Servicing your StorageWorks subsystem

HSJ50 Array Controllers

HSOF Version 5.0

StorageWorks

Part Number: EK-HSJ50-SV.A01
July, 1996

While Digital Equipment Corporation believes the information included in this manual is correct as of the date of publication, it is subject to change without notice. Digital makes no representations that the interconnection of its products in the manner described in this document will not infringe existing or future patent rights, nor do the descriptions contained in this document imply the granting of licenses to make, use, or sell equipment or software in accordance with the description. No responsibility is assumed for the use or reliability of firmware on equipment not supplied by Digital or its affiliated companies. Possession, use, or copying of the software or firmware described in this documentation is authorized only pursuant to a valid written license from Digital, an authorized sublicensor, or the identified licensor.

Commercial Computer Software, Computer Software Documentation and Technical Data for Commercial Items are licensed to the U.S. Government with Digital's standard commercial license and, when applicable, the rights in DFAR 252.227-7015, "Technical Data—Commercial Items."

© Digital Equipment Corporation 1996
Printed in U.S.A.
All rights reserved.

Alpha, CI, DCL, DECconnect, DECserver, Digital, DSSI, HSC, HSJ, HSD50, HSZ, MSCP, OpenVMS, StorageWorks, TMSCP, VAX, VAXcluster, VAX 7000, VAX 10000, VMS, VMScluster, and the Digital logo are trademarks of Digital Equipment Corporation. All other trademarks and registered trademarks are the property of their respective holders.
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Restrictions apply to the use of the local-connection port on this series of controllers; failure to observe these restrictions may result in harmful interference. Always disconnect this port as soon as possible after completing the setup operation. Any changes or modifications made to this equipment may void the user's authority to operate the equipment.

Warning!
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Avertissement!
Cet appareil est un appareil de Classe A. Dans un environnement résidentiel cet appareil peut provoquer des brouillages radioélectriques. Dans ce cas, il peut être demandé à l' utilisateur de prendre les mesures appropriées.

Contents

1 Troubleshooting, 1
Introduction, 2
Fault isolation guide, 3
Interpreting controller LED codes, 7
Interpreting host event log messages, 12
Reading a DECevent error log, 16
Using FMU to Describe Event Log Codes, 20
Testing disks (DILX), 24
Testing tapes (TILX), 37
Monitoring system performance with the VTDPY utility, 52
CI/DSSI host port characteristics, 57
SCSI host port characteristics, 58
CI performance display, 60
DSSI performance display, 61
CI/DSSI connection status, 62
CI/DSSI host path status, 64
Device SCSI status, 66
Unit status (abbreviated), 68
Unit status (full), 72
Device status, 76
Device SCSI port performance, 79
Help example, 80

2 Replacing field-replaceable units, 81
Electrostatic discharge protection, 82
Replacing controllers and cache modules using C_swap, 84
Replacing a controller and cache module in a single controller configuration, 95
Replacing one dual-redundant controller and write-back cache module, 103
Replacing cache modules, 111
Replacing SBB battery modules (external cache batteries), 116
Replacing power supplies, 129
Replacing storage devices, 132
Replacing tape drives, 135
Replacing a solid-state disk drive, optical, or CD-ROM drives, 137
Replacing internal CI cables, 139
Replacing SCSI device port cables, 141

3 Installation, 145
Precautions, 146
Patching controller software, 147
Formatting disk drives, 156
Installing new firmware on a device, 159
Enabling a licensed option (FLS Utility), 169
Installing a controller and cache module (single controller configuration), 178
Installing a second controller and cache module, 184
Adding a second controller using C_SWAP, 191
Installing a cache module, 196
Adding Cache Memory, 204
Installing power supplies, 212
Installing storage building blocks, 217

4 Moving storagesets and devices, 223
Precautions, 224
Moving storagesets, 225
Moving storageset members, 228

Moving a single disk-drive unit, 230
Moving devices, 232

5 Removing, 235
Precautions, 236
Removing a patch, 237
Disabling a licensed option, 241
Removing a license key, 244
Removing a controller and cache module, 247
Removing storage devices, 252

Appendix, 357
Instance codes and definitions, 258
Last fail codes, 290
Repair action codes, 329

Glossary, 339

Index, 357

Related documents

The following table lists documents that contain information related to this product.

Document Name	Order number
StorageWorks HSZ40 Array Controller Utility for Digital UNIX, System Manager's Guide for HSZterm	AA–QC39B–TE
DECevent Analysis and Notification Utility for OpenVMS User and Reference Guide	AA–Q73LA–TE
DECevent Installation Guide	AA–Q73JA–TE
DECevent Translation and Reporting Utility for OpenVMS User and Reference Guide	AA–Q73KA-TE
StorageWorks BA350–MA Controller Shelf User's Guide	EK–350MA–UG
StorageWorks Configuration Manager for DEC OSF/1 Installation Guide	AA–QC38A–TE
StorageWorks Configuration Manager for DEC OSF/1 System Manager's Guide for HSZterm	AA–QC39A–TE
StorageWorks Family StorageWorks Building Blocks User's Guide	EK–SBB35–UG
StorageWorks Solutions Configuration Guide	EK–BA350–CG
StorageWorks Solutions Shelf and SBB User's Guide	EK–BA350–UG
StorageWorks Solutions SW300-Series RAID Enclosure Installation and User's Guide	EK–SW300–UG
StorageWorks SW500-Series Cabinet Installation and User's Guide	EK–SW500–IG
StorageWorks SW500-Series Cabinet Cable Distribution Unit Installation Guide	EK–SW5CU–IG
StorageWorks SW800-Series Data Center Cabinet Cable Distribution Unit Installation Sheet	EK–SWCDU–IS
StorageWorks SW800-Series Data Center Cabinet Installation and User's	EK–SW800–IG

Guide	
The Digital Guide to RAID Storage Technology	EC–B1960–45
The RAIDBOOK—A Source for RAID Technology	RAID Advisory Board
VAXcluster Console System User's Guide	AA–GV45D–TE
VAXcluster Systems Guidelines for VAXcluster System Configurations	EK–VAXCS–CG

1 Troubleshooting

Fault isolation guide

Interpreting controller LED codes

Interpreting host event log messages

Reading a DECevent error log

Using FMU to describe event log codes

Testing disk drives

Testing tapes

Monitoring subsystem performance

Introduction

This chapter is designed to help you quickly isolate the source of any problems that you might encounter while working with StorageWorks HSJ controllers, and take steps to correct the situation.

If your subsystem is currently experiencing a problem use the information in this chapter to determine the likely source of those symptoms.

If your subsystem is not currently experiencing a problem and you're just looking for useful information, read the first few pages of this chapter to learn:

- how this chapter is laid out to help in troubleshooting
- what tools are available to aid in troubleshooting
- how to be configure your subsystem to aid in troubleshooting any problems that might arise.

Fault isolation guide

This chapter is structured to help you match the symptoms that you are seeing (console message, unit not available, and so on) with the source of those symptoms.

Controller is not operating

Symtpoms

- Controller is not operating.
- Green RESET LED is on solid.
- Controller does not restart when you press the RESET button.

Likely Cause

In dual-redundant configurations, when one controller stops, the surviving controller asserts a “kill” line, which prevents the controller from restarting.

Solution

1. Establish a local or remote terminal connection to the operating controller.
2. From the CLI, tell the operating controller to allow the other controller to restart:

   ```
   CLI> RESTART OTHER_CONTROLLER
   ```

3. Press the RESET button on the non-operating controller and verify that it returns to normal service.

Unable to see units from host

Symtpoms

- Units have been created in the subsystem, but cannot be seen from the host.

Likely Cause

Settings are not correct or enabled to allow the subsystem to communicate with the host.

Solution

- Check that the console version includes HSJ50 device support.
- Check that PATH_A and PATH_B are enabled on the HSJ50 (SHOW THIS).
- Check that the CIXCD is set up correctly:
  - Quiet Slot Count = 10 (Tick Count)
  - CI Node number for the subsystem does not conflict with another CI node.
  - CIXCD transition card is plugged into the right backplane slot and seated properly.
  - CI cables are wired correctly: Transmit to Transmit and Receive to Receive
- Check that the screws that attach the internal CI cable to the controller are tightened.

VMS shadowsets go into mount verify

Symtpoms

- HSJ40 units that are members of VMS shadowsets intermittently go into Mount Verification during heavy I/O operations such as backup or shadow copy.
- VMS errorlog shows “DATAGRAM FOR NON-EXISTING UCB” at the time of the mount verifications.
- HSJ50 controller error log shows instance code 4007640A.

Likely Cause

The HSJ50 declared a timeout on the CI, which momentarily closed its VC with the host node.

Solution

The Quiet Slot may not be set correctly on the host nodes to work with the HSJ50 controllers. Set the Quiet Slot to 10.

Units are Host Unavailable

Symtpoms

- The OpenVMS host reports all disk or tape units in the StorageWorks subsystem as host unavailable.
- The host can see the controller.

Likely Cause

The CI connections are not complete.

The MSCP and/or TMSCP allocation class settings on the controller have been changed while the cluster was up.

Solution

Check the CI cable connections.

Check the MSCP and TMSCP allocation class in the controller.

```
CLI> SHOW THIS_CONTROLLER
CLI> SHOW OTHER_CONTROLLER
```

If the settings are not correct, you must either change them and the restart the cluster, or change the controller's SCS_NODENAME.

If the SCS_NODENAME contains characters such as "_" or "$", the controller will not establish a VMS disk or tape class connection. Change the SCS_NODENAME and restart the controller.

Foreign disk drive is not usable

Symtpoms

- An RZ disk drive moved from another environment to the StorageWorks subsystem is not usable from the host.
- You want to keep the data that is on the foreign disk drive.

Likely Cause

The disk does not contain controller metadata, and is not set as TRANSPORTABLE. The HSJ controller can only present foreign disks when they are set as TRANSPORTABLE.

Solution

1. From the controller CLI, set the disk drive as transportable:

   ```
   CLI> SET disk-name TRANSPORTABLE
   ```

   where *disk-name* is the name that you gave the foreign drive with the ADD DISK command.

2. Look for the disk as a DKA device in VMS.

Interpreting controller LED codes

The operator control panel (OCP) on each HSJ controller contains a green reset LED and six device bus LEDs. These LEDs light in patterns to display codes when there is a problem with a device configuration, a device, or a controller.

- During normal operation, the green reset LED on each controller flashes once per second, and the device bus LEDs are not lit.
- The amber LED for a device bus lights continuously when the installed devices do not match the controller configuration, or when a device fault occurs.
- The green reset LED lights continuously and the amber LEDs display a code when a controller problem occurs. Solid LED codes indicate a fault detected by internal diagnostic and initialization routines. Flashing LED codes indicate a fault that occurred during core diagnostics.

Look up the LED code that is showing on your controller in Table 1 or Table 2 to determine its meaning and find the corrective action.

Table 1
Solid controller LED codes

Code	Description of Error	Corrective Action
●●●●●●●	DAEMON hard error	Replace controller module.
●●●●●●❍	Repeated firmware bugcheck	Replace controller module.
●●●●●❍●	NVMEM version mismatch	Replace program card with later version of firmware.
●●●●●❍❍	NVMEM write error	Replace controller module.
●●●●❍●●	NVMEM read error	Replace controller module.
●●●●❍●❍	NMI error within firmware bugcheck	Reset the controller.
●●●●❍❍●	Inconsistent NVMEM structures repaired	Reset the controller.
●●●●❍❍❍	Bugcheck with no restart	Reset the controller.

Code	Description of Error	Corrective Action
●●●❍●●●	Firmware induced restart following bugcheck failed to occur	Replace controller module.
●●●❍●●❍	Hardware induced restart following bugcheck failed to occur	Replace controller module.
●●●❍●❍●	Bugcheck within bugcheck controller	Reset controller module.
●●●❍❍●●	NVMEM version is too low	Verify the card is the latest revision. If the problem still exists, replace the module.
●●●❍❍●❍	Program card write fail	Replace the card.
●●●❍❍❍●	ILF$INIT unable to allocate memory	Reset the controller.
●●●❍❍❍❍	Bugcheck before subsystem initialization completed	Reset the controller.
●❍❍❍❍❍❍	No program card seen	Try the card in another module. If the problem follows the card, replace the card. Otherwise, replace the controller.

Table 2
Flashing controller LED codes

Code	Description of Error	Corrective Action
●❍❍❍❍❍✵	Program card EDC error	Replace program card.
●❍❍❍✵❍❍	Timer zero in the timer chip will run when disabled	Replace controller module.
●❍❍❍✵❍✵	Timer zero in the timer chip decrements incorrectly	Replace controller module.
●❍❍❍✵✵❍	Timer zero in the timer chip did not interrupt the processor when requested	Replace controller module.
●❍❍❍✵✵✵	Timer one in the timer chip decrements incorrectly	Replace controller module.
●❍❍✵❍❍❍	Timer one in the timer chip did not interrupt the processor when requested	Replace controller module.
●❍❍✵❍❍✵	Timer two in the timer chip decrements	Replace controller module.

Code	Description of Error	Corrective Action
	incorrectly	
● ❍ ❍ ❄ ❍ ❄ ❍	Timer two in the timer chip did not interrupt the processor when requested	Replace controller module.
● ❍ ❍ ❄ ❍ ❄ ❄	Memory failure in the I/D cache	Replace controller module.
● ❍ ❍ ❄ ❄ ❍ ❍	No hit or miss to the I/D cache when expected	Replace controller module.
● ❍ ❍ ❄ ❄ ❍ ❄	One or more bits in the diagnostic registers did not match the expected reset value	Replace controller module.
● ❍ ❍ ❄ ❄ ❄ ❍	Memory error in the nonvolatile journal SRAM	Replace controller module.
● ❍ ❍ ❄ ❄ ❄ ❄	Wrong image seen on program card	Replace program card
● ❍ ❄ ❍ ❍ ❍ ❍	At least one register in the controller DRAB does not read as written	Replace controller module.
● ❍ ❄ ❍ ❍ ❍ ❄	Main memory is fragmented into too many sections for the number of entries in the good memory list	Replace controller module.
● ❍ ❄ ❍ ❍ ❄ ❍	The controller DRAB or DRAC chip does not arbitrate correctly	Replace controller module.
● ❍ ❄ ❍ ❍ ❄ ❄	The controller DRAB or DRAC chop failed to detect forced parity, or detected parity when not forced	Replace controller module.
● ❍ ❄ ❍ ❄ ❍ ❍	The controller DRAB or DRAC chip failed to verify the EDC correctly	Replace controller module.
● ❍ ❄ ❍ ❄ ❍ ❄	The controller DRAB or DRAC chip failed to report forced ECC	Replace controller module.
● ❍ ❄ ❍ ❄ ❄ ❍	The controller DRAB or DRAC chip failed some operation in the reporting, validating, and testing of the multibit ECC memory error	Replace controller module.
● ❍ ❄ ❍ ❄ ❄ ❄	The controller DRAB or DRAC chip failed some operation in the reporting, validating, and testing of the multiple single-bit ECC memory error	Replace controller module.
● ❍ ❄ ❄ ❍ ❍ ❍	The controller main memory did not write correctly in one or more sized memory transfers	Replace controller module.
● ❍ ❄ ❄ ❍ ❍ ❄	The controller did not cause an I-to-N bus timeout when accessing a "reset" host port	Replace controller module.

Code	Description of Error	Corrective Action
	chip	
● ❍ ✵ ✵ ❍ ✵ ❍	The controller DRAB or DRAC did not report an I-to-N bus timeout when accessing a "reset" host port chip.	Replace controller module.
● ❍ ✵ ✵ ❍ ✵ ✵	The controller DRAB or DRAC did not interrupt the controller processor when expected	Replace controller module.
● ❍ ✵ ✵ ✵ ❍ ❍	The controller DRAB or DRAC did not report an NXM error when nonexistent memory was accessed	Replace controller module.
● ❍ ✵ ✵ ✵ ❍ ✵	The controller DRAB or DRAC did not report an address parity error when one was forced	Replace controller module.
● ❍ ✵ ✵ ✵ ✵ ❍	There was an unexpected nonmaskable interrupt from the controller DRAB or DRAC during the DRAB memory test.	Replace controller module.
● ❍ ✵ ✵ ✵ ✵ ✵	Diagnostic register indicates there is no cache module, but an interrupt exists from the non-existent cache module	Replace controller module.
● ✵ ❍ ❍ ❍ ❍ ❍	The required amount of memory available for the code image to be loaded from the program cad is insufficient	Replace controller module.
● ✵ ❍ ❍ ❍ ❍ ✵	The required amount of memory available in the pool area is insufficient for the controller to run	Replace controller module.
● ✵ ❍ ❍ ❍ ✵ ✵	The required amount of memory available in the buffer area is insufficient for the controller to run	Replace controller module.
● ✵ ❍ ❍ ✵ ❍ ❍	The code image was not the same as the image on the card after the contents were copied to memory	Replace controller module.
● ✵ ❍ ❍ ✵ ❍ ✵	Diagnostic register indicates that the cache module does not exist, but access to that cache module caused an error	Replace controller shelf backplane.
● ✵ ❍ ❍ ✵ ✵ ❍	Diagnostic register indicates that the cache module does not exist, but access to that cache module did not cause an error	Replace controller shelf backplane.
● ✵ ✵ ❍ ❍ ❍ ❍	the journal SRAM battery is bad	Replace controller module.

Code	Description of Error	Corrective Action
● ✲ ✲ ✲ ❍ ✲ ❍	There was an unexpected interrupt from a read cache or the present and lock bits are not working correctly	Replace controller module.
● ✲ ✲ ✲ ❍ ✲ ✲	There is an interrupt pending on the controller's policy processor when there should be none	Replace controller module.
● ✲ ✲ ✲ ✲ ❍ ❍	There was an unexpected fault during initialization	Replace controller module.
● ✲ ✲ ✲ ✲ ❍ ✲	There was an unexpected maskable interrupt received during initialization	Replace controller module.
● ✲ ✲ ✲ ✲ ✲ ❍	There was an unexpected nonmaskable interrupt received during initialization	Replace controller module.
● ✲ ✲ ✲ ✲ ✲ ✲	An illegal process was activated during initialization	Replace controller module.

Interpreting host event log messages

This section explains how to interpret event messages sent to the host system by StorageWorks HSJ controllers. Some of these messages are information-only, others report significant events, and others report subsystem and controller failures.

