cable connections on the DSSI panel.
4. Disconnect the cables connected to the DSSI panel. They are:
   - Power cable at top left of the DSSI panel.
   - Backplane cable at top right of the DSSI panel.
   - Drive cable(s) (up to three) at the left side of the DSSI panel.

5. If you are removing the DSSI panel, separate it from the drive cover plate.

   If you are removing the TK70 tape drive, move the DSSI panel and drive cover plate to a grounded ESD workmat and continue with this procedure.

6. Locate the release tab for the retaining bracket. It is between the TK70 tape drive and the right side of the chassis.

7. Push the release tab to the right and, with a firm grip on the TK70 tape drive, pull it out until you can see the two cable connections at the rear of the drive.

   NOTE

   When you install the new TK70 tape drive, push it into the retaining bracket until it snaps into place.

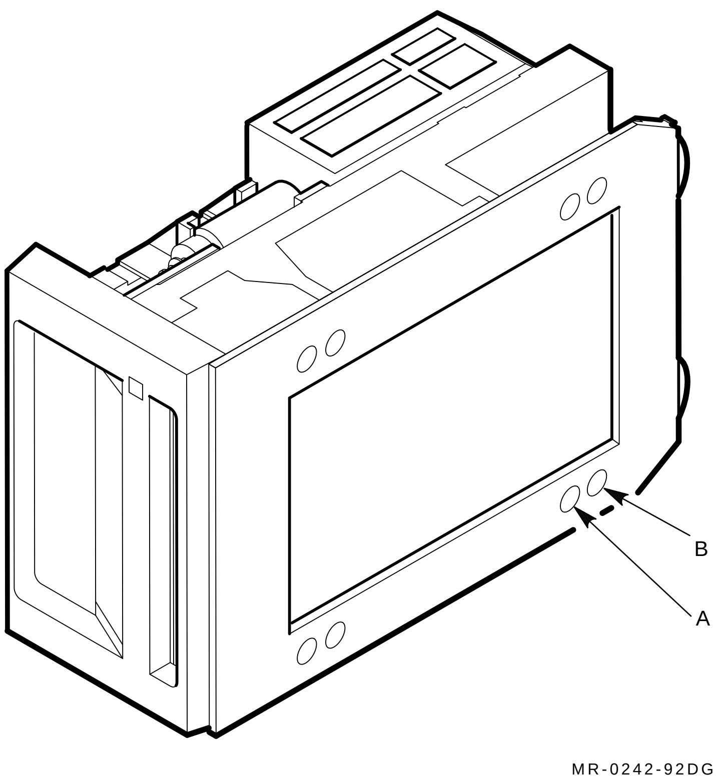
8. Unplug the two cables (controller and power) from the rear of the TK70 tape drive. Then pull the drive out of the cabinet.

   NOTE

   Make sure that the unused connectors of the DSSI bus cable (large gray ribbon cable connected to the disk drive(s)) are away from the TK70 tape drive enclosure. This prevents possible interference during operation of the drive.

9. On the old TK70 tape drive, the four mounting screws that secured the drive to the assembly were in the forward set of holes. See Figure 4–8, callout A. On the new TK70 tape drive, the mounting screws are in the other set of holes. See Figure 4–8, callout B. Move the screws on the new drive to the forward set of holes. See Figure 4–8, callout A. This positions the drive as required for the model 110 system.

Figure 4–8 TK70 Tape Drive Mounting Screws



4.10 RF31 HDA, RF31 DSSI Controller, RF72 HDA, or RF72 DSSI Controller

NOTE

Warm swapping (described in Appendix A) is not supported for the model 110 system.

The RF-series disk drives consist of two subunits:

- An HDA that contains the DSSI controller
- The DSSI controller

The drives are removed from the cabinet as a single unit and then separated into the two subunits.

RF-series disk drives are housed in the top of the cabinet in both zone A and zone B. Each zone has four slots. The RF31 disk drive takes up one slot. The RF72 disk drive takes up two slots. The following restrictions apply to model 110 drive configurations that include both RF31 and RF72 disk drives:

- The drive configurations in zone A and zone B should be the same, to accomplish shadowing.
- If a TK70 tape drive is used, it takes up two of the four slots in zone B. In this case, the corresponding two slots in zone A are unused.
- Power supply limitations allow only three RF31 disk drives in one zone.
- The RF-series disk drives are mounted in a two-slot skid-plate assembly. Two RF31 disk drives or one RF72 disk drive fill(s) an assembly. If an assembly holds only one RF31, a filler module must be installed in the unused slot.

Use the following procedure to remove an RF-series HDA or DSSI controller. Refer to the figures in Section 4.4.

1. Issue a STOP/ZONE command to the faulty zone.
2. Remove the front cover (pedestal model only). Refer to Section 4.1.4.
3. Power down the faulty zone.
4. While holding the drive cover plate in place, remove and save the four retaining screws (one in each corner of the plate).
5. Tilt the plate toward you to gain access to the cable connections on the DSSI panel.

6. Disconnect the cables connected to the DSSI panel. They are:
   - Power cable at top left of the DSSI panel.
   - Backplane cable at top right of the DSSI panel.
   - Drive cable(s) (up to three) at the left side of the DSSI panel.
7. Remove the drive cover plate with the DSSI panel attached, and place it on a grounded ESD workmat.
8. Disconnect the three cables connected to the RF-series disk drive. They are:
   - Power cable
   - DSSI bus cable
   - Cable to the DSSI panel
9. Release the four captive screws (two above and two below the drive assembly) that hold the drive assembly in place on the skid plates.
10. Pull the drive assembly out slowly, holding the cables out of the way.

NOTE

The address jumpers on the DSSI controller are not used in this application. The drive address is established by the drive connection to the DSSI panel. The three connections specify different addresses to their connected drive(s).

11. Remove the screws (two on each side of an RF31, four on each side of an RF72) that secure the disk drive to the top and bottom skid plates. Remove the disk drive.
12. Remove the screws that secure the HDA to the disk drive.
13. Separate the HDA and the DSSI controller.
14. Disconnect the cables connecting the HDA and the DSSI controller.

NOTE

Make sure that the unused connectors of the DSSI bus cable (large gray ribbon cable connected to the disk drive(s)) are away from the TK70 tape drive enclosure. This prevents possible interference during operation of the drive.

When you install an RF-series disk drive, lift it up until the ramps on the back of the drive assembly slide onto the ears at the back of the shock assembly. Install the top screws first.

4.11 Backplane

The backplane is removed from the rear of the system cabinet.

The first three steps of the following procedure apply to the pedestal model only. Refer to the figures in Section 4.4.

1. Remove the cabinet front cover (Section 4.1.4).
2. From the front of the cabinet, remove the ten screws (five on each side) that secure the cabinet cover (Figure 4–1).
3. Remove the plastic cabinet cover.
4. Remove the TK70 tape drive, if one is present (Section 4.9).
5. Remove all disk drives from the affected zone (Section 4.10).
6. Remove the power supply from the affected zone (Section 4.5).
7. Remove the fan assembly from the affected zone (Section 4.6).
8. Disconnect all the modules in the affected zone from the backplane, but leave the modules in the system cabinet.
9. From the front of the cabinet, reach in through the upper drive area and disconnect the two cables from the top of the backplane (DSSI bus cable and DSSI panel cable).
10. From the front of the cabinet, reach in through the lower fan area and disconnect the two cables from the bottom of the backplane (console protection module cable and –10 V converter cable).
11. Remove the screws that secure the backplane rear cover in the affected zone. Remove the backplane cover.
12. From the rear of the cabinet, remove the six screws (three at the top and three at the bottom) that secure the backplane to the cabinet chassis. Remove the backplane.

4.12 DSF32 Y-Box

Refer to the *VAXft Systems Site Preparation and Installation Guide* (EK-VXFT1-IN) for information on replacing the DSF32 Y-Box.

5
Model 310 and 410 Removal and Replacement Procedures

This chapter describes how to remove and replace the model 310 and 410 field replaceable units (FRUs), which include the following:

- System cables
- System modules
- Power supplies
- Fans
- Peripheral devices
- Backplanes
- Summary panel

When specific installation/replacement procedures are not given, replace or install an FRU by reversing the steps in the removal procedure.

NOTE

Throughout this chapter, the DSF32 module is referred to as the WAN module.

A complete list of the model 310 and 410 FRUs is given in Table 5–1. A list of the WAN module diagnostic tools is given in Table 5–2.

Table 5–1 Model 310 and 410 FRUs

FRU	Part Number
KA520 processor module	T3005-AA
KA550 processor module	T3007-AA
WAN 620 module (DSF32)	T3004-AA
KFE52 I/O controller module	T3001-AA
MS520 memory module (32 MB)	MS520-BA
RF31 disk drive adapter	54-19250-01
RF31 DSSI controller	54-18329-01
RF31 HDA assembly	70-24697-01
TF70 tape drive adapter	54-20211-01
TF70 DSSI controller	54-19085-01
RF72 DSSI controller	54-19091-01
TF70 tape drive	TK70-AX
RF72 HDA assembly	70-25972-01
Card cage, system cabinet	70-27877-01
Six-pack backplane, expander cabinet	54-19483-01
DSSI backplane	54-19260-01
Console protection module	54-19491-01
Summary panel, system cabinet	54-19481-01
Summary panel, expander cabinet	70-26104-01
AC power supply	H407-A
DC power supply, system cabinet	H7233-AA
DC power supply, expander cabinet	H7233-BA
Uninterruptible power supply (UPS)	30-29639-01[1]
Fan assembly, system cabinet	70-26102-01

[1]The UPS is not stocked locally because the shelf life of the battery is relatively short. This part must be P-1 ordered.

Table 5–1 (Continued) Model 310 and 410 FRUs

FRU	Part Number
Fan assembly, expander cabinet	70-26107-01
Fan assembly, dc power supply	70-26865-01
Cable, cross-link	17-02194-01
Cable, PCIM	17-02285-02
Cable, DSSI with terminator (39 inches, red)	17-02245-01
Cable, DSSI with terminator (62 inches, blue)	17-02245-02
Cable, synchronous communication	17-02390-01
Cable, synchronous communication monitor	17-02740-01
Personality cable type RS-422, V.11	17-01108-01
Personality cable	17-01109-01
Personality cable type RS-232, V.24	17-01110-01
Personality cable type RS-423, V1.0	17-01111-01
Personality cable type V.35	17-01112-01
Cable, disk PCIM	17-02120-01
Cable, disk control	17-02121-01
Cable, DSSI logic	17-02122-01
Cable, lower fan	17-02266-01
Cable	17-02362-01
Y-box	70-27483-01
DSSI terminator	12-29258-01
AC power cord, 47–63 Hz, 120 Vac	17-00083-23

Table 5–2 WAN Module Diagnostic Tools

Tool	Part Number
100-pin loopback	12-33192-01[1]
20-pin loopback	12-33193-01[1]
Universal loopback	12-25852-01 (H3199)
Personality loopback V.35	H3250
Personality loopback RS-232, V.24	H3248
Personality loopback RS-422, 423, 449, V.11	12-26259-01 (H3198)
Personality loopback X.21	12-26811-01 (H3047)

[1]A 100-pin and a 20-pin loopback ships with every WAN option.

5.1 Before You Begin

WARNING

Hazadous voltages exist within the system. Bodily injury or equipment damage can result when service procedures are performed incorrectly.

NOTE

FRUs should be removed/replaced only by qualified maintenance personnel.

You do not need to shut down the entire VAXft system to remove and replace an option or FRU. In most cases, you can shut down the zone that houses the failing FRU while the other zone continues to operate. (Section 5.1.2 explains how to shut down a zone.)

There are two types of FRU removal and replacement procedures: *cold swaps*, and *warm swaps*. During a cold swap, you shut down the zone that houses the failing FRU while the operating software continues to run in the other zone. FRUs that require a cold swap include the logic modules, fans, battery backup unit, backplanes, power supplies, and the summary panel.

During a warm swap, all cabinets remain powered on. The application continues to run in both zones while the FRU is replaced. FRUs that require a warm swap include the cannister tape drive, the cannister disk drive, and the carrier disk drive.

5.1.1 Model 310 and 410 FRU Handling

Static electricity can damage the FRUs. Use an ESD wrist strap and a grounded ESD workmat whenever you perform removal and replacement procedures. Wear the wrist strap and attach both the wrist strap and the grounded workmat to the system chassis.

Spare FRUs are shipped in an antistatic ESD box. Before you open the ESD box, attach a ground strap from the ESD box to the system chassis.

Use great care when handling the FRUs. Do not drop them or bump them.

5.1.2 Shutting Down a Zone

Cold swap procedures require you to shut down the zone where the removal and replacement is to take place. A red Fault indicator on the summary panel blinks to identify the zone that houses the faulty FRU.

Typically, the shutdown is performed by the system manager or the operator because it requires CMKRNL privileges. Before shutting down the zone, use the SHOW ZONE command to see the status of each zone. The system lists one of the following status messages for each zone.

- Active — The zone is running.
- Stopped — The zone is not running the system software. It may be running diagnostics or is available for synchronizing.
- Absent — The zone is not available.
- Synchronizing — The zone is in the process of synchronizing with the other zone.
- Providing I/O only — The zone has detected a CPU/MEM fault, and has placed the CPU and memory off-line.

The DCL command STOP/ZONE *zone-id* shuts down the zone. Example 5–1 shows how to shut down a zone. User input is underlined.

Example 5–1 How to Shut Down a Zone

```
$ SHOW ZONE                        ! Displays the status of each zone.
  Zone A is ACTIVE                 ! Zone A is running.
  Zone B is PROVIDING I/O ONLY     ! Zone B has a faulty component.

$ STOP/ZONE B                      ! Shuts down zone B.
```

At the console terminal of the zone that continues to run (in this case, zone A), the OPCOM messages show that synchronization has been lost with the other zone, and that the virtual circuit is closing.

The SHOW ZONE command may be used to verify that the STOP/ZONE *zone-id* command executed correctly. Example 5–2 shows how to verify the zone is shut down. User input is underlined.

Example 5–2 How to Verify the Zone is Shut Down

```
$ SHOW ZONE                        ! Displays the status of each zone.
  Zone A is ACTIVE                 ! Zone A is running.
  Zone B is ABSENT                 ! Zone B has been shut down.
```

5.1.3 Starting Up a Zone

NOTE

The zone to be started must be in the stopped state prior to the START/ZONE command being issued for successful execution.

Typically, the startup is performed by the system manager or the operator because it requires CMKRNL privileges. The DCL command START /ZONE *zone-id* starts up the zone after a shutdown.

5.1.4 Accessing the Model 310 and 410 FRUs

Figure 5–1 shows the front doors and base cap of the model 310 system cabinets.

Figure 5–1 also shows the three-position front panel latch and its functions. (The upper door may be opened by itself or both doors may be opened together.) A key (Digital PN 12-17119-01) must be used to turn the latch and is supplied with each cabinet. All operating and service access takes place from the front of the system.

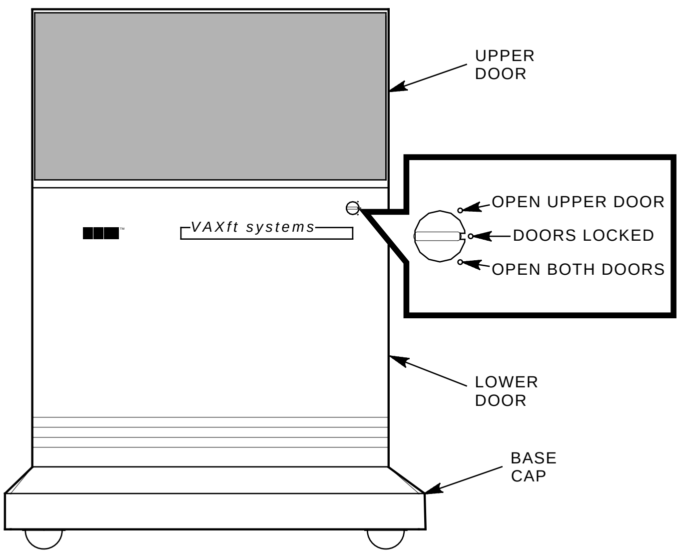
- The upper door provides access to the summary panel and cannister drives.
- The lower door is opened only for maintenance purposes. The lower door provides access to the cables and main circuit breaker in each cabinet, to the logic modules in the system cabinets, and to the carrier disk drives in the expander cabinets.

CAUTION

Installation and maintenance procedures may be performed only by qualified personnel. They must be familiar with the electrostatic discharge (ESD) procedures and power procedures for the VAXft system. Excessive shock or incorrect handling can damage the logic modules.

- The base cap provides additional access for routing and installing cables.

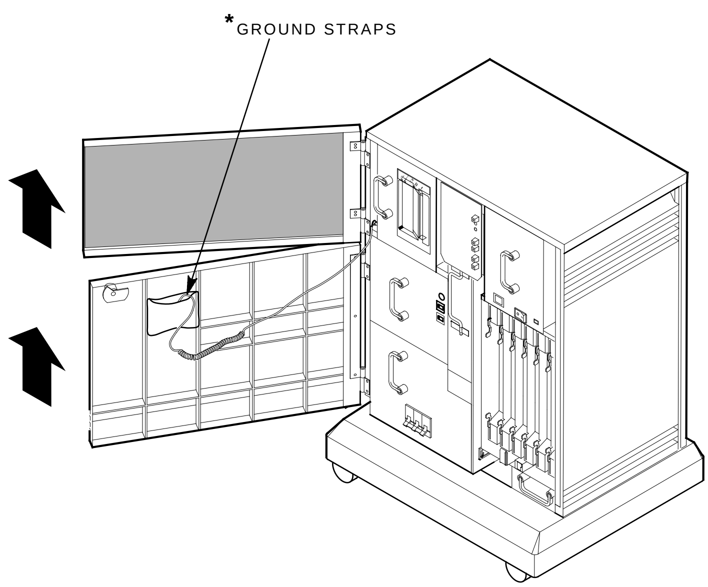
Figure 5–1 Model 310 Cabinet Latch



Use the following procedure to remove the front doors.

1. With the key, turn the latch to the up (open upper door) position.
2. Pulling from the right side of the door, swing the upper door open (Figure 5–2).

Figure 5–2 Model 310 Cabinet, Front Doors Open



3. Lift the upper door from its hinges, and set it aside if you wish. This step is not necessary, but you may find it easier to work on the system with the front doors removed.
4. With the key, turn the latch to the down (open both doors) position.
5. Pulling from the right side of the door, swing the lower door open (Figure 5–2).
6. Remove the ground straps from the pouch on the lower door, and put on the ESD wrist strap.
7. Lift the lower door from its hinges, and set it aside if you wish. This step is not necessary, but you may find it easier to work on the system with the front doors removed.

5.1.5 Filler Modules and Blank Slots

Each system cabinet contains a card cage with seven slots. A module **must** be present in each of the seven slots to maintain cooling airflow. When a configuration does not use all the card cage slots, T3999 filler modules are placed in the unused slots.

In the future, add-on options may require the removal of a filler module to make a card cage slot available. Also, future deinstallation options may require use of a filler module to replace the removed module.

A module **must** be present in each of the DSSI backplane slots to maintain cooling airflow. When a configuration does not use all the DSSI backplane slots, blank cannister modules are placed in the disk or tape cannister slots.

In an expander cabinet, blank carrier modules are placed in all unused six-pack backplane slots.

5.2 System Cables

This section describes how to route, remove, and replace the following system cables:

- Cross-link
- DSSI
- PCIM

CAUTION

An ESD wrist strap must be worn during the following procedures until all cables are connected and secured to the module handles.

5.2.1 Cross-Link Cables

All cables should be routed under the cabinets before making any of the connections. This makes it easier to handle and position the cables within the limited access space. The connections may be made when all of the cables are in place.

Figure 5–3 numbers the steps used to connect the cross-link cables between the processor modules in slot 3 of the system cabinets. (The lower connectors cannot be plugged in with the upper connectors in place.)

NOTE

The upper and lower connectors on the processor modules are keyed so the cables can be installed correctly. The connectors must be plugged in with the cable routed downward as shown in Figure 5–3.

Locate the two cross-link cables (PN 17-02194-01). Route each cable between the system cabinets, behind the front wheels, and on top of the floor surface. Do **not** bring the cables up through the cabinet front at this time.

System with expansion: If you are installing a system with expansion, skip the following steps and proceed to Section 5.2.2.

Base system: If you are installing a base system, connect the cross-link cables as follows:

❶ In the left system cabinet, bring the lower processor module connector up through the cabinet access hole.

Plug the cable into the lower connector and secure the spring clips. Do **not** connect the other end of the cable at this time.

❷ In the right system cabinet, bring the lower processor module connector up through the cabinet access hole.

Plug the cable into the lower connector and secure the spring clips.

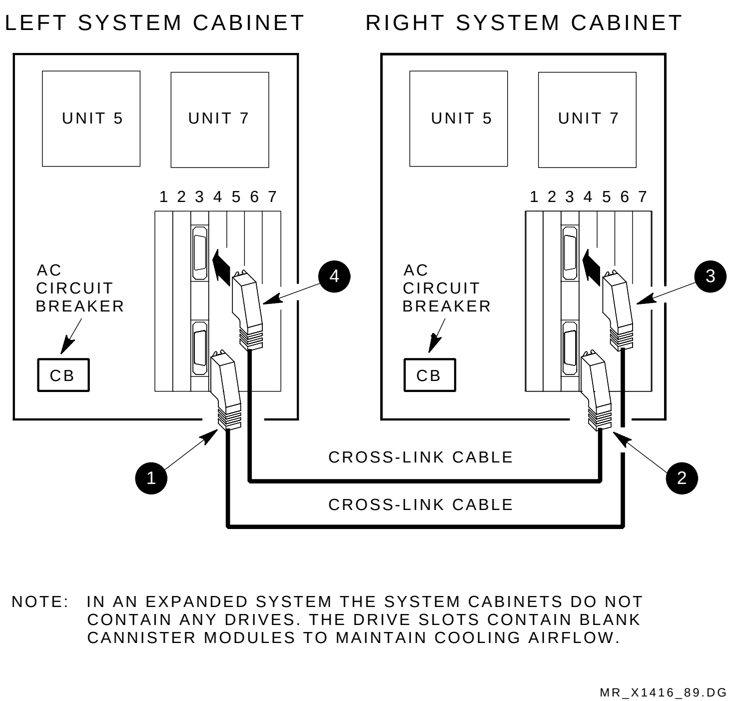
❸ In the right system cabinet, bring the upper processor module connector up through the cabinet access hole.

Plug the cable into the upper connector and secure the spring clips.

❹ In the left system cabinet, bring the upper processor module connector up through the cabinet access hole.

Plug the cable into the upper connector and secure the spring clips.

Figure 5–3 Model 310 and 410 Cross-Link Cable Connections



Refer to Figure 5–3 as you remove and replace the cross-link cables between the processor modules in slot 3 of the system cabinets:

1. In the left system cabinet, release the spring clips at one end of the cross-link cable attached to the upper or lower connector of the processor module.
2. Disconnect the cross-link cable.
3. Route the cable through the access hole into the right system cabinet.
4. In the right system cabinet, release the spring clips at the other end of the cross-link cable attached to the upper or lower processor module.
5. Disconnect the cable.

5.2.2 DSSI Cables

Locate the two short (red labeled) DSSI cables (PN 17-02245-01) and the two long DSSI cables (PN 17-02245-02). Figure 5–4 shows how to connect the DSSI cables between the expander cabinets and system cabinets.

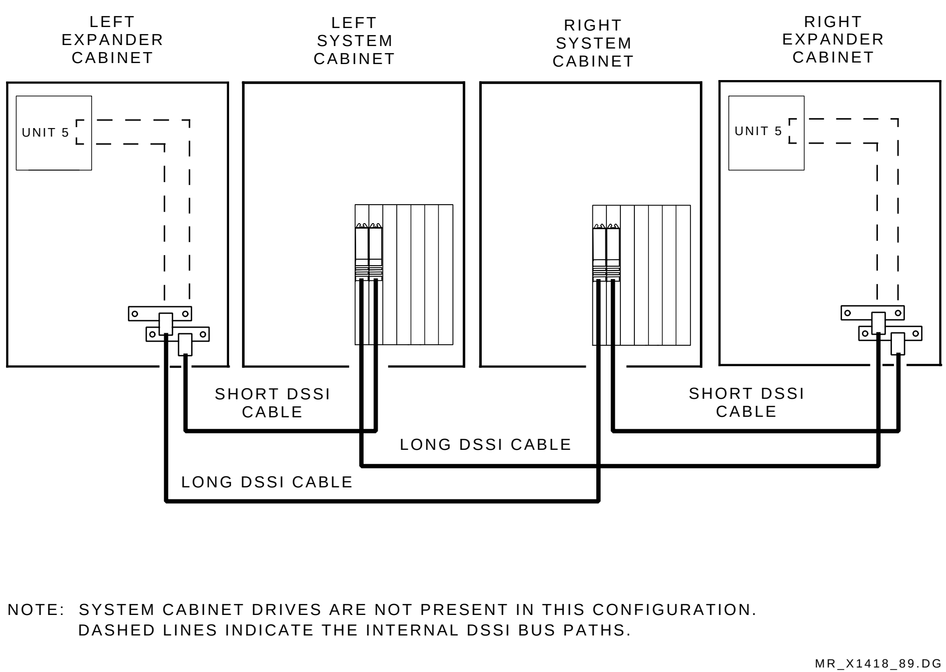
NOTE

The connectors on the system I/O controller module end of the cables must be plugged in with the cables routed downward as shown in Figure 5–4. The T-shaped connectors must be plugged in to the expander cabinets.

Route each DSSI cable between the system cabinets, behind the front wheels, and on top of the floor surface as follows. Do not bring the cables up through the cabinet access holes at this time:

1. Route a short DSSI cable from the left (adjoining) expander cabinet to the left system cabinet.
2. Route a short DSSI cable from the right (adjoining) expander cabinet to the right system cabinet.
3. Route a long DSSI cable from the left expander cabinet to the right system cabinet.
4. Route a long DSSI cable from the right expander cabinet to the left system cabinet.

Figure 5–4 Model 310 and 410 DSSI Cable Connections



Refer to Figure 5–4 as you remove and replace the DSSI cables between the system cabinets and expander cabinets.

First remove the long DSSI cables:

1. In the left system cabinet, loosen the screws that secure one end of the DSSI cable to the KFE52 I/O controller module.
2. Route the long DSSI cable connector up through the access hole into the right expander cabinet.
3. Disconnect the T-shaped connector from the upper DSSI connector (DSSI 1).
4. In the right system cabinet, loosen the screws that secure one end of the DSSI cable to the KFE52 I/O controller module.
5. Route the long DSSI cable connector up through the access hole into the left expander cabinet.
6. Disconnect the T-shaped connector from the upper DSSI connector (DSSI 1).

Now remove the short DSSI cables:

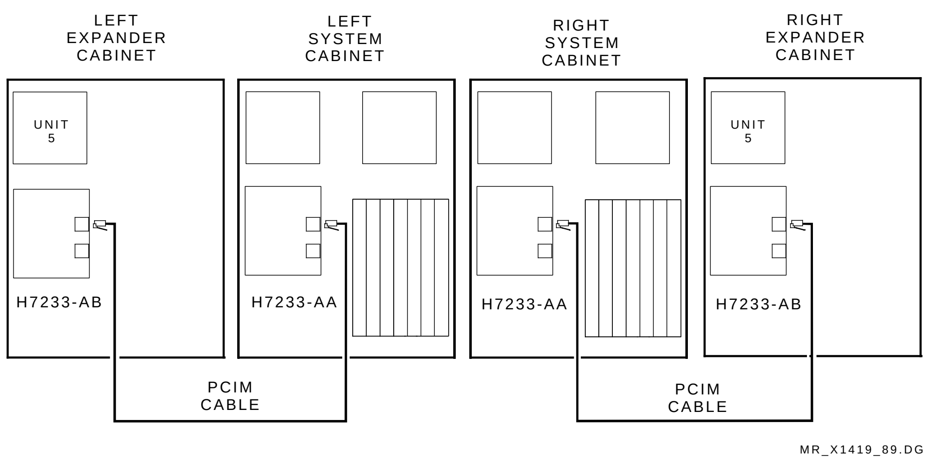
1. In the left system cabinet, loosen the screws that secure one end of the DSSI cable to the KFE52 I/O controller module.
2. Route the short DSSI cable connector up through the access hole into the left (adjoining) expander cabinet.
3. Disconnect the T-shaped connector from the lower DSSI connector (DSSI 2).
4. In the right system cabinet, loosen the screws that secure one end of the DSSI cable to the KFE52 I/O controller module.
5. Route the short DSSI cable connector up through the access hole into the right (adjoining) expander cabinet.
6. Disconnect the T-shaped connector from the lower DSSI connector (DSSI 2).

5.2.3 PCIM Cables

Locate the two PCIM cables (PN 17-02285-02).

Figure 5–5 shows how the PCIM cables are connected between the expander cabinets and system cabinets.

Figure 5–5 Model 310 and 410 PCIM Cable Connections



5.3 Logic Modules

This section describes how to remove or install a logic module in a system cabinet. Observe the module handling and ESD procedures (Section 5.3.1) whenever you remove, install, or replace a logic module in a system cabinet.

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 5.3.1 whenever you handle the logic modules.

NOTE

Before you use any of the following procedures on a system that is running, you must first contact the responsible customer representative, system manager, or application manager to shut down the zone and power off the system cabinet. The *VAXft System Services Manager's Guide* (AA-NL35A-TE) describes how to shut down the zone and power off the system cabinet from the console.

5.3.1 Module Handling and ESD Procedures

Two grounding cords are stored in the lower front door of the system cabinet (Figure 5–2). One cord is connected to a wrist strap. The other cord is connected to a grounding clip for attaching to an antistatic ESD box. When the wrist strap is in place, there must be no more than 10 MΩ through the grounding cord, wrist strap, and your wrist.

T3000-series modules are fragile and static sensitive. Use the grounding cords and observe the following precautions when handling logic modules.