You can use the Fault Management Utility (FMU) in the controller to get more information on any specific event. The FMU can provide a description of instance codes, last failure codes, and memory system failure codes. The FMU can also provide recommended repair actions for each code. Because the subsystem and controller might be out of service after an event that generates a last failure code, you might not be able to run FMU. Instance codes and last failure codes are listed in this chapter.

Finding the Instance Code in an Event Message

To work with and understand the event logs, use these steps and guidelines.

1. Note the MSLG$B_FORMAT field in the upper portion of the log. Also note the CONTROLLER DEPENDENT INFORMATION in the lower portion of the log: this information varies according to the MSLG$B_FORMAT field.

2. Locate a 32-bit instance code in the CONTROLLER DEPENDENT INFORMATION area. This is the key to interpreting error logs. The instance code uniquely identifies the following:

   – The error or condition

   – The component reporting the condition

   – The recommended repair action

3. Keep in mind that the 32-bit instance code appears in LONGWORD 1 of CONTROLLER DEPENDENT INFORMATION, with the following exceptions:

   - When MSLG$B_FORMAT reads 09 BAD BLOCK REPLACEMENT ATTEMPT, the instance code does not appear, because ERF does not provide CONTROLLER DEPENDENT INFORMATION.
   - When MSLG$B_FORMAT reads 0A MEDIA LOADER LOG, the instance code appears in LONGWORD 2.
   - When MSLG$B_FORMAT reads 00 CONTROLLER LOG, the instance code appears in part of both LONGWORD 1 and LONGWORD 2.
   - For the 00 CONTROLLER LOG MSLG$B_FORMAT, the code is skewed and not directly readable as a longword. (The code's low-order bytes appear in the two high-order bytes of LONGWORD 1, and the code's high-order bytes appear in the two low-order bytes of LONGWORD 2.) For example:

```
CONTROLLER DEPENDENT INFORMATION
       LONGWORD 1.     030A0000
                                    /..../
       LONGWORD 2.     24010102
                                    /...$/
```

4. The following VMS example shows an example of an Error Reporting Formatter (ERF) translated host error log (a Disk Transfer Event log). Locate MSLG$B_FORMAT and CONTROLLER DEPENDENT INFORMATION in the example.

```
V M S                SYSTEM ERROR REPORT         COMPILED  9-AUG-1994 13:41:37
                                                                    PAGE 758.
******************************* ENTRY    1122. *******************************
ERROR SEQUENCE 5.                              LOGGED ON:  CPU_TYPE 00000002
DATE/TIME 28-APR-1994 11:39:40.33                           SYS_TYPE 00000003
SYSTEM UPTIME: 0 DAYS 00:01:41
SCS NODE: MTX2                                            OpenVMS AXP X6.1-FT7

HW_MODEL: 00000401 Hardware Model = 1025.
ERL$LOGMESSAGE ENTRY DEC 7000 Model 610

I/O SUB-SYSTEM, UNIT _MAT$DUA450:

      MESSAGE TYPE        0001
                                  DISK MSCP MESSAGE
      MSLG$L_CMD_REF  00000000
      MSLG$W_UNIT         01C2
                                  UNIT #450.
      MSLG$W_SEQ_NUM      0015
                                  SEQUENCE #21.
      MSLG$B_FORMAT         02
                                  DISK TRANSFER LOG
      MSLG$B_FLAGS          00
                                  UNRECOVERABLE ERROR
      MSLG$W_EVENT        014B
                                  DRIVE ERROR
                                  CNTRLR DETECTED PROTOCOL ERROR
      MSLG$Q_CNT_ID   01280009 40802576
                                  UNIQUE IDENTIFIER, 000940802576(X)
                                  MASS STORAGE CONTROLLER
                                  MODEL = 40.
      MSLG$B_CNT_SVR        14
                                  CONTROLLER SOFTWARE VERSION #20.
      MSLG$B_CNT_HVR        49
                                  CONTROLLER HARDWARE REVISION #73.
      MSLG$W_MULT_UNT     0035
      MSLG$Q_UNIT_ID  02FF0000 00000022
                                  UNIQUE IDENTIFIER, 000000000022(X)
                                  DISK CLASS DEVICE (166)
                                  HSXnn
      MSLG$B_UNIT_SVR       01
                                  UNIT SOFTWARE VERSION #1.
      MSLG$B_UNIT_HVR       43
                                  UNIT HARDWARE REVISION #67.
      MSLG$B_LEVEL          01
      MSLG$B_RETRY          00
      MSLG$L_VOL_SER  00000000
                                  VOLUME SERIAL #0.
      MSLG$L_HDR_CODE 00000000
                                  LOGICAL BLOCK #0.
                                  GOOD LOGICAL SECTOR
```

```
CONTROLLER DEPENDENT INFORMATION

      LONGWORD 1.     030C4002
                                    /.@../
      LONGWORD 2.     00003C51
                                    /Q<../
      LONGWORD 3.     00000000
                                    /..../
      LONGWORD 4.     000B9331
                                    /1.../
      LONGWORD 5.     00000000
                                    /..../
      LONGWORD 6.     00000000
                                    /..../
      LONGWORD 7.     00000000
                                    /..../
      LONGWORD 8.     00000000
                                    /..../
      LONGWORD 9.     1F000504
                                    /..../
      LONGWORD 10.    36325A52
                                    /RZ26/
      LONGWORD 11.    20202020
                                    /    /
      LONGWORD 12.    29432820
                                    / (C)/
      LONGWORD 13.    43454420
                                    / DEC/
      LONGWORD 14.    34333533
                                    /3534/
      LONGWORD 15.    37313739
                                    /9717/
      LONGWORD 16.    00000000
                                    /..../
      LONGWORD 17.    00000004
                                    /..../
      LONGWORD 18.    00000000
                                    /..../
      LONGWORD 19.    853F0000
                                    /..?./
      LONGWORD 20.    00000000
```

5. Once you locate and identify the instance code, see the Appendix for information about instance codes, last fail codes and recommended repair actions.

6. If possible, use the FMU to interpret the event codes. See *Using FMU to describe event log codes* in this chapter for details about using the FMU.

Reading a DECevent error log

DECevent-generated error reports, while containing basically the same information as ERF-generated reports, are far easier to interpret. This is true because more of the binary log is translated. Some of the information directly available from the ASCII report output includes the following:

- Instance code
- Recommended repair action
- Recovery threshold
- PTL of the faulty device
- ASC/ASCQ code values
- Template type
- MSCP event code
- Controller model

The error log example that follows illustrates the difference between event logs generated by ERF shown in the ERF example in the previous section. This DECevent log translates the same event.

Beginning on page xx there are several examples of DECevent logs along with information about what you should look for when trying to identify a problem.s

When using DECevent to translate event information, you should not need to refer as frequently to the information and tables included in the remaining sections of this chapter. However, familiarity with the ERF error log format and other elements of the event logs will help you understand the wide variety of events that might be reported, regardless of the translation utility you are using.

```
******************************** ENTRY 1122 ********************************


Logging OS                         3. OpenVMS AXP
OS version                            X6.1-FT7
Event sequence number              5.
Timestamp of occurrence               28-APR-1994 11:39:40
System uptime in seconds         101.
VMS error mask              x00000000
VMS flags                       x0001  Dynamic Device Recognition present
Host name                             MTX2

AXP HW model                          DEC 7000 Model 610
System type register        x00000003  DEC 7000
Unique CPU ID               x00000002
mpnum                       x000000FF
mperr                       x000000FF

Event validity                    -1. Unknown validity code
Event severity                    -1. Unknown severity code
Entry type                       100.
Major Event class                  3. IO Subsystem
AXP Device Type                    0.

IO Minor Class                     1. MSCP
IO Minor Sub Class                 5. Logged Message

---- Device Profile ----
Vendor
Product Name                          HSX00 MSCP basic disk
Unit Name                             MAT$DUA
Unit Number                      450.
Device Class                    x0001  Disk

---- IO SW Profile ----
VMS DC$_CLASS                      1.
VMS DT$_TYPE                     141.

---- MSCP Logged Msg ----


Command Reference number    x00000000
Unit Number                      450.
MSCP Sequence number              21.
Logged Message Format              2. Disk Transfer Error
MSCP Flags                      x00  No MSCP Flags indicated



MSCP Unique Controller-ID x0000000940802576
MSCP Controller Model             40. HSJ40 HS Array Controller
MSCP Controller Class              1. Mass Storage Controller class
Controller SW version             20.
Controller HW version             73.

MSCP Unique Unit-ID       x0000000000000022
```

```
MSCP Unit Model                  -1. HSX0n MSCP basic/virtual disk
MSCP Unit Class                   2. Disk class - DEC Std 166 disk
Unit SW version                   1.
Unit HW version                  67.

MSCP Event Code                x014B  Major Event =  Drive Error
                                      Sub-event =  Controller Detected Protocol
                                                   Error
Multiunit code                 x0035
Error recovery Level               1.
Retry count                        0.
Volume Serial Number               0.
Header code                x00000000  Flags=  Good LBN
                                      LBN  =   0.

------- HSAC Data -------
Instance Code              x030C4002  A Drive failed because a Test Unit Ready
                                      command or a Read Capacity command failed.

                                      Component ID =   Device Services.
                                      Event Number =   x0000000C
                                      Repair Action =   x00000040
                                      NR Threshold =   x00000002
Template Type                   x51  Disk Transfer Error.
Power On Time Value        x00000000000B9331

Completed Byte Count               0.
Starting LBN                       0.
Device Locator             x00000504 Port    =   4.
                                     Target  =   5.
                                     LUN     =   0.
SCSI Device Type                x1F  Device Type not decoded.
Drive Product Name                   RZ26     (C) DEC
Drive Serial Number                  35349717
Command Opcode                  x00  Test Unit Ready



Sense Data Qualifier            x00  Buf Mode =   The target shall not report
                                                   GOOD status on write commands
                                                   until the data blocks are
                                                   actually written on the
                                                   medium.
                                     UWEUO =   zero, not defined
                                     MSBD =   zero, not defined
                                     FBW =   zero, not defined
                                     DSSD =   Sense Data fields were generated
                                              by the HSAC controller on behalf
                                              of the target devices because the
                                              Sense Data could not be obtained
                                              from that device.
--- HSAC Sense Data ---

Error Code                      x00  Error Code no decoded
Segment #                       x00
Information Bytes          x00000000
```

```
CMD Specific Info          x00000000
Sense Key                        x04  Hardware Error

ASC & ASCQ                   x3F85  ASC  =   x003F
                                    ASCQ =   x0085
                                    Test Unit Ready or Read Capacity Command
                                    failed

FRU Code                         x00
Sense Key Specific Data    x00000000  Sense Key Data NOT Valid
                                      Byte 1 =   x00000000
                                      Byte 2 =   x00000000
                                      Byte 3 =   x00000000
```

Using FMU to Describe Event Log Codes

FMU has a DESCRIBE function that you can use to interpret event codes produced by the controller. Use this function to understand events that have occurred in the subsystem (instance codes) and to find the recommended repair action (repair action codes), as well as to interpret other codes.

The types of codes that FMU can describe are:

- INSTANCE_CODE
- REPAIR_ACTION_CODE
- LAST_FAILURE_CODE
- ASC_ASCQ_CODE
- COMPONENT_CODE
- CONTROLLER_UNIQUE_ASC_ASCQ_CODE
- DEVICE_TYPE_CODE
- EVENT_THRESHOLD_CODE
- RESTART_TYPE
- SCSI_COMMAND_OPERATION_CODE
- SENSE_DATA_QUALIFIERS
- SENSE_KEY_CODE
- TEMPLATE_CODE

To translate a code:

1. Start FMU from the CLI.

   ```
   CLI> RUN FMU
   ```

2. Use the correct DESCRIBE command and give it the code number that you want translated.

```
FMU> DESCRIBE code-type code-number [additional
numbers]
```

For Example...

```
CLI> RUN FMU

Fault Management Utility

FMU> DESCRIBE INSTANCE_CODE 030C4002

Instance Code: 030C4002 Description:

A Drive failed because a Test Unit Ready command or a
Read Capacity command failed.

Reporting Component: 3.(03) Description:

Device Services

Reporting component's event number: 12.(0C)

Event Threshold: 2.(02) Classification:

HARD. Failure of a component that affects controller
performance or precludes access to a device connected
to the controller is indicated.

FMU> DESCRIBE REPAIR_ACTION_CODE 22

Recommended Repair Action Code: 34.(22) Description:

Replace the indicated cache module.
```

If you are unsure what value to enter with the DESCRIBE command, type a question mark (?) in place of a parameter to see the value and range required. For those code types that require multiple values, you must supply values for the earlier parameters before entering a question mark for the later values.

For Example...

```
FMU> DESCRIBE ASC_ASCQ_CODE ?
Your options are:
   ASC value (range: 0 through FF hexadecimal)
FMU> DESCRIBE ASC_ASCQ_CODE 0 ?
Your options are:
   ASCQ value (range: 0 through FF hexadecimal)
FMU> DESCRIBE ASC_ASCQ_CODE 0 0 ?
Your options are:
   SCSI Device Type value (range: 0 through FF
```

```
hexadecimal)
FMU>
```

Using FMU to Describe Recent Last Fail or Memory System Failure Codes

HSJ controllers store the four most recent last failure codes and memory system failure codes. You can use the FMU utility to retrieve these codes and their descriptions.

To view a last failure or memory system failure code:

1. Start FMU from the CLI.

   ```
   CLI> RUN FMU
   ```

2. To see all of the stored last failure or memory system failure events:

   ```
   FMU> DESCRIBE LAST_FAILURE ALL
   ```

   or

   ```
   FMU> DESCRIBE MEMORY_SYSTEM_FAILURE ALL
   ```

3. To see the most recent last failure or memory system failure events:

   ```
   FMU> DESCRIBE LAST_FAILURE MOST_RECENT
   ```

   or

   ```
   FMU> DESCRIBE MEMORY_SYSTEM_FAILURE MOST_RECENT
   ```

4. To see one of the four stored last failure or memory system failure events:

   ```
   FMU> DESCRIBE LAST_FAILURE n
   ```

   or

   ```
   FMU> DESCRIBE MEMORY_SYSTEM_FAILURE n
   ```

   where *n* is the stored event number from 1-4.

For Example...

```
CLI> RUN FMU

Fault Management Utility

FMU> SHOW LAST_FAILURE MOST_RECENT

Last Failure Entry: 1. Flags: 000FF301
 Template: 1.(01) Description: Last Failure Event
 Occurred on 07-DEC-1995 at 09:21:44
 Controller Model: HSJ40
 Serial Number: ZG51909900 Hardware Version: 0000(00)
 Controller Identifier:
 Unique Device Number: 01519090 Model: 40.(28) Class:
1.(01)
 Firmware Version: W18J(FF)
 Node Name: "HSJA3" CI Node Number: 12.(0C)
 Informational Report
 Instance Code: 01010302 Description:
  An unrecoverable hardware detected fault occurred.
 Reporting Component: 1.(01) Description:
  Executive Services
 Reporting component's event number: 1.(01)
 Event Threshold: 2.(02) Classification:
  HARD. Failure of a component that affects controller
  performance or precludes access to a device connected to
  the controller is indicated.
 Last Failure Code: 018800A0 (No Last Failure Parameters)
 Last Failure Code: 018800A0 Description:
  A processor interrupt was generated with an indication
  that the program card was removed.
 Reporting Component: 1.(01) Description:
  Executive Services
 Reporting component's event number: 136.(88)
 Restart Type: 2.(02) Description: Automatic hardware
restart
```

Testing disks (DILX)

HSJ-series controllers have a Disk In-line Exerciser (DILX) that you can use to test suspect disks. When you run DILX, you can specify many parameters for the test, such as starting and ending block numbers, the duration of the test, and whether the test should be read-only or read/write.

Note

DILX places a heavy load on the controllers. You should stop normal I/O operations before running DILX, or run DILX during periods of low activity.

DILX can test several disks at the same time. Before starting DILX, you must configure the disks that you want to test as single-disk units. In other words, the disks cannot be part of any storageset, and they must have a unit number assigned.

There are four tests that you can run with DILX: a quick disk test, an initial test on all disks, a basic function test, and an advanced user-defined test.

Running a quick disk test

This section provides instructions on how to run a quick DILX test on one or more disks. This is a 10-minute read-only test that uses the default DILX settings.

1. Start DILX from the CLI prompt.

   ```
   CLI> RUN DILX
   ```

2. Skip the auto-configure option so that you can specify which disk drives to test.

   ```
   Do you wish to perform an Auto-configure (y/n) ? n
   ```

3. Accept the default settings.

   ```
   Use all defaults and run in read only mode (y/n)? y
   ```

4. The system displays a list of all single-disk units (by unit number) that you can choose for DILX testing. Select the first disk that you want to test. Do not include the letter "D" in the unit number.

```
Enter unit number to be tested? 350
```

5. DILX indicates whether it has been able to allocate the disk. If you want to test more disks, enter the unit numbers when prompted. Otherwise, enter n to start the test.

```
Select another unit (y/n) [n] n

DILX testing started at <date> <time>
Test will run for 10 minutes
```

6. DILX will run for 10 minutes and then display the results of the testing. If you want to interrupt the test early:
   - Type ^G (Control G) to get a performance summary without stopping the test (^T if you are running DILX through VCS).
   - Type ^C to terminate the current DILX test.
   - Type ^Y to terminate the current test and exit DILX.

Running an initial test on all disks

Caution

The initial test performs write operations. Make sure that the disks that you use do not contain customer data.

This section provides instructions on how to run a DILX test on all single-disk units in the subsystem. This is a read/write basic function test that uses the default DILX settings. The test performs an initial write pass, followed by a repeating 10-minute cycle consisting of eight minutes of random I/O and two minutes of data-intensive transfers. You can set the duration of the test.