- Always put on a grounded wrist strap **before** handling a logic module.
- Be sure that nothing touches the module or the components on the module because leads can be damaged. Avoid contact with the wrist strap, grounding cord, clothing, jewelry, cables, or other modules.
- Minimize any potential for physical or ESD damage as follows:
  - Remove all unnecessary materials in the service area (tools, documents, paper, plastics, polystyrene).
  - Avoid clothing that contains more than 80% nonconductive materials (silk or synthetic fiber).
  - Do not wear a jacket. Wear a short-sleeve shirt or roll up the sleeves on a long-sleeve shirt.
  - Do not wear jewelry.
  - Loose clothing, such as a necktie, must be fastened in place.
- Before removing a module from an ESD box, place the box on a clean surface. Do not allow the box to fall.

NOTE

Never place an ESD box on the floor.

- Keep the module in the antistatic ESD box until you are ready to install it.

- Before removing a module from an ESD box, attach the grounding clip to the ESD box.
- If you are replacing a module, put the module you just removed on a grounded ESD workmat on a clean surface in the service area. Put the module side 2 down on the ESD workmat.
- Save the ESD box for future use. Store a module in the ESD box until you are ready to install it.
- When removing or installing a module, be sure the module does not come into contact with a cable or another module. And be sure that nothing else touches the module or any module components.
- Hold a module **only** by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.
- Do not slide the module across any surface because the leads are fragile and can be damaged.
- An ESD sensitive module may come into contact with the following items **only**:
  - — An approved ESD workmat
  - — Antistatic packaging on the ESD workmat
  - — Tools and test equipment on the ESD workmat
  - — The chassis being serviced
  - — The hands of someone wearing an ESD wrist strap

5.3.2 Removing KA520 or KA550 Processor Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 5.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove a KA520 or KA550 processor module from slot 3 in a system backplane. Remember to observe all FRU handling procedures (Section 5.1.1).

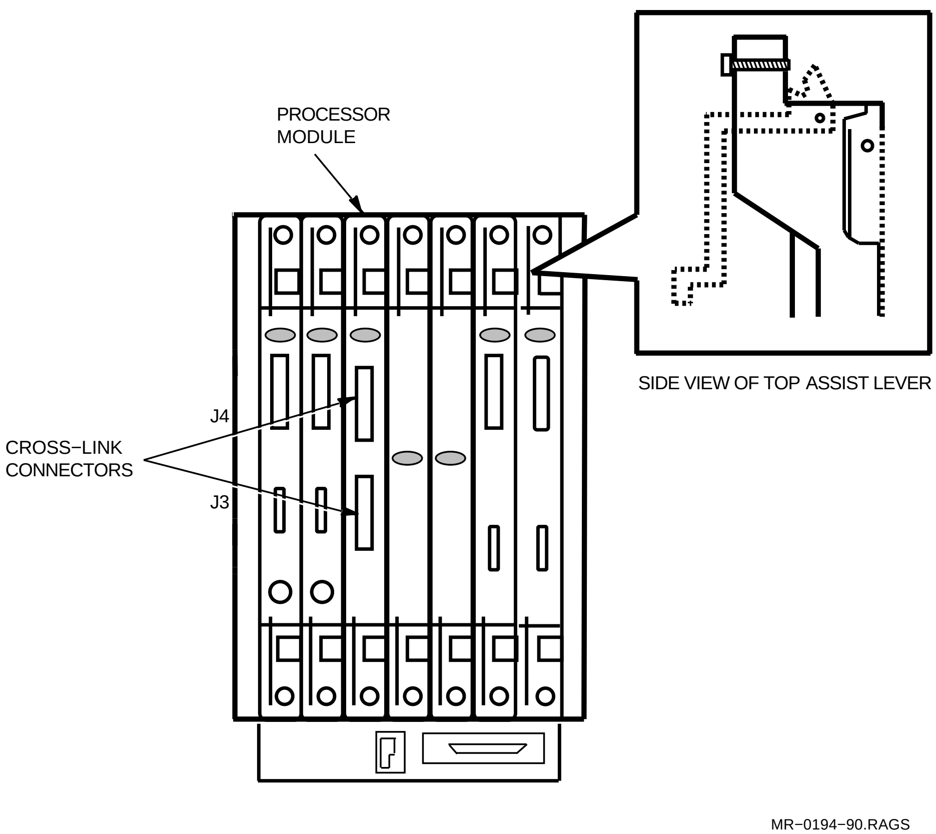
1. Ask the system manager or the operator to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Figure 5–6 shows connectors J3 and J4. Disconnect the cross-link cables from the module.
5. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

6. Use both hands to remove the module. Pull the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
7. Grasp the module handle. Slide the module out of the card cage slot.

Figure 5–6 Removing a KA520 or KA550 Processor Module



5.3.3 Removing MS520 Memory Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 5.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove an MS520 memory module from a system backplane (Figure 5–7). Remember to observe all FRU handling procedures (Section 5.1.1).

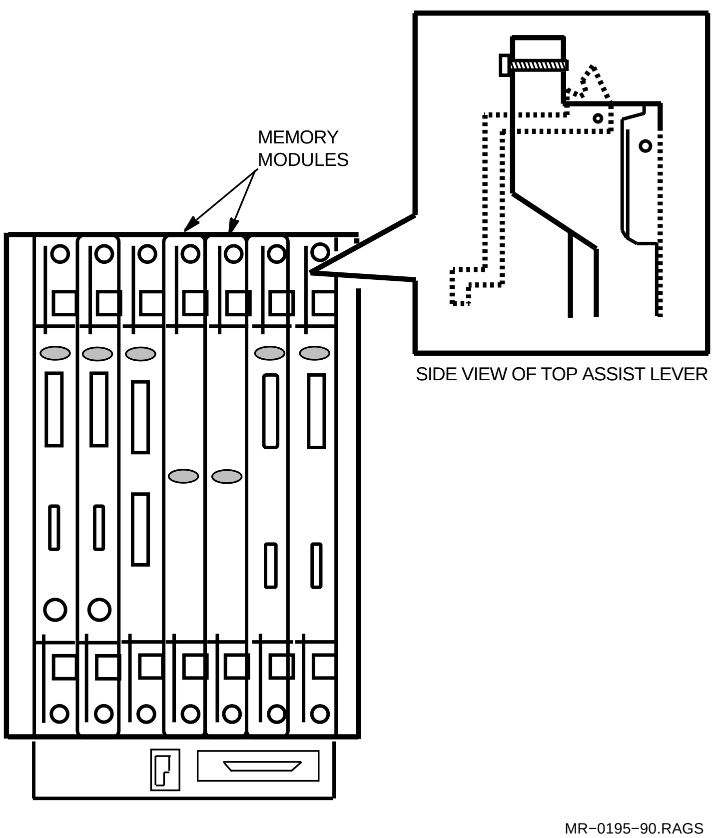
1. Ask the operator or the system manager to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

5. Use both hands to remove the module. Pull the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
6. Grasp the module handle. Slide the module out of the card cage slot.

Figure 5–7 Removing an MS520 Memory Module



5.3.4 Removing WAN 620 Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 5.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove a WAN 620 module from a system backplane. Remember to observe all FRU handling procedures (Section 5.1.1).

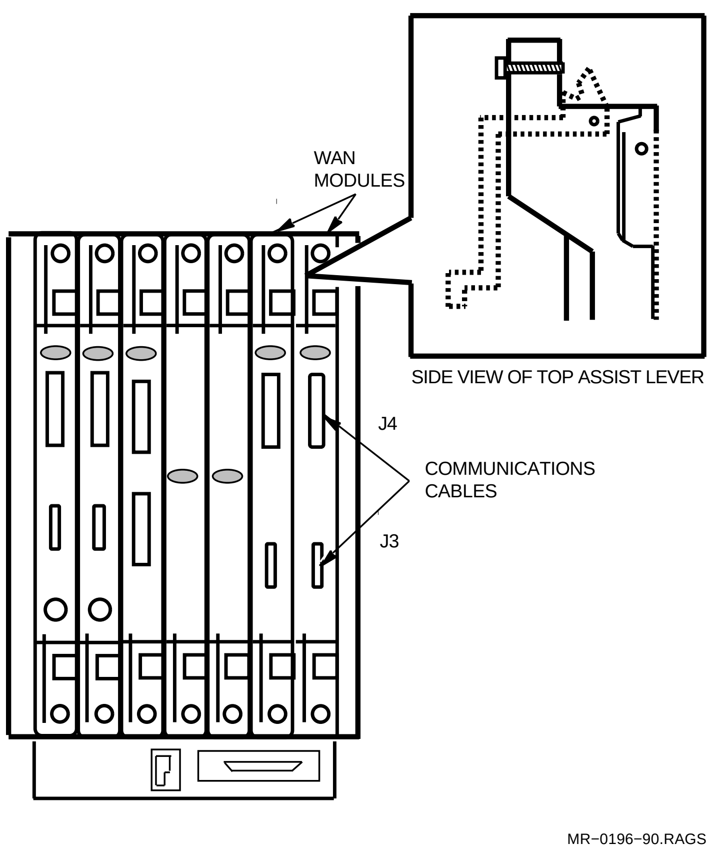
1. Ask the operator or the system manager to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Figure 5–8 shows connectors J3 and J4. Disconnect the communications cable(s) from the module.
5. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

6. Use both hands to remove the module. Pull on the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
7. Grasp the module handle. Slide the module out of the card cage slot.

Figure 5–8 Removing a WAN 620 Module



5.3.5 Removing KFE52 I/O Controller Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 5.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove a KFE52 I/O controller module from a system backplane (Figure 5–9). Remember to observe all FRU handling procedures (Section 5.1.1).

1. Ask the operator or the system manager to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Disconnect the DSSI cable or terminator from J4.

   CAUTION

   Make sure that the cable clip is unlocked before disconnecting the thickwire cable. Failure to do so may result in damage to the cable and/or the connector.

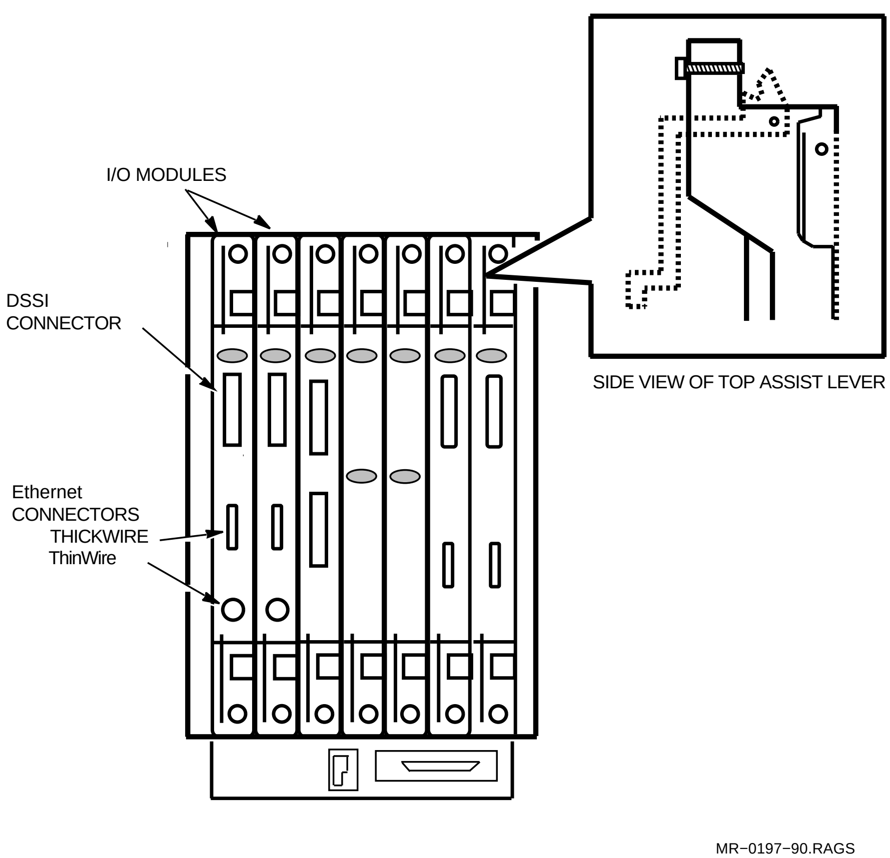
5. Disconnect the Ethernet cable if one is installed.
6. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

7. Use both hands to remove the module. Pull on the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
8. Grasp the module handle. Slide the module out of the card cage slot.

Figure 5–9 Removing a KFE52 I/O Controller Module

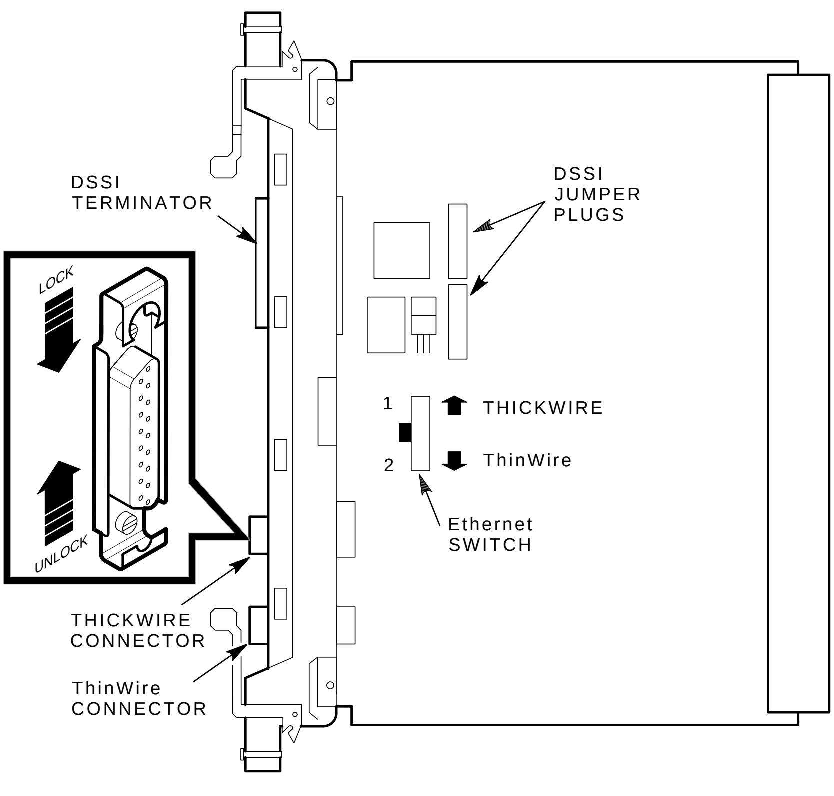


5.3.5.1 Installing/Replacing KFE52 I/O Controller Module

To install/replace a KFE52 I/O controller module:

1. Note the Ethernet switch position (Figure 5–10) on the KFE52 I/O controller module you just removed.
2. Set the Ethernet switch on the new module to the same position (up for thickwire, down for ThinWire).

Figure 5–10 KFE52 I/O Controller Module



3. Remove the DSSI jumper plugs from the new module if they were removed from the old one.[1]
4. Now reverse steps 1 through 8 of Section 5.3.5.

5.4 Carrier Disk Drive

You do not need to power off the cabinet to remove or replace an RF-series carrier disk drive. See Appendix A for detailed procedures.

Each RF-series carrier disk drive is assigned a unit number according to the slot in which it is housed. Figure 5–11 shows the slot numbers and the corresponding controls on the summary panel.

Use the following procedure to remove a carrier disk drive from a system cabinet. Remember to observe all FRU handling procedures (Section 5.1.1).

1. Ask the operator or system manager to dismount the disk to be removed.
2. Take the drive off-line by pressing the summary panel Ready/OnLine switch in. The corresponding indicator should be dark (unlit).
3. Set the drive power switch to off (0). Wait 45 seconds (for disk drive to stop spinning and interlock solenoid to release).
4. See Figure 5–12. Release the captive thumb screw. Then pull the drive straight out of the slot.

CAUTION

Use great care when removing, replacing, or transporting a drive. Do not drop the drive or allow it to come into contact with any object while you carry it.

[1] The DSSI jumper plugs are needed only on the slot-2 I/O controller module in a base system. If a second I/O controller module is added to a base system, the plugs must be removed from the second I/O controller module. The DSSI jumper plugs must also be removed from all I/O controller modules in an expanded system. An LED on the I/O controller module indicates if the plugs are installed. The *VAXft Site Preparation and Installation Guide* provides more information about the I/O controller module configuration.

Figure 5–11 Disk Drive Slot Numbers

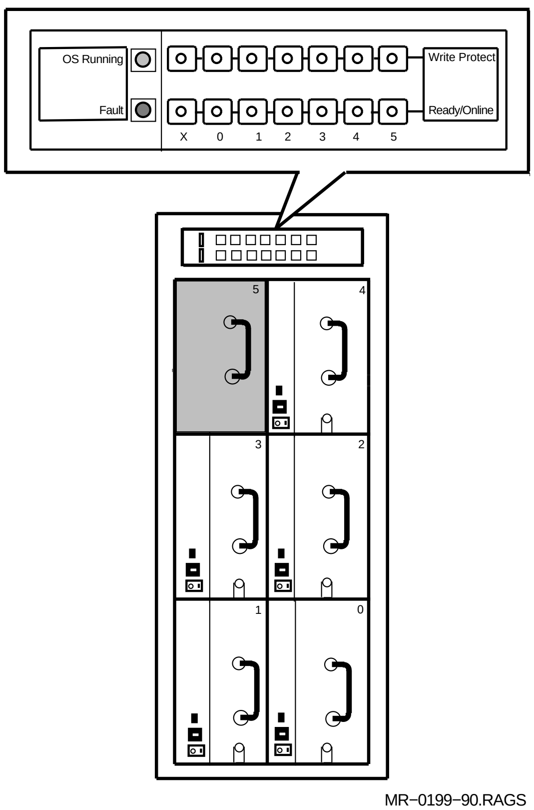
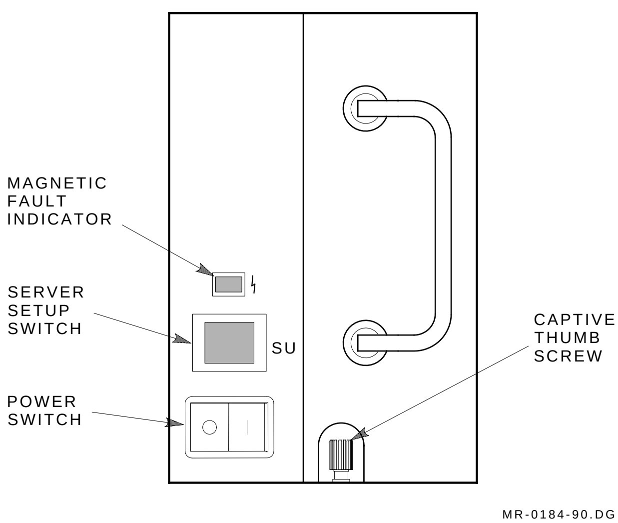


Figure 5–12 Removing a Carrier Disk Drive



5.4.1 RF-Series Controller/HDA Assembly

Use the following procedure to remove the RF-series controller/HDA assembly. Each part is a separate FRU, but because they are connected they share the same removal procedure.

1. Complete steps 1 through 4 from Section 5.4.
2. Place the carrier disk drive on a grounded antistatic mat.
3. Disconnect the three cable blocks from the disk adapter module.
4. Turn the carrier disk drive right side up.
5. Disconnect the DSSI cable.
6. Disconnect the OCP cable.
7. Disconnect the power cable.

8. Remove four Phillips screws, two from the right side, and two from the bottom of the carrier disk drive.
9. Carefully lift the controller/HDA assembly out of the carrier disk drive and place it on the grounded antistatic mat.
10. Remove the four screws that hold the controller on the HDA assembly.
11. Carefully lift the DSSI-cable-connector end of the controller to expose the top of the HDA assembly. The other end of the controller is connected by a flex cable.
12. Remove the flex cable from the controller.

5.4.2 RF-Series Disk Adapter

Use the following procedure to remove the RF-series disk adapter.

1. Complete steps 1 through 4 from Section 5.4.
2. Remove the four screws on the back of the carrier disk drive.
3. Pull the disk adapter out about 2 inches.
4. Note the placement of the six cables, and remove them.
5. Lift the disk adapter away from the carrier disk drive.

5.5 Cannister Disk Drive

You do not need to power off the cabinet to remove or replace an RF-series cannister disk drive. See Appendix A for detailed procedures.

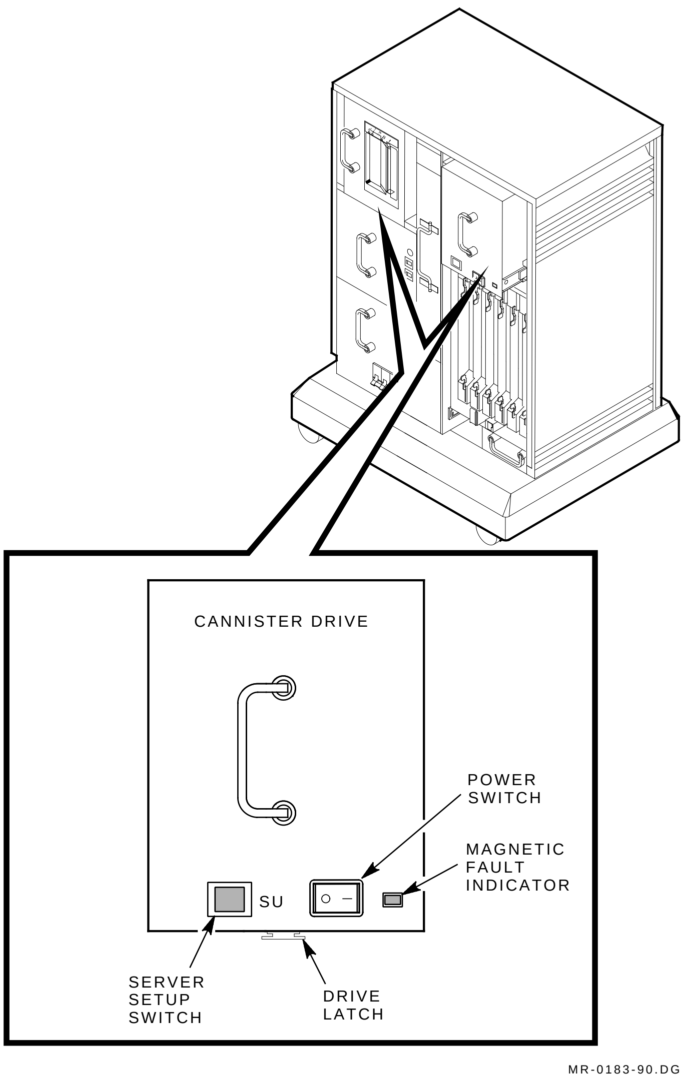
Use the following procedure to remove a cannister disk drive from a system cabinet. Remember to observe all FRU handling procedures (Section 5.1.1).

1. Ask the operator or system manager to dismount the disk to be removed.
2. Take the disk drive off-line by pressing the summary panel Ready /Online switch in. The corresponding indicator should be dark (unlit).
3. Set the drive power switch to off (0). Wait 45 seconds (for drive to stop spinning and interlock solenoid to release).
4. See Figure 5–13. Push the drive latch down and pull the drive straight out of the slot.

CAUTION

Use great care when removing, replacing, or transporting a drive. Do not drop the drive or allow it to come into contact with any object while you carry it.

Figure 5–13 Removing a Cannister Disk Drive



5.5.1 RF-Series Controller/HDA Assembly

Use the following procedure to remove the RF-series controller/HDA assembly. Each part is a separate FRU, but because they are connected they share the same removal procedure.

1. Complete steps 1 through 4 from Section 5.5.
2. Place the cannister disk drive on a grounded antistatic mat.
3. Remove four screws (two on each side) from the front plate. Remove the front plate.
4. Remove two screws from the top of the cannister, and remove the top plate.
5. Remove four screws from the back of the cannister, and pull the back plate out about 2 inches.
6. Locate the three cables that are connected to the disk adapter. Note their placement, label them if necessary, and disconnect them.
7. Remove four screws (two on each side of the cannister) that secure the shock mounts.
8. Carefully lift the controller/HDA assembly out of the cannister disk drive and place it on the grounded antistatic mat.
9. Remove the four screws and the signal connectors from the controller.

5.5.2 RF-Series Disk Adapter

1. Complete steps 1 through 4 from Section 5.5.
2. Remove four screws from the back of the cannister, and remove the back plate.
3. Note the placement of the six cables connected to the disk adapter. Label them if necessary, and then remove them.
4. Remove the disk adapter.

5.6 Cannister Tape Drive

You do not need to power off the cabinet to remove or replace a TF70 cannister tape drive. See Appendix A for detailed procedures.

1. Ask the operator or system manager to dismount the tape drive.
2. Unload the tape cartridge if one is loaded (Figure 5–14).
3. Set the drive power switch to off (0). All indicators on the tape drive should be dark (unlit).[1]
4. See Figure 5–14. Push the release tab down and pull the drive straight out of the slot.

5.6.1 TF70 Mechanical Set

1. Complete steps 1 through 4 from Section 5.6.
2. Place the cannister disk drive on a grounded antistatic mat.
3. Remove four screws (two on each side) from the front plate. Remove the front plate. See Figure 5–15, callout ❶.
4. Remove two screws from the top of the cannister, and remove the top plate. See Figure 5–15, callout ❷.
5. Remove four screws from the back of the cannister, and pull the back plate out about 2 inches. See Figure 5–15, callout ❸.
6. Locate the three cables that are connected to the tape adapter. See Figure 5–15, callout ❺. Note their placement, label them if necessary, and disconnect them.
7. Carefully lift the controller/HDA assembly (Figure 5–16, callout ❷) out of the cannister tape drive and place it on the grounded antistatic mat.
8. Remove the signal connectors from the controller module. See Figure 5–16, callout ❸.

[1] The summary panel switches have no effect on the cannister tape drives. Use the switches and indicators on the tape cartridge.

Figure 5–14 Removing a Cannister Tape Drive

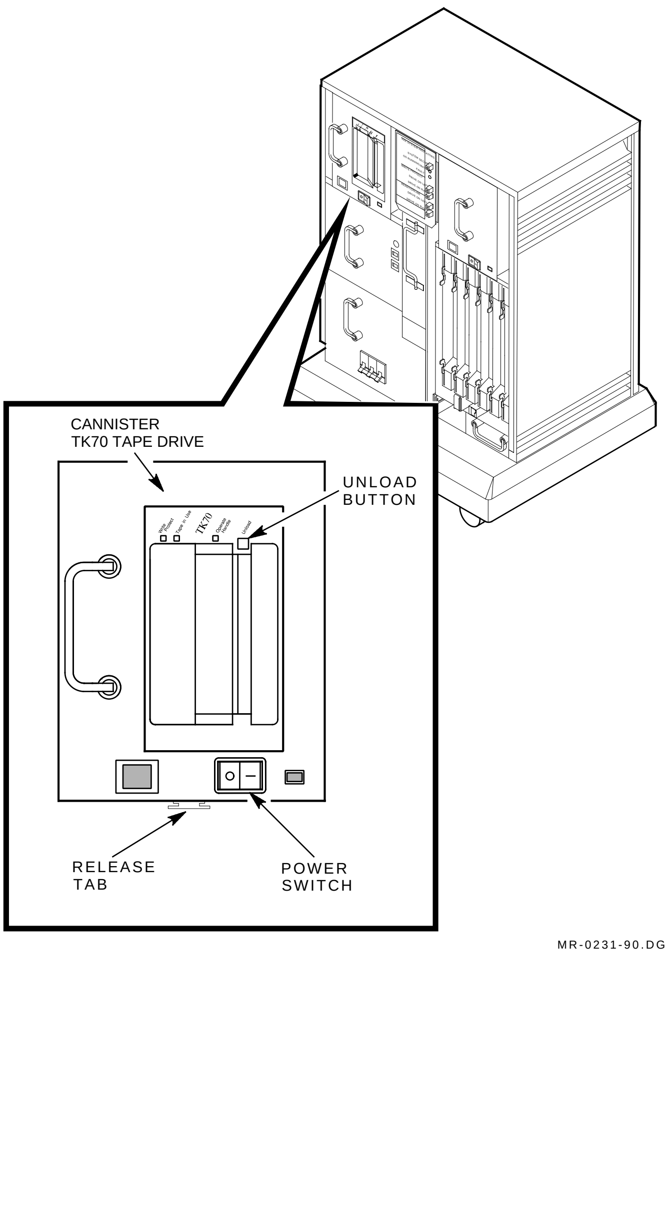
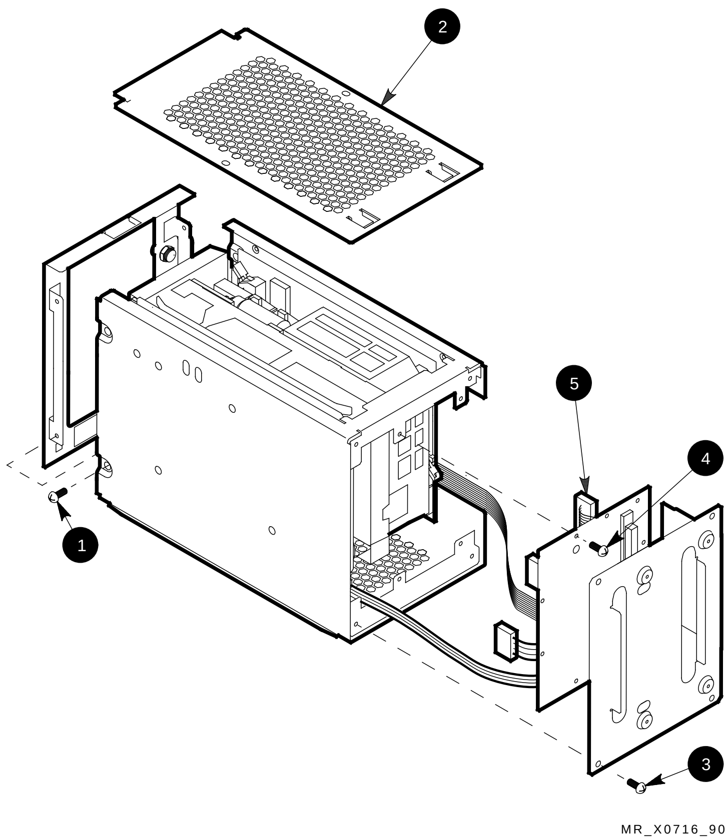


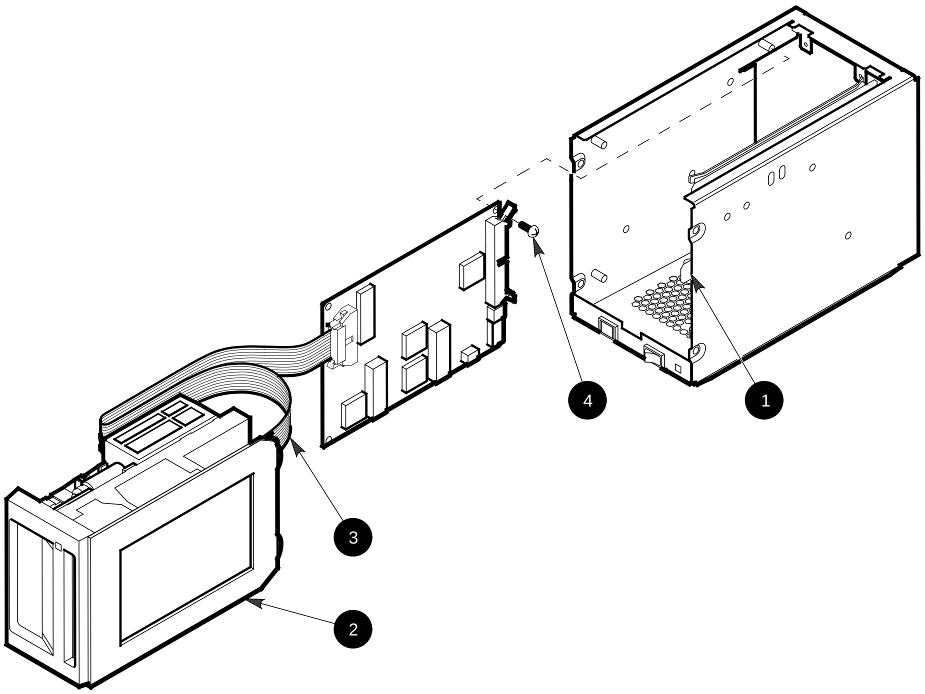
Figure 5–15 TF70 Tape Cannister



5.6.2 TF70 DSSI Controller

1. Complete steps 1 through 4 from Section 5.6.
2. Complete steps 2 through 8 from Section 5.6.1.
3. Remove the four screws that secure the controller module to the tape cannister. See Figure 5–16, callout ❹.
4. Lift the controller module out of the cannister.

Figure 5–16 TF70 Tape Cannister, DSSI Controller



5.6.3 TF70 Tape Drive Adapter

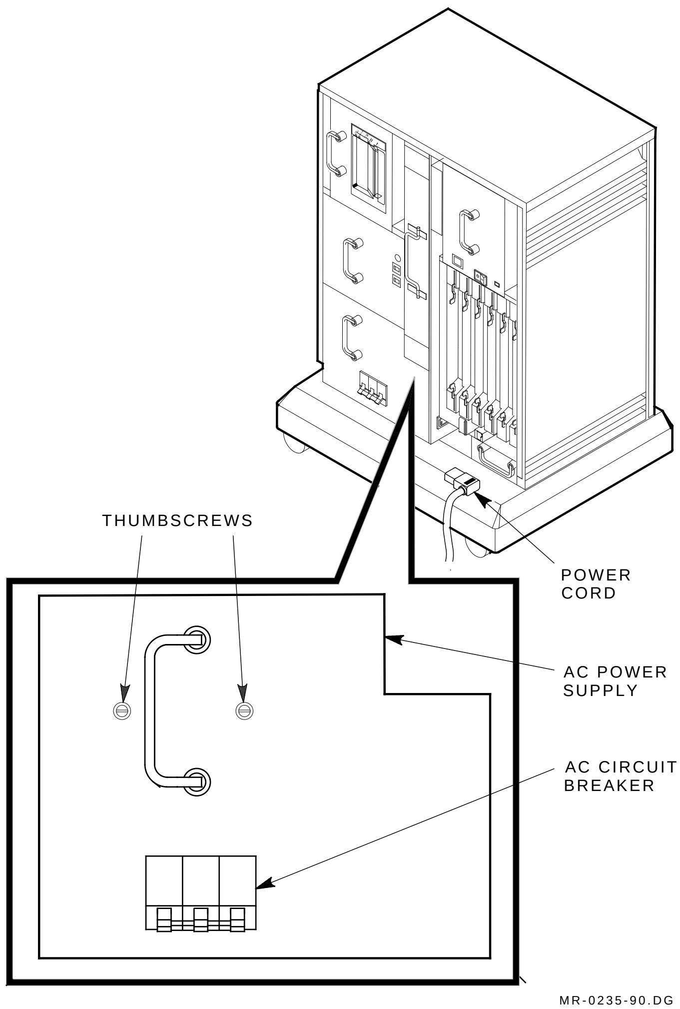
1. Complete steps 1 through 4 from Section 5.6.
2. Remove four screws from the back of the cannister, and remove the back plate. See Figure 5–15, callout ❸.
3. Note the placement of the six cables connected to the disk adapter. Label them if necessary, and then remove them. See Figure 5–15, callout ❺.
4. Remove the disk adapter.

5.7 AC Power Supply

Use the following procedure to remove the ac power supply from the system cabinet or the expander cabinet.

1. Ask the operator or system manager to shut down the zone that houses the faulty power supply. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Disconnect the ac power cord from the ac power supply (Figure 5–17).
5. Loosen the two thumbscrews by turning them to the left.
6. Grasp the handle. Pull the ac power supply out of the cabinet.

Figure 5–17 AC Power Supply



5.8 DC Power Supply

The dc power supply for the expander cabinet differs slightly from the dc power supply for the system cabinet. They are **not** interchangeable, so make sure you have the correct part:

H7233-AA	System cabinet dc power supply
H7233-BA	Expander cabinet dc power supply

Use the following procedure to remove a dc power supply.

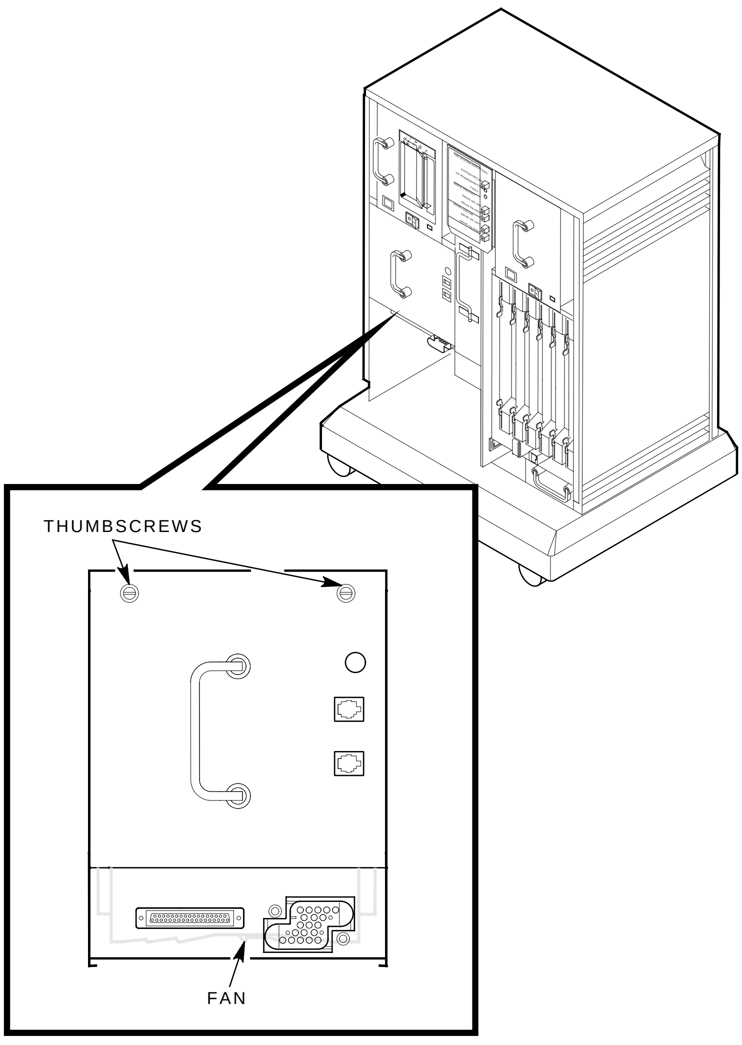
1. If any PCIM cables are attached to the dc power supply, note their location, label them if necessary, and disconnect them.
2. Remove the ac power supply. (See Section 5.7.)
3. See Figure 5–18. Loosen the two thumbscrews by turning them to the left.

CAUTION

Support the weight of the dc power supply as you pull it out of the cabinet. If you drop it, damage to the internal components could result.

4. Grasp the handle. Pull the dc power supply out of the cabinet.

Figure 5–18 DC Power Supply



5.9 Uninterruptible Power Supply

The uninterruptible power supply (UPS) provides battery backup to the entire cabinet for up to 15 minutes following power failure.

CAUTION

Never install a cold UPS in a VAXft system because damage to the UPS could result. If the replacement UPS was in an environment where the temperature was below freezing, allow it to come up to room temperature before you install it.

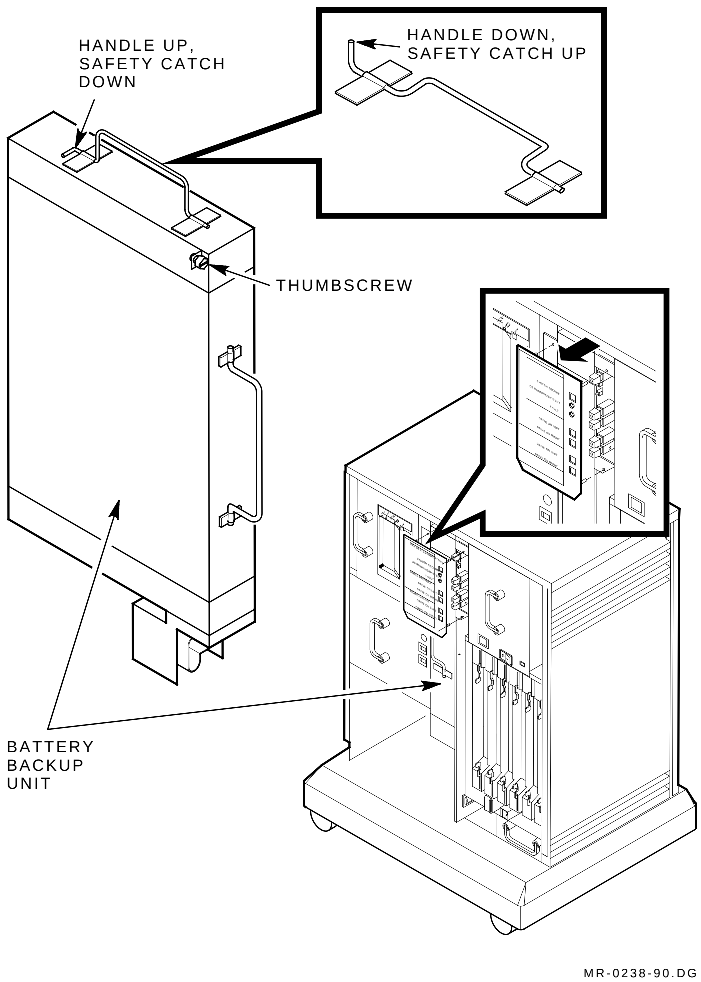
Use the following procedure to remove a UPS from a system cabinet or an expander cabinet.

WARNING

The UPS battery backup unit is very heavy. It weighs approximately 17.3 kg (38 lb). Use great care when lifting and handling it.

1. Ask the operator or system manager to shut down the zone that houses the faulty UPS. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the ac power supply. (See Section 5.7.)
5. Remove the summary panel cover from the system or expander cabinet by pulling it straight out. The cover is secured with four standoffs and should snap off easily.
6. See Figure 5–19. Loosen the thumbscrew by turning it to the left.
7. Slide the UPS toward you. The catch at the top of the unit should stop you when the UPS is about 3/4 of the way out of the cabinet.
8. Raise the handle at the top of the unit. This releases the catch.
9. Carefully slide the UPS completely out of the cabinet.

Figure 5–19 Uninterruptible Power Supply

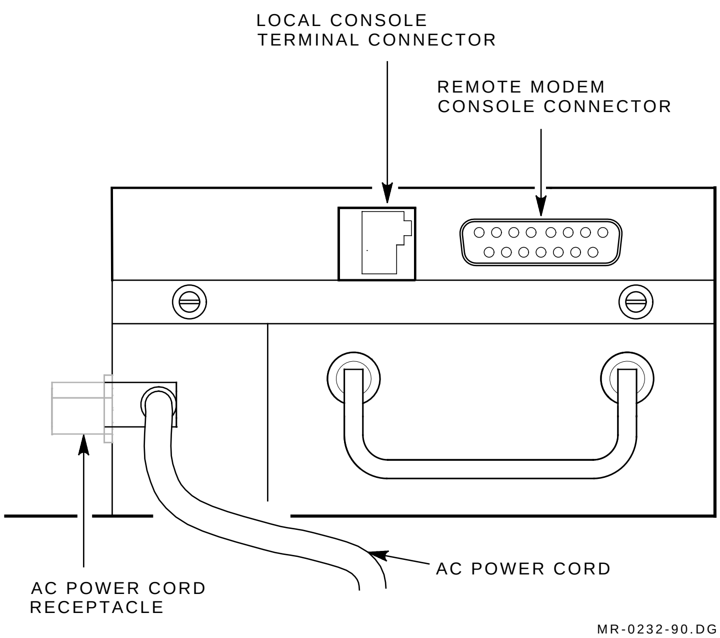


5.10 System Cabinet Fan

The system cabinet has two fans. The system cabinet fan is located beneath the logic card cage, and the dc power supply fan is located inside the dc power supply assembly. If one of these fans needs to be replaced, you should replace the other fan at the same time.

1. Ask the system manager or operator to shut down the zone that houses the faulty fan. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Note the placement of all cables connected to all modules, and label them if necessary. Disconnect all module cables and tuck them under the system cabinet or base cap.
5. Disconnect the ac power cord from the ac power supply (Figure 5–20).
6. Remove the local and remote console cables from the modem port and tuck them under the system cabinet or base cap.
7. Loosen the two thumbscrews by turning them to the left.
8. Remove the fan by sliding it straight out of the system cabinet.

Figure 5–20 System Cabinet Fan



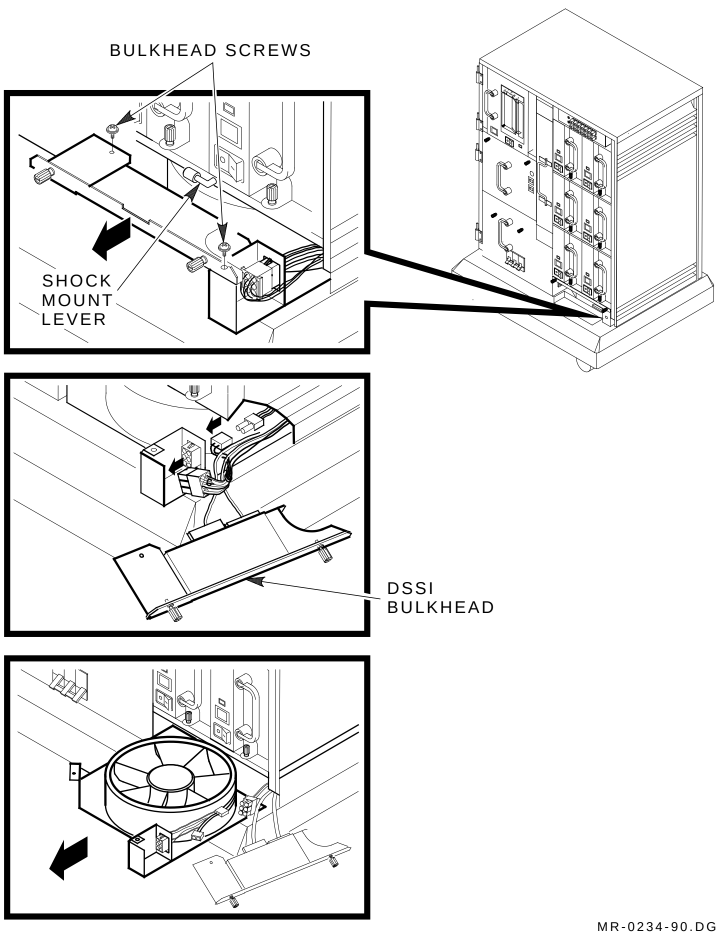
5.11 Expander Cabinet Fan

The expander cabinet has two fans. The expander cabinet fan is located beneath the six-pack backplane, and the dc power supply fan is located inside the dc power supply assembly. If one of these fans needs to be replaced, you should replace the other fan at the same time.

1. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
2. To power off the expander cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
3. Disconnect the ac power cord from the ac power supply (Figure 5–20).
4. Note the placement of the DSSI cables, label them if necessary, and disconnect them from the DSSI bulkhead.
5. Loosen the two thumbscrews by turning them to the left (Figure 5–21).
6. Slide the fan assembly toward you until it is about 1/4 of the way out of the cabinet.
7. Raise the shock mount lever.
8. Disconnect the fan power cable.
9. Disconnect the fan control cable.
10. Remove the two Phillips screws from the DSSI bulkhead.
11. Lift the DSSI bulkhead assembly off the fan assembly, and place it to the right.
12. Remove the fan assembly by sliding it straight out of the expander cabinet.

When replacing the fan assembly, angle it up towards the back for proper alignment.

Figure 5–21 Expander Cabinet Fan



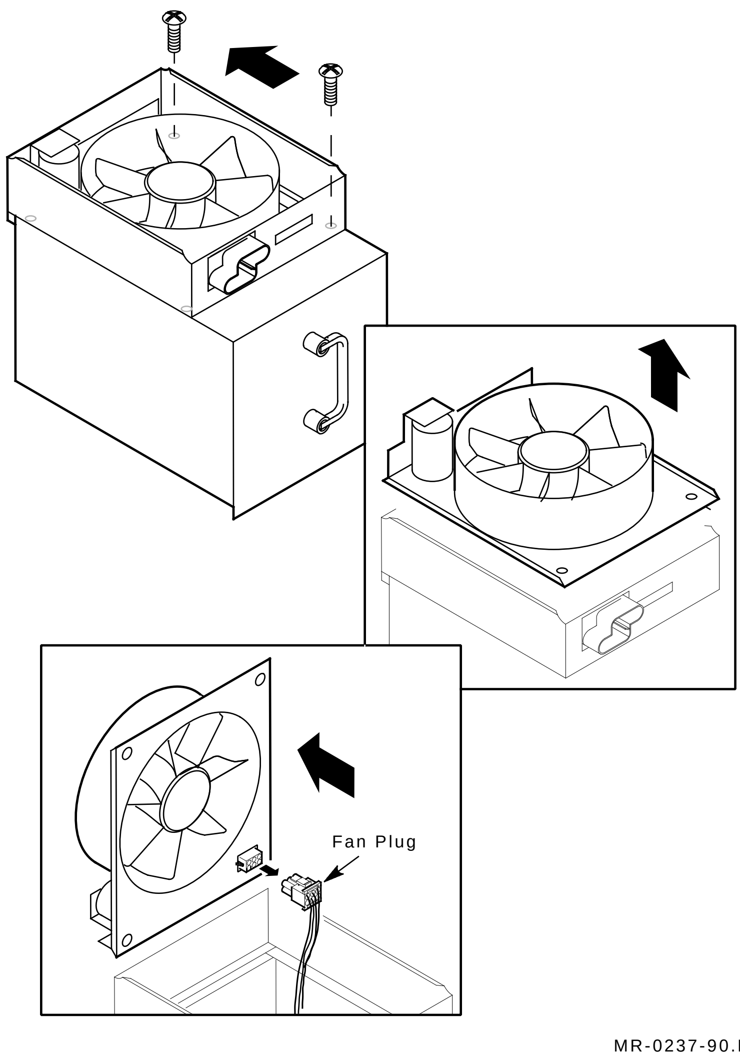
5.12 DC Power Supply Fan Assembly

Both the system cabinet and the expander cabinet have two fans. One fan is located in the lower right side of the cabinet, and the other fan is located inside the dc power supply assembly. If one of these fans needs to be replaced, you should replace the other fan at the same time.

Use the following procedure to remove a dc power supply fan from the system or expander cabinet.

1. Ask the system manager or operator to shut down the zone that houses the faulty fan. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the dc power supply (Section 5.8).
5. Place the dc power supply upside down on a grounded antistatic mat.
6. Remove four slotted hex screws (one in each corner) from the fan assembly (Figure 5–22).
7. Lift the rear of the fan assembly slightly.
8. Slide the fan assembly to the back and under the cable connectors on the dc power supply.
9. Lift the fan assembly to expose the fan plug.
10. Disconnect the fan plug.
11. Lift the fan assembly up and away from the dc power supply.

Figure 5–22 DC Fan Assembly

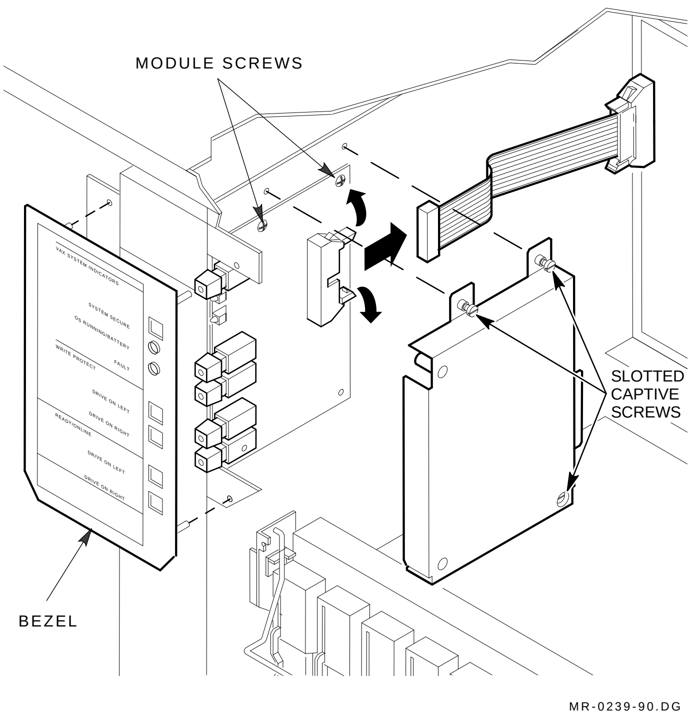


5.13 System Cabinet Summary Panel

Use the following procedure to remove a summary panel from a system cabinet.

1. Ask the system manager or operator to shut down the zone that includes the faulty panel. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the summary panel cover by pulling it away from the system cabinet. The panel cover is secured with four standoffs and should pull off easily.
5. Remove the device in the top-right peripheral slot (Section 5.5).
6. Remove three slotted screws that hold the summary panel in place (Figure 5–23).
7. Pull the summary panel (bezel) away from the cabinet.
8. Disconnect the summary panel cable by releasing the pushlocks, and then tugging on the pull tab.
9. Remove the two module screws (Figure 5–23).

Figure 5–23 System Cabinet Summary Panel

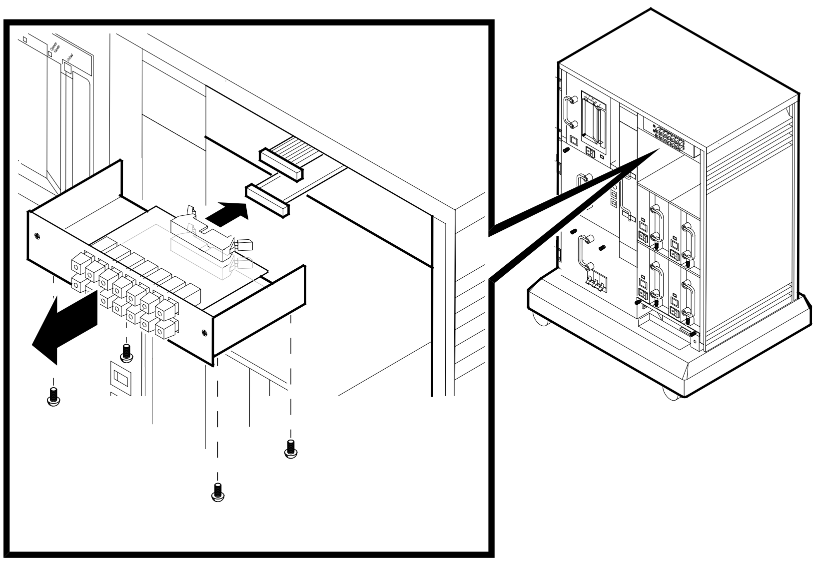


5.14 Expander Cabinet Summary Panel

Use the following procedure to remove a summary panel from an expander cabinet.

1. Ask the system manager or operator to shut down the zone that includes the faulty panel. (Zone shutdown is described in Section 5.1.2.)
2. Open or remove both front doors. (This procedure is described in Section 5.1.4.)
3. To power off the expander cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the summary panel cover by pulling it away from the expander cabinet. The panel cover is secured with four standoffs and should pull off easily.
5. Remove the devices in peripheral slots 6 and 7 (Section 5.4).
6. Loosen the four screws that hold the summary panel in place (Figure 5–24).
7. Release the summary panel by pulling it forward and pushing it up.
8. Locate the two summary panel cables, and label them if necessary. Be sure you do not mix them up.
9. Disconnect the summary panel cable by releasing the pushlocks, and then tugging on the pull tab.

Figure 5–24 Expander Cabinet Summary Panel



MR-0240-90.DG

5.15 Console Protection Module

Use the following procedure to remove a console protection module.

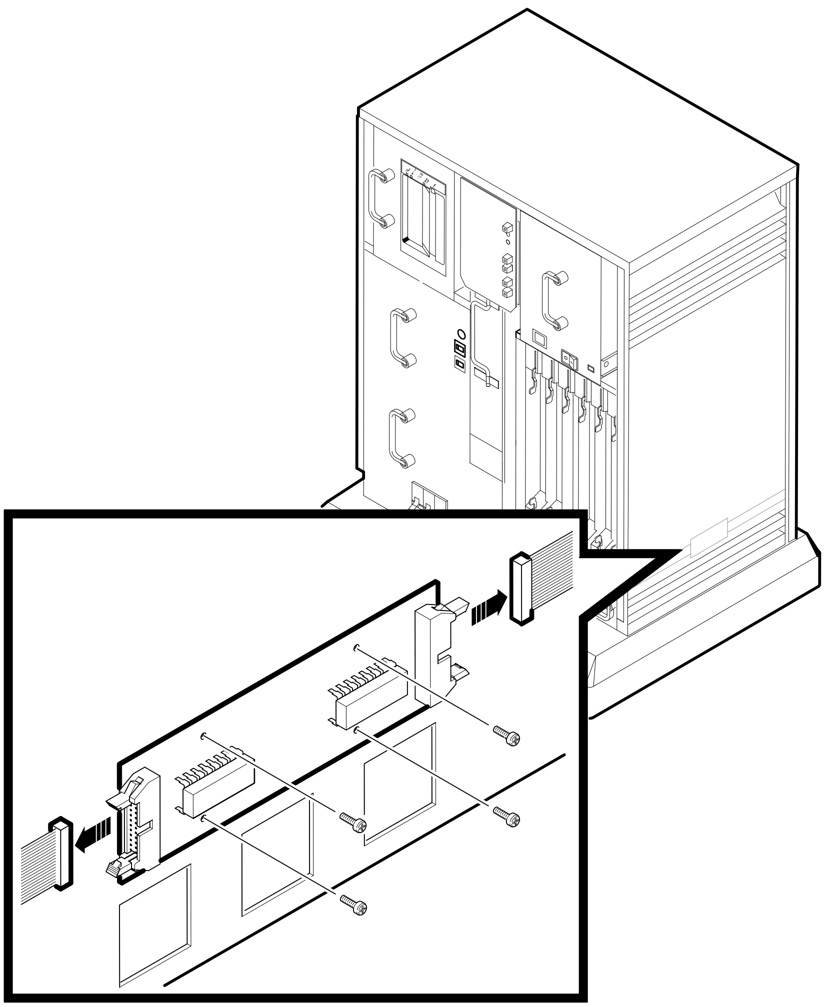
1. Remove the system cabinet fan. (See Section 5.10.)
2. Locate the console protection module. It is connected to the right side of the system cabinet behind the console cable connectors (Figure 5–25).
3. Disconnect the cable at the front of the console protection module.
4. Remove the four screws that hold the console protection module in place.

CAUTION

Make sure you use the same screws when you replace the console protection module. The wrong size screw could short out components on the module.

5. Pull the console protection module away from the cabinet.
6. Disconnect the cable at the back of the console protection module.

Figure 5–25 Console Protection Module



5.16 Cabinet Skins

Use the following procedure to remove the skins from the system or expander cabinet.

1. With the key, turn the latch to the down (open both doors) position.
2. Pulling from the right side of the door, swing the upper door open.
3. Lift the upper door from its hinges, and set it aside.
4. Pulling from the right side of the door, swing the lower door open.
5. Lift the lower door from its hinges, and set it aside.
6. Remove the hinge and set it aside.
7. Remove the door latch bracket.
8. Remove eight screws (five on the left side and three on the right side) from the front flange of the cabinet.
9. Remove the sides, top, and back of the cabinet. Grasp each of these pieces and push it up and away from the cabinet.

5.17 System Cabinet Card Cage

Whenever you replace the card cage, you should also replace the following cables.