1. Start DILX from the CLI prompt.

```
CLI> RUN DILX
```

2. Choose the auto-configure option to test all single-disk units.

```
Do you wish to perform an Auto-configure (y/n) [n]?
y
```

3. Choose option 1 (test all disks) if you have a single-controller system; choose option 2 (test half of the disks) if you have a dual-redundant controller system.

```
Enter auto-configure option (1:3) [3]? 1
```

4. DILX displays a warning indicating that data on the disks will be destroyed. Either exit the test, or enter y to continue.

```
All data on the Auto-Configured disks will be
destroyed.
You *MUST* be sure of yourself.
Are you sure you want to continue (y/n) [n]? y
```

5. Enter the amount of time that you want the test to run. A single complete pass takes 10 minutes (after the initial write pass).

```
Enter execution time limit in minutes (1:65535)
[60] ? 25
```

6. If you want to see performance summaries while DILX is running, specify how often DILX should display the summaries.

```
Enter performance summary interval in minutes
(1:65535) [60] ? 5
```

7. The normal DILX summary simply indicates whether it detected any errors on each unit. Additionally, you can choose to see statistics on how many read and write operations were performed during the test.

```
Include performance statistics in performance
summary (y/n) [n] y
```

8. DILX displays a list of the units that it is able to test and begins the initial write pass and test.

```
DILX testing started at <date> <time>
Test will run for <nn> minutes
```

9. DILX will run for the amount of time that you selected and then display the results of the testing. If you want to interrupt the test early:
   - Type ^G (Control G) to get a current performance summary without stopping the test (^T if you are running DILX through VCS).
   - Type ^C to terminate the current DILX test.
   - Type ^Y to terminate the current test and exit DILX.

Running a disk basic function test

This section provides instructions on how to run a DILX basic function test on one or more disks. The test performs an optional initial write pass, followed by a repeating 10-minute cycle consisting of eight minutes of random I/O and two minutes of data-intensive transfers. You can set the percentage of the test that will be read operations, the data pattern to use for write command, and other parameters.

1. Start DILX from the CLI prompt.

```
CLI> RUN DILX
```

2. Skip the auto-configure option to get to the basic function test.

```
Do you wish to perform an Auto-configure (y/n) ? n
```

3. Do not accept the default settings.

```
Use all defaults and run in read only mode (y/n)? n
```

4. Enter the amount of time that you want the test to run. A single complete pass takes 10 minutes (after the initial write pass).

   ```
   Enter execution time limit in minutes (1:65535)
   [60] ? 25
   ```

5. If you want to see performance summaries while DILX is running, specify how often DILX should display the summaries.

   ```
   Enter performance summary interval in minutes
   (1:65535) [60] ? 5
   ```

6. The normal DILX summary simply indicates whether it detected any errors on each unit. Additionally, you can choose to see statistics on how many read and write operations were performed during the test.

   ```
   Include performance statistics in performance
   summary (y/n) [n] y
   ```

7. DILX asks if you want hard and soft errors (sense data and deferred errors) displayed. If you do, answer **y** and respond to the rest of the questions. If you don't want to see the errors displayed, answer **n** and proceed to the next step.

   ```
   Display hard/soft errors? y

   Display hex dump of Error Information Packet
   Requester Specific information (y/n) [n] ? y

   When the hard error limit is reached, the unit will
   be dropped from testing.  Enter hard error limit
   (1:65535) [65535] ? 100

   When the soft error limit is reached, soft errors
   will no longer be displayed but testing will
   continue for the unit.  Enter soft error limit
   (1:65535) [32] ? 32
   ```

8. Set the maximum number of outstanding I/Os for each unit.

```
Set the I/O queue depth (1:12) [4] ? 9
```

9. Select to run the basic function test.

```
*** Available tests are:
    1. Basic Function
    2. User Defined

Use the Basic Function test 99.9% of the time. The
User Defined test is for special problems only.

Enter test number (1:2) [1] ? 1
```

Caution

If you choose to write-enable disks during the test, make sure that the disks do not contain customer data.

10. Set the test as read-only or read/write.

```
Write enable disk unit(s) to be tested (y/n) [n]? y
```

11. Set the percentage of requests that will be read requests during the random I/O phase. The remaining requests will be write requests.

```
Enter read percentage for Random IO and Data
Intensive phase (0:100) [67] ? 80
```

12. If you set the test to allow write operations, specify the data pattern to be used for the writes. Unless you have some specific requirement, select 0 to use all patterns. See Table 3 for a listing of available patterns.

```
Enter data pattern number 0=ALL, 19=USER_DEFINED,
(0:19) [0] ? 0
```

13. If you set the test to allow write operations and you want to test data integrity, enable or disable the initial write pass. The initial write pass writes the selected data patterns to the entire specified data space. This allows the data to be verified later, but it may take a long time to complete the write operation.

```
Perform initial write (y/n) [n] ? y
```

14. During the data intensive phase, DILX only executes access and erase commands. Set the percentage of commands that will be access commands; the remaining commands will be erase commands.

```
The erase percentage will be set automatically.
Enter access percentage for Seek Intensive phase
(0:100) [90] ?
```

15. If you enabled the initial write pass and want to test data integrity, set the percentage of read and write commands that will have a data compare operation performed.

```
Perform data compare (y/n) [n] ? y
Enter compare percentage (1:100) [5] ? 10
```

16. The system displays a list of all single-disk units (by unit number) that you can choose for DILX testing. Select the first disk that you want to test. Do not include the letter "D" in the unit number.

```
Enter unit number to be tested? 350
```

17. DILX indicates whether it has been able to allocate the disk. If you enabled the read/write test, DILX gives you a final warning that the data on the disk will be destroyed.

```
Unit 350 will be write enabled.
Do you still wish to add this unit (y/n) [n] ? y
```

18. If you want to test more disks, enter the unit numbers when prompted. Otherwise, enter **n** to start the test.

```
Select another unit (y/n) [n] n

DILX testing started at <date> <time>
Test will run for <nn> minutes
```

19. DILX will run for the amount of time that you selected and then display the results of the testing. If you want to interrupt the test early:
    - Type ^G (Control G) to get a performance summary without stopping the test (^T if you are running DILX through VCS).
    - Type ^C to terminate the current DILX test.
    - Type ^Y to terminate the current test and exit DILX.

Running an advanced disk test

This section provides instructions on how to run an advanced DILX test in which you define the commands that make up the test (read, write, access, and so on). Only select this test if you are very knowledgeable about disk testing. You should use the basic function test in almost all situations.

1. Start DILX from the CLI prompt.

   ```
   CLI> RUN DILX
   ```

2. Skip the auto-configure option to get to the user-defined test.

   ```
   Do you wish to perform an Auto-configure (y/n) ? n
   ```

3. Do not accept the default settings.

   ```
   Use all defaults and run in read only mode (y/n)? n
   ```

4. Enter the amount of time that you want the test to run. A single complete pass takes 10 minutes (after the initial write pass).

   ```
   Enter execution time limit in minutes (1:65535)
   [60] ? 25
   ```

5. If you want to see performance summaries while DILX is running, specify how often DILX should display the summaries.

```
Enter performance summary interval in minutes
(1:65535) [60] ? 5
```

6. The normal DILX summary simply indicates whether it detected any errors on each unit. Additionally, you can choose to see statistics on how many read and write operations were performed during the test.

```
Include performance statistics in performance
summary (y/n) [n] y
```

7. DILX asks if you want hard and soft errors (sense data and deferred errors) displayed. If you do, answer **y** and respond to the rest of the questions. If you don't want to see the errors displayed, answer **n** and proceed to the next step.

```
Display hard/soft errors? y

Display hex dump of Error Information Packet
Requester Specific information (y/n) [n] ? y

When the hard error limit is reached, the unit will
be dropped from testing.  Enter hard error limit
(1:65535) [65535] ? 100

When the soft error limit is reached, soft errors
will no longer be displayed but testing will
continue for the unit.  Enter soft error limit
(1:65535) [32] ? 32
```

8. Set the maximum number of outstanding I/Os for each unit.

```
Set the I/O queue depth (1:12) [4] ? 9
```

9. Select to run the user-defined test.

```
*** Available tests are:
    1. Basic Function
    2. User Defined

Use the Basic Function test 99.9% of the time. The
User Defined test is for special problems only.

Enter test number (1:2) [1] ? 2
```

Caution

If you define write or erase commands, user data will be destroyed.

10. Define the test sequence by entering command number 1 and its associated parameters. You may define up to 20 commands, and they will be executed in the order in which you enter them.

```
Enter command number 1 (read, write, access, erase,
quit) [] ? read
Enter starting lbn for this command ? 0
Enter the IO size in 512 byte blocks for this
command (1:128) [] ? 20
Enter in HEX, the MSCP Command Modifiers[0] ? 0
```

11. Repeat step 0 until you have defined the entire command sequence (up to 20). When you have finished entering commands, type **quit**.

12. The system displays a list of all single-disk units (by unit number) that you can choose for DILX testing. Select the first disk that you want to test. Do not include the letter "D" in the unit number.

```
Enter unit number to be tested? 350
```

13. DILX indicates whether it has been able to allocate the disk. If you enabled the read/write test, DILX gives you a final warning that the data on the disk will be destroyed.

```
Unit 350 will be write enabled.
Do you still wish to add this unit (y/n) [n] ? y
```

14. If you want to test more disks, enter the unit numbers when prompted. Otherwise, enter n to start the test.

```
Select another unit (y/n) [n] n

DILX testing started at <date> <time>
Test will run for <nn> minutes
```

15. DILX will run for the amount of time that you selected and then display the results of the testing. If you want to interrupt the test early:

- Type ^G (Control G) to get a performance summary without stopping the test (^T if you are running DILX through VCS).
- Type ^C to terminate the current DILX test.
- Type ^Y to terminate the current test and exit DILX.

DILX error codes

If DILX detects an error, the performance display for the unit includes:

- the controller instance code (IC)
- the device PTL location (PTL)
- the SCSI sense key (Key)
- the ASC and ASCQ codes (ASC/Q)
- the number of hard and soft errors (HC/SC)

In addition, you will see the message

```
DILX detected error, code x.
```

where x is 1, 2, 3, or 4. The meanings of the codes are:

Message:
Code 1: Illegal Data Pattern Number found in data pattern header. Unit *x*

Explanation:
DILX read data from the disk and found that the data was not in a pattern that DILX previously wrote to the disk.

Message:
```
Code 2: No write buffers correspond to data pattern Unit x.
```

Explanation:
DILX read a legal data pattern from the disk at a place where DILX wrote to the disk, but DILX does not have any write buffers that correspond to the data pattern. Thus, the data has been corrupted.

Message:
```
Code 3: Read data do not match what DILX thought was
written to the  media.  Unit x.
```

Explanation:
DILX writes data to the disk and then reads it and compares it against what was written to the disk. This indicates a compare failure. More information is displayed to indicate where in the data buffer the compare operation failed and what the data was and should have been.

Message:
```
Code 4: Compare Host Data should have reported a compare
error but did not.  Unit x
```

Explanation:
A compare host data compare was issued in a way that DILX expected to receive a compare error but no error was received.

DILX data patterns

Table 3 defines the data patterns used with the DILX Basic Function or User-Defined tests. There are 18 unique data patterns. These data patterns were selected as worst case,

or the ones most likely to produce errors on disks connected to the controller.

Table 3
DILX data patterns

Pattern Number	Pattern in Hexadecimal Numbers
1	0000
2	8B8B
3	3333
4	3091
5, shifting 1s	0001, 0003, 0007, 000F, 001F, 003F, 007F, 00FF, 01FF, 03FF, 07FF, 0FFF, 1FFF, 3FFF, 7FFF
6, shifting 0s	FIE, FFFC, FFFC, FFFC, FFE0, FFE0, FFE0, FFE0, FE00, FC00, F800, F000, F000, C000, 8000, 0000
7, alternating 1s, 0s	0000, 0000, 0000, FFFF, FFFF, FFFF, 0000, 0000, FFFF, FFFF, 0000, FFFF, 0000, FFFF, 0000, FFFF
8	B6D9
9	5555, 5555, 5555, AAAA, AAAA, AAAA, 5555, 5555, AAAA, AAAA, 5555, AAAA, 5555, AAAA, 5555, AAAA, 5555
10	DB6C
11	2D2D, 2D2D, 2D2D, D2D2, D2D2, D2D2, 2D2D, 2D2D, D2D2, D2D2, 2D2D, D2D2, 2D2D, D2D2, 2D2D, D2D2
12	6DB6
13, ripple 1	0001, 0002, 0004, 0008, 0010, 0020, 0040, 0080, 0100, 0200, 0400, 0800, 1000, 2000, 4000, 8000
14, ripple 0	FIE, FFFD, FFFB, FFF7, FFEF, FFDF, FFBF, FF7F, FEFF, FDFF, FBFF, F7FF, EFFF, BFFF, DFFF, 7FFF
15	DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D
16	3333, 3333, 3333, 1999, 9999, 9999, B6D9, B6D9, B6D9, B6D9, FFFF, FFFF, 0000, 0000, DB6C, DB6C
17	9999, 1999, 699C, E99C, 9921, 9921, 1921, 699C, 699C, 0747, 0747, 0747, 699C, E99C, 9999, 9999
18	FFFF
Default—Use all of the above patterns in a random method	

Testing tapes (TILX)

HSJ-series controllers have a Tape In-line Exerciser (TILX) that you can use to test suspect tape drives. When you run TILX, you can specify many parameters for the test, such as the I/O queue depth, the duration of the test, and whether the test should be read-only or read/write.

Note

TILX places a heavy load on the controllers. You should stop normal I/O operations before running TILX, or run TILX during periods of low activity.

TILX can test several tape drives at the same time. Each tape drive that you want to test must be configured as a unit, but it must be dismounted from the host.

There are four tests that you can run with TILX: a quick tape test, a basic function test, a read-only test, and a user-defined test.

Running a quick tape test

This section provides instructions on how to run a quick TILX test on one or more tape drives. This is a 10-minute read-only test that uses the default TILX settings.

1. Start TILX from the CLI prompt.

   ```
   CLI> RUN TILX
   ```

2. Use the default settings.

   ```
   Use all defaults (y/n) [y]? y
   ```

3. The system displays a list of all tape drive units (by unit number) that you can choose for TILX testing. Select the first tape drive that you want to test. Do not include the letter “T” in the unit number.

   ```
   Enter unit number to be tested? 350
   ```

4. Check to be sure that a tape is loaded in the drive, then answer yes to the next question.

   ```
   Is a tape loaded and ready, answer Yes when ready?Y
   ```

5. TILX indicates whether it has been able to allocate the tape drive. If you want to test more tape drives, enter the unit numbers when prompted. Otherwise, enter n to start the test.

```
Select another unit (y/n) [n] n

TILX testing started at <date> <time>
Test will run for 10 minutes
```

6. TILX will run for 10 minutes and then display the results of the testing. If you want to interrupt the test early:
   - Type ^G (Control G) to get a performance summary without stopping the test (^T if you are running TILX through VCS).
   - Type ^C to terminate the current TILX test.
   - Type ^Y to terminate the current test and exit TILX.

Running a tape drive basic function test

Caution

The basic function test performs write operations. Make sure that the tapes that you use do not contain customer data.

This section provides instructions on how to run a TILX basic function test on one or more tape drives. The test performs a repeating cycle of a write pass followed by a read pass. The write pass executes in two phases:

- Data intensive—The first one third of the specified number of records are written as 16 kilobyte records. With this high byte count and the default queue depth, this phase should test the streaming capability (if supported) of the tape unit.
- Random—The remaining two thirds of the records are written with random byte counts. The command sequence is *write, reposition back one record, read*, and is repeated three times. Tape mark writing is intermixed in the test.

The read pass consists of three phases:

- Data intensive—Read operations of fixed record sizes with a byte count equal to the expected tape record size. Forward position commands are issued when tape marks are encountered.
- Random—Begins at the point where random-sized records were written to the tape. Most read operations are issued with a byte count equal to the expected tape record byte count. Occasionally, read operations are intemixed with a byte count less than or greater than the expected tape record byte count. Forward position commands are issued when tape marks are encountered.
- Position Intensive—Begins halfway down from the start of the area where random-sized records are located. Read operations and position commads are intermixed so that the test gradually proceeds toware the EOT. Forward position commands are issued when tape marks are encountered.

In all phases, if the EOT is detected, the tape is rewound to the beginning of tape (BOT) and the write pass starts again.

To run a basic function test:

1. Start TILX from the CLI prompt.

   ```
   CLI> RUN TILX
   ```

2. Do not accept the default settings.

   ```
   Use all defaults (y/n)? n
   ```

3. Enter the amount of time that you want the test to run.

   ```
   Enter execution time limit in minutes (10:65535)
   [10] ? 25
   ```

4. If you want to see performance summaries while TILX is running, specify how often TILX should display the summaries.

   ```
   Enter performance summary interval in minutes
   (1:65535) [10] ? 5
   ```

5. The normal TILX summary simply indicates whether it detected any errors on each unit. Additionally, you can choose to see statistics on how many operations were performed and how much data was transferred during the test.

   ```
   Include performance statistics in performance
   summary (y/n) [n] y
   ```

6. TILX asks if you want hard and soft errors (sense data and deferred errors) displayed. If you do, answer **y** and respond to the rest of the questions. If you don't want to see the errors displayed, answer **n** and proceed to the next step.

   ```
   Display hard/soft errors? y

   Display hex dump of Error Information Packet
   Requester Specific information (y/n) [n] ? y

   When the hard error limit is reached, the unit will
   be dropped from testing.  Enter hard error limit
   (1:65535) [32] ? 100

   When the soft error limit is reached, soft errors
   will no longer be displayed but testing will
   continue for the unit.  Enter soft error limit
   (1:65535) [32] ? 32
   ```

7. Set the maximum number of outstanding I/Os for each unit.

   ```
   Set the I/O queue depth (1:12) [4] ? 6
   ```

8. Suppress caching.

```
Suppress caching (y,n) [n] ? n
```

9. Select to run the basic function test.

```
*** Available tests are:
    1. Basic Function
    2. User Defined
    3. Read Only

Use the Basic Function test 99.9% of the time. The
User Defined test is for special problems only.

Enter test number (1:3) [1] ? 1
```

10. Specify the data pattern to be used for the writes. Unless you have some specific requirement, select 0 to use all patterns. See Table 3 for a listing of available patterns.

```
Enter data pattern number 0=ALL, 19=USER_DEFINED,
(0:19) [0] ? 0
```

11. Set the number of records to be written/read during the test.

```
Enter record count (1:4294967295) [4096] ? 1000
```

12. If you want to test data integrity, set the percentage of read and write commands that will have a data compare operation performed.

```
Perform data compare (y/n) [n] ? y
Enter compare percentage (1:100) [2] ? 1
```

13. The system displays a list of all tape drive units (by unit number) that you can choose for TILX testing. Select the first tape drive that you want to test. Do not include the letter “T” in the unit number.

```
Enter unit number to be tested? 350
```

14. Check to be sure that a tape is loaded in the drive, then answer yes to the next question.

```
Is a tape loaded and ready, answer Yes when ready?Y
```

15. TILX indicates whether it has been able to allocate the tape drive. If you want to test more tape drives, enter the unit numbers when prompted. Otherwise, enter **n** to start the test.

```
Select another unit (y/n) [n] n

TILX testing started at <date> <time>
Test will run for <nn> minutes
```

16. TILX will run for the amount of time that you selected and then display the results of the testing. If you want to interrupt the test early:

    – Type ^G (Control G) to get a performance summary without stopping the test (^T if you are running TILX through VCS).