- Disk PCIM cable
- Disk control cable
- DSSI/logic cable
- Lower fan cable

Use the following procedure to remove the card cage from the system cabinet.

1. Ask the system manager or operator to shut down the zone that houses the faulty card cage. (Zone shutdown is described in Section 5.1.2.)
2. Remove the cabinet skins. (See Section 5.16.)

3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the device in the right peripheral slot. (See Section 5.5.)
5. Remove all modules from the card cage.
6. Remove the system cabinet fan. (See Section 5.10, steps 4 through 8.)
7. Disconnect the summary panel cable from the DSSI backplane.
8. Disconnect the fan power and control cable.
9. Disconnect the console protection module cable.
10. At the back of the system, remove 20 screws around the edge of the back cover plate. Remember to support the weight of the cover plate as you do this.
11. Set the back cover plate aside.
12. Remove the eight screws that secure the flex circuit to the backplane.
13. Locate the four power distribution cables and label them if necessary.
14. Remove the four screws that secure the power distribution cables on the backplane.
15. Disconnect the cable from J8, and cut any tie wraps that secure it on the backplane.
16. Disconnect the cable from J15, and cut any tie wraps that secure it on the backplane.
17. Disconnect the cable from J12, and cut any tie wraps that secure it on the backplane.
18. Loosen slightly the 10 screws that secure the backplane on the cabinet frame.
19. Remove the 10 screws while supporting the weight of the backplane.

5.18 DSSI Backplane

The peripheral device in the left side of the cabinet uses its own backplane, called the DSSI backplane. Whenever you replace the DSSI backplane, you should also replace the following cables.

- Disk control cable
- DSSI/logic cable

Use the following procedure to replace the DSSI backplane in the system or expander cabinet.

1. Ask the system manager or operator to shut down the zone that houses the faulty DSSI backplane. (Zone shutdown is described in Section 5.1.2.)
2. Remove the cabinet skins. (See Section 5.16.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the device in the left peripheral slot. (See Section 5.5.)
5. At the back of the system, remove 20 screws around the edge of the back cover plate. Remember to support the weight of the cover plate as you do this.
6. Set the back cover plate aside.
7. If you are removing the DSSI backplane from an expander cabinet, disconnect the DSSI cable.
8. Disconnect the summary panel cable from J2.
9. Disconnect the DSSI interplane cable from J3 and J4 in the expander cabinet.
10. Locate the four power distribution cables and label them if necessary.
11. Remove the four screws that secure the power distribution cables on the backplane.
12. Loosen slightly the six screws that secure the backplane on the cabinet frame.
13. Remove the six screws while supporting the weight of the backplane.

5.18.1 Replacement

1. Set the address jumpers (W1 through W3) on the new backplane to match the jumpers on the backplane you removed.

NOTE

If you fail to set the address jumpers correctly, the system could crash or be unable to recognize the peripheral devices.

2. If you are replacing the DSSI backplane in a system cabinet, move the DSSI terminator from the old backplane to the new one.
3. Reverse steps 1 through 13 from Section 5.18.

5.19 Six-Pack Backplane

Whenever you replace the six-pack backplane, you should also replace the following cables.

- Disk PCIM cable
- Disk control cable
- DSSI/logic cable

Use the following procedure to remove the six-pack backplane from the expander cabinet.

1. Ask the system manager or operator to shut down the zone that houses the faulty six-pack backplane. (Zone shutdown is described in Section 5.1.2.)
2. Remove the cabinet skins. (See Section 5.16.)
3. To power off the expander cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove all disks from the six-pack backplane.
5. At the back of the system, remove 20 screws around the edge of the back cover plate. Remember to support the weight of the cover plate as you do this.
6. Set the back cover plate aside.
7. Disconnect the summary panel cable from J12.
8. Disconnect the cable from J11.
9. Disconnect the interplane cable from J10.

10. Disconnect the DSSI to DSSI backplane cables from J7 and J9.
11. Disconnect the fan assembly to PCIM cable from J8, and cut any tie wraps that secure the cable on the backplane.
12. Disconnect the DSSI to bulkhead cables from J14 and J15.
13. Disconnect the fan assembly cable from J13.
14. Check the 16 power distribution cables and label them if necessary.
15. Remove the 16 screws that secure the power distribution cables on the backplane.
16. Loosen slightly the 12 screws that secure the backplane on the cabinet frame.
17. Remove the 12 screws while supporting the weight of the backplane.

6

Model 610 and 612 Removal and Replacement Procedures

This chapter describes how to remove and replace the model 610 and 612 field replaceable units (FRUs), which include the following:

- System cables
- System modules
- Power supplies
- Fans
- Peripheral devices
- Backplanes
- Summary panel

When specific installation/replacement procedures are not given, replace or install an FRU by reversing the steps in the removal procedure.

NOTE

Throughout this chapter, the DSF32 module is referred to as the WAN module.

A complete list of the model 610 and 612 FRUs is given in Table 6–1. A list of the WAN module diagnostic tools is given in Table 6–2.

Table 6–1 Model 610 and 612 FRUs

FRU	Part Number
KA550 processor module	T3007-AA
WAN 620 module (DSF32)	T3004-AA
KFE52 I/O controller module	T3001-AA
MS520 memory module (32 MB)	MS520-BA
MS520 memory module (64 MB)	MS520-CA/CB
RF31 cannister drive assembly	RF31-JA
RF31 carrier drive assembly	RF31-KA
RF31 disk drive adapter	54-19250-01
RF31 DSSI controller	54-18329-01
RF31 HDA assembly	70-24697-01
TF857-CA cannister tape drive assembly	TF857-CA
TF70C cannister tape drive assembly	TF70C-AA
TK70 drive	TK70-EA
TF70 tape drive adapter	54-20211-01
TF70 DSSI controller	54-19085-01
TF85 cannister tape drive assembly	TF85-AA
TK85 HDA assembly with DSSI controller	TF85-BA
RF72 cannister drive assembly	RF72-JA
RF72 carrier drive assembly	RF72-KA
RF72 DSSI controller	54-19091-01
RF73 cannister drive assembly	RF73-JA
RF73 carrier drive assembly	RF73-KA
RF72 HDA assembly	70-25972-01
Backplane assembly, CPU cabinet	70-27877-01
Six-pack backplane, expander cabinet	54-19483-01
Module, backplane drive	54-19260-02

Table 6–1 (Continued) Model 610 and 612 FRUs

FRU	Part Number
Summary panel, system cabinet	54-19481-01
Summary panel, expander cabinet A	54-19485-01
Summary panel, expander cabinet B	54-19485-02
AC power supply	H407-A
DC power supply, system cabinet	H7233-AA
DC power supply, expander cabinet	H7233-BA
AC distribution box, 120 V	888-A
AC distribution box, 240 V	888-B
Uninterruptible power supply (UPS)	30-29639-01[1]
Fan assembly, system cabinet	70-26102-01
Fan assembly, expander cabinet	70-26107-01
Fan assembly, dc power supply	70-26865-01
Cable, cross-link	17-02194-01
Cable, PCIM	17-02285-02
Cable, DSSI unterminated, 40-inch, white	17-02420-01
Cable, DSSI with terminator, 39-inch, red	17-02245-01
Cable, DSSI with terminator, 62-inch, blue	17-02245-02
Cable, DSSI with terminator, 84-inch, green	17-02245-03
Cable, DSSI unterminated, 40-inch, white	17-03023-01
Cable, synchronous communication	17-02390-01
Cable, synchronous communication monitor	17-02740-01
Personality cable type RS-422, V.11	17-01108-01
Personality cable	17-01109-01
Personality cable type RS-232, V.24	17-01110-01

[1]The UPS is not stocked locally because the shelf life of the battery is relatively short. This part must be P-1 ordered.

Table 6–1 (Continued) Model 610 and 612 FRUs

FRU	Part Number
Personality cable type RS-423, V1.0	17-01111-01
Personality cable type V.35	17-01112-01
Cable, disk PCIM	17-02120-01
Cable, disk control	17-02121-01
Cable, DSSI logic	17-02122-01
Cable, lower fan	17-02266-01
Cable	17-02362-01
Y-box	70-27483-01
100-pin terminator	12-33191-01
DSSI terminator	12-29258-01
AC power cord, 47–63 Hz, 120 Vac	17-00442-17
AC power cord, 47–63 Hz, 120 Vac	17-00442-38
AC power cord, 47–63 Hz, 120 Vac	17-00442-39

Table 6–2 WAN Module Diagnostic Tools

Tool	Part Number
100-pin loopback	12-33192-01[1]
20-pin loopback	12-33193-01[1]
Universal loopback	12-25852-01 (H3199)
Personality loopback V.35	H3250
Personality loopback RS-232, V.24	H3248
Personality loopback RS-422, 423, 449, V.11	12-26259-01 (H3198)
Personality loopback X.21	12-26811-01 (H3047)

[1] A 100-pin and a 20-pin loopback ships with every WAN option.

6.1 Before You Begin

WARNING

Hazadous voltages exist within the system. Bodily injury or equipment damage can result when service procedures are performed incorrectly.

NOTE

FRUs should be removed/replaced only by qualified maintenance personnel.

You do not need to shut down the entire VAXft system to remove and replace an option or FRU. In most cases, you can shut down the zone that houses the failing FRU while the other zone continues to operate. (Section 6.1.2 explains how to shut down a zone.)

There are two types of FRU removal and replacement procedures: *cold swaps*, and *warm swaps*. During a cold swap, you shut down the zone that houses the failing FRU while the operating software continues to run in the other zone. FRUs that require a cold swap include the logic modules, fans, battery backup unit, backplanes, power supplies, and the summary panel.

During a warm swap, all cabinets remain powered on. The application continues to run in both zones while the FRU is replaced. FRUs that allow a warm swap include the cannister tape drive, the cannister disk drive, and the carrier disk drive. A cold swap of the disk and tape drives can be performed when the cabinet that houses the drives is permitted.

6.1.1 Model 610 and 612 FRU Handling

Static electricity can damage the FRUs. Use an ESD wrist strap and a grounded ESD workmat whenever you perform removal and replacement procedures. Wear the wrist strap and attach both the wrist strap and the grounded workmat to the system chassis.

Spare FRUs are shipped in an antistatic ESD box. Before you open the ESD box, attach a ground strap from the ESD box to the system chassis.

Use great care when handling the FRUs. Do not drop them or bump them.

6.1.2 Shutting Down a Zone

Cold swap procedures require you to shut down the zone where the removal and replacement is to take place. A red Fault indicator on the summary panel blinks to identify the zone that houses the faulty FRU.

Typically, the shutdown is performed by the system manager or the operator because it requires CMKRNL privileges. Before shutting down the zone, use the SHOW ZONE command to see the status of each zone. The system lists one of the following status messages for each zone.

- Active — The zone is running.
- Stopped — The zone is not running the system software. It may be running diagnostics or is available for synchronizing.
- Absent — The zone is not available.
- Synchronizing — The zone is in the process of synchronizing with the other zone.
- Providing I/O only — The zone has detected a CPU/MEM fault, and has placed the CPU and memory off-line.

The DCL command STOP/ZONE *zone-id* shuts down the zone. Example 6–1 shows how to shut down a zone. User input is underlined.

Example 6–1 How to Shut Down a Zone

```
$ SHOW ZONE                         ! Displays the status of each zone.
  Zone A is ACTIVE                  ! Zone A is running.
  Zone B is PROVIDING I/O ONLY      ! Zone B has a faulty component.

$ STOP/ZONE B                       ! Shuts down zone B.
```

At the console terminal of the zone that continues to run (in this case, zone A), the OPCOM messages show that synchronization has been lost with the other zone, and that virtual circuits are closed.

The SHOW ZONE command may be used to verify that the STOP/ZONE *zone-id* command executed correctly. Example 6–2 shows how to verify the zone is shut down. User input is underlined.

Example 6–2 How to Verify the Zone is Shut Down

```
$ SHOW ZONE                       ! Displays the status of each zone.
  Zone A is ACTIVE                ! Zone A is running.
  Zone B is ABSENT                ! Zone B has been shut down.
```

6.1.3 Starting Up a Zone

NOTE

The zone to be started must be in the stopped state prior to the START/ZONE command being issued for successful execution.

Typically, the startup is performed by the system manager or the operator because it requires CMKRNL privileges. The DCL command START /ZONE *zone-id* starts up the zone after a shutdown.

6.1.4 Accessing the Model 610 and 612 FRUs

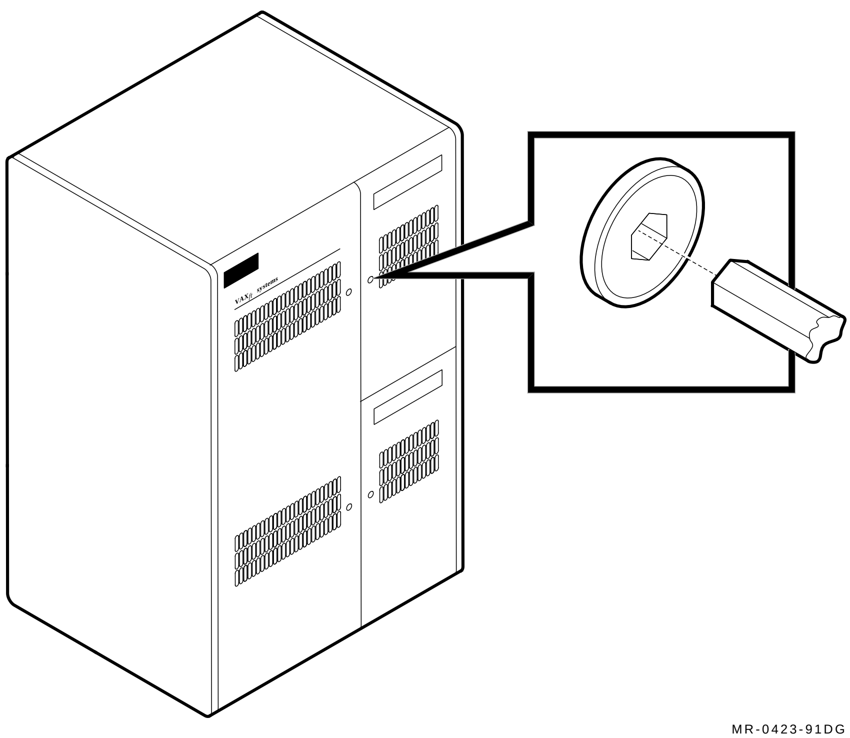
Figure 6–1 shows the front doors of the model 610 system cabinets. Figure 6–2 shows the location of the ESD kit. A special key must be used to open the doors and is supplied with each cabinet.

- The left door provides access to the logic modules and power supplies in zones A and B.
- The upper and lower right doors provide access to the summary panels, ac distribution boxes, and tape options in zones A and B.

CAUTION

Installation and maintenance procedures may be performed only by qualified personnel. They must be familiar with the electrostatic discharge (ESD) procedures and power procedures for the VAXft system. Excessive shock or incorrect handling can damage the logic modules.

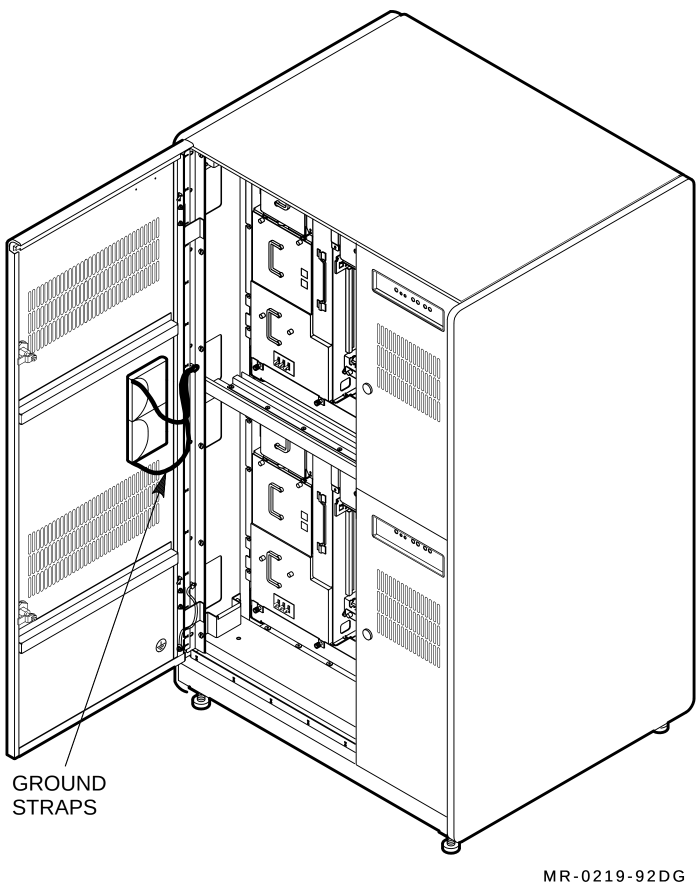
Figure 6–1 Model 610 Cabinet Front Doors



Use the following procedure to open the cabinet front doors.

1. Insert the special key as shown in Figure 6–1 and turn it to the left.
2. Swing the doors open (Figure 6–2).
3. Remove the ground straps from the pouch on the left door, and put on the ESD wrist strap.

Figure 6–2 Model 610 Cabinet, Front Doors Open



6.1.5 Filler Modules and Blank Slots

Each system cabinet contains a card cage with seven slots. A module **must** be present in each of the seven slots to maintain cooling airflow. When a configuration does not use all the card cage slots, T3999 filler modules are placed in the unused slots.

In the future, add-on options may require the removal of a filler module to make a card cage slot available. Also, future deinstallation options may require use of a filler module to replace the removed module.

A module **must** be present in each of the DSSI backplane slots to maintain cooling airflow. When a configuration does not use all the DSSI backplane slots, blank cannister modules are placed in the disk or tape cannister slots.

In an expander cabinet, blank carrier modules are placed in all unused six-pack backplane slots.

6.2 System Cables

This section describes how to remove and replace the following system cables:

- Cross-link
- Power
- DSSI
- PCIM

Review the following cable routing guidelines before you begin, and refer to Figures 6–3 and 6–4.

- When routing cables between cabinets, place the cables in the cable tray at the bottom of each zone and feed them through the access holes in the vertical rails.
- When routing cables within a system cabinet (CPU 1 or CPU 2), route the cables along the middle vertical rail.
- When routing cables within expander cabinet one (EXP 1), route the cables along the left vertical rail.

- When routing cables within expander cabinet two (EXP 2), route the cables along the right vertical rail.
- After routing, secure the cables with cable clamps.
- Route console A and B cables to the consoles from the rear of the CPU cabinets.

Figure 6–3 Model 610 CPU Cabinet Cable Routing

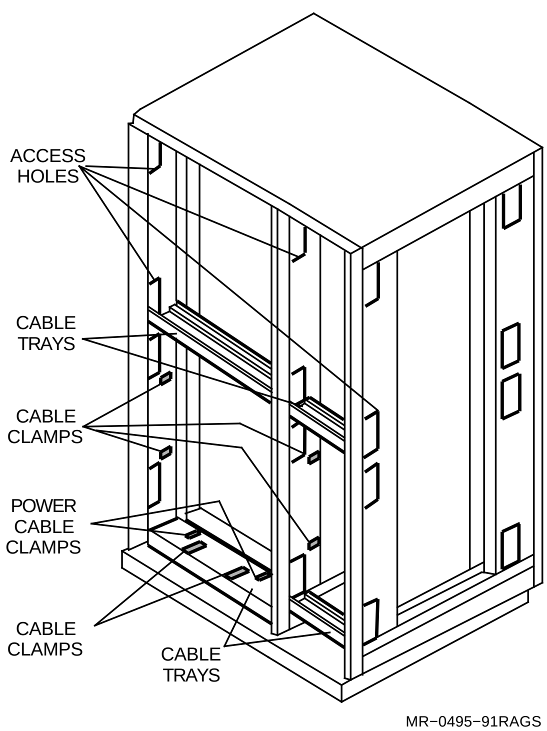
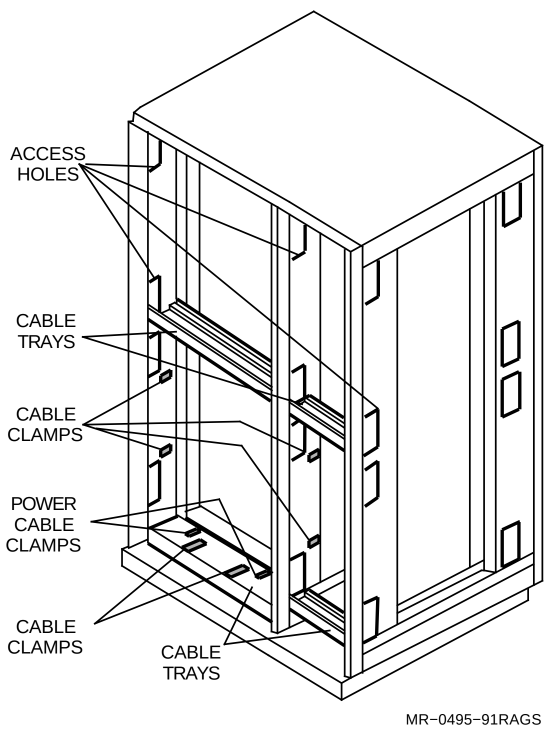


Figure 6–4 Model 610 CPU Expander Cabinet Cable Routing

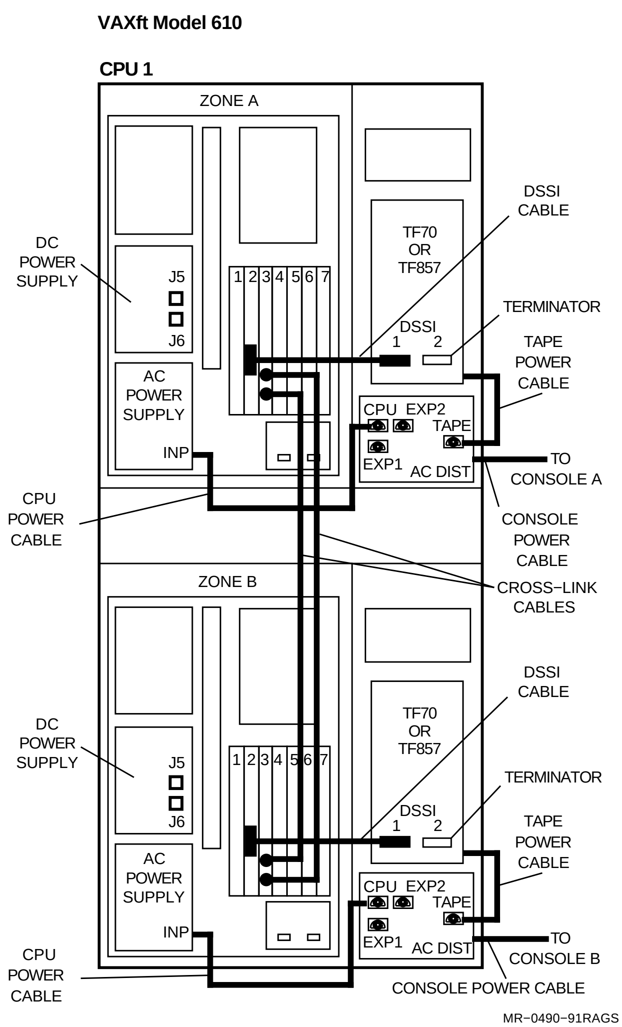


6.2.1 Cross-Link Cables

The following steps apply to all configurations. Refer to Figure 6–5 as you remove and replace the cross-link cables in the CPU cabinets.

1. Release the spring clips at one end of the cross-link cable (PN 17-02194-01) attached to the upper or lower connector of the processor module in slot 3 of zone A.
2. Unplug the cross-link cable connector and route the cable between the cable tray and the logic modules.
3. Release the spring clips at one end of the cross-link cable (PN 17-02194-01) attached to the upper or lower connector of the processor module in slot 3 of zone B.
4. Unplug the cross-link cable connector and remove it from the system.

Figure 6–5 Cable Connections in a Model 610 Base System



6.2.2 Power Cables

Refer to Figures 6–5 through 6–9 as you remove and replace the power cables.

1. Disconnect one end of the power cable (PN 17-00442-17) from the console plug at the rear of the ac distribution box in zone A or B of the system cabinet (CPU 1). Disconnect the other end of the same power cable from console A or B.
2. Disconnect one end of the power cable (PN 17-00442-38) from the input plug of the ac power supply in zone A or B of CPU 1. Disconnect the other end of the same power cable from the CPU plug of the ac distribution box in zone A or B of CPU 1.
3. Disconnect one end of the power cable (PN 17-00422-39) from the tape plug of the ac distribution box in zone A or B of CPU 1. Disconnect the other end of the same power cable from the power plug at the rear of the TF-series storage device in zone A or B of CPU 1.

   If an expander cabinet is present in the configuration:

4. Disconnect one end of the power cable (PN 17-00442-38) from the EXP 1 or EXP 2 plug of the ac distribution box in zone A or B of CPU 1 or CPU 2. Route the power cable through the access hole to the appropriate zone of EXP 1 or EXP 2.
5. Disconnect the other end of the same power cable from the input plug of the ac power supply in zone A or B of EXP 1 or EXP 2.

6.2.3 DSSI Cables

Refer to Figures 6–5 through 6–9 as you remove and replace the DSSI cables.

1. Loosen the screws that secure one end the DSSI cable (PN 17-02420-01) to the KFE52 I/O controller module.
2. Disconnect the DSSI cable from the KFE52 I/O controller module.
3. Loosen the screws that secure the other end of the DSSI cable to the DSSI 1 connector on the tape option.

Figure 6–6 Cable Connections in a Model 610 Expanded System

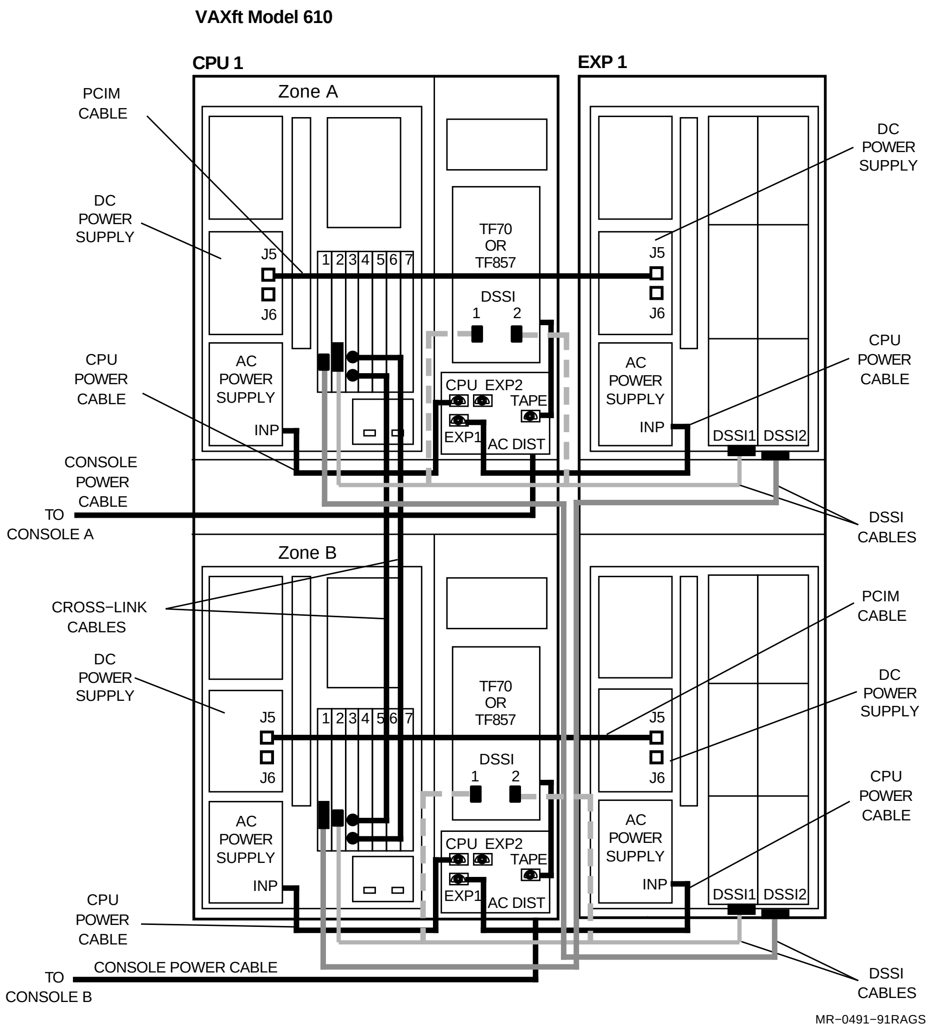


Figure 6–7 Cable Connections in a Model 610 Expanded System

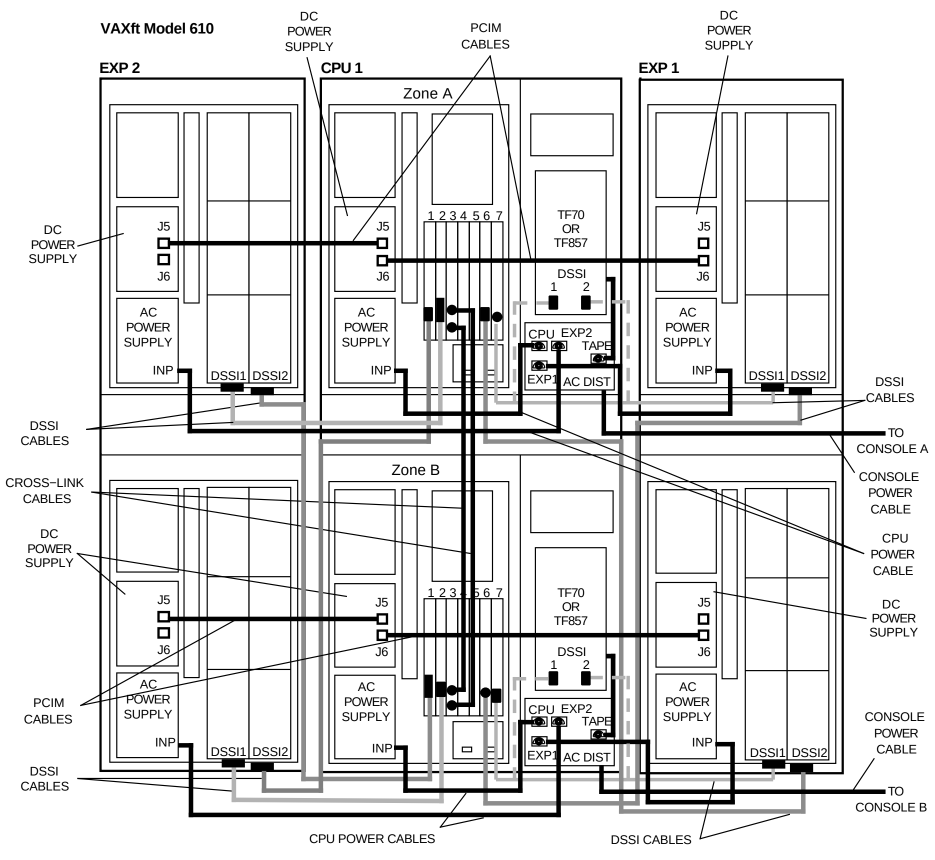
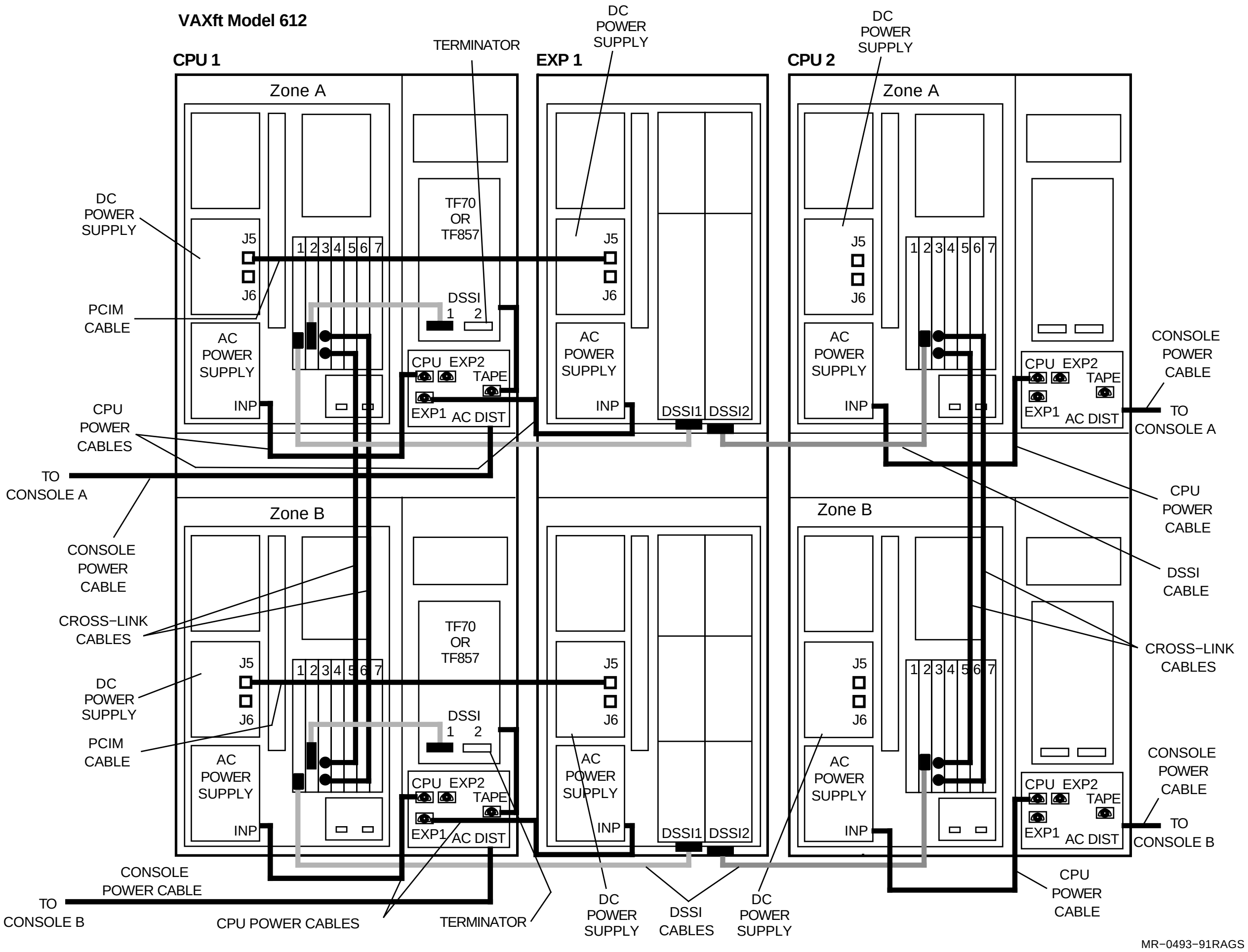


Figure 6–8 Cable Connections in a Model 612 System



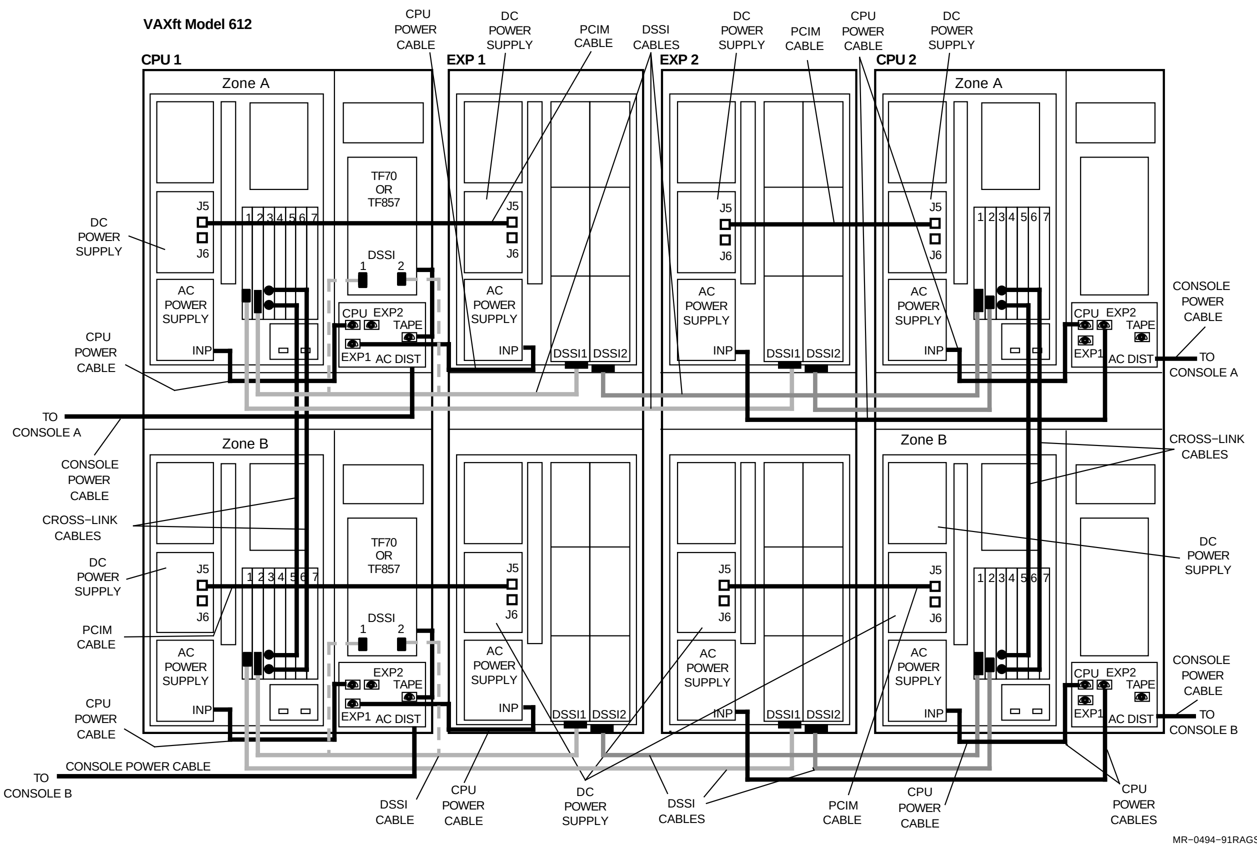


Figure 6–9 Cable Connections in a Model 612 Expanded System

If an expander cabinet is present in the configuration:

4. Perform steps 1, 2, and 3.
5. Loosen the screws that secure one end of the DSSI cable to the DSSI 2 connector on the tape option.
6. Disconnect the other end of the DSSI cable from the DSSI 2 connector on the tape option.
7. Loosen the screws that secure one end of the DSSI cable to the DSSI 1 or DSSI 2 connector in the expander cabinet.
8. Disconnect the DSSI cable from the DSSI 1 or DSSI 2 connector in the expander cabinet.

If no TF-series storage device is present:

9. Loosen the screws that secure one end of the DSSI cable (PN 17-02245-02) to the KFE52 I/O controller module in zone A or B of the CPU cabinet.
10. Disconnect the DSSI cable from the KFE52 I/O controller module.
11. Loosen the screws that secure the other end of the DSSI cable to the DSSI 1 or DSSI 2 connector in the expander cabinet.

6.2.4 PCIM Cables

Refer to Figure 6–6 through Figure 6–9 as you remove and replace the PCIM cables.

1. Disconnect one end of the PCIM cable from J5 of the dc power supply in zone A or B of the CPU cabinet.
2. Disconnect the other end of the PCIM cable from J5 of the dc power supply in zone A or B of the expander cabinet.

6.3 Logic Modules

This section describes how to remove or install a logic module in a system cabinet. Observe the module handling and ESD procedures (Section 6.3.1) whenever you remove, install, or replace a logic module in a system cabinet.

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 6.3.1 whenever you handle the logic modules.

NOTE

Before you use any of the following procedures on a system that is running, you must first contact the responsible customer representative, system manager, or application manager to shut down the zone and power off the system cabinet. The *VAXft System Services Manager's Guide* (AA-NL35A-TE) describes how to shut down the zone and power off the system cabinet from the console.

6.3.1 Module Handling and ESD Procedures

Two grounding cords are stored in the left door of the system cabinet (Figure 6–2). One cord is connected to a wrist strap. The other cord is connected to a grounding clip for attaching to an antistatic ESD box. When the wrist strap is in place, there must be no more than 10 MΩ of impedance through the grounding cord, wrist strap, and your wrist.

T3000-series modules are fragile and static sensitive. Use the grounding cords and observe the following precautions when handling logic modules.

- Always put on a grounded wrist strap **before** handling a logic module.
- Be sure that nothing touches the module or the components on the module because leads can be damaged. Avoid contact with the wrist strap, grounding cord, clothing, jewelry, cables, or other modules.
- Minimize any potential for physical or ESD damage as follows:
  - Remove all unnecessary materials in the service area (tools, documents, paper, plastics, polystyrene).
  - Avoid clothing that contains more than 80% nonconductive materials (silk or synthetic fiber).
  - Do not wear a jacket. Wear a short-sleeve shirt or roll up the sleeves on a long-sleeve shirt.
  - Do not wear jewelry.
  - Loose clothing, such as a necktie, must be fastened in place.
- Before removing a module from an ESD box, place the box on a clean surface. Do not allow the box to fall.

NOTE

Never place an ESD box on the floor.

- Keep the module in the antistatic ESD box until you are ready to install it.

- Before removing a module from an ESD box, attach the grounding clip to the ESD box.
- If you are replacing a module, put the module you just removed on a grounded ESD workmat on a clean surface in the service area. Put the module side 2 down on the ESD workmat.
- Save the ESD box for future use. Store a module in the ESD box until you are ready to install it.
- When removing or installing a module, be sure the module does not come into contact with a cable or another module. And be sure that nothing else touches the module or any module components.
- Hold a module **only** by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.
- Do not slide the module across any surface because the leads are fragile and can be damaged.
- An ESD sensitive module may come into contact with the following items **only**:
  - An approved ESD workmat
  - Antistatic packaging on the ESD workmat
  - Tools and test equipment on the ESD workmat
  - The chassis being serviced
  - The hands of someone wearing an ESD wrist strap

6.3.2 Removing KA550 Processor Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 6.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove a KA550 processor module from slot 3 in a system backplane. Remember to observe all FRU handling procedures (Section 6.1.1).

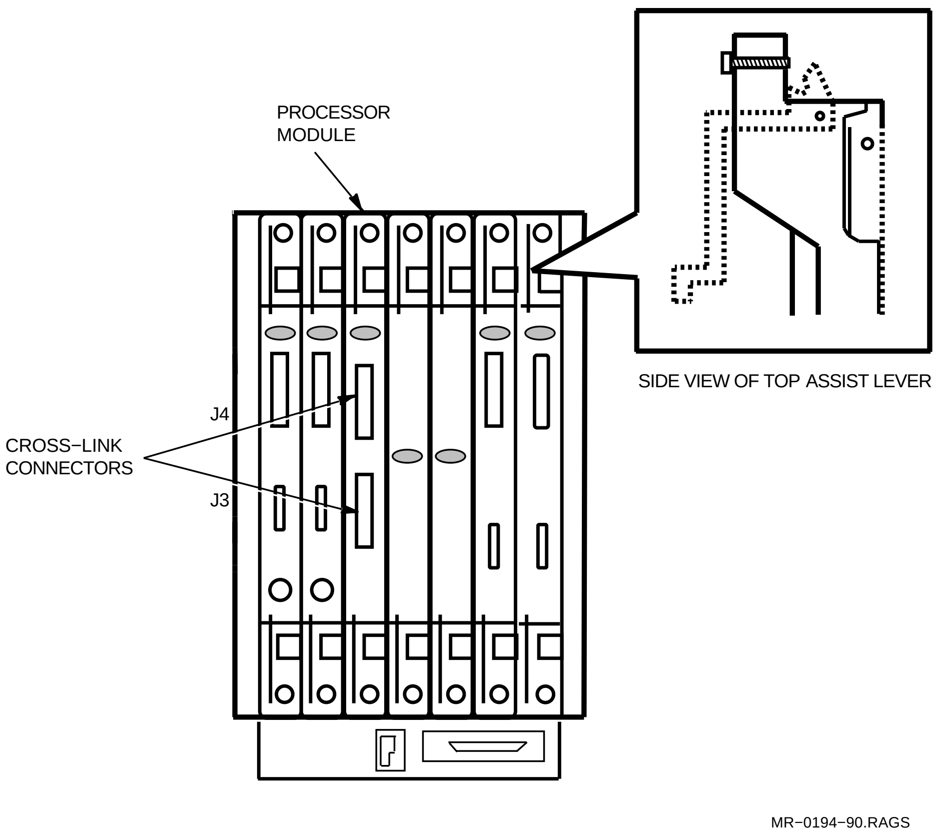
1. Ask the system manager or the operator to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Figure 6–10 shows connectors J3 and J4. Disconnect the cross-link cables from the module.
5. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

6. Use both hands to remove the module. Pull the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
7. Grasp the module handle. Slide the module out of the card cage slot.

Figure 6–10 Removing a KA550 Processor Module



6.3.3 Removing MS520 Memory Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 6.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove an MS520 memory module from a system backplane (Figure 6–11). Remember to observe all FRU handling procedures (Section 6.1.1).

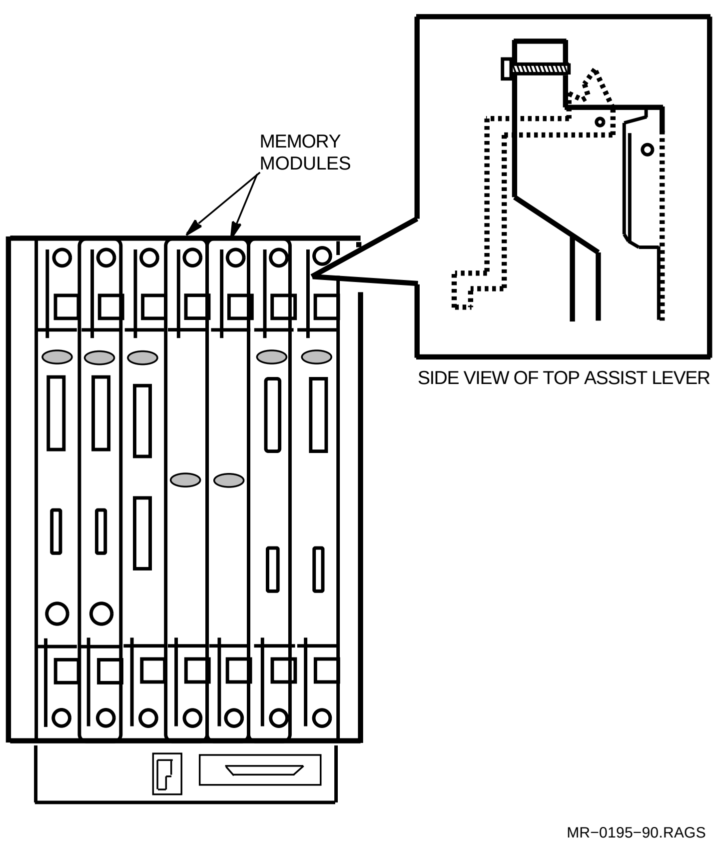
1. Ask the operator or the system manager to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

5. Use both hands to remove the module. Pull the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
6. Grasp the module handle. Slide the module out of the card cage slot.

Figure 6–11 Removing an MS520 Memory Module



6.3.4 Removing WAN 620 Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 6.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove a WAN 620 module from a system backplane. Remember to observe all FRU handling procedures (Section 6.1.1).

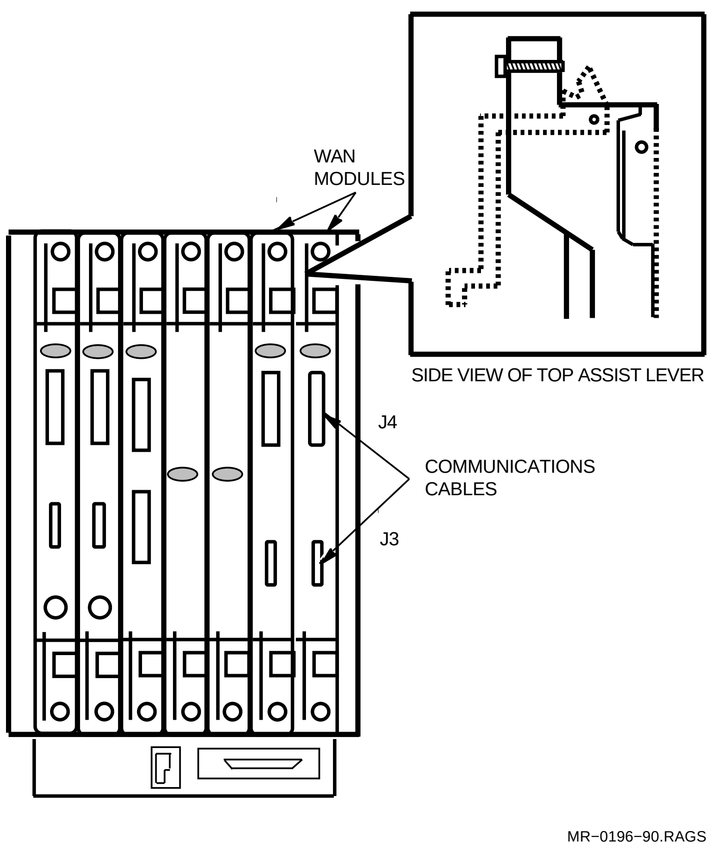
1. Ask the operator or the system manager to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Figure 6–12 shows connectors J3 and J4. Disconnect the communications cable(s) from the module.
5. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

6. Use both hands to remove the module. Pull on the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.
7. Grasp the module handle. Slide the module out of the card cage slot.

Figure 6–12 Removing a WAN 620 Module



6.3.5 Removing KFE52 I/O Controller Module

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used as described in Section 6.3.1 whenever you handle the logic modules.

Before removing a replacement module from an ESD box, attach the grounding clip to the ESD box.

Hold a module only by the handle or by the edges with your hands flat and perpendicular to the circuit board. Do not touch the etch circuit or any components, leads, or connector pins. Do not bend the module.

Use the following procedure to remove a KFE52 I/O controller module from a system backplane (Figure 6–13). Remember to observe all FRU handling procedures (Section 6.1.1).

1. Ask the operator or the system manager to shut down the zone that houses the faulty module. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Disconnect the DSSI cable or terminator from J4.

   CAUTION

   Make sure that the cable clip is unlocked before disconnecting the thickwire cable. Failure to do so may result in damage to the cable and/or connector.

5. Disconnect the Ethernet cable if one is installed.
6. Release the fasteners at the top and bottom of the module handle. Push in each fastener and turn it one quarter turn to the left.

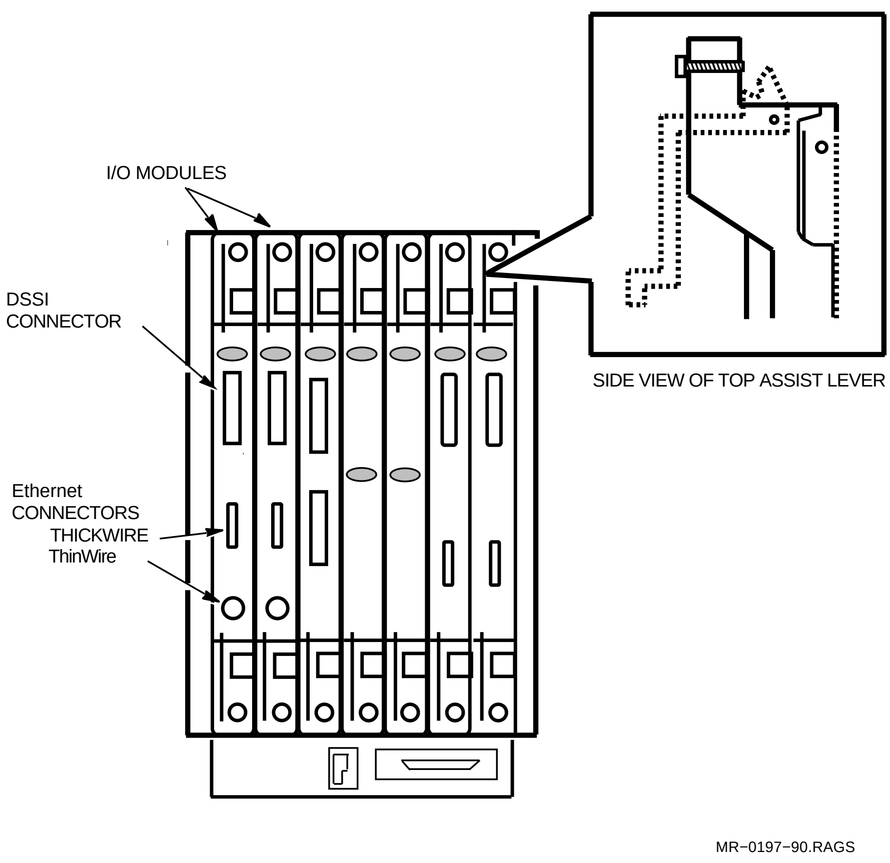
   CAUTION

   Use care when handling the module. A sudden shock to the module could cause component damage.

7. Use both hands to remove the module. Pull on the module levers to disengage the backplane connector. You may hear a “snap” when the connector disengages.

8. Grasp the module handle. Slide the module out of the card cage slot.

Figure 6–13 Removing a KFE52 I/O Controller Module

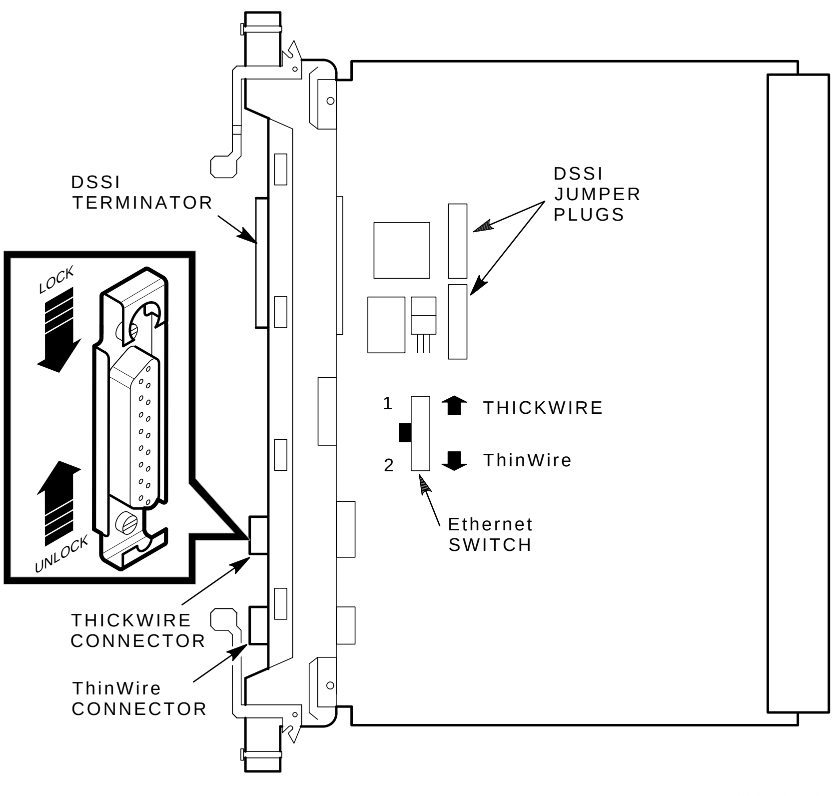


6.3.5.1 Installing/Replacing KFE52 I/O Controller Module

To install/replace a KFE52 I/O controller module:

1. Note the Ethernet switch position (Figure 6–14) on the KFE52 I/O controller module you just removed.
2. Set the Ethernet switch on the new module to the same position (up for thickwire, down for ThinWire).

Figure 6–14 KFE52 I/O Controller Module



3. Remove the DSSI jumper plugs from the new module if they were removed from the old one.[1]
4. Now reverse steps 1 through 8 of Section 6.3.5.

6.4 Carrier Disk Drive

You do not need to power off the cabinet to remove or replace an RF-series carrier disk drive. See Appendix A for detailed procedures.

Each RF-series carrier disk drive is assigned a unit number according to the slot in which it is housed. Figure 6–15 shows the slot numbers and the corresponding controls on the summary panel.

Use the following procedure to remove a carrier disk drive from a system cabinet. Remember to observe all FRU handling procedures (Section 6.1.1).

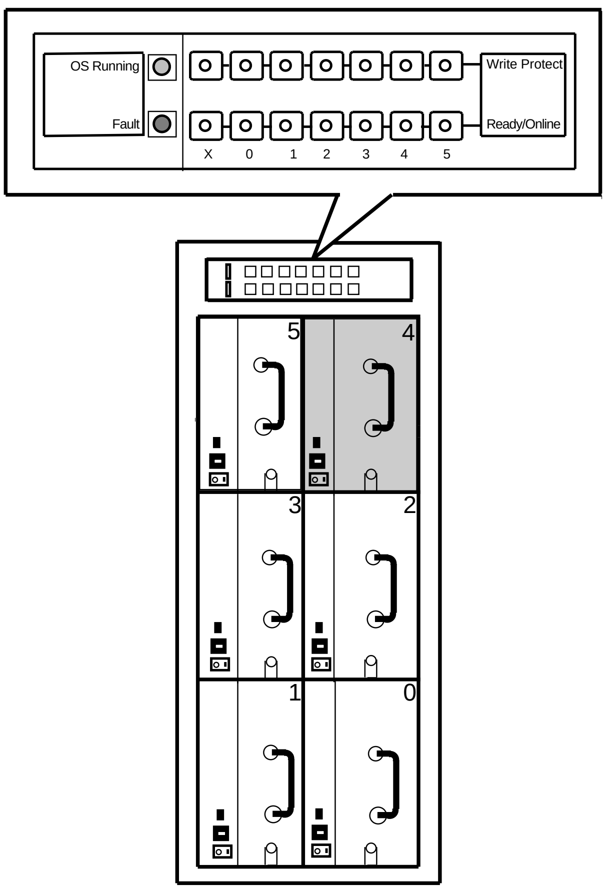
1. Ask the operator or system manager to dismount the disk to be removed.
2. Take the drive off-line by pressing the summary panel Ready/Online switch in. The corresponding indicator should be dark (unlit).
3. Set the drive power switch to off (0). Wait 45 seconds (for disk drive to stop spinning and interlock solenoid to release).
4. See Figure 6–16. Release the captive thumb screw. Then pull the drive straight out of the slot.

CAUTION

Use great care when removing, replacing, or transporting a drive. Do not drop the drive or allow it to come into contact with any object while you carry it.

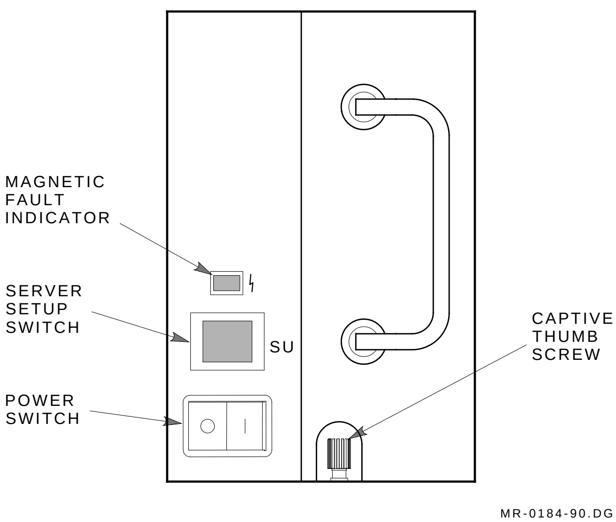
[1] The DSSI jumper plugs are needed only on the slot-2 I/O controller module in a base system. If a second I/O controller module is added to a base system, the plugs must be removed from the second I/O controller module. The DSSI jumper plugs must also be removed from all I/O controller modules in an expanded system. An LED on the I/O controller module indicates if the plugs are installed. The *VAXft Site Preparation and Installation Guide* provides more information about the I/O controller module configuration.