    – Type ^C to terminate the current TILX test.

    – Type ^Y to terminate the current test and exit TILX.

Running a tape drive read-only test

This section provides instructions on how to run a TILX read-only test on one or more tape drives. The test only verifies that a tape is readable. The test performs an initial read pass until it reaches the EOT or the selected number of records. It then rewinds the tape and starts another read pass. The test ignores tape marks. Since the test will most likely perform read operations with incorrect record sizes, it ignores record size mismatches. The test records all other errors.

To run a read-only TILX test:

1. Start TILX from the CLI prompt.

```
CLI> RUN TILX
```

2. Do not accept the default settings.

```
Use all defaults (y/n)? n
```

3. Enter the amount of time that you want the test to run.

```
Enter execution time limit in minutes (10:65535)
[10] ? 25
```

4. If you want to see performance summaries while TILX is running, specify how often TILX should display the summaries.

```
Enter performance summary interval in minutes
(1:65535) [10] ? 5
```

5. The normal TILX summary simply indicates whether it detected any errors on each unit. Additionally, you can choose to see statistics on how many operations were performed and how much data was transferred during the test.

```
Include performance statistics in performance
summary (y/n) [n] y
```

6. TILX asks if you want hard and soft errors (sense data and deferred errors) displayed. If you do, answer **y** and respond to the rest of the questions. If you don't want to see the errors displayed, answer **n** and proceed to the next step.

```
Display hard/soft errors? y

Display hex dump of Error Information Packet
Requester Specific information (y/n) [n] ? y

When the hard error limit is reached, the unit will
be dropped from testing.  Enter hard error limit
(1:65535) [32] ? 100
```

```
When the soft error limit is reached, soft errors
will no longer be displayed but testing will
continue for the unit.  Enter soft error limit
(1:65535) [32] ? 32
```

7. Set the maximum number of outstanding I/Os for each unit.

```
Set the I/O queue depth (1:12) [4] ? 6
```

8. Suppress caching.

```
Suppress caching (y,n) [n] ? n
```

9. Select to run the read-only test.

```
*** Available tests are:
    1. Basic Function
    2. User Defined
    3. Read Only

Use the Basic Function test 99.9% of the time. The
User Defined test is for special problems only.

Enter test number (1:3) [1] ? 3
```

10. Set the number of records to be written/read during the test.

```
Enter record count (1:4294967295) [4096] ? 1000
```

11. If you want to test data integrity, set the percentage of read and write commands that will have a data compare operation performed.

```
Perform data compare (y/n) [n] ? y
Enter compare percentage (1:100) [2] ? 1
```

12. The system displays a list of all tape drive units (by unit number) that you can choose for TILX testing. Select the first tape drive that you want to test. Do not include the letter “T” in the unit number.

```
Enter unit number to be tested? 350
```

13. Check to be sure that a tape is loaded in the drive, then answer yes to the next question.

```
Is a tape loaded and ready, answer Yes when ready?Y
```

14. TILX indicates whether it has been able to allocate the tape drive. If you want to test more tape drives, enter the unit numbers when prompted. Otherwise, enter **n** to start the test.

```
Select another unit (y/n) [n] n

TILX testing started at <date> <time>
Test will run for <nn> minutes
```

15. TILX will run for the amount of time that you selected and then display the results of the testing. If you want to interrupt the test early:

    - Type ^G (Control G) to get a performance summary without stopping the test (^T if you are running TILX through VCS).
    - Type ^C to terminate the current TILX test.
    - Type ^Y to terminate the current test and exit TILX.

Running an advanced tape drive test

This section provides instructions on how to run an advanced TILX test in which you define the commands that make up the test (read, write, reposition, and so on). Only select this test if you are very knowledgeable about tape drive testing. You should use the basic function test in almost all situations.

1. Start TILX from the CLI prompt.

```
CLI> RUN TILX
```

2. Do not accept the default settings.

```
Use all defaults and run in read only mode (y/n)? n
```

3. Enter the amount of time that you want the test to run.

```
Enter execution time limit in minutes (10:65535)
[10] ? 25
```

4. If you want to see performance summaries while TILX is running, specify how often TILX should display the summaries.

```
Enter performance summary interval in minutes
(1:65535) [10] ? 5
```

5. The normal TILX summary simply indicates whether it detected any errors on each unit. Additionally, you can choose to see statistics on how many operations were performed and how much data was transferred during the test.

```
Include performance statistics in performance
summary (y/n) [n] y
```

6. TILX asks if you want hard and soft errors (sense data and deferred errors) displayed. If you do, answer **y** and respond to the rest of the questions. If you don't want to see the errors displayed, answer **n** and proceed to the next step.

```
Display hard/soft errors? y

Display hex dump of Error Information Packet
Requester Specific information (y/n) [n] ? y

When the hard error limit is reached, the unit will
be dropped from testing.  Enter hard error limit
(1:65535) [32] ? 100

When the soft error limit is reached, soft errors
will no longer be displayed but testing will
```

```
continue for the unit.  Enter soft error limit
(1:65535) [32] ? 32
```

7. Set the maximum number of outstanding I/Os for each unit.

```
Set the I/O queue depth (1:12) [4] ? 6
```

8. Suppress caching.

```
Suppress caching (y,n) [n] ? n
```

9. Select to run the basic function test.

```
*** Available tests are:
    1. Basic Function
    2. User Defined
    3. Read Only

Use the Basic Function test 99.9% of the time. The
User Defined test is for special problems only.

Enter test number (1:3) [1] ? 2
```

10. Define the test sequence by entering command number 1 and its associated parameters. You may define up to 20 commands, and they will be executed in the order in which you enter them.

    If you define write or erase commands, user data will be destroyed.

```
Enter command number 1 (read, write, access, erase,
quit) [] ? read
Enter starting lbn for this command ? 0
Enter the IO size in 512 byte blocks for this
command (1:128) [] ? 20
Enter in HEX, the MSCP Command Modifiers[0] ? 0
```

11. Repeat step 0 until you have defined the entire command sequence (up to 20). When you have finished entering commands, type **quit**.

12. The system displays a list of all single-tape drive units (by unit number) that you can choose for TILX testing. Select the first tape drive that you want to test. Do not include the letter "D" in the unit number.

```
Enter unit number to be tested? 350
```

13. TILX indicates whether it has been able to allocate the tape drive. If you enabled the read/write test, TILX gives you a final warning that the data on the tape drive will be destroyed.

```
Unit 350 will be write enabled.
Do you still wish to add this unit (y/n) [n] ? y
```

14. If you want to test more tape drives, enter the unit numbers when prompted. Otherwise, enter n to start the test.

```
Select another unit (y/n) [n] n

TILX testing started at <date> <time>
Test will run for <nn> minutes
```

15. TILX will run for the amount of time that you selected and then display the results of the testing. If you want to interrupt the test early:

    - Type ^G (Control G) to get a performance summary without stopping the test (^T if you are running TILX through VCS).
    - Type ^C to terminate the current TILX test.
    - Type ^Y to terminate the current test and exit TILX.

TILX error codes

If TILX detects an error, the performance display for the unit includes:

- the controller instance code (IC)

- the device PTL location (PTL)
- the SCSI sense key (Key)
- the ASC and ASCQ codes (ASC/Q)
- the number of hard and soft errors (HC/SC)

In addition, you will see one of the following error code messages:

Message:

```
TILX detected error, code 1:
Illegal Data Pattern Number found in data pattern
header.  Unit x
```

Explanation:

TILX read data from the tape and found that the data was not in a pattern that TILX previously wrote to the tape.

Message:

```
TILX detected error, code 2:
No write buffers correspond to data pattern Unit x.
```

Explanation:

TILX read a legal data pattern from the tape at a place where TILX wrote to the tape, but TILX does not have any write buffers that correspond to the data pattern. Thus, the data has been corrupted.

Message:

```
TILX detected error, code 3:
Read data do not match write buffer.  Unit x.
```

Explanation:

TILX writes data to the tape and then reads it and compares it against what was written. This indicates a compare failure. More information is displayed to indicate where in the data buffer the compare operation failed and what the data was and should have been.

Message:

```
TILX detected error, code 4:
TILX/TAPE record size mismatch.  Unit x
```

Explanation:

The size of the record that TILX read from the tape did not match the size of the record that was written on the previous write pass.

Message:

```
TILX detected error, code 5:
A tape mark was detected in a place where it was not
expected.  Unit x
```

Explanation:

TILX encountered a tape mark where it was not expected. The tape drive may not be able to accurately position the tape.

Message:

```
TILX detected error, code 7:
EOT encountered in unexpected position.  Unit x
```

Explanation:

The tape reached EOT before TILX expected it. The tape drive may not be able to accurately position the tape.

TILX data patterns

Table 3 defines the data patterns used with the TILX Basic Function or User-Defined tests. There are 18 unique data patterns. These data patterns were selected as worst case, or the ones most likely to produce errors on tape drives connected to the controller.

Table 4
TILX data patterns

Pattern Number	Pattern in Hexadecimal Numbers
1	0000
2	8B8B
3	3333
4	3091
5, shifting 1s	0001, 0003, 0007, 000F, 001F, 003F, 007F, 00FF, 01FF, 03FF, 07FF, 0FFF, 1FFF, 3FFF, 7FFF
6, shifting 0s	FIE, FFFC, FFFC, FFFC, FFE0, FFE0, FFE0, FFE0, FE00, FC00, F800, F000, F000, C000, 8000, 0000
7, alternating 1s, 0s	0000, 0000, 0000, FFFF, FFFF, FFFF, 0000, 0000, FFFF, FFFF, 0000, FFFF, 0000, FFFF, 0000, FFFF
8	B6D9
9	5555, 5555, 5555, AAAA, AAAA, AAAA, 5555, 5555, AAAA, AAAA, 5555, AAAA, 5555, AAAA, 5555, AAAA, 5555
10	DB6C
11	2D2D, 2D2D, 2D2D, D2D2, D2D2, D2D2, 2D2D, 2D2D, D2D2, D2D2, 2D2D, D2D2, 2D2D, D2D2, 2D2D, D2D2
12	6DB6
13, ripple 1	0001, 0002, 0004, 0008, 0010, 0020, 0040, 0080, 0100, 0200, 0400, 0800, 1000, 2000, 4000, 8000
14, ripple 0	FIE, FFFD, FFFB, FFF7, FFEF, FFDF, FFBF, FF7F, FEFF, FDFF, FBFF, F7FF, EFFF, BFFF, DFFF, 7FFF
15	DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D, B6DB, 6DB6, DB6D
16	3333, 3333, 3333, 1999, 9999, 9999, B6D9, B6D9, B6D9, B6D9, FFFF, FFFF, 0000, 0000, DB6C, DB6C
17	9999, 1999, 699C, E99C, 9921, 9921, 1921, 699C, 699C, 0747, 0747, 0747, 699C, E99C, 9999, 9999
18	FFFF
Default—Use all of the above patterns in a random method	

Monitoring system performance with the VTDPY utility

The VTDPY utility gathers and displays system state and performance information for the HS family of modular storage controllers. The information displayed includes processor utilization, host port activity and status, device state, logical unit state, and cache and I/O performance.

The VTDPY utility requires a video terminal that supports ANSI control sequences, such as a VT220, VT320, or VT420 terminal. A graphics display that provides emulation of an ANSI compatible video terminal can also be used. For DSSI and CI based HS controllers, VTDPY can be run on terminals either directly connected to the HS controller or on terminals connected through a host-based DUP connection. For SCSI based HS controllers, VTDPY can be run only on terminals connected to the HS controller maintenance terminal port. Note that VCS can be used only from a terminal attached to the terminal port on the front bezel of the HS array controller.

The following sections show how to use the VTDPY utility.

How to run VTDPY

You can run only one VTDPY session on each controller at one time. Prior to running VTDPY, set the terminal to NOWRAP mode to prevent the top line of the display from scrolling off of the screen.

To initiate VTDPY from a maintenance terminal at the CLI> prompt, enter the following command:

```
CLI> RUN VTDPY
```

To initiate VTDPY from a virtual terminal use the following command. (This command applies only to HSJ or HSD controllers from VMS.)

```
$ SET HOST/DUP/SERVER=MSCP$DUP<controller_name> /TASK=VTDPY
```

Using the VTDPY control keys

Use the following control key sequences with the VTDPY display.

Table 5
VTDPY control keys

Control Key Sequence	Function
Ctrl/C	Prompts for commands.
Ctrl/G	Updates the screen (same as Ctrl/Z).
Ctrl/O	Pauses or resumes screen updates.
Ctrl/R	Refreshes current screen display (same as Ctrl/W).
Ctrl/W	Refreshes current screen display (same as Ctrl/R).
Ctrl/Y	Terminates VTDPY and resets screen characteristics.
Ctrl/Z	Updates the screen (same as Ctrl/G).

While VTDPY and a maintenance terminal interface support passing all of the listed control characters, some host-based terminal interfaces restrict passing some of the characters. All of the listed characters have equivalent text string commands, defined in the table in *Using the VTDPY command line*.

Using the VTDPY command line

VTDPY contains a command line interpreter that you can invoke by entering Ctrl/C any time after starting the program. The command line interpreter is used to modify the characteristics of the VTDPY display. The following table lists the VTDPY commands.

Table 6
VTDPY commands

Command String	Function
DISPLAY CACHE	Use 132 column unit caching statistics display.
DISPLAY DEFAULT	Use default 132 column system performance display.
DISPLAY DEVICE	Use 132 column device performance display.
DISPLAY STATUS	Use 80 column controller status display.

Command String	Function
EXIT	Terminates program (same as QUIT).
INTERVAL <seconds>	Changes update interval.
HELP	Displays help message text.
REFRESH	Refreshes the current display.
QUIT	Terminates program (same as EXIT).
UPDATE	Updates screen display.

The keywords in the command strings can be abbreviated to the minimum number of characters that are necessary to uniquely identify the keyword. Entering a question mark (?) after a keyword causes the parser to provide a list of keywords or values that can follow the supplied keyword. The command line interpreter is not case sensitive, so keywords can be entered in uppercase, lowercase, or mixed case.

Upon successful execution of a command other than HELP, the command line interpreter is exited and the display is resumed. Entering a carriage return without a command also exits the command line interpreter and resumes the display. If an error occurs in the command, the user prompts for command expansion help, or the HELP command is entered, the command line interpreter prompts for an additional command instead of returning to the display.

How to interpret the VTDPY display fields

This section contains an example default VTDPY display and includes descriptions of the major fields in the VTDPY displays.

```
HSZ40 S/N: CX12345678 SW: V20Z HW: 00-00
                                        61.4% Idle      927 KB/S      300 Rq/S                                    Up:    0  1:32.46
Pr   Name  Stk/Max Typ Sta  CPU% SCSI Target  2                 Unit  ASWC  KB/S  Rd% Wr% Cm% HT% Unit  ASWC  KB/S  Rd% Wr% Cm% HT%
 0    NULL   0/  0      Rn  61.4                                D0000 o^ b    112  62  37   0   0
 2   RECON  10/  1 FNC  Bl   0.0                                D0001 o^ b    118  61  38   0   0
 3    SHIS  40/  7 FNC  Rn  32.3 Xfer Rate                      D0002 o^ b    122  67  32   0   0
 8   VTDPY  10/  3 DUP  Rn   0.2  Id   Mhz                      D0003 o^ b    128  65  34   0   0
18  SCSIVT  10/  1 FNC  Bl   0.0  0 = Asynch                    D0004 o^ b     93  69  30   0   0
19   DS_HB  10/  1 FNC  Bl   0.0  1 = Asynch           Target  D0005 o^ b    112  67  32   0   0
24      VA  10/  1 FNC  Bl   0.0  2 = This            01234567 D0006 o^ b    156  66  33   0   0
25    DS_1  40/  6 FNC  Bl   5.5  3 = Asynch         P1D D D  H D0007 o^ b     83  71  28   0   0
26    DS_0  20/  1 FNC  Bl   0.4  4 = Asynch         o2 D D DDH
27 CLIMAIN  16/  7 FNC  Bl   0.0  5 = Asynch         r3D D D  H
28   NVFOC  10/  1 FNC  Bl   0.0  6 =  3.57          t4 D D  DH
29  REMOTE  10/  1 FNC  Bl   0.0  7 = Asynch          5D D D  H
30     FOC  20/  2 FNC  Bl   0.0                       6 D D DDH
31   DUART  10/  1 FNC  Bl   0.0
```

The display and subdisplay you see depend on the type of controller: CI and DSSI-based controllers or SCSI and HS-based controllers. Characteristics for each are included in the field description sections that follow.

CI/DSSI host port characteristics

```
Node HSJ501 ❶ Port 13 ❷
SysId 4200100D0720 ❸
```

Description

This subdisplay shows the current host port identification information. This subdisplay is available only for CI or DSSI based controllers.

1. ❶SCS node name
2. ❷Port number
3. ❸SCS system ID

SCSI host port characteristics

```
Xfer Rate
T❶W❷I❸Mhz❹
1 W 7 10.00
2 W Async❺
```

Description

This subdisplay shows the current host port SCSI target identification, any initiator which has negotiated synchronous transfers, and the negotiated transfer method currently in use between the controller and the initiators. This subdisplay is available only for SCSI based HS controllers.

1. ❶SCSI host port target ID.
2. ❷Transfer width. **W** indicates 16 bit or wide transfers are being used. A space indicates 8 bit transfers are being used.
3. ❸The initiator with which synchronous communication has been negotiated.
4. ❹A numeric value indicates the synchronous data rate which has been negotiated with the initiator at the specified SCSI ID. The value is listed in megahertz (Mhz). In this example, the negotiated synchronous transfer rate is approximately 3.57 Mhz. To convert this number to the nanosecond period, invert and multiply by 1000. The period for this is approximately 280 nanoseconds.

   If the field is still Async, this might indicate a failure to establish communication between host adapter and HSZ. The problem could be one of the following:

   - Host port
   - SCSI bus configuration
   - SCSI termination
   - SCSI cables

– HSZ

5. ❺**Async** indicates communication between this target and all initiators is being done in asynchronous mode. This is the default communication mode and is used unless the initiator successfully negotiates for synchronous communications. If there is no communication with a given target ID, the communication mode is listed as asynchronous.

CI performance display

```
Path A Pkts  Pkts/S
RCV     5710    519 ❶
ACK    11805   1073 ❷
NAK     2073    188 ❸
NOR     1072     97 ❹

Path B Pkts  Pkts/S
RCV     5869    533
ACK    11318   1028
NAK     2164    196
NOR      445     40
```

Description

This display indicates the number of packets sent and received over each CI path and the packet rate. This display is available only on CI based controllers.

1. ❶Packets received from a remote node
2. ❷Packets sent to a remote node that were ACKed
3. ❸Packets sent to a remote node that were NAKed
4. ❹Packets sent to a remote node for which no response was received

DSSI performance display

```
DSSI    Pkts  Pkts/S
RCV     5710     519 ❶
ACK    11805    1073 ❷
NAK     2073     188 ❸
NOR     1072      97 ❹
```

Description

This display indicates the number of packets sent and received through the DSSI port and the packet rate. This display is available only on DSSI based controllers.

1. ❶Packets received from a remote node
2. ❷Packets sent to a remote node that were ACKed
3. ❸Packets sent to a remote node that were NAKed
4. ❹Packets sent to a remote node for which no response was received

CI/DSSI connection status

```
Connections
 0123456789 ❶
0........MM ❷
1..C.MV....
2..........
3..
```

Description

This display shows the current status of any connections to a remote CI or DSSI node. This display is available only on CI and DSSI based controllers.

1. ❶Each position in the data field represents one of the possible nodes to which the controller can communicate. To locate the connection status for a given node, use the column on the left to determine the high order digit of the node number, and use the second row to determine the low order digit of the node number. For CI controllers, the number of nodes displayed is determined by the controllers MAX NODE parameter. The maximum supported value for this parameter is 32. For DSSI controllers, the number of nodes is fixed at 8.

2. ❷Each location in the grid contains a character to indicate the connection status:

   - **C** indicates one connection to that node. In this example, node 12 shows one connection. This usually happens if a host has multiple adapters and it is using more than one adapter for load balancing.

   - **M** indicates multiple connections to that node. Because each host system can make a separate connection to each of the disk, tape, and DUP servers, this field frequently shows multiple connections to a host system. In this example, nodes 8, 9, and 14 show multiple connections.

   - **V** indicates that only a virtual circuit is open and no connection is present. This happens prior to

establishing a connection. It also happens when there is another controller on the same network and when there are systems with multiple adapters connected to the same network. Node 15 demonstrates this principle.

- If a period (.) is in a position corresponding to a node, that node does not have any virtual circuits or connections to this controller.
- A space indicates the address is beyond the visible node range for this controller.

CI/DSSI host path status

```
Path Status
 0123456789 ❶
0........^^ ❷
1..A.B^....
2.......X..
3..
```

Description

This display indicates the path status to any system for which a virtual circuit exists. This display is available only on CI and DSSI based controllers.

1. ❶Each position in the data field represents one of the possible nodes to which the controller can communicate. To locate the path status for a given node, use the column on the left to determine the high order digit of the node number, and use the second row to determine the low order digit of the node number. For CI controllers, the number of nodes displayed is determined by the controllers MAX NODE parameter. The maximum supported value for this parameter is 32. For DSSI controllers, the number of nodes is fixed at 8.

2. ❷Each location in the grid contains a character to indicate the path status:

   - **A** indicates only CI path A is functioning properly. In this example, node 12 demonstrates this. This value is not displayed for DSSI based controllers.
   - **B** indicates only CI path B is functioning properly. In this example, node 14 demonstrates this. This value is not displayed for DSSI based controllers.
   - **X** indicates the CI cables are crossed. In this example, node 27 demonstrates this. This value is not displayed for DSSI based controllers.
   - A circumflex (^) indicates the single DSSI path or both CI paths are functioning properly. In this example, nodes 8, 9, and 15 demonstrate this.

- If a period (.) is in a position corresponding to a node, that node does not have any virtual circuits or connections to this controller so either the path status cannot be determined, or neither path is functioning properly.
- A space indicates the address is beyond the visible node range for this controller.

Device SCSI status

```
Target
  01234567 ❶
P1 DDDDFhH ❷
o2TTT T hH
r3DDD   hH
t4DDDDDDhH
 5DDDD  hH
 6      hH❸
```

Description

This display shows what devices the controller has been able to identify on the device busses.

The controller does not look for devices that are not configured into the nonvolatile memory using the CLI ADD command.

1. ❶The column headings indicate the SCSI target numbers for the devices. SCSI targets are in the range 0 through 7. Target 7 is always used by a controller. In a dual controller configuration, target 6 is used by the second controller.
2. ❷The device grid contains a letter signifying the device type in each port/target location where a device has been found:
   - **C** indicates a CD–ROM device.
   - **D** indicates a disk device.
   - **F** indicates a device type not listed above.
   - **H** indicates bus position of this controller.
   - **h** indicates bus position of the other controller.
   - **L** indicates a media loader.
   - **T** indicates a tape device.
   - A period (.) indicates the device type is unknown.

- A space indicates there is no device configured at this location.

3. ❸This subdisplay contains a row for each SCSI device port supported by the controller. The subdisplay for a controller that has six SCSI device ports is shown.

Unit status (abbreviated)

```
Unit❶ ASWC❷ KB/S❸ Rd%❹ Wr%❺ Cm%❻ HT%❼
D0110  a^ r      0     0     0     0     0
D0120  a^ r      0     0     0     0     0
D0130  o^ r    236   100     0     0   100
T0220  av        0     0     0     0     0
T0230  o^      123     0   100     0     0
```

Description

This subdisplay shows the status of the logical units that are known to the controller firmware. It also indicates performance information for the units. Up to 42 units can be displayed in this subdisplay.

1. ❶The **Unit** column contains a letter indicating the type of unit followed by the unit number of the logical unit. The list is sorted by unit number. There may be duplication of unit numbers between devices of different types. If this happens, the order of these devices is arbitrary. The following device type letters may appear:
   - **D** indicates a disk device.
   - **T** indicates a tape device.
   - **L** indicates a media loader.
   - **C** indicates a CD–ROM device.
   - **F** indicates a device type not listed above.
   - **U** indicates the device type is unknown.
2. ❷The **ASWC** columns indicate respectively the availability, spindle state, write protect state, and cache state of the logical unit.

   For HSZ controllers, on line in this column means that the unit is on line to the HSZ controller only. It does not indicate that the unit is mounted by the host.

   The availability state is indicated using the following letters:

- **a**—Available. Available to be mounted by a host system.
- **d**—Offline, Disabled by Digital Multivendor Customer Services. The unit has been disabled for service.
- **e**—Online, Exclusive Access. Unit has been mounted for exclusive access by a user.
- **f**—Offline, Media Format Error. The unit cannot be brought available due to a media format inconsistency.
- **i**—Offline, Inoperative. The unit is inoperative and cannot be brought available by the controller.
- **m**—Offline, Maintenance. The unit has been placed in maintenance mode for diagnostic or other purposes.
- **o**—Online. Mounted by at least one of the host systems. For HSZ controllers, on line in this column means that the unit is on line to the HSZ controller only. It does not indicate that the unit is mounted by the host.
- **r**—Offline, Rundown. The CLI SET NORUN command has been issued for this unit.
- **v**—Offline, No Volume Mounted. The device does not contain media.
- **x**—Online to other controller. Not available for use by this controller.
- A space in this column indicates the availability is unknown.

The spindle state is indicated using the following characters:

- **^**—For disks, this symbol indicates the device is at speed. For tapes, it indicates the tape is loaded.

- **>**—For disks, this symbol indicates the device is spinning up. For tapes, it indicates the tape is loading.
- **<**—For disks, this symbol indicates the device is spinning down. For tapes, it indicates the tape is unloading.
- **v**—For disks, this symbol indicates the device is stopped. For tapes, it indicates the tape is unloaded.
- For other types of devices, this column is left blank.

For disks and tapes, a **w** in the write protect column indicates the unit is write protected. This column is left blank for other device types.

The data caching state is indicated using the following letters:

- **b**—Both Read caching and Write Back caching are enabled.
- **r**—Read caching is enabled.
- **w**—Write Back caching is enabled.
- A space in this column indicates caching is disabled.

3. **❸KB/S**—This column indicates the average amount of kilobytes of data transferred to and from the unit in the previous screen update interval. This data is available only for disk and tape units.
4. **❹Rd%**—This column indicates what percentage of data transferred between the host and the unit were read from the unit. This data is contained only in the **DEFAULT** display for disk and tape device types.
5. **❺Wr%**—This column indicates what percentage of data transferred between the host and the unit were written to the unit. This data is contained only in the **DEFAULT** display for disk and tape device types.

6. ❻**Cm%**—This column indicates what percentage of data transferred between the host and the unit were compared. A compare operation can be accompanied by either a read or a write operation, so this column is not cumulative with read percentage and write percentage columns. This data is contained only in the **DEFAULT** display for disk and tape device types.

7. ❼**HT%**—This column indicates the cache hit percentage for data transferred between the host and the unit.

Unit status (full)

Unit❶	ASWC❷	KB/S❸	Rd%❹	Wr%❺	Cm%❻	HT%❼	PH%❽	MS%❾	Purge❿	BlChd⓫	BlHit⓬	
D0003	o^ r	382	0	100	0	0	0	0	0	6880		0
D0250	o^ r	382	100	0	0	0	0	100	0	6880		0
D0251	o^ r	284	100	0	0	0	0	100	0	5120		0
D0262	a^ r	0	0	0	0	0	0	0	0	0		0
D0280	o^ r	497	44	55	0	0	0	100	0	9011		0
D0351	a^ r	0	0	0	0	0	0	0	0	0		0
D0911	a^ r	0	0	0	0	0	0	0	0	0		0
D1000	a^ r	0	0	0	0	0	0	0	0	0		0

Description

This subdisplay shows the status of the logical units that are known to the controller firmware. It also shows I/O performance information and caching statistics for the units. Up to 42 units can be displayed in this subdisplay.

1. ❶The **Unit** column contains a letter indicating the type of unit followed by the unit number of the logical unit. The list is sorted by unit number. There may be duplication of unit numbers between devices of different types. If this happens, the order of these devices is arbitrary. The following device type letters may appear:
   - **D** indicates a disk device.
   - **T** indicates a tape device.
   - **L** indicates a media loader.
   - **C** indicates a CD–ROM device.
   - **F** indicates a device type not listed above.
   - **U** indicates the device type is unknown.
2. ❷The **ASWC** columns indicate the availability, spindle state, write protect state, and cache state respectively of the logical unit..

   For HSZ controllers, on line in this column means that the unit is on line to the HSZ controller only. It does not indicate that the unit is mounted by the host.

The availability state is indicated using the following letters:

- **a**—Available. Available to be mounted by a host system.
- **d**—Offline, Disabled by Digital Multivendor Customer Services. The unit has been disabled for service.
- **e**—Online, Exclusive Access. Unit has been mounted for exclusive access by a user.
- **f**—Offline, Media Format Error. The unit cannot be brought available due to a media format inconsistency.
- **i**—Offline, Inoperative. The unit is inoperative and cannot be brought available by the controller.
- **m**—Offline, Maintenance. The unit has been placed in maintenance mode for diagnostic or other purposes.
- **o**—Online. Mounted by at least one of the host systems. For

  HSZ controllers, on line in this column means that the unit is on line to the HSZ controller only. It does not indicate that the unit is mounted by the host.
- **r**—Offline, Rundown. The CLI SET NORUN command has been issued for this unit.
- **v**—Offline, No Volume Mounted. The device does not contain media.
- **x**—Online to other controller. Not available for use by this controller.
- A space in this column indicates the availability is unknown.

The spindle state is indicated using the following characters:

- **^**—For disks, this symbol indicates the device is at speed. For tapes, it indicates the tape is loaded.
- **>**—For disks, this symbol indicates the device is spinning up. For tapes, it indicates the tape is loading.
- **<**—For disks, this symbol indicates the device is spinning down. For tapes, it indicates the tape is unloading.
- **v**—For disks, this symbol indicates the device is stopped. For tapes, it indicates the tape is unloaded.

For other types of devices, this column is left blank.

For disks and tapes, a **w** in the write protect column indicates the unit is write protected. This column is left blank for other device types.

The data caching state is indicated using the following letters:

- **b**—Both Read caching and Write Back caching are enabled.
- **r**—Read caching is enabled.
- **w**—Write Back caching is enabled.
- A space in this column indicates caching is disabled.

3. **❸KB/S**—This column indicates the average amount of kilobytes of data transferred to and from the unit in the previous screen update interval. This data is only available for disk and tape units.
4. **❹Rd%**—This column indicates what percentage of data transferred between the host and the unit were read from the unit. This data is only contained in the **DEFAULT** display for disk and tape device types.
5. **❺Wr%**—This column indicates what percentage of data transferred between the host and the unit were written

to the unit. This data is only contained in the **DEFAULT** display for disk and tape device types.

6. ❻**Cm%**—This column indicates what percentage of data transferred between the host and the unit were compared. A compare operation may be accompanied by either a read or a write operation, so this column is not cumulative with read percentage and write percentage columns. This data is only contained in the **DEFAULT** display for disk and tape device types.

7. ❼**HT%**—This column indicates the cache hit percentage for data transferred between the host and the unit.

8. ❽**PH%**—This column indicates the partial cache hit percentage for data transferred between the host and the unit.

9. ❾**MS%**—This column indicates the cache miss percentage for data transferred between the host and the unit.

10. ❿**Purge**—This column shows the number of blocks purged from the write back cache in the last update interval.

11. ➀**BlChd**—This column shows the number of blocks added to the cache in the last update interval.

12. ➁**BlHit**—This column shows the number of cached data blocks “hit” in the last update interval.

Device status

PTL❶	ASWF❷	Rq/S❸	RdKB/S❹	WrKB/S❺	Que❻	Tg❼	CR❽	BR❾	TR❿
D100	A^	0	0	0	11	0	0	0	0
D120	A^	0	0	0	0	0	0	0	0
D140	A^	0	0	0	0	0	0	0	0
D210	A^	11	93	0	1	1	0	0	0
D230	A^	0	0	0	0	0	0	0	0
D300	A^	11	93	0	2	1	0	0	0
D310	A^	0	0	0	0	0	0	0	0
D320	A^	36	247	0	12	10	0	0	0
D400	A^	11	93	0	2	1	0	0	0
D410	A^	0	0	0	0	0	0	0	0
D420	A^	36	247	0	10	8	0	0	0
D430	A^	0	0	0	0	0	0	0	0
D440	A^	0	0	0	0	0	0	0	0
D450	A^	0	0	0	0	0	0	0	0
D500	A^	11	93	0	1	1	0	0	0
D510	A^	0	0	0	0	0	0	0	0
D520	A^	0	0	0	0	0	0	0	0
D530	A^	47	0	375	6	5	0	0	0

Description

This subdisplay shows the status of the physical storage devices that are known to the controller firmware. It also shows I/O performance information and bus statistics for these devices. Up to 42 devices can be displayed in this subdisplay.

1. ❶The **PTL** column contains a letter indicating the type of device followed by the SCSI Port, Target, and LUN of the device. The list is sorted by port, target, and LUN. The following device type letters may appear:
   - **D** indicates a disk device.
   - **T** indicates a tape device.
   - **L** indicates a media loader.
   - **C** indicates a CD–ROM device.
   - **F** indicates a device type not listed above.
   - **U** indicates the device type is unknown.

2. ❷The **ASWF** columns indicate the allocation, spindle state, write protect state, and fault state respectively of the device.

   The availability state is indicated using the following letters:

   - **A**—Allocated to this controller.
   - **a**—Allocated to the other controller.
   - **U**—Unallocated, but owned by this controller.
   - **u**—Unallocated, but owned by the other controller.
   - A space in this column indicates the allocation is unknown.

   The spindle state is indicated using the following characters:

   - **^**—For disks, this symbol indicates the device is at speed. For tapes, it indicates the tape is loaded.
   - **>**—For disks, this symbol indicates the device is spinning up. For tapes, it indicates the tape is loading.
   - **<**—For disks, this symbol indicates the device is spinning down. For tapes, it indicates the tape is unloading.
   - **v**—For disks, this symbol indicates the device is stopped. For tapes, it indicates the tape is unloaded.
   - For other types of devices, this column is left blank.

   For disks and tapes, a **W** in the write protect column indicates the device is hardware write protected. This column is left blank for other device types.

   A **F** in the fault column indicates an unrecoverable device fault. If this field is set, the device fault indicator also is illuminated.

3. ❸**Rq/S**—This column shows the average I/O request rate for the device during the last update interval. These requests are up to eight kilobytes long and are either generated by host requests or cache flush activity.

4. ❹**RdKB/S**—This column shows the average data transfer rate from the device in kilobytes during the previous screen update interval.

5. ❺**WrKB/S**—This column shows the average data transfer rate to the device in kilobytes during the previous screen update interval.

6. ❻**Que**—This column shows the maximum number of transfer requests waiting to be transferred to the device during the last screen update interval.

7. ❼**Tg**—This column shows the maximum number of transfer requests queued to the device during the last screen update interval. If a device does not support tagged queuing, the maximum value is 1.

8. ❽**CR**—This column indicates the number of SCSI command resets that occurred since VTDPY was started.

9. ❾**BR**—This column indicates the number of SCSI bus resets that occurred since VTDPY was started.

10. ❿**TR**—This column indicates the number of SCSI target resets that occurred since VTDPY was started.

Device SCSI port performance

Port❶	Rq/S❷	RdKB/S❸	WrKB/S❹	CR❺	BR❻	TR❼
1	0	0	0	0	0	0
2	11	93	0	0	0	0
3	48	341	0	0	0	0
4	48	340	0	0	0	0
5	58	93	375	0	0	0
6	0	0	0	0	0	0

Description

This subdisplay shows the accumulated I/O performance values and bus statistics for the SCSI device ports. The subdisplay for a controller that has six SCSI device ports in shown.