Figure 6–15 Disk Drive Slot Numbers



MR−0247−92RAGS

Figure 6–16 Removing a Carrier Disk Drive



6.4.1 RF-Series Controller/HDA Assembly

Use the following procedure to remove the RF-series controller/HDA assembly. Each part is a separate FRU, but because they are connected they share the same removal procedure.

1. Complete steps 1 through 4 from Section 6.4.
2. Place the carrier disk drive on a grounded antistatic mat.
3. Disconnect the three cable blocks from the disk adapter module.
4. Turn the carrier disk drive right side up.
5. Disconnect the DSSI cable.
6. Disconnect the OCP cable.
7. Disconnect the power cable.
8. Remove four Phillips screws, two from the right side, and two from the bottom of the carrier disk drive.
9. Carefully lift the controller/HDA assembly out of the carrier disk drive and place it on the grounded antistatic mat.
10. Remove the four screws that hold the controller on the HDA assembly.

11. Carefully lift the DSSI-cable-connector end of the controller to expose the top of the HDA assembly. The other end of the controller is connected by a flex cable.
12. Remove the flex cable from the controller.

6.4.2 RF-Series Disk Adapter

Use the following procedure to remove the RF-series disk adapter.

1. Complete steps 1 through 4 from Section 6.4.
2. Remove the four screws on the back of the carrier disk drive.
3. Pull the disk adapter out about 2 inches.
4. Note the placement of the six cables, and remove them.
5. Lift the disk adapter away from the carrier disk drive.

6.5 Cannister Disk Drive

You do not need to power off the cabinet to remove or replace an RF-series cannister disk drive. See Appendix A for detailed procedures.

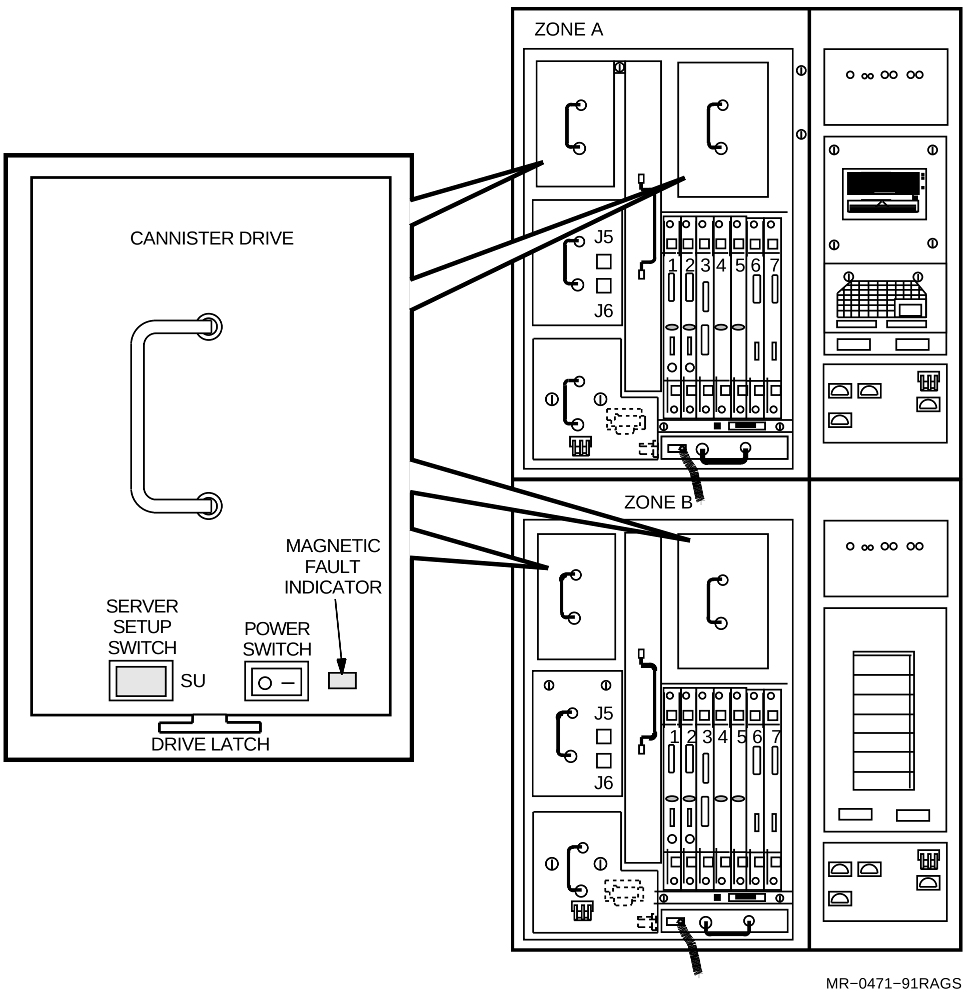
Use the following procedure to remove a cannister disk drive from a system cabinet. Remember to observe all FRU handling procedures (Section 6.1.1).

1. Ask the operator or system manager to dismount the disk to be removed.
2. Take the disk drive off-line by pressing the summary panel Ready/Online switch in. The corresponding indicator should be dark (unlit).
3. Set the drive power switch to off (0). Wait 45 seconds (for drive to stop spinning and interlock solenoid to release).
4. See Figure 6–17. Push the drive latch down and pull the drive straight out of the slot.

CAUTION

Use great care when removing, replacing, or transporting a drive. Do not drop the drive or allow it to come into contact with any object while you carry it.

Figure 6–17 Removing a Cannister Disk Drive



6.5.1 RF-Series Controller/HDA Assembly

Use the following procedure to remove the RF-series controller/HDA assembly. Each part is a separate FRU, but because they are connected they share the same removal procedure.

1. Complete steps 1 through 4 from Section 6.5.
2. Place the cannister disk drive on a grounded antistatic mat.
3. Remove four screws (two on each side) from the front plate. Remove the front plate.
4. Remove two screws from the top of the cannister, and remove the top plate.
5. Remove four screws from the back of the cannister, and pull the back plate out about 2 inches.
6. Locate the three cables that are connected to the disk adapter. Note their placement, label them if necessary, and disconnect them.
7. Remove four screws (two on each side of the cannister) that secure the shock mounts.
8. Carefully lift the controller/HDA assembly out of the cannister disk drive and place it on the grounded antistatic mat.
9. Remove the four screws and the signal connectors from the controller.

6.5.2 RF-Series Disk Adapter

1. Complete steps 1 through 4 from Section 6.5.
2. Remove four screws from the back of the cannister, and remove the back plate.
3. Note the placement of the six cables connected to the disk adapter. Label them if necessary, and then remove them.
4. Remove the disk adapter.

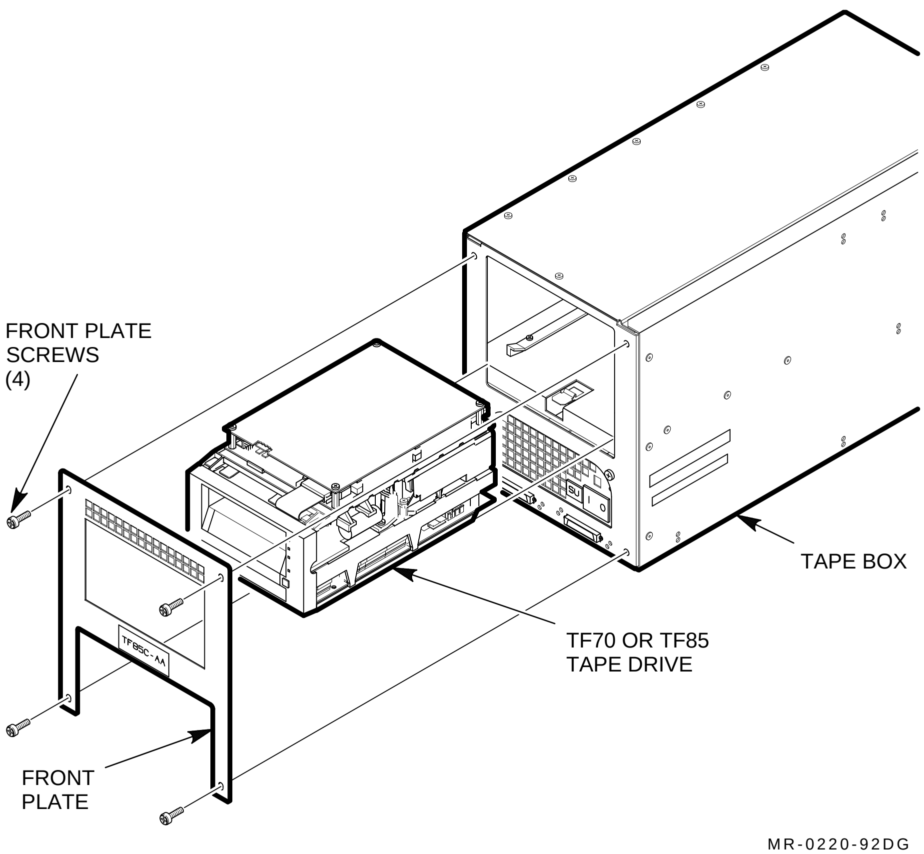
6.6 TF70C-AA or TF85C-AA Tape Drive

Use the following procedure to remove a TF70C-AA or TF85C-AA tape drive. Remember to observe all FRU handling procedures (Section 6.1.1).

1. Ask the operator or the system manager to shut down the zone that houses the tape drive. (Zone shutdown is described in Section 6.1.2.)
2. Ask the operator or system manager to dismount the tape drive.
3. Unload the tape magazine if one is loaded (Figure 6–18).
4. Set the drive power switch to off (0). All indicators on the tape drive should be dark (unlit).[1]
5. See Figure 6–18. Remove four screws that secure the front plate to the tape drive box.
6. Push the release tab down and pull the drive straight out of the slot.

[1] The summary panel switches have no effect on the cannister tape drives. Use the switches and indicators on the tape cartridge.

Figure 6–18 Removing a TF70C-AA or TF85C-AA Tape Drive

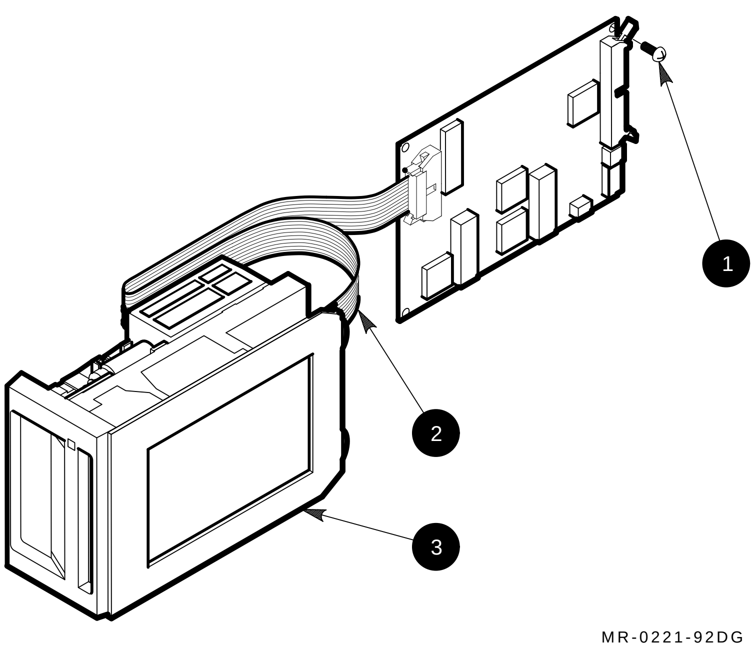


6.7 TF70C-AA or TF85C-AA Controller/HDA Assembly

Use the following procedure to remove a TF70C-AA or TF85C-AA controller/HDA assembly. Remember to observe all FRU handling procedures (Section 6.1.1).

1. Place the tape drive on a grounded antistatic mat.
2. Remove four screws that secure the controller module to the HDA assembly. See Figure 6–19, callout ❶.
3. Remove the signal cable connector from the controller module. See Figure 6–19, callout ❷.
4. Remove the signal cable connector from the HDA assembly. See Figure 6–19, callout ❸.

Figure 6–19 TF70C-AA or TF85C-AA Tape Drive FRUs



6.8 TF70C-AA or TF85C-AA Tape Drive Box

Use the following procedure to remove a TF70C-AA or TF85C-AA tape drive box.

1. Complete steps 1 through 6 from Section 6.6.
2. Disconnect any DSSI cables connected to the tape drive.
3. Disconnect the ac power cable from the rear of the tape drive box.

WARNING

Two people are required to lift and carry the tape drive box.

4. See Figure 6–20. Remove two screws from the back of the cabinet. From the front of the cabinet, remove four screws that secure the mounting tray to the chassis.
5. Lift the tape drive box out of the cabinet and place it on a flat surface with the mounting tray positioned as shown in Figure 6–20.
6. See Figure 6–21. Using a small flat-blade screwdriver, remove four gauge pins from the front of the tape drive box.
7. Remove four screws that secure the mounting tray to the tape drive box. See Figure 6–21.

NOTE

The TF70 or TF85 tape drive node ID is set to 4 at the factory.

Figure 6–20 Removing a Mounting Tray

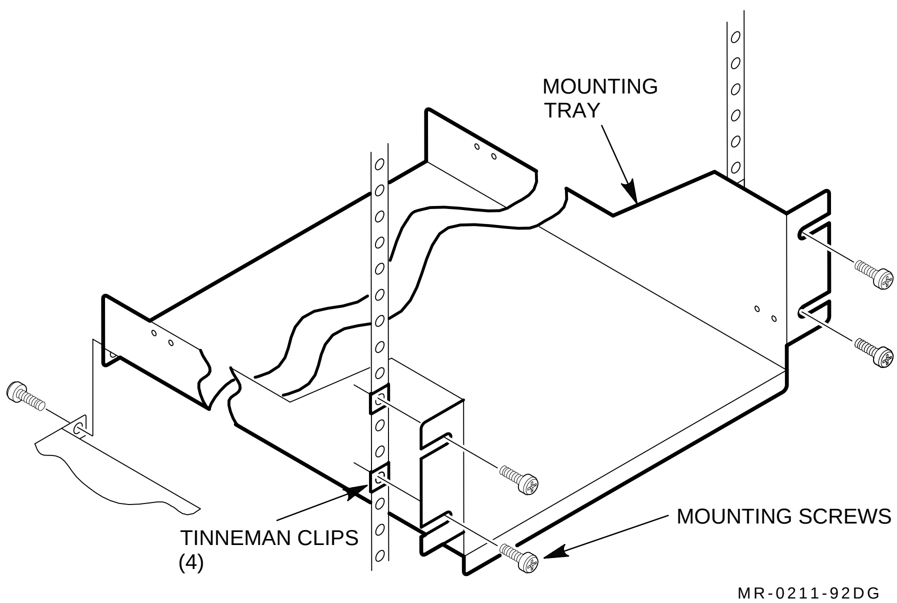
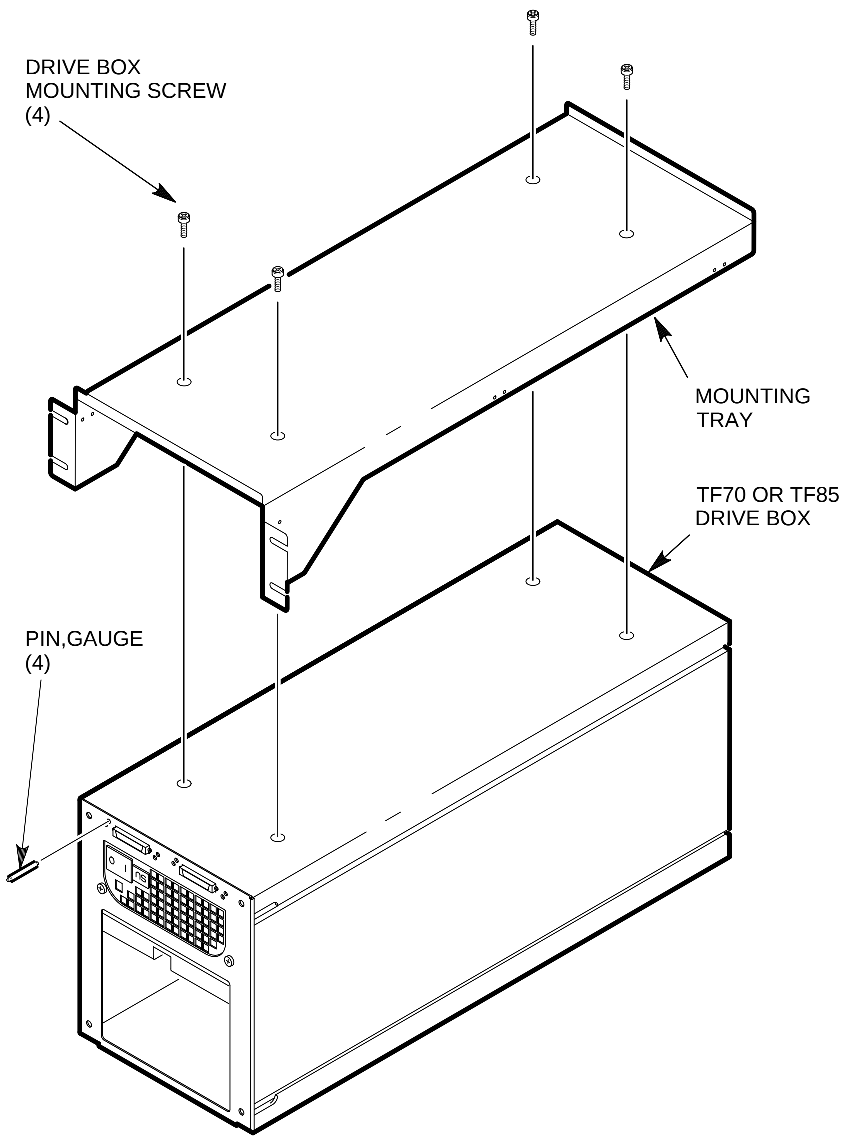


Figure 6–21 Removing a Tape Drive Box



6.9 TF857-CA Tape Loader

Use the following procedure to remove a TF857-CA tape loader.

1. Ask the operator or the system manager to shut down the zone that houses the tape loader. (Zone shutdown is described in Section 6.1.2.)
2. Ask the operator or system manager to dismount the tape drive.
3. Unload the tape magazine if one is loaded.
4. Set the drive power switch to off (0). All indicators on the tape drive should be dark (unlit).[1]
5. See Figure 6–22. Disconnect the DSSI cables and power cable.
6. Cut any tie wraps securing the DSSI cables to the fan assembly. See Figure 6–22.
7. See Figure 6–23. Loosen the shipping restraint screw until the shipping bracket drops.

   NOTE

   If the shipping bracket does not drop when the shipping restraint screw is loosened, push the shipping bracket down with a screwdriver.

8. From the front of the cabinet, slide the tape loader out of the cannister.

---

[1] The summary panel switches have no effect on the cannister tape drives. Use the switches and indicators on the tape cartridge.

Figure 6–22 TF857-CA Tape Loader, Rear Connections

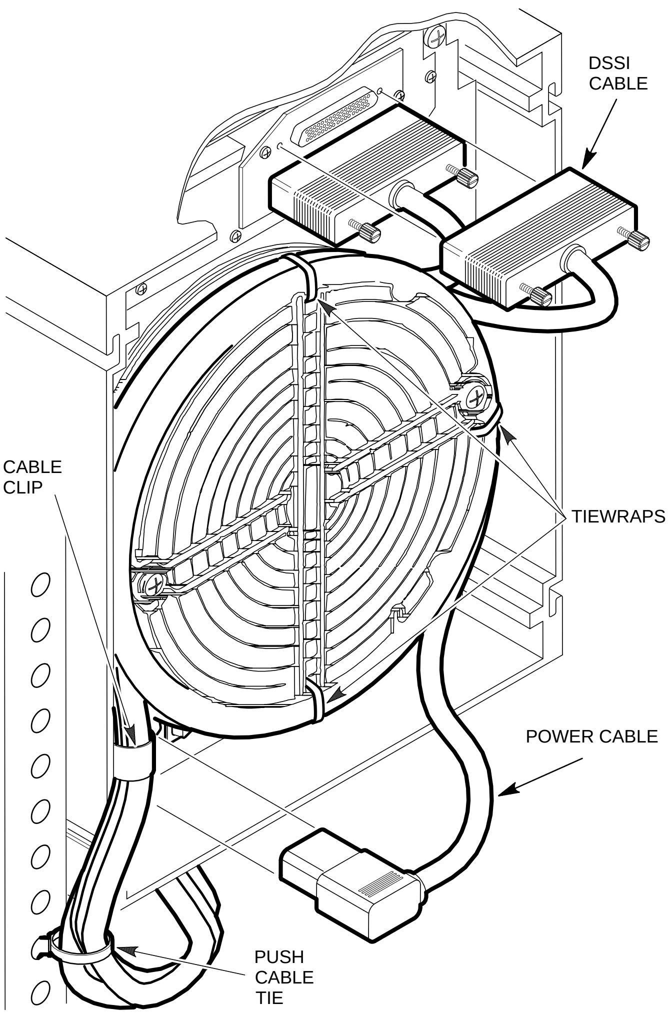
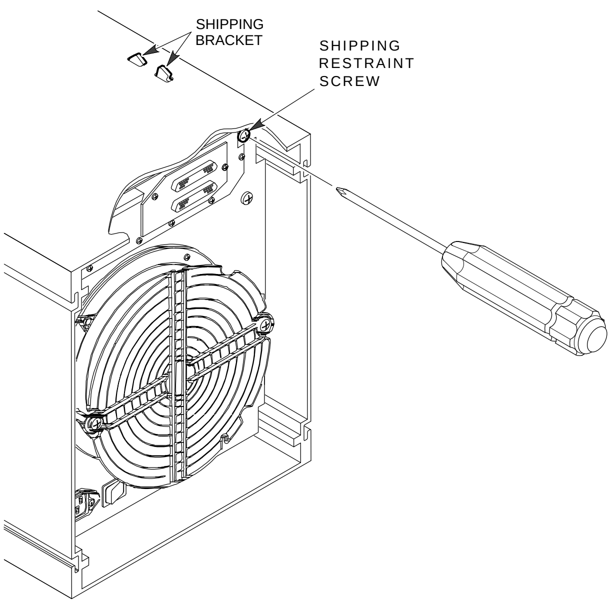
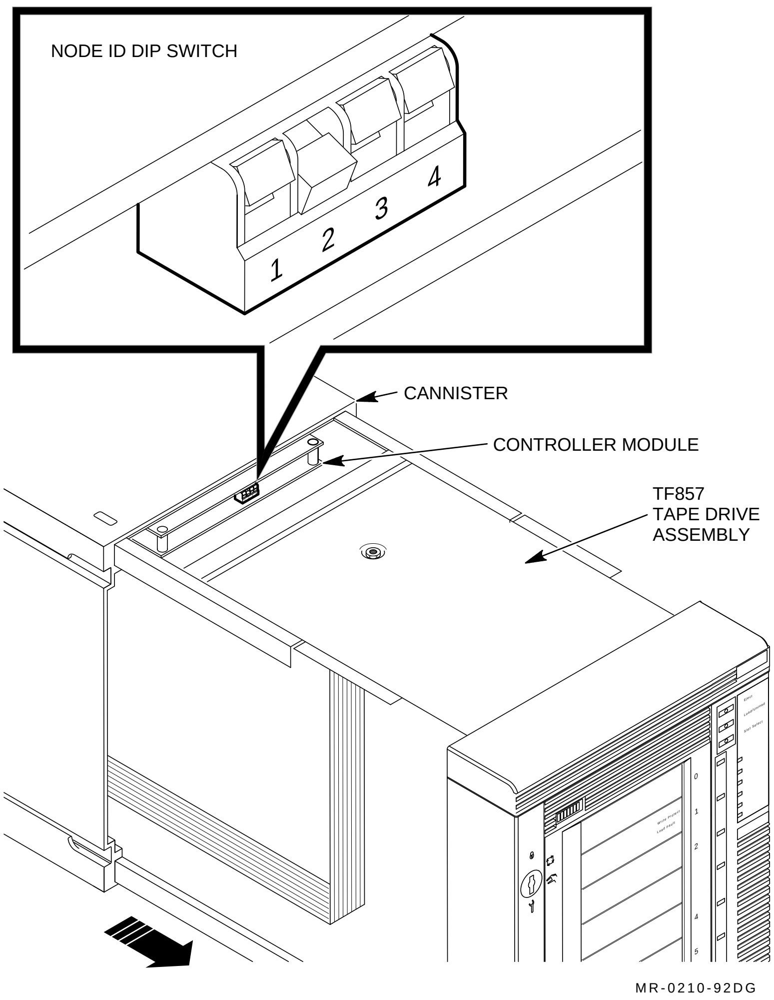


Figure 6–23 Loosening the Shipping Restraint Screw



9. Slide the new tape loader to the stop position. You will be able to see the four-position node ID DIP switch. See Figure 6–24.
10. Set the DIP switch as shown in Figure 6–24.
11. Slide the tape loader into the operating position.
12. From the rear of the cabinet, secure the shipping bracket by tightening the shipping restraint screw. Connect the DSSI and power cables.

Figure 6–24 Setting the TF857-CA Tape Loader Node ID



Use the following procedure to install a TF857-CA tape loader.

1. Ask the operator or the system manager to shut down the zone that will house the tape loader. (Zone shutdown is described in Section 6.1.2.)
2. See Figure 6–20. Remove two screws from the back of the cabinet. From the front of the cabinet, remove four screws that secure the mounting tray to the chassis.
3. Leave the Tinnerman clips in place.
4. Place the mounting tray on a flat surface. Place the tape loader in the mounting tray as shown in Figure 6–25.
5. See Figure 6–23. Loosen the shipping restraint screw until the shipping bracket drops.

NOTE

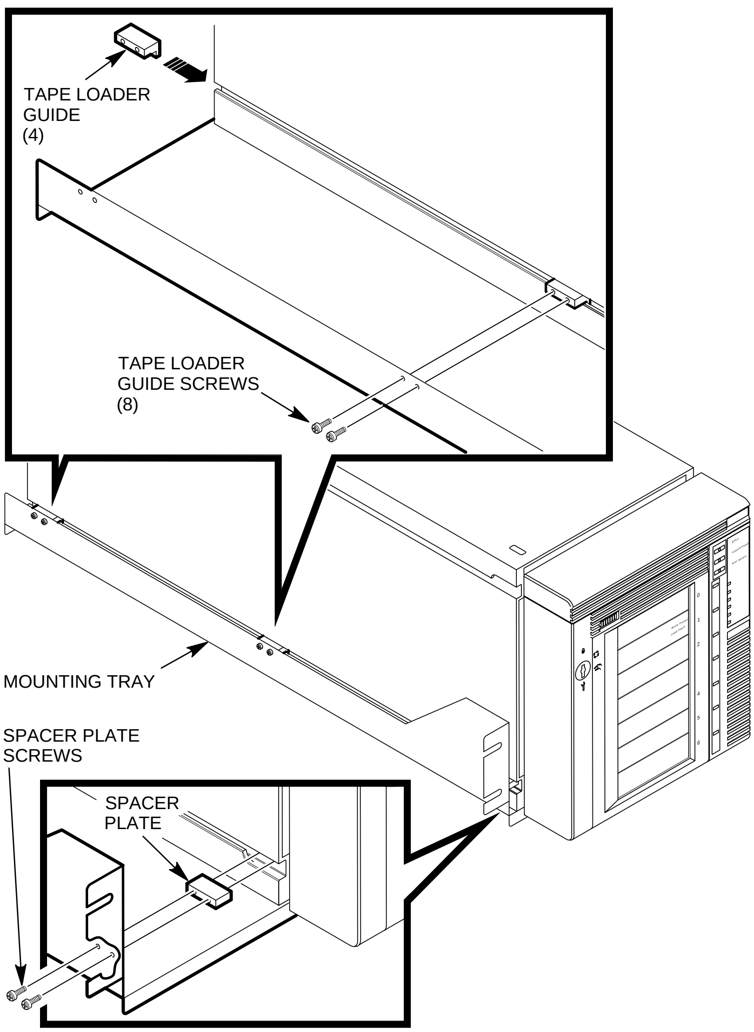
If the shipping bracket does not drop when the shipping restraint screw is loosened, push the shipping bracket down with a screwdriver.

6. Slide the tape loader to the stop position.
7. Set the DIP switch as shown in Figure 6–24.
8. Slide the tape loader into the operating position.
9. From the rear of the cabinet, secure the shipping bracket by tightening the shipping restraint screw.
10. See Figure 6–25. Position four tape loader guides (one on each side) at the center and at the rear of the tape loader.
11. Secure the tape loader guides with eight screws.
12. See Figure 6–25. Position two spacer plates (one on each side) at the front of the tape loader.
13. Secure the spacer plates with four screws.

WARNING

Two people are required to lift and carry the tape loader assembly.