1. ❶The **Port** column indicates the number of the SCSI device port.
2. ❷**Rq/S**—This column shows the average I/O request rate for the port during the last update interval. These requests are up to eight kilobytes long and are either generated by host requests or cache flush activity.
3. ❸**RdKB/S**—This column shows the average data transfer rate from all devices on the SCSI bus in kilobytes during the previous screen update interval.
4. ❹**WrKB/S**—This column shows the average data transfer rate to all devices on the SCSI bus in kilobytes during the previous screen update interval.
5. ❺**CR**—This column indicates the number of SCSI command resets that occurred since VTDPY was started.
6. ❻**BR**—This column indicates the number of SCSI bus resets that occurred since VTDPY was started.
7. ❼**TR**—This column indicates the number of SCSI target resets that occurred since VTDPY was started.

Help example

```
VTDPY> HELP

Available VTDPY commands:

^C - Prompt for commands
^G or ^Z - Update screen
^O - Pause/Resume screen updates
^Y - Terminate program
^R or ^W - Refresh screen
DISPLAY CACHE - Use 132 column unit caching statistics
display
DISPLAY DEFAULT - Use default 132 column system performance
display
DISPLAY DEVICE - Use 132 column device performance display
DISPLAY STATUS - Use 80 column controller status display
EXIT - Terminate program (same as QUIT)
INTERVAL <seconds> - Change update interval
HELP - Display this help message
REFRESH - Refresh the current display
QUIT - Terminate program (same as EXIT)
UPDATE - Update screen display

VTDPY>
```

Description

This is the sample output from executing the HELP command

2 Replacing field-replaceable units

Controller and cache modules using C_Swap

Controller and acache module (single controller)

One dual-redundant controller and cache module

Both dual redundant controllers and cache modules

Cache modues

SBB battery modules

Power supplies

Disk drives

Tape drives

Solid state disks, optical and CD-ROM drives

Host and device cables

Electrostatic discharge protection

The following sections describe necessary precautions for preventing component damage while servicing your HSJ50 subsystem. Use the following guidelines when performing any of the replacement procedures.

Electrostatic discharge (ESD) can damage system components. Use the following guidelines when handling subsystem components.

Handling controllers or cache modules

After removing a controller or cache module from the shelf, place the module into an approved antistatic bag or onto a grounded antistatic mat.

When removing write-back cache modules, always disconnect the external cache battery cable from the ECB module and the cache module.

- If power is removed from the controller shelf or cabinet during a procedure, disable the ECB by pressing the battery disable switch, then disconnect the battery cable at the cache module.
- If power is not to be removed during the procedure, disconnect the ECB cable starting at the cache module end and then the ECB. After the cable is removed, disable the ECB by pressing the battery disable switch.

Handling the program card

Use the following guidelines when handling the program card:

- Cover the program card with the snap-on ESD cover when the card is installed in the controller.
- Keep the program card in its original carrying case when not in use.

- Do not twist or bend the program card.
- Do not touch the program card contacts.

Handling controller host-port cables

Use the following guidelines when handling controller host-port cables:

- When installing host port cables, use care not to touch the connector's pins.
- Use care not to bend any connector pins when plugging the host cables into the controller CI connector.

Replacing controllers and cache modules using C_swap

This section presents controller and controller component replacement procedures for HSJ50 controllers. Also, replacement procedures for cache modules and write-back cache batteries are provided.

Note

Use this procedure when you cannot shut down the system and one controller is still fully functioning.

Controller and cache module warm-swap procedure

Use the warm-swap procedure to replace a controller that has failed and failover already has taken place. Also, use this procedure if you a suspect that a controller is not operating properly (that is, one or more controller ports have failed). Use this procedure when you cannot shut down the system and only if the controller is in a dual-redundant configuration.

To replace a controller using the C_SWAP method, a minimum of two power supplies are required in SW500 and SW800 cabinets. If you are performing the replacement procedure in an SW300 cabinet, a minimum of five power supplies are required.

Required tools

The tools listed in Table 7 are required to replace a controller and/or cache module.

Table 7
Required tools

Required tools	Purpose
Maintenance terminal	To shut down controllers, restart controllers, execute CLI commands, and invoke utilities
ESD wrist strap and ESD mat	To protect all equipment against ESD
Small flat head screwdriver	To loosen CI connector, and front bezel captive screws
5/32-Allen wrench	To unlock the SW800 - Series cabinet

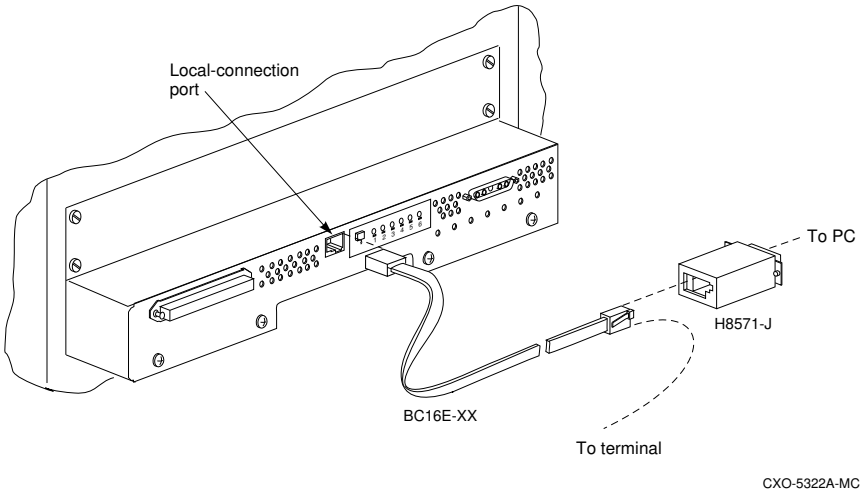
Preparing the subsystem

1. Terminate all running utilities and disable all other terminals.

2. Have the replacement modules at hand. The modules should be factory-fresh or should have been shut down cleanly (with the SHUTDOWN command) in their last application.

3. Connect a maintenance terminal to the controller that you are *not* replacing (see Figure 1).

Figure 1
Connecting a maintenance terminal to the controller



4. Prefer all units to the controller that you are not replacing.

   ```
   CLI> SET unit-number PREFERRED_PATH=THIS_CONTROLLER
   ```

   Repeat the command for each unit that is preferred to the controller that you are replacing.

5. Disable the CI paths by issuing the following CLI commands:

   ```
   CLI> SET OTHER_CONTROLLER NOPATH_A
   CLI> SET OTHER CONTROLLER NOPATH_B
   ```

6. If the controller to be replaced is still functioning, use the SHUTDOWN command to take it out of service. When using this command, do not specify any command switches:

   _

When the controller halts, the green Reset (//) LED stops flashing and stays lit.

7. Take the operating controller out of dual-redundant (failover) mode:

   ```
   CLI> SET NOFAILOVER
   ```

8. With a small flat-head screwdriver, loosen the captive screws that secure the CI connector to the controller.

9. Loosen the two captive retaining screws at each corner of the controller and cache module front bezel. Do not remove the module yet.

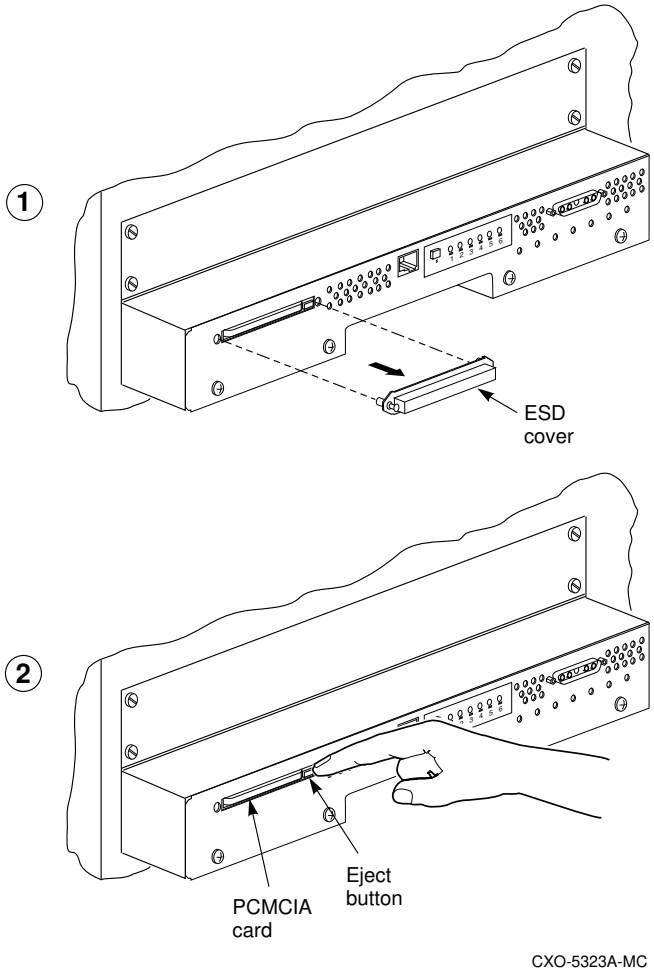
10. Obtain and place the ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.

11. Attach or clip the other end of the ESD wrist strap to the cabinet grounding stud or a convenient cabinet grounding point (nonpainted surface).

12. Unsnap and remove the program card ESD cover on the controller you are removing.

13. Remove the program card by pushing the eject button next to the card (see Figure 2). Pull the card out and save it for use in the replacement controller module.

Figure 2
Removing the program card



14. Start the C_SWAP program:

```
CLI> RUN C_SWAP
```

Removing the modules

1. Indicate that you are going to remove the controller module.

```
Do you wish to remove the other HSJ50 y/n [n] ?
```

2. Press "**Y**" for yes.
3. Indicate if you are also going to remove the cache module.

```
Will its cache module also be removed Y/N [n] ?
```

4. Wait for the following text to be displayed at the console:

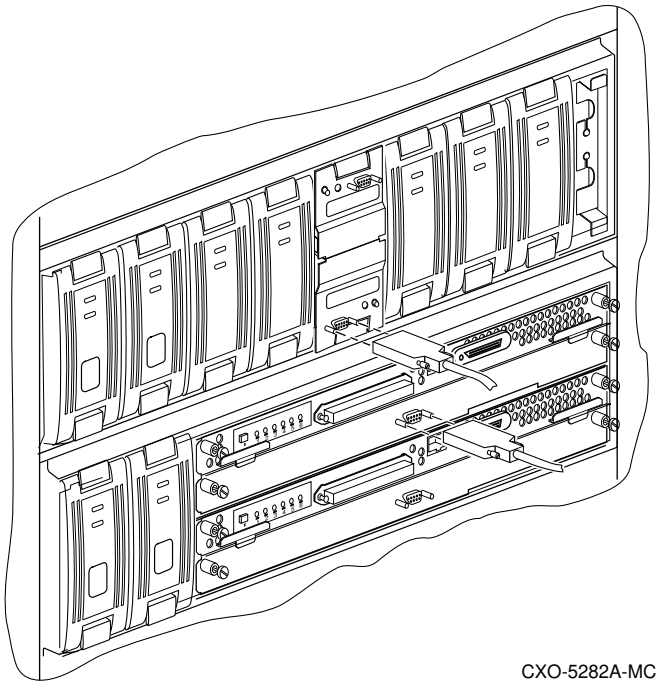
```
Port 1 quiesced.
Port 2 quiesced.
Port 3 quiesced.
Port 4 quiesced.
Port 5 quiesced.
Port 6 quiesced.
All ports quiesced.
Remove the other controller (the one WITHOUT a blinking
green LED) within 5 minutes.
Time remaining 4 minutes 50 seconds.
```

Note

If the cache module is not to be removed, the time allowed to remove the controller will be 2 minutes.

5. Remove the CI connector from the controller.
6. Disconnect the ECB cable (external cache battery) from the cache module. While holding the battery cable in one hand, disable the ECB by pressing the battery disable switch (see Figure 3).

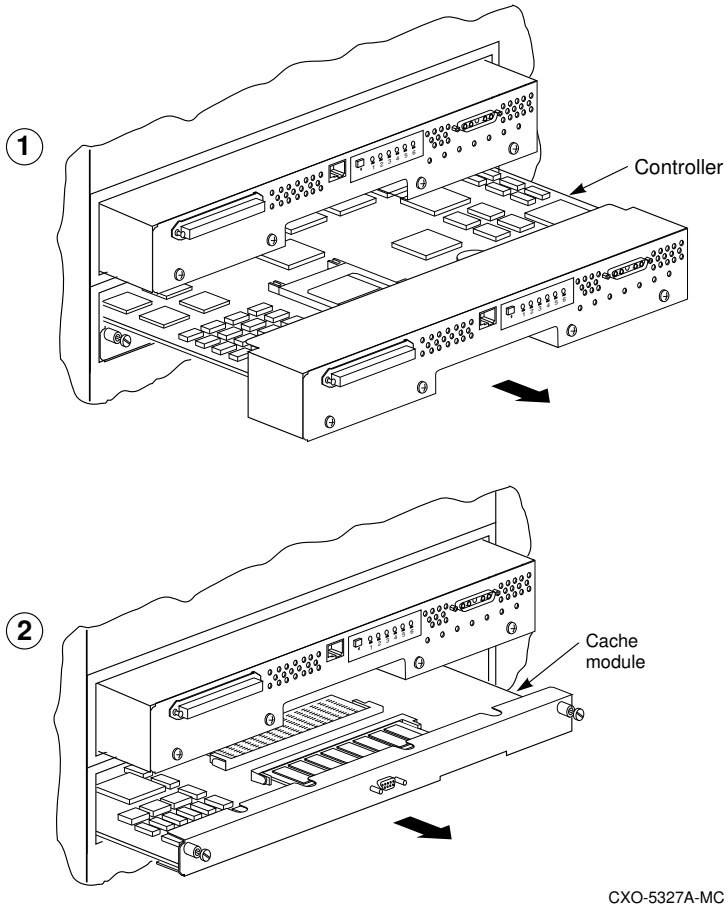
Figure 3 Disconnecting the ECB cable



CXO-5282A-MC

7. Slide the controller and cache modules out of the shelf. Note in which rails the module was seated (see and place the modules on an ESD mat (see Figure 4).

Figure 4
Removing the controller and cache modules



8. Wait for the following text to be displayed at the operating controller's console:

```
Port 1 restarted.
Port 2 restarted.
Port 3 restarted.
Port 4 restarted.
Port 5 restarted.
Port 6 restarted.
```

Note

You may remove the cache module before or after port activity has restarted.

9. If required, remove the cache module.

Installing the new modules

1. When the controller prompts you, answer the questions:

```
Do you have a replacement HSJ50 readily available? [N]
? y
```

2. If you have a replacement module available, enter "**YES**"
3. Answer the question:

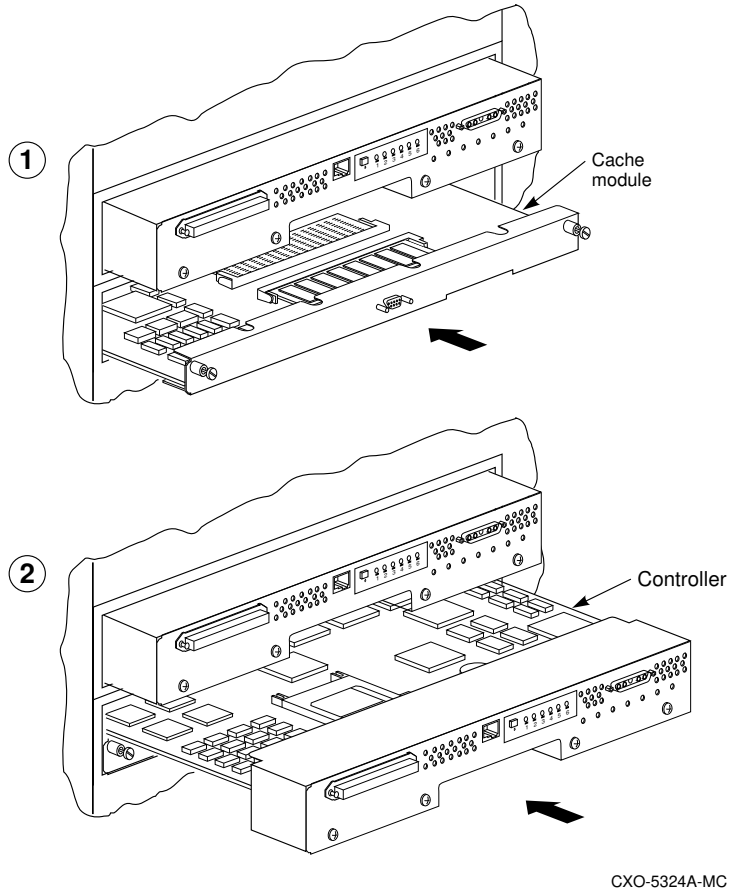
```
***Sequence to INSERT the other HSJ50 has begun.***

Do you wish to INSERT the other HSJ50 [N] ?
```

4. Press "**Y**" for yes.
5. Wait for the following text to appear on the operating controller's console:

```
Attempting to quiesce all ports.
Port 1 quiesced.
Port 2 quiesced.
Port 3 quiesced.
Port 4 quiesced.
Port 5 quiesced.
Port 6 quiesced.
All ports quiesced.
Insert the other HSJ50 WITHOUT its program card, and
press Return.
```

6. If necessary, install the cache module. Slide the module straight in along the rails and then push firmly to seat it in the backplane (see Figure 5).

Figure 5
Installing the new cache and controller module



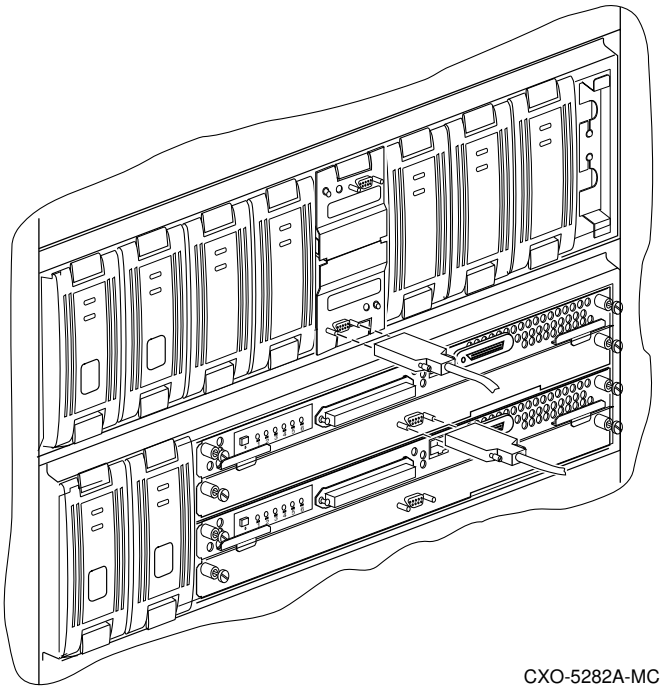
7. Slide the module straight in along the rails and then push firmly to seat it in the backplane (see Figure 5).