Figure 6–25 Placing TF857-CA Tape Loader in Mounting Tray



14. Position the tape loader assembly in the cabinet and align the mounting tray screws with the Tinnerman clips. See Figure 6–21.
15. Secure the tape loader with six mounting screws (four in the front, two in the rear).
16. Route the two DSSI cables under the mounting tray. The paddle end of each cable should be at the rear of the tape loader and the pin end of each cable should be at the front of the tape loader.
17. See Figure 6–22. Connect the two DSSI cables and tighten the thumb screws.
18. Route the power cable under the mounting tray and plug it into the outlet at the rear of the tape loader. See Figure 6–22.
19. Plug the other end of the power cable into the tape outlet on the ac distribution box.
20. See Figure 6–26. From the front of the tape loader, secure the pin end of each of the two DSSI cables to the connector panel.
21. Secure eight guide pins to the connector panel. See Figure 6–26.
22. Secure the connector panel to the cabinet with four mounting screws. See Figure 6–26.
23. Connect the tape loader to the appropriate KFE52 I/O controller module following the procedures in Section 6.2.3, DSSI Cables.
24. See Figure 6–27. Attach the two adhesive-backed cable clips to the underside of the mounting tray, approximately 6 to 8 inches from each end.
25. See Figure 6–22. Attach a third adhesive-backed cable clip to the rear of the tape loader.
26. Mount a push cable tie into a hole at the rear of the tape loader box. See Figure 6–22.
27. Dress the cables as shown in Figures 6–27 and 6–22.
28. Bind the the cables together with three tie wraps. See Figure 6–22.

Figure 6–26 TF857-CA Tape Loader, DSSI Cable Connections

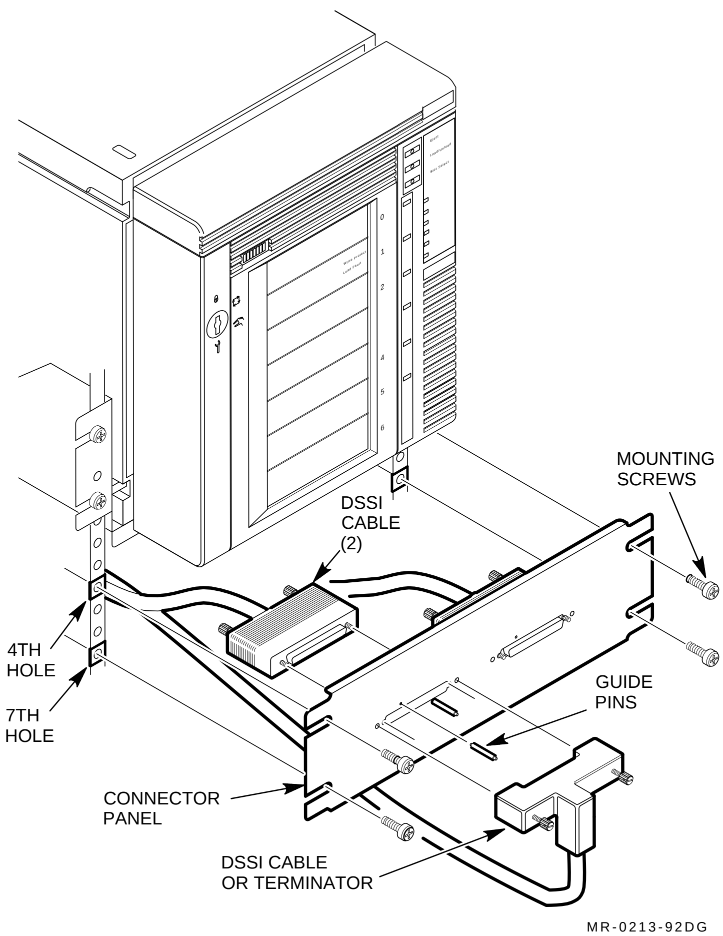
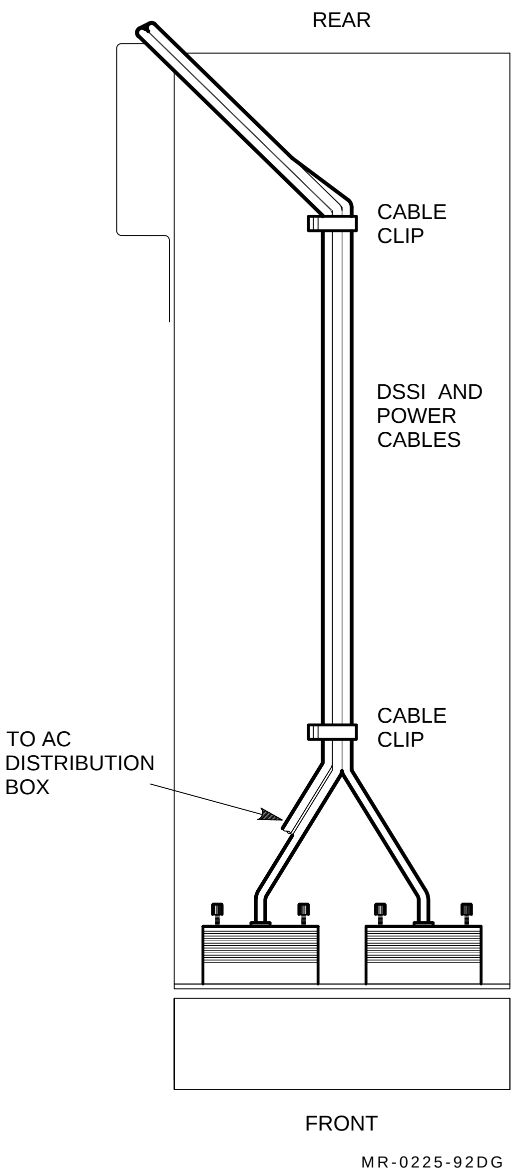


Figure 6–27 Attaching the Cable Clips

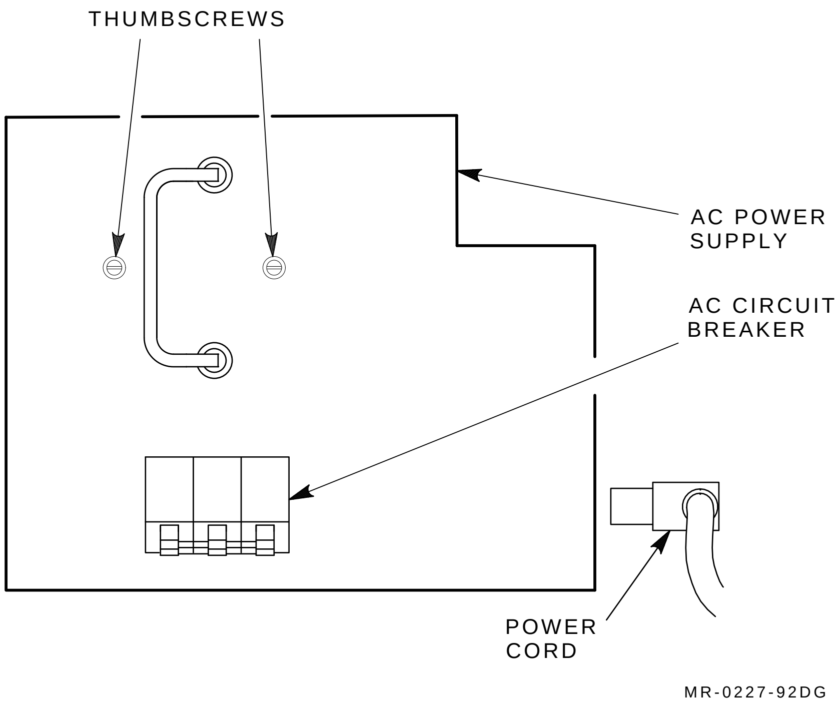


6.10 AC Power Supply

Use the following procedure to remove the ac power supply from the system cabinet or the expander cabinet.

1. Ask the operator or system manager to shut down the zone that houses the faulty power supply. (Zone shutdown is described in Section 6.1.2.
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Disconnect the ac power cord from the ac power supply.
5. See Figure 6–28. Loosen the two thumbscrews by turning them to the left.
6. Grasp the handle. Pull the ac power supply out of the cabinet.

Figure 6–28 AC Power Supply



6.11 DC Power Supply

The dc power supply for the expander cabinet differs slightly from the dc power supply for the system cabinet. They are **not** interchangeable, so make sure you have the correct part:

H7233-AA	System cabinet dc power supply
H7233-BA	Expander cabinet dc power supply

Use the following procedure to remove a dc power supply.

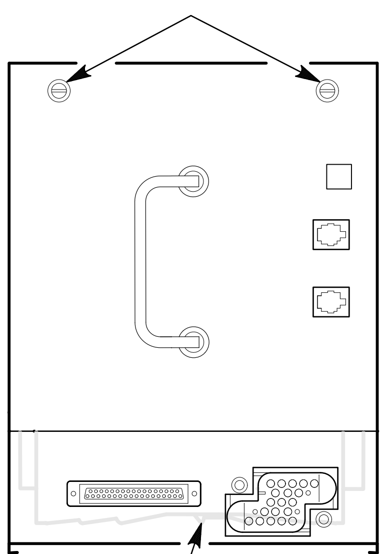
1. If any PCIM cables are attached to the dc power supply, note their location, label them if necessary, and disconnect them.
2. Remove the ac power supply. (See Section 6.10.)
3. See Figure 6–29. Loosen the two thumbscrews by turning them to the left.

CAUTION

Support the weight of the dc power supply as you pull it out of the cabinet. If you drop it, damage to the internal components could result.

4. Grasp the handle. Pull the dc power supply out of the cabinet.

Figure 6–29 DC Power Supply



6.12 Uninterruptible Power Supply

The uninterruptible power supply (UPS) provides battery backup to the entire cabinet for up to 15 minutes following power failure.

CAUTION

Never install a cold UPS in a VAXft system because damage to the UPS could result. If the replacement UPS was in an environment where the temperature was below freezing, allow it to come up to room temperature before you install it.

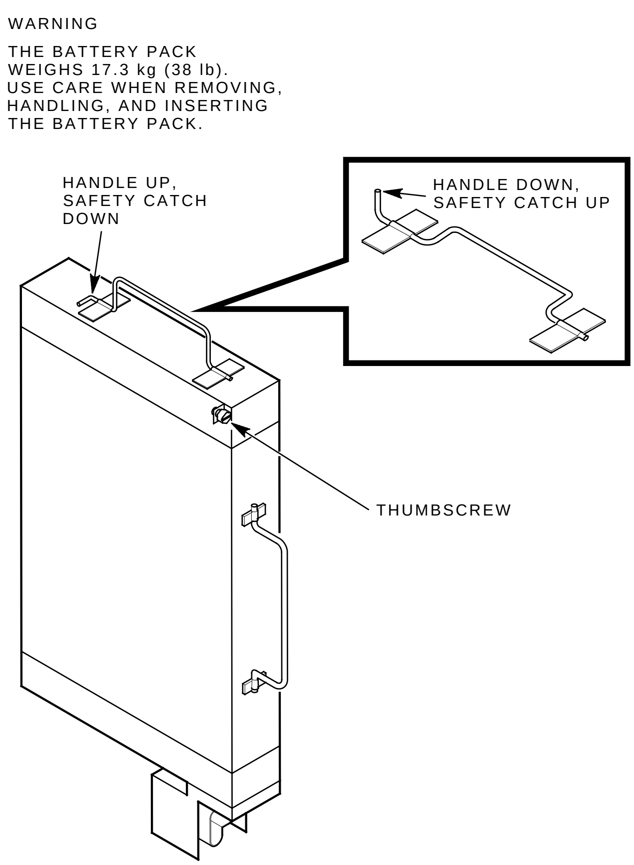
Use the following procedure to remove a UPS from a system cabinet or an expander cabinet.

WARNING

The UPS battery backup unit is very heavy. It weighs approximately 17.3 kg (38 lb). Use great care when lifting and handling it.

1. Ask the operator or system manager to shut down the zone that houses the faulty UPS. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the ac power supply. (See Section 6.10.)
5. See Figure 6–30. Loosen the thumbscrew by turning it to the left.
6. Slide the UPS toward you. The catch at the top of the unit should stop you when the UPS is about 3/4 of the way out of the cabinet.
7. Raise the handle at the top of the unit. This releases the catch.
8. Carefully slide the UPS completely out of the cabinet.

Figure 6–30 Uninterruptible Power Supply



6.13 AC Distribution Box

Use the following procedure to remove the ac distribution box.

1. Ask the operator or system manager to shut down the zone that houses the ac distribution box. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.

WARNING

Two people are required to lift and carry the ac distribution box.

4. See Figure 6–31. Disconnect any power cables from the front of the ac distribution box.
5. See Figure 6–32. Disconnect the local console terminal connector and power cable at the rear of the ac distribution box.
6. Disconnect the ac power cable from facility power. See Figure 6–32.
7. From the rear of the cabinet, remove four flat-blade screws that secure the ac distribution box to the chassis. See Figure 6–32.
8. From the front of the cabinet, remove three flat-blade screws that secure the ac distribution box to the chassis. See Figure 6–31.
9. Remove three hex screws that secure the ac distribution box to the front bracket. See Figure 6–31.
10. Carefully remove the ac distribution box from the cabinet.

Figure 6–31 AC Distribution Box, Front View

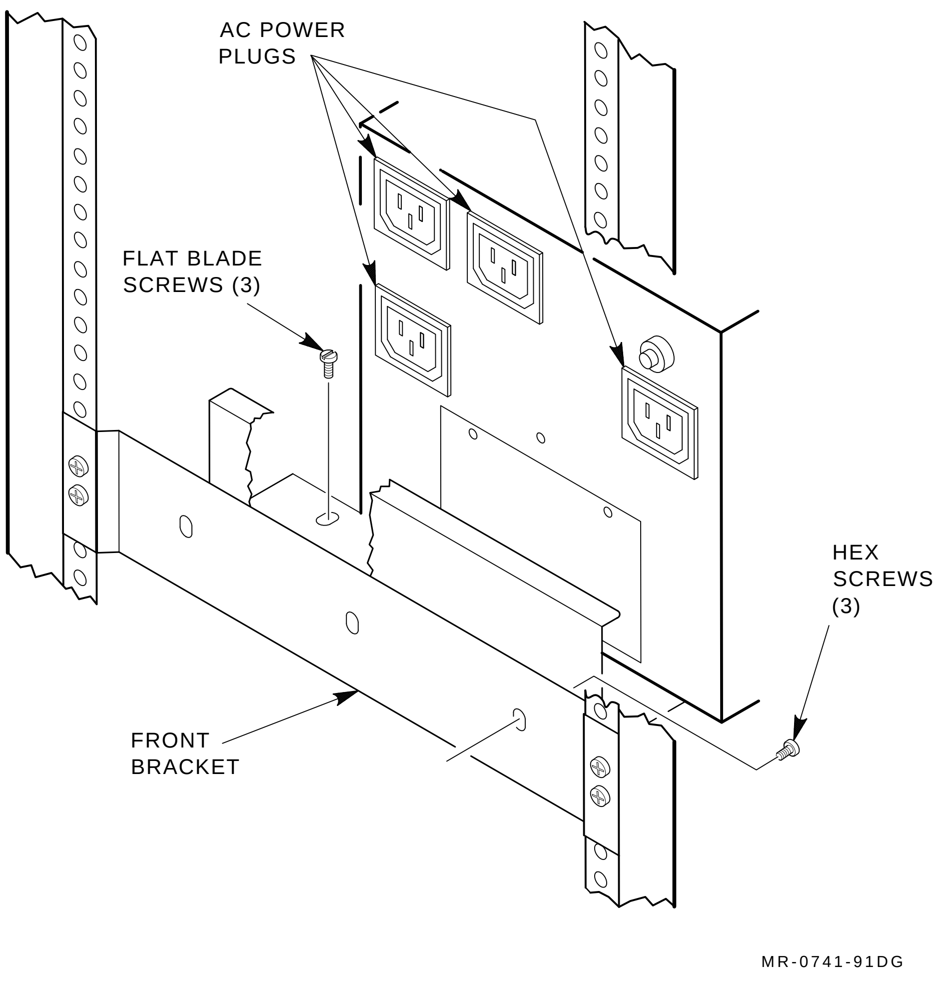
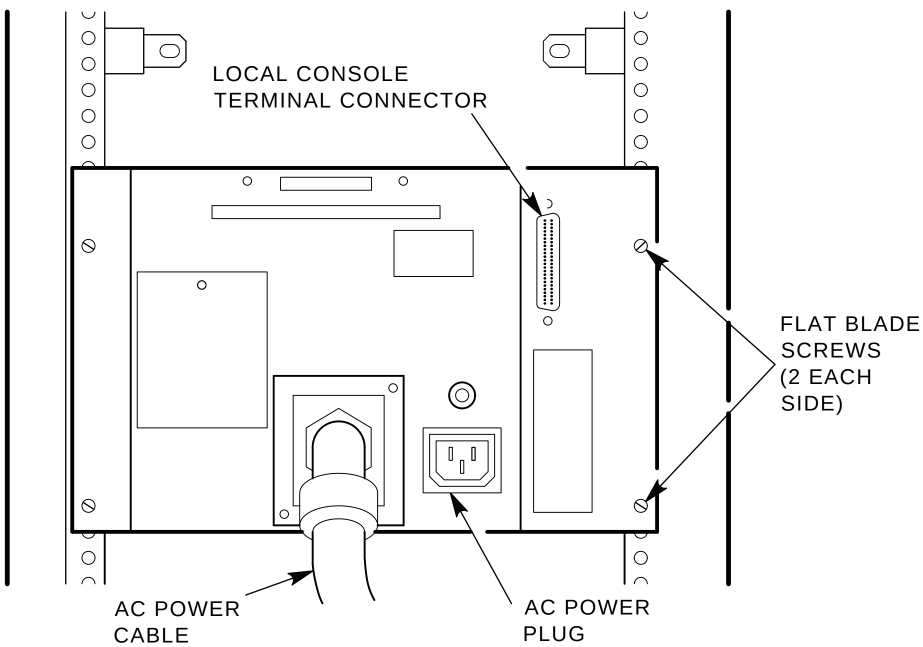


Figure 6–32 AC Distribution Box, Rear View



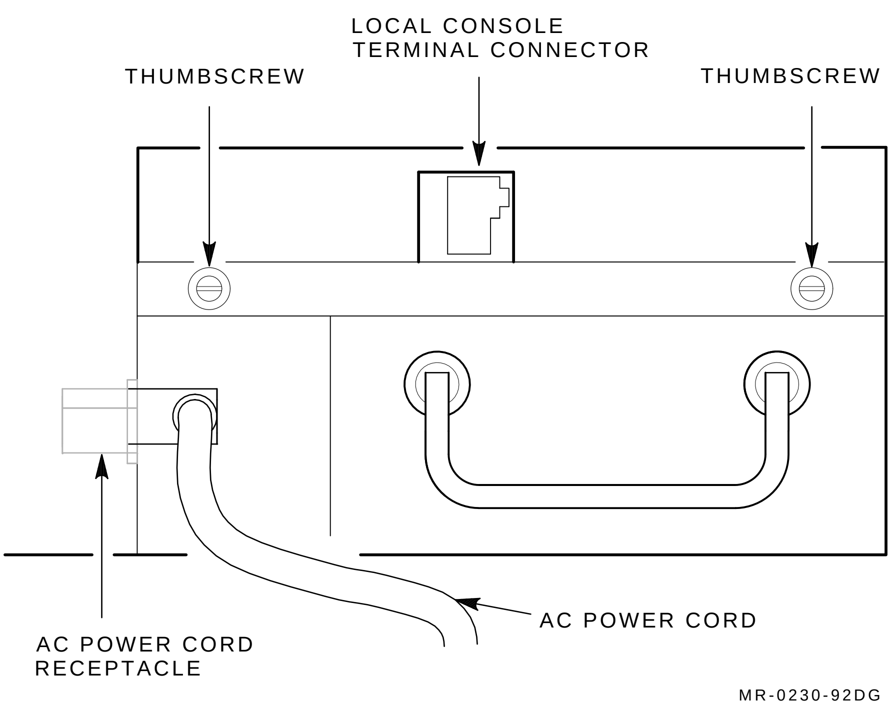
6.14 System Cabinet Fan

The system cabinet has two fans. The system cabinet fan is located beneath the logic card cage, and the dc power supply fan is located inside the dc power supply assembly. If one of these fans needs to be replaced, you should replace the other fan at the same time.

1. Ask the system manager or operator to shut down the zone that houses the faulty fan. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.

4. Note the placement of all cables connected to all modules, and label them if necessary. Disconnect all module cables and tuck them under the system cabinet.
5. Disconnect the ac power cord from the ac power supply (Figure 6–33).
6. Remove the local and remote console cables from the modem port and tuck them under the system cabinet.
7. Loosen the two thumbscrews by turning them to the left.
8. Remove the fan by sliding it straight out of the system cabinet.

Figure 6–33 System Cabinet Fan



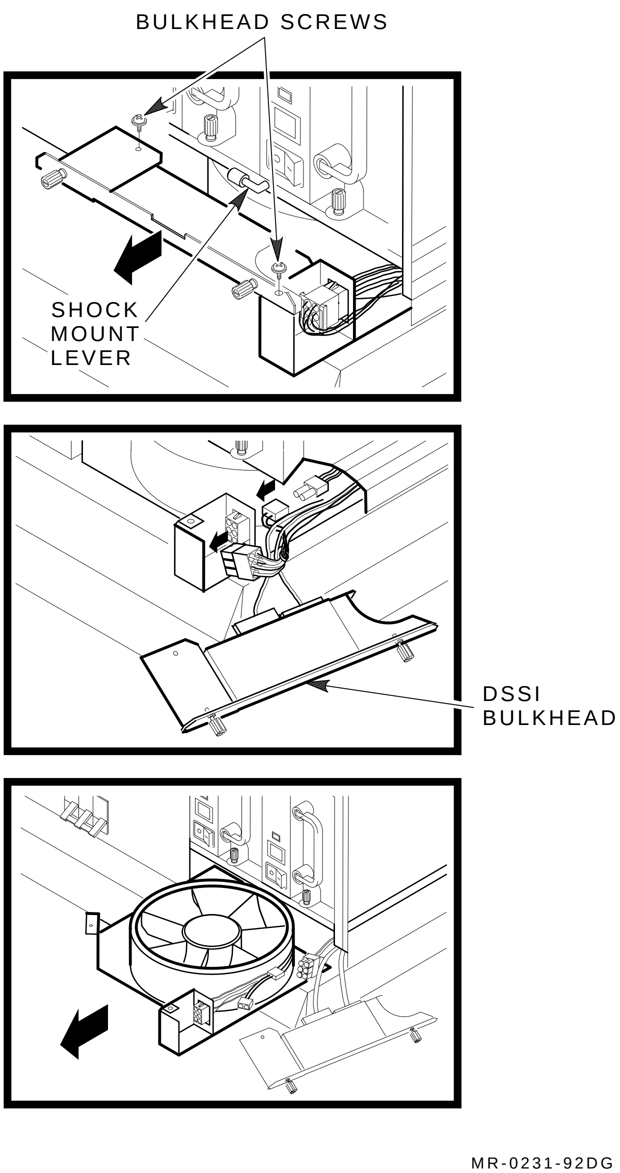
6.15 Expander Cabinet Fan

The expander cabinet has two fans. The expander cabinet fan is located beneath the six-pack backplane, and the dc power supply fan is located inside the dc power supply assembly. If one of these fans needs to be replaced, you should replace the other fan at the same time.

1. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
2. To power off the expander cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
3. Disconnect the ac power cord from the ac power supply (Figure 6–33).
4. Note the placement of the DSSI cables, label them if necessary, and disconnect them from the DSSI bulkhead.
5. Loosen the two thumbscrews by turning them to the left (Figure 6–34).
6. Slide the fan assembly toward you until it is about 1/4 of the way out of the cabinet.
7. Raise the shock mount lever.
8. Disconnect the fan power cable.
9. Disconnect the fan control cable.
10. Remove the two Phillips screws from the DSSI bulkhead.
11. Lift the DSSI bulkhead assembly off the fan assembly, and place it to the right.
12. Remove the fan assembly by sliding it straight out of the expander cabinet.

When replacing the fan assembly, angle it up towards the back for proper alignment.

Figure 6–34 Expander Cabinet Fan



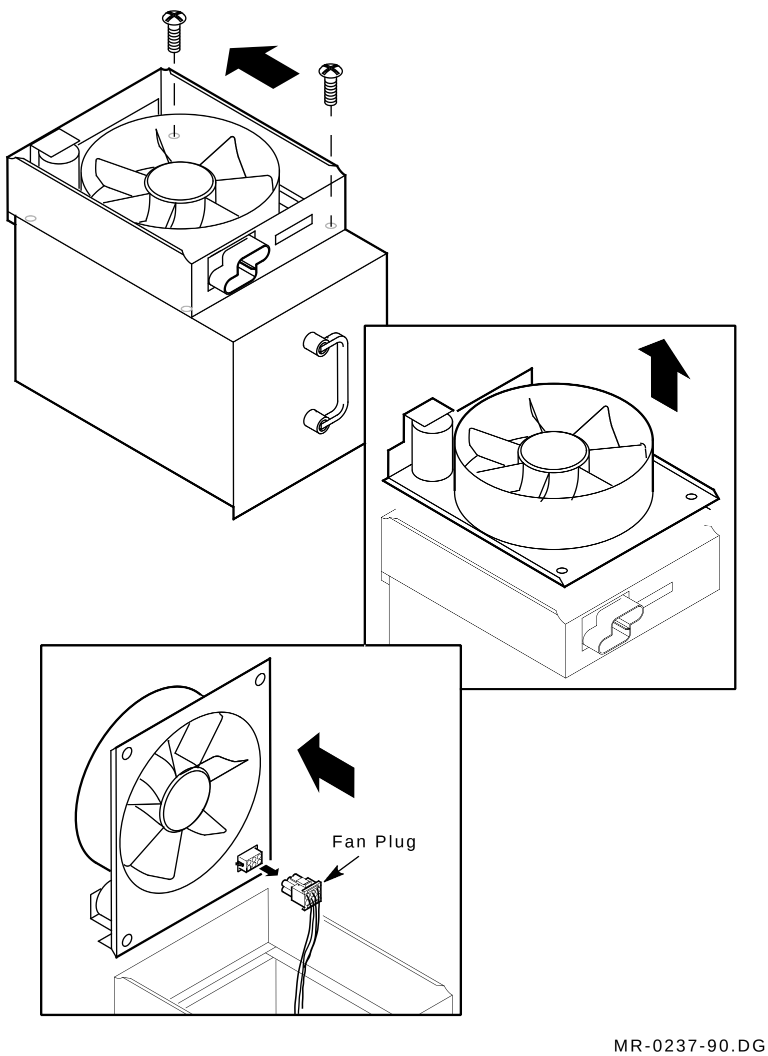
6.16 DC Power Supply Fan Assembly

Both the system cabinet and the expander cabinet have two fans. One fan is located in the lower right side of the cabinet, and the other fan is located inside the dc power supply assembly. If one of these fans needs to be replaced, you should replace the other fan at the same time.

Use the following procedure to remove a dc power supply fan from the system or expander cabinet.

1. Ask the system manager or operator to shut down the zone that houses the faulty fan. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the ac power supply (Section 6.10).
5. Remove the dc power supply (Section 6.11).
6. Place the dc power supply upside down on a grounded antistatic mat.
7. Remove four slotted hex screws (one in each corner) from the fan assembly (Figure 6–35).
8. Lift the rear of the fan assembly slightly.
9. Slide the fan assembly to the back and under the cable connectors on the dc power supply.
10. Lift the fan assembly to expose the fan plug.
11. Disconnect the fan plug.
12. Lift the fan assembly up and away from the dc power supply.

Figure 6–35 DC Fan Assembly

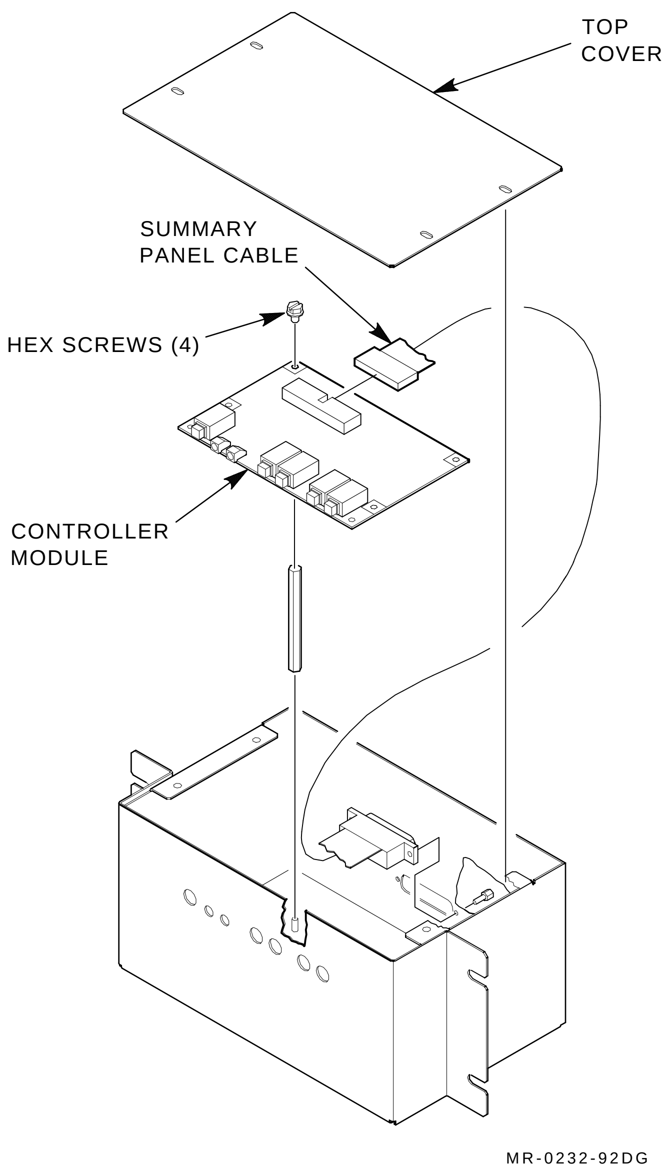


6.17 System Cabinet Summary Panel

Use the following procedure to remove a summary panel from a system cabinet.

1. Ask the system manager or operator to shut down the zone that includes the faulty panel. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the system cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the summary panel cover by pulling it away from the system cabinet. The panel cover is secured with four standoffs and should pull off easily.
5. Remove four slotted hex screws that hold the summary panel in place (Figure 6–36).
6. Pull the summary panel away from the cabinet.
7. Disconnect the summary panel cable by loosening the two screws that secure the cable to the rear of the assembly.
8. Remove the top cover by loosening the four hex screws that secure it to the assembly (Figure 6–36).
9. Disconnect the summary panel cable from the controller module (Figure 6–36).
10. Remove the controller module by loosening the four hex screws that secure it to the assembly (Figure 6–36).