Caution

Do not overtighten the controller's front panel captive screws. Damage to the controller PC board or front panel may result.

8. Tighten the two front panel captive screws on the controller and cache module.
9. Reconnect the CI cable to the controller's front panel.
10. Reconnect the open end of the ECB cable to the cache module (see Figure 6).

Figure 6
Reconnecting the ECB cable



11. Press **Return** on the operating controller's console.

12. Wait for the following text to be displayed on the operating controller's console:

```
Port 1 restarted.
Port 2 restarted.
Port 3 restarted.
Port 4 restarted.
Port 5 restarted.
Port 6 restarted.

Controller Warm Swap terminated.
The configuration has two controllers.
To restart the other HSJ50.
1) Enter the command RESTART OTHER_CONTROLLER.
2) Press and hold in the Reset (//) button while
inserting the program card.
3) Release Reset (//); the controller will initialize.
4) Configure new controller by referring to the
controller's configuring manual.
```

Restarting the subsystem

Note

The following section explains in detail the four steps shown on the terminal's screen

1. Start the new controller by entering the following CLI command:

   ```
   CLI> RESTART OTHER_CONTROLLER
   ```

2. Connect the maintenance terminal to the newly installed controller.

3. Press and hold the Reset (//) button on the new controller while inserting the program card from the replaced controller.

4. Release the Reset (//) button to initialize the controller. Wait for the CLI prompt to appear at the terminal. You will see a "Controllers misconfigured" message, which you can ignore.

5. If the new controller reports an invalid cache error, enter one of the following CLI commands to clear the error.

   If you have replaced the cache module, enter the following command:

   ```
   CLI> CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
   DESTROY_UNFLUSHED_DATA
   ```

   Otherwise, enter:

   ```
   CLI> CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
   NODESTROY_UNFLUSHED_DATA
   ```

6. Ensure that the new controller is not in dual-redundant mode by entering the following command on the new controller:

   ```
   CLI> SET NOFAILOVER
   ```

   If the controller was already in nonredundant mode, you will see a message indicating that.

7. Connect the maintenance terminal to the new controller (see Figure 1).

8. Enter the following command from the *new* controller to put the controllers into dual-redundant mode.

   ```
   CLI> SET FAILOVER COPY=OTHER_CONTROLLER
   ```

   The new controller will initialize.

9. Verify that all host settings are correct:

   ```
   CLI> SHOW THIS_CONTROLLER
   ```

   Modify any incorrect information.

10. If any information has been changed, restart the new controller:

    ```
    CLI> RESTART THIS_CONTROLLER
    ```

11. After the controller has initialized, reconnect the CI cable to the new controller and tighten the captive screws.

12. Enable CI paths by entering the following commands:

    ```
    CLI> SET THIS_CONTROLLER PATH_A
    CLI> SET THIS_CONTROLLER PATH_B
    ```

13. On the ECB module front panel, check the LED status indicator for the appropriate indication (see Table 8).

Table 8
ECB status indicators

LED Status	Battery Status
LED is on continuously	System power is on and the ECB is fully charged.
LED blinks rapidly	System power is on and the ECB is charging.
LED blinks slowly	System power is off and the ECB is supplying power to the cache.
LED is off	System power is off and the ECB is not supplying power to the cache.

Replacing a controller and cache module in a single controller configuration

When you replace the controller module in a nonredundant configuration, device service is interrupted for the duration of the service cycle.

Required tools

The tools listed in Table 9 are required for the replacement of single controllers.

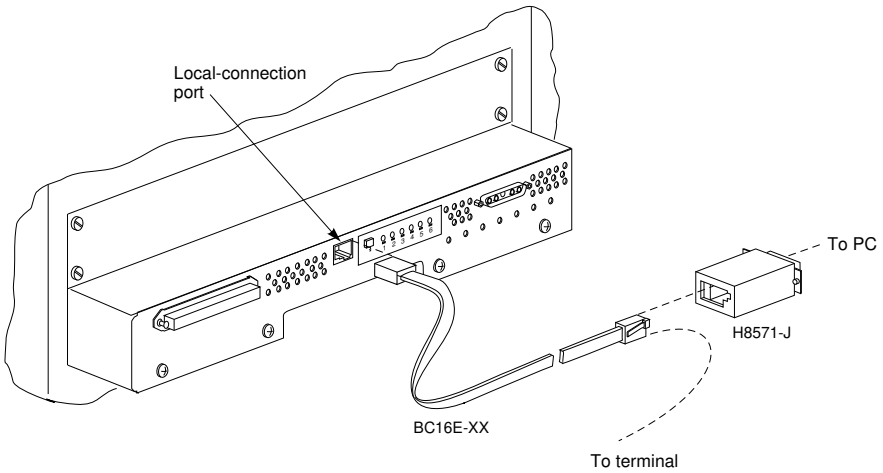
Table 9 Required tools for controller replacement

Required tools	Purpose
Maintenance terminal	To shut down controllers, restart controllers, execute CLI commands, and invoke utilities
ESD wrist strap and ESD mat	To protect all equipment against ESD
Small flat head screwdriver	To loosen CI connector, and front bezel captive screws
5/32-Allen wrench	To unlock the SW800 - Series cabinet

Removing the controller

1. If the controller is still or partially functioning, connect a maintenance terminal to the controller (see Figure 7).

Figure 7 Connecting a maintenance terminal to the controller



2. Take the controller out of service:

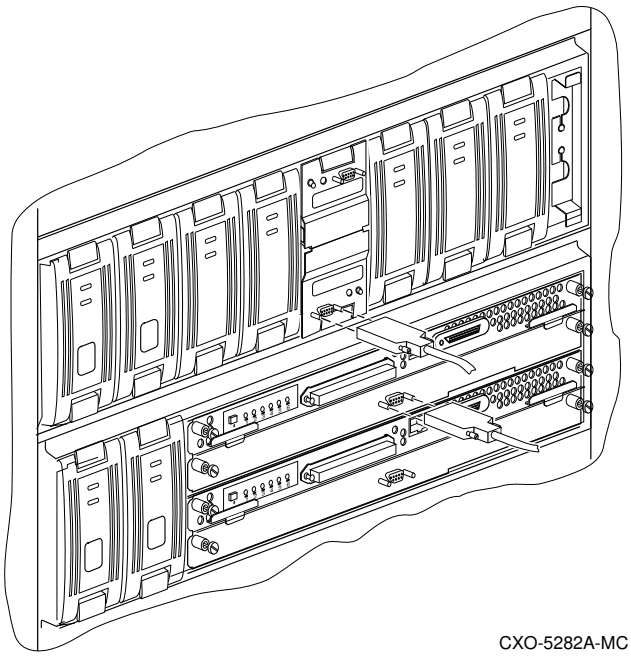
   ```
   CLI> SHUTDOWN THIS_CONTROLLER
   ```

   To ensure that the controller has shut down cleanly, check for the following indication on the controller's OCP (operator control panel):

   - The Reset (//) light is lit continuously.
   - Port lights 1, 2, 3, are also lit continuously.

3. If the controller is no longer functioning, prepare to remove the module by going to step 3.
4. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.
5. Attach or clip the other end of the ESD wrist strap to the cabinet grounding stud or a convenient cabinet grounding point.
6. Remove the power cords from the controller power supplies.
7. Disable the ECB switch by pressing the battery disable switch on the battery module front panel (see Figure 8) on the following page.

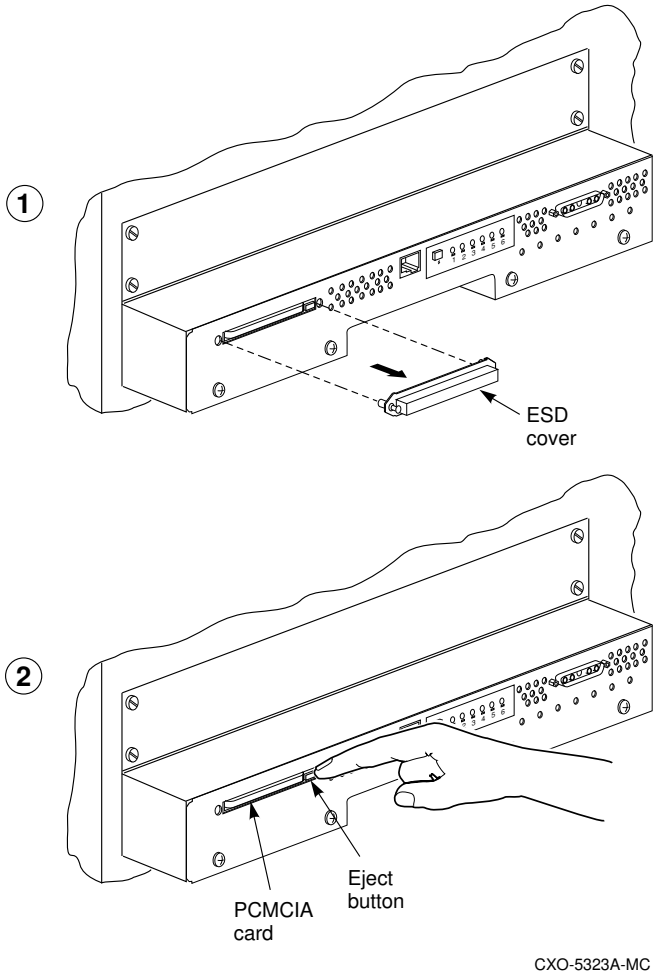
Figure 8
Disconnecting the ECB cable



8. Disconnect the ECB cable from the cache module (see Figure 8).
9. Unsnap and remove the program card ESD cover (see Figure 9).

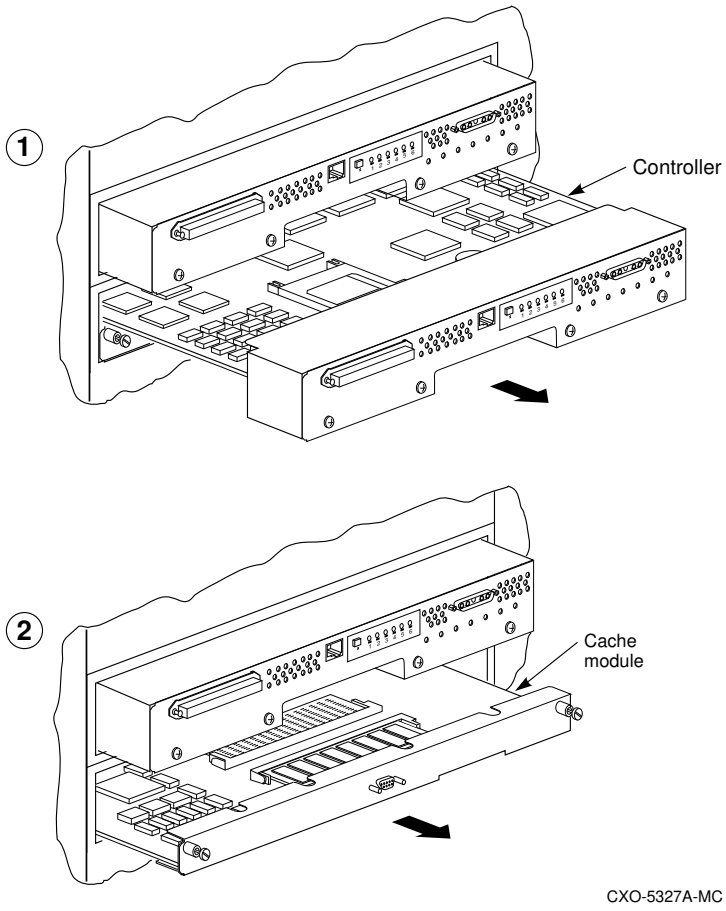
10. Remove the program card by pushing the eject button next to the card (see Figure 9). Pull the card from the controller module. Save the program card for the replacement controller.

Figure 9
Removing the program card



11. With a small flat-head screwdriver, loosen the captive screws on the CI connector at the controller's front panel.

Figure 10
Removing the controller and cache module



12. Loosen the two captive retaining screws at each corner of the the controller's front bezel.

13. Use a gentle rocking motion to loosen the controller module from the shelf backplane.

14. Slide the controller module out of the shelf and place it on an ESD mat (see Figure 10).

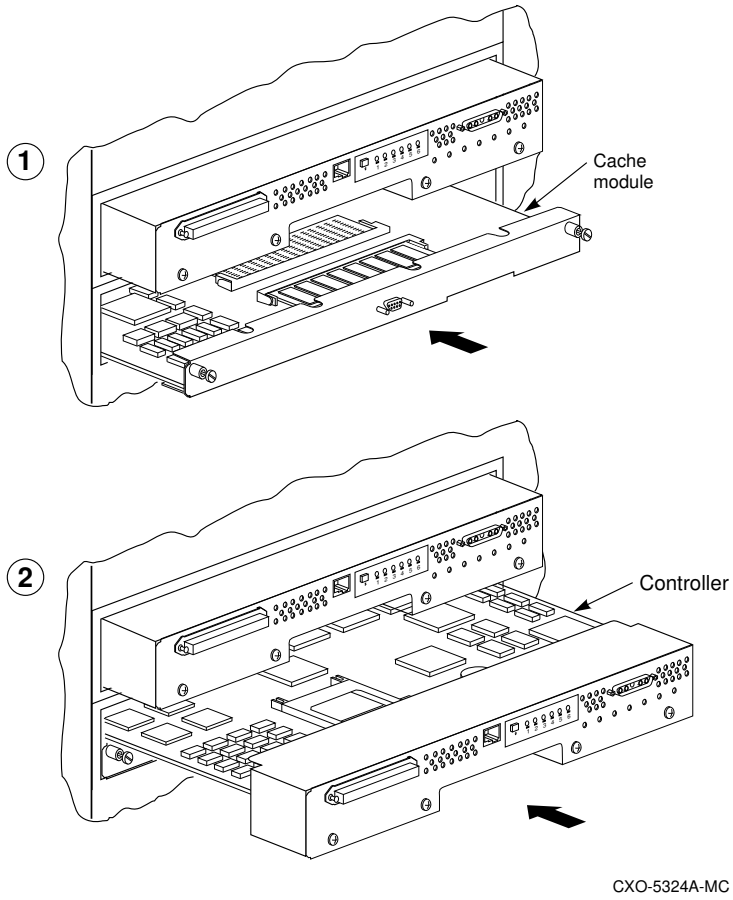
15. If you are also removing the cache module, loosen the captive screws at each corner of the cache module's front bezel. Uuse a gentle rocking motion to loosen the cache from the shelf backplane.

16. Slide the cache module out of the shelf (see Figure 10).

Installing the new module

1. If required, install the replacement cache module into the shelf (see Figure 11).

Figure 11
Installing the new cache and controller modules



2. Slide the new controller module into the shelf using the same rails as the removed module (see Figure 11).

Caution

Do not overtighten the front panel captive screws. Damage to the controller PC board or front panel may result.

3. Tighten the front panel captive screws on the controller and cache module.
4. Reconnect the open end of the ECB cable to the cache module. Tighten the cable mounting screws.
5. Attach a maintenance terminal to the new controller.
6. Press and hold the controller's green reset (//) button, while inserting the program card. The program card eject button will extend when the card is fully inserted.
7. Release the reset button to initialize the controller.
8. If the controller reports an invalid cache error, enter one of the the following CLI command:

   If you have replaced the cache board, enter the following command:

   ```
   CLI >CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
   DESTROY_UNFLUSHED_DATA
   ```

   Otherwise enter:

   ```
   CLI> CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
   NODESTROY_UNFLUSHED _DATA
   ```

9. Reattach the CI cable to the controller's front panel.
10. Check the configuration by entering the following CLI commad:

    ```
    CLI> SHOW THIS_CONTROLLER
    ```

The controller will display the following information (this is a sample only):

```
Controller:
    HSJ50  ZG34901786 Firmware V05-0, Hardware BX11
    Configured for dual-redundancy with ZG61000012
       In dual-redundant configuration
    SCSI address 7
    Time: 15 JUN-1996 16:32:54
Host port:
    Node name: HSJA1, valid CI node 21, 32 max nodes
    Path A is on
    Path B is on
    MSCP allocation class  3
    TMSCP allocation class 3
    CI_ARBITRATION = SYNCHRONOUS
    MAXIMUM HOSTS =9
    NOCI_4K_PACKET _CAPABILITY

Cache:
    128 megabyte write cache, version 3
    Cache is GOOD
    Battery is good
    No unflushed data in cache
    CACHE_FLUSH TIMER = DEFAULT (10 seconds)
    CACHE_POLICY = B
    NOCACHE_UPS
```

Replacing one dual-redundant controller and write-back cache module

When you replace one dual-redundant controller module using the following instructions, device service is interrupted for the duration of the service cycle. Use this procedure when you can't warm swap the controller and or cache module.

Required tools

The tools listed in Table 10 are required for the replacement of controllers.