Figure 6–36 System Cabinet Summary Panel

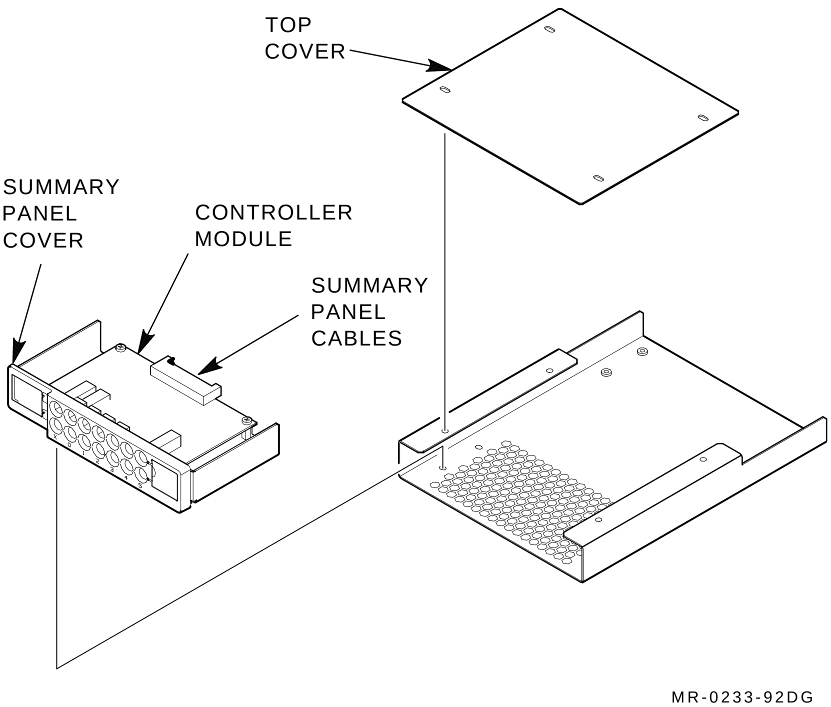


6.18 Expander Cabinet Summary Panel

Use the following procedure to remove a summary panel from an expander cabinet.

1. Ask the system manager or operator to shut down the zone that includes the faulty panel. (Zone shutdown is described in Section 6.1.2.)
2. Open or remove the front doors. (This procedure is described in Section 6.1.4.)
3. To power off the expander cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
4. Remove the summary panel cover by pulling it away from the expander cabinet. The panel cover is secured with four standoffs and should pull off easily.
5. Remove the devices in peripheral slots 6 and 7 (Section 6.4).
6. Loosen the four screws that hold the summary panel in place (Figure 6–37).
7. Release the summary panel by pulling it forward and pushing it up.
8. Remove the top cover by loosening the four hex screws that secure it to the assembly (Figure 6–37).
9. Locate the two summary panel cables, and label them if necessary. Be sure you do not mix them up.
10. Disconnect the summary panel cable by releasing the pushlocks, and then tugging on the pull tab.
11. Remove the controller module by loosening the four screws that secure it to the assembly (Figure 6–37).

Figure 6–37 Expander Cabinet Summary Panel



6.19 DSSI Backplane

Whenever you replace the DSSI backplane, you should also replace the following cables.

- Disk control cable
- DSSI/logic cable

Use the following procedure to replace the DSSI backplane in the system or expander cabinet.

1. Ask the system manager or operator to shut down the zone that houses the faulty DSSI backplane. (Zone shutdown is described in Section 6.1.2.)
2. To power off the cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
3. Remove the device in the left peripheral slot. (See Section 6.5.)
4. At the back of the system, remove 23 screws around the edge of the back cover plate. Remember to support the weight of the cover plate as you do this.
5. Set the back cover plate aside.
6. If you are removing the DSSI backplane from an expander cabinet, disconnect the DSSI cable.
7. Disconnect the summary panel cable from J2.
8. Disconnect the DSSI interplane cable from J3 and J4 in the expander cabinet.
9. Label all cables connected to the backplane. Then disconnect them.
10. Loosen slightly the six screws that secure the backplane on the cabinet frame.
11. Remove the six screws while supporting the weight of the backplane.

6.19.1 Replacement

1. Set the address jumpers (W1 through W3) on the new backplane to match the jumpers on the backplane you removed.

   NOTE

   If you fail to set the address jumpers correctly, the system could crash or be unable to recognize the peripheral devices.

2. If you are replacing the DSSI backplane in a system cabinet, move the DSSI terminator from the old backplane to the new one.
3. Reverse the steps from Section 6.19.

6.20 Six-Pack Backplane

Whenever you replace the six-pack backplane, you should also replace the following cables.

- Disk PCIM cable
- Disk control cable
- DSSI/logic cable

Use the following procedure to remove the six-pack backplane from the expander cabinet.

1. Ask the system manager or operator to shut down the zone that houses the faulty six-pack backplane. (Zone shutdown is described in Section 6.1.2.)
2. To power off the expander cabinet, set the main circuit breaker on the ac power supply to the OFF (down) position.
3. Remove all disks from the six-pack backplane.
4. At the back of the system, remove 23 screws around the edge of the back cover plate. Remember to support the weight of the cover plate as you do this.
5. Set the back cover plate aside.
6. Disconnect the summary panel cable from J12.
7. Disconnect the cable from J11.
8. Disconnect the interplane cable from J10.
9. Disconnect the DSSI to DSSI backplane cables from J7 and J9.

10. Disconnect the fan assembly to PCIM cable from J8, and cut any tie wraps that secure the cable on the backplane.
11. Disconnect the DSSI to bulkhead cables from J14 and J15.
12. Disconnect the fan assembly cable from J13.
13. Check the 16 power distribution cables and label them if necessary.
14. Remove the 16 screws that secure the power distribution cables on the backplane.
15. Loosen slightly the 12 screws that secure the backplane on the cabinet frame.
16. Remove the 12 screws while supporting the weight of the backplane.

A
Managing Integrated Storage Elements

You can use the initially installed configuration for your VAXft system. However, this appendix provides you with alternative ways to manage integrated storage elements (ISEs).

To manage your ISEs, you need to know how to use the VMS diagnostic utility protocol (DUP).

A.1 Using the VMS Diagnostic Utility Protocol

You use the VMS diagnostic utility protocol to change configuration data on mass storage devices. With DUP, you can connect your terminal to a storage controller with the following DCL command:

SET HOST/DUP/SERVER=MSCP$DUP/TASK=taskname nodename

Where:

taskname	=	the utility or diagnostic program name to be executed on the target storage system
nodename	=	the node name of the ISE

You can use the SET HOST/DUP command to create a virtual terminal connection to the MSCP$DUP server and to execute a utility or diagnostic program on the MSCP storage controller that uses the DUP standard dialogue.

Once the connection is established, operations are under the control of the utility or diagnostic program. When the utility or program ends, control returns to the local system.

PARAMS is the DUP management utility that lets you examine and change ISE parameters such as node name, allocation class, and unit number. PARAMS is also used to display the state of the ISE and performance statistics maintained by the ISE.

PARAMS prompts you for a command with the PARAMS> prompt. Once you enter a command, PARAMS executes it, and prompts you for another command.

To stop the PARAMS utility, press Ctrl/C, Ctrl/Y, Ctrl/Z, or type EXIT at the PARAMS prompt.

Table A–1 lists PARAMS commands.

Table A–1 PARAMS Commands

Command	Description
EXIT	Stops the PARAMS utility
HELP	Displays information on how to use PARAMS commands
SET	Changes internal ISE parameters
SHOW	Displays the setting of a parameter or a class of parameters
WRITE	Records in nonvolatile RAM the device parameter changes you made with the SET command

You can find more information on ISE tasks and commands in the RF/TF-series installation guides.

A.2 Using the Server Setup Switch

The server setup (SU) switch facilitates the installation of a new or incorrectly initialized ISE on a running system.

During ISE power on, you press the SU switch to disable the MSCP/TMSCP server within the ISE. Then you can SET HOST from DCL and configure parameters for the ISE with the DUP facility, before VMS recognizes the ISE as an available resource.

The *VAXft Systems Owner's Manual* explains how to use the SU switch.

A.3 Assigning DSSI Unit Numbers

By default, the disk drive forces the unit number to the same value as the DSSI node address for the drive. Since the drives in zone A and zone B initially have the same DSSI unit number, you must reassign unit numbers to remove configuration conflicts and improve system management.

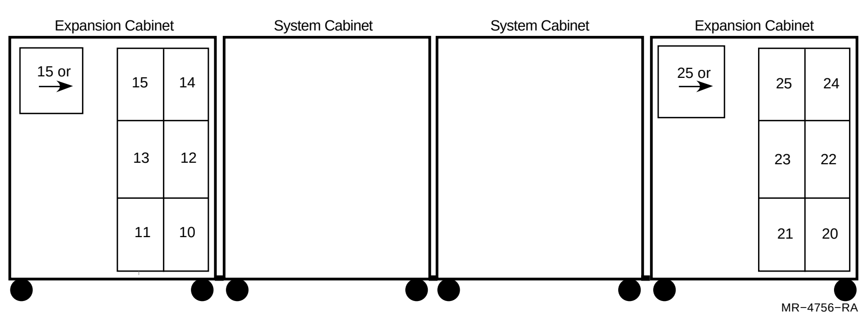
All unit numbers must be unique within an allocation class. You must change the UNITNUM and FORCEUNI ISE parameters (Table A–2) to override the default values that assign the unit the same value as its node address.

One way to achieve this is to reassign unit numbers so that they have values of 8 or higher. For example, you can use a 10- numbering scheme in the first zone and a 20- numbering scheme in the second zone. Figure A–1 shows this drive numbering scheme for an expanded system.

NOTE

The use of the upper left slot in each expander cabinet is mutually exclusive with the slot to its immediate right.

Figure A–1 Unit Number Assignment



A.4 Warm Swapping

NOTE

Warm swapping is not supported for the model 110 system.

Warm swapping is the procedure by which an ISE can be replaced or added to a running system without interrupting system operations.

CAUTION

The procedure must be followed carefully. If a parameter is not entered correctly, then a system reboot is necessary or the ISE (and possibly the system) is rendered unusable. The VMS operating system recognizes an ISE by its unique values for the NODENAME and SYSTEMID parameters. If only one of these parameters is changed, VMS “refuses” connections to both the old and new parameters for the ISE.

NOTE

RF31 ISEs must have V246, or later firmware installed for the warm swap to be successful.

Variations of this procedure depend on the purpose for the warm swap. An ISE can be warm swapped for the following reasons:

- Removal and replacement for storage
- Replacement in a system that is running
- Installation in a system that is running

If you are replacing an ISE or installing a new ISE, you must determine the parameter values for the ISE *before* you perform the warm swap procedure. You must assign values for *each* of the ISE parameters described in Table A–2.

Table A–2 ISE Parameters

Parameter	Description
ALLCLASS[1]	Allocation class. The default value is 0. Set the ALLCLASS value to 0 or the allocation class you have chosen for your system. Note that shadowed disk devices must be set to a nonzero allocation class.

[1]RF-series devices only

Table A–2 (Continued) ISE Parameters

Parameter	Description
FORCENAM	Force name parameter that determines if the ISE is to use the NODENAME parameter value instead of the manufacturing name given to the ISE. The value must be 0. If the value is 1, the ISE uses a generic device name such as RF31**x**.
FORCEUNI	Force unit parameter. To use UNITNUM as the device unit number, set the FORCEUNI parameter to 0. The factory default value of 1 uses the DSSI node address (hardwired on the backplane) as the unit number.
NODENAME	Node name for an ISE. Each ISE has a node name that is stored in EEPROM. The node name is determined in the manufacturing process and is unique to each ISE. The node name can be changed depending on the needs of your site.
SYSTEMID	System identification number. All SYSTEMIDs must be unique within the system. Do not change this parameter when introducing a new ISE to the system.
UNITNUM	Unit number that specifies a numeric value for the device name. You must use a unit number that is unique within the allocation class to which you are configuring the unit. Follow the unit numbering scheme described in Section A.3 or use one that meets your requirements.

You can find more information on ISE parameters in the RF/TF-series installation guides.

A.4.1 Setting ISE Parameters

Digital Equipment Corporation recommends you maintain a worksheet of the parameters for all ISEs, as well as the serial number of each ISE. This is especially important at sites that maintain a set of spare drives that may be stored for some time before they are used.

The worksheet aids in:

- Preventing duplicate parameters, which render an ISE unusable until the duplication is isolated and corrected
- Finding the parameter settings of a nonoperational ISE to create a replacement unit with identical parameters

Use the ISE parameter worksheets (Figures A–2 and A–3) to identify and record critical parameter names. If you are installing a new ISE, select parameter values that meet your site ISE configuration or guidelines. Then continue with Section A.4.5. If you are replacing an ISE, make sure the parameters you select are not being used for another ISE in the configuration.

Figure A–2 Individual ISE Worksheet

Serial Number: ______________________________

NODENAME: ______________________________

SYSTEMID: ______________________________

ALLCLASS: ______________________________

UNITNUM: ______________________________

FORCEUNI: ______________________________

FORCENUM: ______________________________

Serial Number: ______________________________

NODENAME: ______________________________

SYSTEMID: ______________________________

ALLCLASS: ______________________________

UNITNUM: ______________________________

FORCEUNI: ______________________________

FORCENUM: ______________________________

Figure A–3 System ISE Worksheet

Serial Number: ______________________________

NODENAME: ______________________________

SYSTEMID: ______________________________

ALLCLASS: ______________________________

UNITNUM: ______________________________

FORCEUNI: ______________________________

FORCENUM: ______________________________

Serial Number: ______________________________

NODENAME: ______________________________

SYSTEMID: ______________________________

ALLCLASS: ______________________________

UNITNUM: ______________________________

FORCEUNI: ______________________________

FORCENUM: ______________________________

If the parameter values were not recorded, use the following steps to extract the information you need from your system:

1. Find the node name (NODENAME) for an ISE needing replacement by using one of the following DCL commands:
   - SHOW DEVICE [DI or MI]

     Where:

DI	=	disks
MI	=	tapes

     For example:

```
$ SHOW DEVICE DI  Return


Device                 Device     Error   Volume  Free  Trans Mnt
 Name                  Status     Count    Label Blocks Count Cnt
$1$DIA22:   (RIRRBA)   Mounted        0   DISK22 744282    1    1
$1$DIA21    (RICYAA)   Online         5
```

     The node name for the ISE is shown in parentheses.

   - SHOW CLUSTER

     For example:

```
$ SHOW CLUSTER   Return

View of Cluster from system ID 63973 node CLOUDS
+-----------------------------+
|      SYSTEMS      | MEMBERS |
+-----------------------------+
| NODE   | SOFTWARE | STATUS  |
+-----------------------------+
| CLOUDS | VMS V5.4 | MEMBER  |
| RICYAA | RFX V200[1]|         |
| RIRRBA | RFX V200 |         |
+-----------------------------+
```

1 Firmware version number

2. Determine whether the VMS DUP class driver is loaded by entering the following DCL command:

```
$ SHOW DEVICE FYA0  Return
```

If the driver is not loaded, load it as follows:

```
$ MCR SYSGEN  Return
SYSGEN> CONNECT FYA0/NOADAPTER  Return
SYSGEN> EXIT  Return
```

3. Use the SET HOST/DUP command to establish a DUP connection with the ISE.

```
$  SET HOST/DUP/SERVER=MSCP$DUP/TASK=PARAMS nodename
```

This invokes DUP on the ISE and runs the PARAMS utility. If you cannot establish a connection with the ISE DUP, use the DCL command ANALYZE/SYSTEM to find information on some of the parameters.

In the following sample output, the SYSTEMID is 404194100302 and the ALLCLASS is 1.

```
$ ANALYZE/SYSTEM  Return

VMS System Analyzer
SDA> SHOW DEVICE $1$DIA21

I/O data structures
-------------------
$1$DIA21    RF31         UCB address: 802D65D0

Device status:   00021810 online,valid,unload,lcl_valid
Characteristics: 1C4D4108 dir,rct,fod,shr,avl,mnt,elg,idv,odv,rnd
                 000022A1 clu,mscp,srv,nnm,loc


Owner UIC [000010,000001]  Operation count    1116   ORB address  802D6700
      PID        00000000  Error count           0   DDB address  804DA680
Alloc. lock ID   00B000E5  Reference count       1   DDT address  80308BD8
Alloc. class            1  Online count          2   VCB address  802E2750
Class/Type          01/38  BOFF               0000   CRB address  8048C250
Def buf. size         512  Byte count         0000   PDT address  802A5F80
DEVDEPEND        00000000  SVAPTE         00000000   CDDB address 802D6410
DEVDEPND2        00000000  DEVSTS             0004   I/O wait queue  empty
FLCK index             34  RWAITCNT           0000
DLCK address     00000000


    Press RETURN for more.
SDA>  Return

I/O data structures
-------------------

   --- Primary Class Driver Data Block (CDDB) 802D6410 ---

Status:           0040 alcls_set
Controller Flags  80D4 icf_mlths,cf_this,cf_misc,cf_attn,cf_replc
```

```
Allocation class       1   CDRP Queue        empty   DDB address  804DA860
System ID       94100302   Restart Queue     empty   CRB address  8048C250
                    4041   DAP count             3   CDDB link    80344C30
Contrl. ID      94100302   Contr. timeout       60   PDT address  802A5F80
                01644041   Reinit Count          0   Original OCB 00000000
Response ID     00000000   Wait UCB Count        0   UCB chain    802D65D0
MSCP Cmd status FFFFFFFF

  *** I/O request queue is empty ***


    Press RETURN for more.
SDA> EXIT  Return

$
```

4. Enter the DCL command SHOW DEVICE DI to display the following information:

   - Device name

     The device names in the sample output below are 1DIA22 and 1DIA21.

   - NODENAME

     The node name is shown in parentheses. In the following sample output, the node names are RIRRBA and RICYAA.

   - ALLCLASS

     The allocation class is found in the device name between the dollar signs ($). In 1DIA21, the ISE has an allocation class of 1. If the allocation class was 0, the node name would display as RICYAA$DIA21.

   - UNITNUM

     The unit number is the number following the DIA. In 1DIA21, the UNITNUM is 21. It is the MSCP unit number.

- FORCENAM

  The force unit name is set to 0 if NODENAME is anything other than an RF31**x**. The **x** corresponds to a DSSI node ID (A = 0, B = 1, and so on).

- FORCEUNI

  The force unit parameter is not shown in the sample, but it should be 0 if the configuration rules given in the VAXft Systems Configuration Guide were followed.

```
$ SHOW DEVICE DI [Return]

Device                 Device     Error   Volume  Free  Trans Mnt
 Name                  Status     Count    Label Blocks Count Cnt
$1$DIA22    (RIRRBA)   Mounted       0    DISK22 744282    1    1
$1$DIA21    (RICYAA)   Online        5
```

A.4.2 Removal and Replacement for Storage

The following sections describe how to remove an ISE for storage and how to replace the ISE into an existing configuration.

A.4.2.1 Removal

To remove an ISE for storage, perform the following steps:

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used whenever you handle ISEs. Use the static protective service kit (PN 29-262446).

Use great care when handling an ISE. Excessive shock can damage the head/disk assembly (HDA).

1. If the ISE is mounted, logically dismount it from the system.
2. Make the device unavailable to the system with the following DCL command:

```
$ SET DEVICE/NOAVAILABLE devicename [Return]
```

3. Verify that the device has been marked as unavailable by entering the following DCL command:

```
$ SHOW DEVICE RICYAA [Return]

Device                 Device     Error   Volume  Free  Trans Mnt
 Name                  Status     Count    Label Blocks Count Cnt
$1$DIA21    (RICYAA)  Unavailable     5
```

4. Set the ISE power switch to off (0). Wait 45 seconds (for drive to stop spinning and interlock solenoid to release).
5. Remove the ISE from the system or expander cabinet. Follow the steps in the device owner's guide, and observe all FRU handling procedures.
6. Return the repaired/replacement ISE to the appropriate cabinet slot.
7. Restore the parameters for the ISE as described in Section A.4.4.
8. Remember to avoid excessive shock or vibration as you move the ISE to a storage location.

A.4.2.2 Replacement

To replace an ISE from storage, perform the following steps:

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used whenever you handle ISEs. Use the static protective service kit (PN 29-262446).

Use great care when handling an ISE. Excessive shock can damage the HDA.

1. Install the ISE into the correct cabinet.
2. Set the ISE power switch to on (1). Wait for the drive to start spinning and the interlock solenoid to lock.
3. Make the device available to the system with the following DCL command:

```
$ SET DEVICE/AVAILABLE devicename [Return]
```

4. Verify that the device has been marked as available by entering the following DCL command:

```
$ SHOW DEVICE devicename [Return]
```

5. Logically mount the ISE in the system.

A.4.3 Replacement in a System that is Running

When you are replacing an ISE, you must initialize the new ISE with the same parameters as the ISE you are replacing. Refer to the worksheet you maintain for that ISE. (See Section A.4.1.)

You can power off and replace an ISE in a running system without interrupting system services or users. When the ISE is replaced, the new ISE must be correctly initialized to:

- Supersede preset manufacturing values
- Store the modified values in EEPROM

To replace an ISE in a system that is running, perform the following steps:

CAUTION

An ESD wrist strap, ground clip, and grounded ESD workmat must be used whenever you handle ISEs. Use the static protective service kit (PN 29-262446).

Use great care when handling an ISE. Excessive shock can damage the HDA.

1. If the ISE is mounted, logically dismount it from the system.
2. Make the device unavailable to the system with the following DCL command:

```
$ SET DEVICE/NOAVAILABLE devicename [Return]
```

3. Verify that the device has been marked as unavailable by entering the following DCL command:

```
$ SHOW DEVICE devicename [Return]
```

4. Set the ISE power switch to off (0). Wait 45 seconds (for drive to stop spinning and interlock solenoid to release).
5. Remove the ISE from the system or expander cabinet. Follow the steps in the device owner's guide, and observe all FRU handling procedures.
6. Return the repaired/replacement ISE to the appropriate cabinet slot.
7. Restore the parameters for the ISE as described in Section A.4.4.

A.4.4 Restoring ISE Parameters

If you are replacing an ISE in a system that is running, use the following steps to restore the parameters from the ISE you replaced. If you are installing a new ISE in a system that is running, use the steps in Section A.4.5.

1. Press and hold the ISE server setup (SU) switch. This disables the MSCP/TMSCP server.
2. Set the ISE power switch to on (1).
3. Release the server setup switch.
4. Find the NODENAME parameter for the replacement ISE by using the DCL command SHOW CLUSTER. (SHOW DEVICE will not work at this time.) In the sample output below, R1QSAA is the replacement ISE.

```
$ SHOW CLUSTER  Return

View of Cluster from system ID 63973 node CLOUDS
+----------------------------+
|      SYSTEMS      | MEMBERS |
+----------------------------+
| NODE   | SOFTWARE | STATUS  |
+----------------------------+
| CLOUDS | VMS V5.4 | MEMBER  |
| RICYAA | RFX V200¹|         |
| RIRRBA | RFX V200 |         |
| R1QSAA | RFX V200 |         |
+----------------------------+
```

5. Determine whether the VMS DUP class driver is loaded by entering the following DCL command:

```
$ SHOW DEVICE FYA0  Return
```

If the driver is not loaded, load it by entering the following:

```
$ MCR SYSGEN  Return
SYSGEN> CONNECT FYA0/NOADAPTER  Return
SYSGEN> EXIT  Return
```

---

[1] Firmware version number

6. Use the SET HOST/DUP command to establish a DUP connection with the ISE.

```
$  SET HOST/DUP/SERVER=MSCP$DUP/TASK=PARAMS nodename
```

This invokes DUP on the ISE and runs the PARAMS utility.

7. Refer to the parameters listed in Table A–2, and use the SET command to set appropriate values for the parameters. Be sure to record the new parameters on the worksheet for the ISE.

For example:

```
$ SET HOST/DUP/SERVER=MSCP$DUP/TASK=PARAMS R1QSAA  [Return]
  %HSCPAD-I-LOCPROGEXE, Local program executing - type ^\ to exit
  Copyright (C) 1990 Digital Equipment Corporation

  PARAMS> SHOW NODENAME  [Return]
  Parameter     Current       Default      Type       Radix
  ---------- -------------  -------------- ---------- ---------
  NODENAME      R1QSAA          RF31       String     Ascii

PARAMS> SET NODENAME RICYAA  [Return]

PARAMS> SHOW SYSTEMID [Return]
Parameter     Current       Default      Type       Radix
---------- ------------  -------------- ---------- ---------
SYSTEMID    593200495860  0000000000000  Quadword    Hex       B

PARAMS> SET SYSTEMID 0404194100302 [Return]

PARAMS> SHOW ALLCLASS  [Return]
Parameter     Current       Default      Type       Radix
---------- ------------  -------------- ---------- ---------
ALLCLASS               0               0    Byte       Dec     B

PARAMS> SET ALLCLASS 1  [Return]

PARAMS> SHOW FORCENAM [Return]
Parameter     Current       Default      Type       Radix
---------- ------------  -------------- ---------- ---------
FORCENAM               0              0   Boolean     0/1      B

PARAMS> SHOW UNITNUM [Return]
Parameter     Current       Default      Type       Radix
---------- ------------  -------------- ---------- ---------
UNITNUM                 0              0    Word       Dec     U

PARAMS> SET UNITNUM 21  [Return]

PARAMS> SHOW FORCEUNI [Return]
Parameter     Current       Default      Type       Radix
---------- ------------  -------------- ---------- ---------
FORCEUNI               1              1   Boolean     0/1      U

PARAMS> SET FORCEUNI 0  [Return]


PARAMS> WRITE  [Return]
```

```
Changes require controller initialization, ok? [Y/(N)] Y
Initializing...

HSCPAD-S-REMPGMEND, Remote program terminated - message number 3
%HSCPAD-S-END, Control returned to CLOUDS
$
```

When initialization is complete, the replacement ISE and its parameters are made available to the VMS operating system.

NOTE

The SHOW CLUSTER command continues to show the name of the ISE you replaced. This does not harm the system. After the next reboot, the replacement ISE name appears.

Note also that the following message is displayed if another node is already assigned the same SYSTEMID and NODENAME:

```
%PWA0-REMOTE SYSTEM CONFLICTS WITH KNOWN SYSTEM
```

In this case, shut down the new node and issue a unique SYSTEMID and NODENAME for the new node.

A.4.5 Installation in a System that is Running

When you are installing a new ISE in a system that is running, use the following steps to initialize the new ISE parameters.

1. Press and hold the ISE server setup (SU) switch. This disables the MSCP/TMSCP server.
2. Set the ISE power switch to on (1).
3. Release the server setup switch.
4. Refer to Table A–2 and Section A.4.1, and select values for the following parameters:
   - ALLCLASS
   - FORCENAM
   - FORCEUNI
   - NODENAME
   - UNITNUM

5. Determine whether the VMS DUP class driver is loaded by entering the following DCL command:

```
$ SHOW DEVICE FYA0  Return
```

   If the driver is not loaded, load it by entering the following:

```
$ MCR SYSGEN Return
SYSGEN> CONNECT FY0/NOADAPTER Return
SYSGEN> EXIT Return
```

6. Use the SET HOST/DUP command to establish a DUP connection with the ISE.

```
$  SET HOST/DUP/SERVER=MSCP$DUP/TASK=PARAMS nodename
```

   This invokes DUP on the ISE and runs the PARAMS utility.

7. Use the SET command to set appropriate values for the parameters. Be sure to record the new parameters on the worksheet for the ISE.

   In the following sample output, the new ISE is configured to be device 1DIA22. The device is initialized with these parameters:

   - ALLCLASS — 1
   - FORCENAM — 0
   - FORCEUNI — 0
   - NODENAME — DISK22
   - SYSTEMID — no change
   - UNITNUM — 22

```
$ SET HOST/DUP/SERVER=MSCP$DUP/TASK=PARAMS R1QSAA  Return
%HSCPAD-I-LOCPROGEXE, Local program executing - type ^\ to exit
Copyright (C) 1990 Digital Equipment Corporation

PARAMS> SHOW NODENAME  Return
Parameter     Current       Default      Type       Radix
---------- ------------  ------------- ---------- ---------
NODENAME      R1QSAA            RF31     String     Ascii
```

```
PARAMS> SET NODENAME DISK22  Return

PARAMS> SHOW ALLCLASS  Return
Parameter     Current       Default      Type       Radix
---------- ------------  ------------- ---------- ---------
ALLCLASS              0               0    Byte       Dec     B

PARAMS> SET ALLCLASS 1  Return

PARAMS> SHOW FORCENAM  Return
Parameter     Current       Default      Type       Radix
---------- ------------  ------------- ---------- ---------
FORCENAM              0              0   Boolean     0/1      B

PARAMS> SHOW UNITNUM  Return
Parameter     Current       Default      Type       Radix
---------- ------------  ------------- ---------- ---------
UNITNUM               0              0    Word       Dec      U

PARAMS> SET UNITNUM 22  Return

PARAMS> SHOW FORCEUNI  Return
Parameter     Current       Default      Type       Radix
---------- ------------  ------------- ---------- ---------
FORCEUNI              1              1   Boolean     0/1      U

PARAMS> SET FORCEUNI 0  Return


PARAMS> WRITE  Return

Changes require controller initialization, ok? [Y/(N)] Y
Initializing...

HSCPAD-S-REMPGMEND, Remote program terminated - message number 3
%HSCPAD-S-END, Control returned to CLOUDS
$
```

When initialization is complete, the new ISE and its parameters are made available to the VMS operating system.

NOTE

The SHOW CLUSTER command continues to show the name of the ISE you replaced. This does not harm the system. After the next reboot, the new ISE name appears.

Index

M

P

R

W

Z