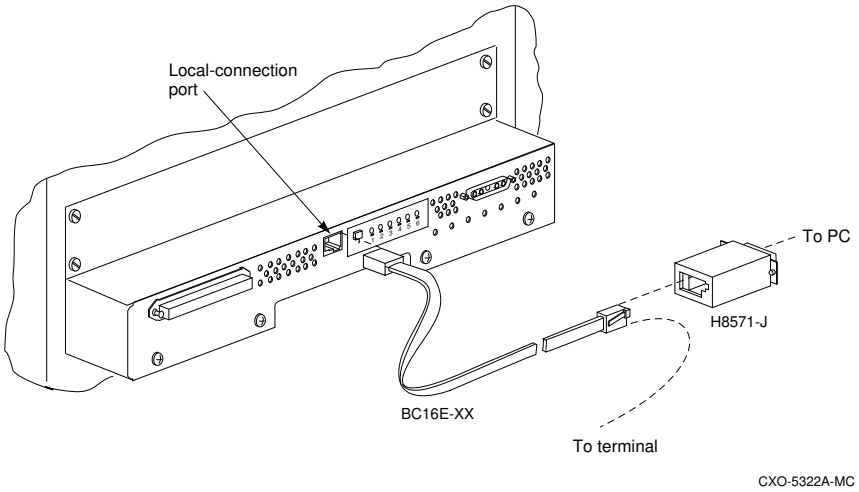
Table 10 Required tools for controller replacement

Required tools	Purpose
Maintenance terminal	To shut down controllers, restart controllers, execute CLI commands, and invoke utilities
ESD wrist strap and ESD mat	To protect all equipment against ESD
Small flat head screwdriver	To loosen CI connector, and front bezel captive screws
5/32-Allen wrench	To unlock the SW800 - Series cabinet

Removing the controller

1. Determine that one controller is still operating properly.
2. If the controller you are removing is partially functioning, connect a maintenance terminal to the controller. If the controller has failed, connect a maintenance terminal to the other controller (see Figure 12).

Figure 12
Connecting a maintenance terminal to the controller



3. At the partially functioning controller or at the operating controller's console, enter:

   ```
   CLI> SHUTDOWN THIS_CONTROLLER
   ```

   To ensure that the controller has shut down cleanly, check for the following indication on the controller's OCP:

   - The Reset (//) light is lit continuously.
   - Port lights 1, 2, 3, are also lit continuously.

4. After shut down is complete, connect the maintenance terminal to the other controller. Shut down the controller by entering:

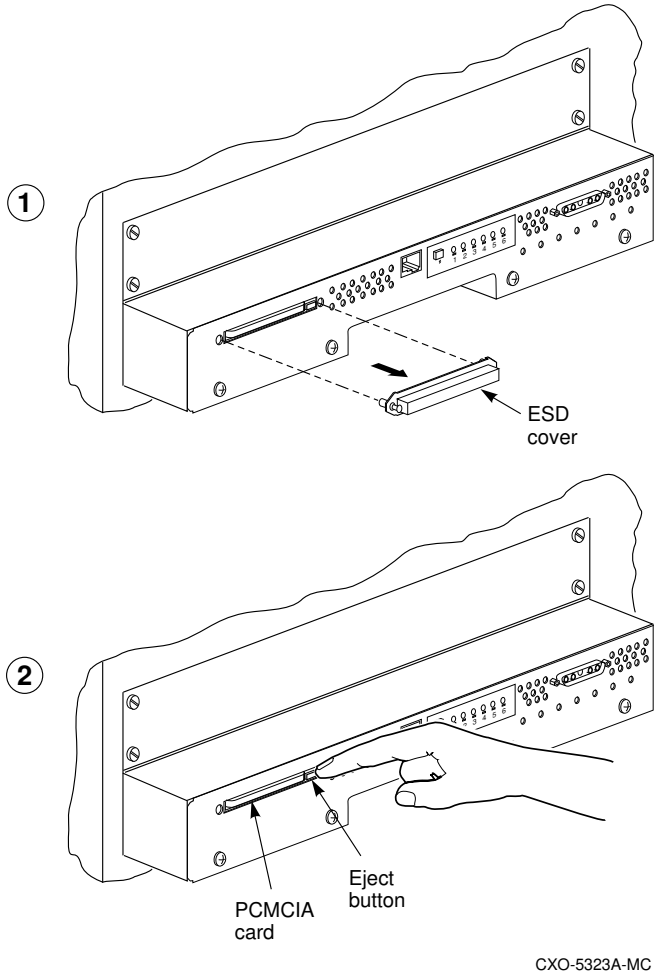
   ```
   CLI> SHUTDOWN THIS_CONTROLLER
   ```

5. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.

6. Attach or clip the other end of the ESD wrist strap to the cabinet grounding stud or a convenient cabinet grounding point.

7. Unsnap and remove the program card ESD cover (see Figure 13).

Figure 13
Removing the program card

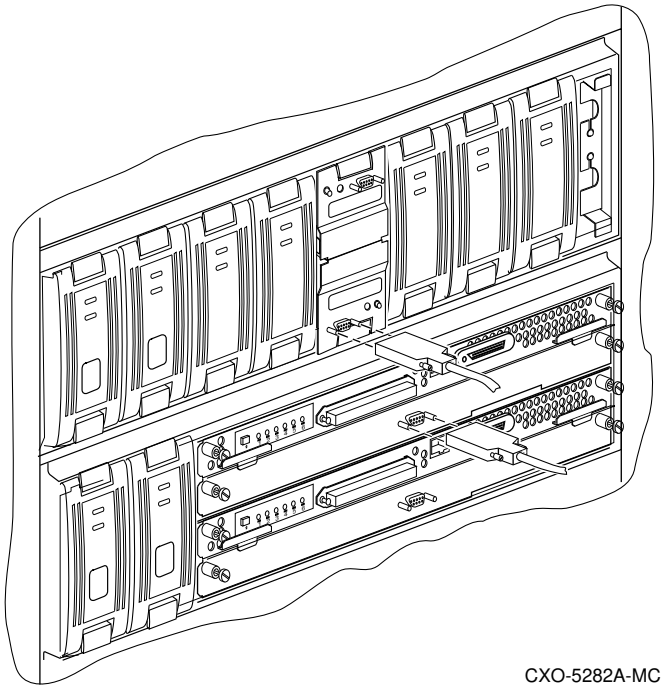


8. Remove the program card by pushing the eject button next to the card (see Figure 13). Pull the card out and save it for use in the replacement controller module.

9. With a small flat-head screwdriver, remove the CI connector from the controller's front panel.

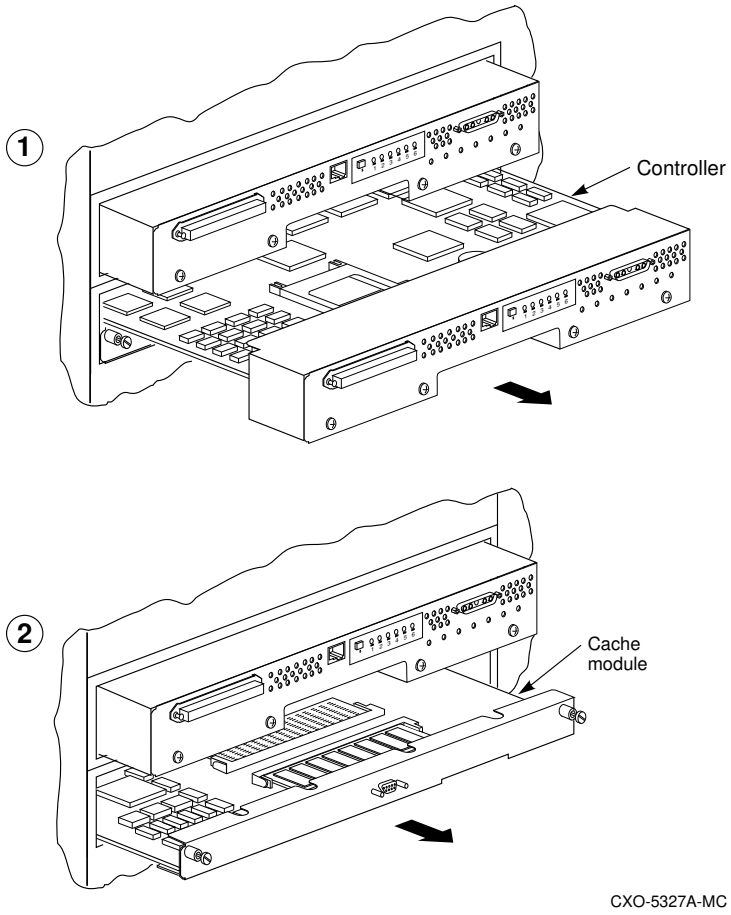
10. Disconnect the ECB cable from the cache module. While holding the battery cable in one hand, disable the ECB by pressing the battery disable switch(see Figure 14).

Figure 14
Disconnecting the ECB cable



11. Loosen the front bezel captive screws on the controller and cache module.
12. Use a gentle rocking motion to loosen the controller module from the shelf backplane.
13. Slide the controller module out of the shelf (noting which rails the module was seated in) and place it on an approved ESD mat (see Figure 15).
14. If necessary remove the cache moduleand note in which rails it was seated. Place the module on an approved ESD mat (see Figure 15).

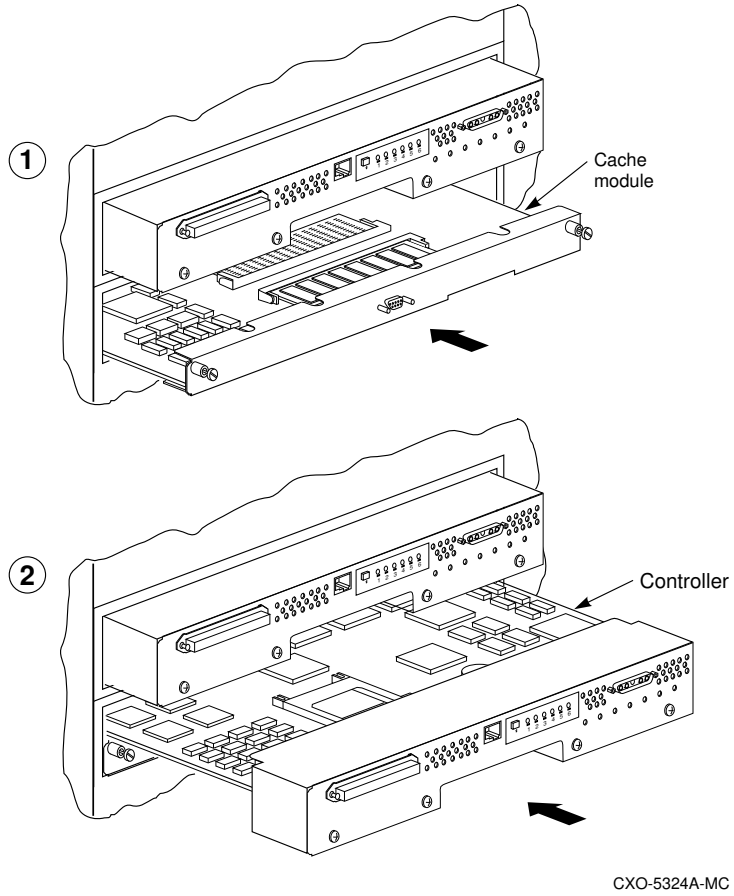
Figure 15
Removing the controller and cache modules



Installing the new controller

1. Reinstall the cache module if it has been removed (see Figure 16).
2. Use a gentle rocking motion to help seat the module into the backplane. Press firmly on the module until it is seated.

Figure 16
Installing the new cache and controller module



3. Slide the controller module into the shelf using the same rails as the removed module (see Figure 16).
4. Tighten the two captive retaining screws on the front panel of the cache and controller modules.
5. Reconnect the CI connector to the controller's front panel.
6. Reconnect the open end of the ECB cable to the new controller.
7. On both controllers, press and hold the green reset (//) button, while inserting the program card. The program card eject button will extend when the card is fully inserted.

8. Release the reset buttons to initialize the controllers.
9. Attach the maintenance terminal to the replaced controller.
10. If the controller reports an invalid cache error, enter one of the the following CLI command:
    - If you have replaced the cache module, enter the following command:

      ```
      CLI >CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
      DESTROY_UNFLUSHED_DATA
      ```

    - Otherwise enter:

      ```
      CLI> CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
      NODESTROY_UNFLUSHED _DATA
      ```

11. Ensure that the controllers are not in dual-redundant mode:

    ```
    CLI> SET NOFAILOVER
    ```

12. Enter the following command from the surviving controller to put both controllers into dua-redundant mode:

    ```
    CLI> SET FAILOVER COPY=OTHER_CONTROLLER
    ```

13. To check controller parameters:

    ```
    CLI> SHOW THIS_CONTROLLER
    ```

A listing of controller information will be displayed:

```
Controller:
    HSJ50  ZG34901786 Firmware V05.0-0, Hardware BX11
    Configured for dual-redundancy with ZG61000012
       In dual-redundant configuration
    SCSI address 7
    Time: 15 JUN-1996 16:32:54
Host port:
    Node name: HSJA1, valid CI node 21, 32 max nodes
    Path A is on
    Path B is on
    MSCP allocation class  3
    TMSCP allocation class 3
    CI_ARBITRATION = SYNCHRONOUS
    MAXIMUM HOSTS =9
    NOCI_4K_PACKET _CAPABILITY
Cache:
    128 megabyte write cache, version 3
    Cache is GOOD
    Battery is good
    No unflushed data in cache
    CACHE_FLUSH TIMER = DEFAULT (10 seconds)
    CACHE_POLICY = B
    NOCACHE_UPS
```

Repeat for the other controller:

```
CLI> SHOW OTHER_CONTROLLER
```

Replacing cache modules

This section contains replacement procedures for write-back cache modules for the HSJ50 controllers.

If you are replacing one cache modules in a dual-redundant configuration, use the Controller and cach module warm-swap procedure in this manual.

The controller module is seated in front of the cache module. Any time you service a cache module in a single controller configuration, you must shut down the subsystem. In a dual-redundant configuration, use the controller warm swap procedure to replace a failed cache module.

Required tools

The tools listed in Table 11 are required for replacing cache modules.

Table 11
Required tools

Required tools	Purpose
Maintenance terminal	To shut down controllers, restart controllers, execute CLI commands, and invoke utilities
ESD wrist strap and ESD mat	To protect all equipment against ESD
Small flat head screwdriver	To loosen CI connector, and front bezel captive screws
5/32-Allen wrench	To unlock the SW800 - Series cabinet

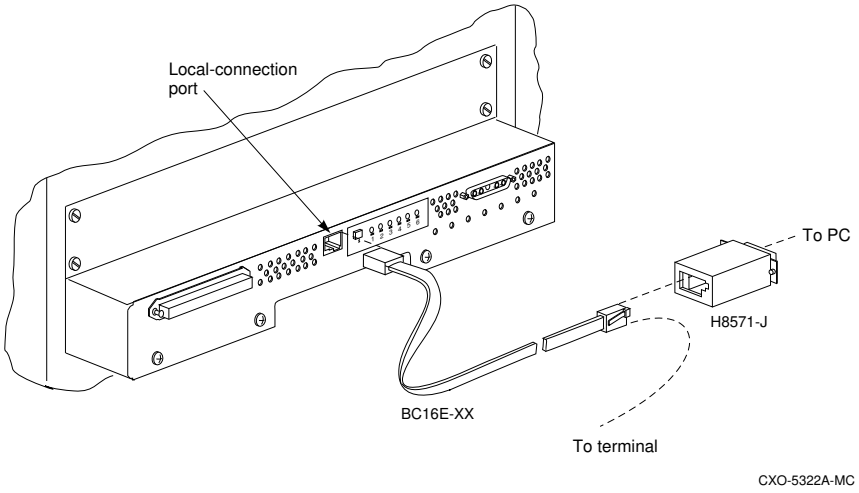
Removing a write-back cache module in a single controller configuration

1. Connect a maintenance terminal to the controller that contains the cache module to be replaced (see Figure 17).

2. Take the controller out of servoce.

```
CLI> SHUTDOWN THIS_CONTROLLER
```

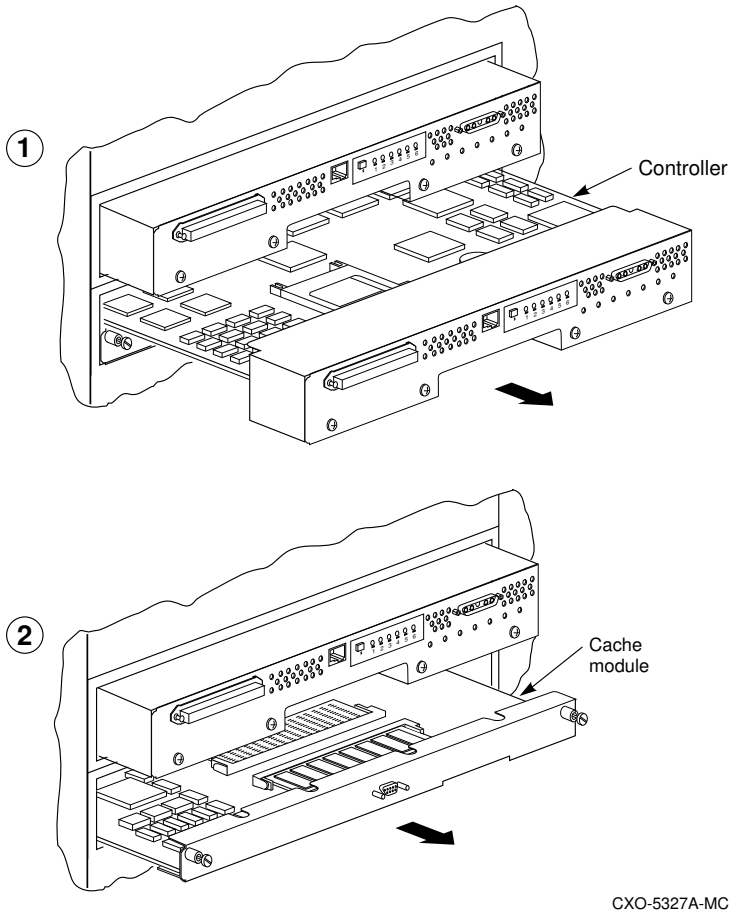
Figure 17
Connecting a maintenance terminal to the controller



3. To ensure that the controller has shut down cleanly, check for the following indication on the controller's OCP:
   - The Reset (//) light is lit continuously.
   - Port lights 1, 2, 3, are also lit continuously.
4. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.
5. Attach or clip the other end of the ESD wrist strap to the cabinet grounding stud or a convenient cabinet grounding point.
6. Remove the power cords from the controller power supplies.
7. Disable the ECB by pressing the battery disable switch on the battery module's front pane.
8. Disconnect the ECB cable from the cache module.
9. With a small flat-head screwdriver, remove the CI connector from the controller's front panel.
10. Loosen the two captive retaining screws on the controller and cache module front panel.

11. Use a gentle rocking motion to loosen the controller module from the shelf backplane.

Figure 18
Removing controller and cache modules.



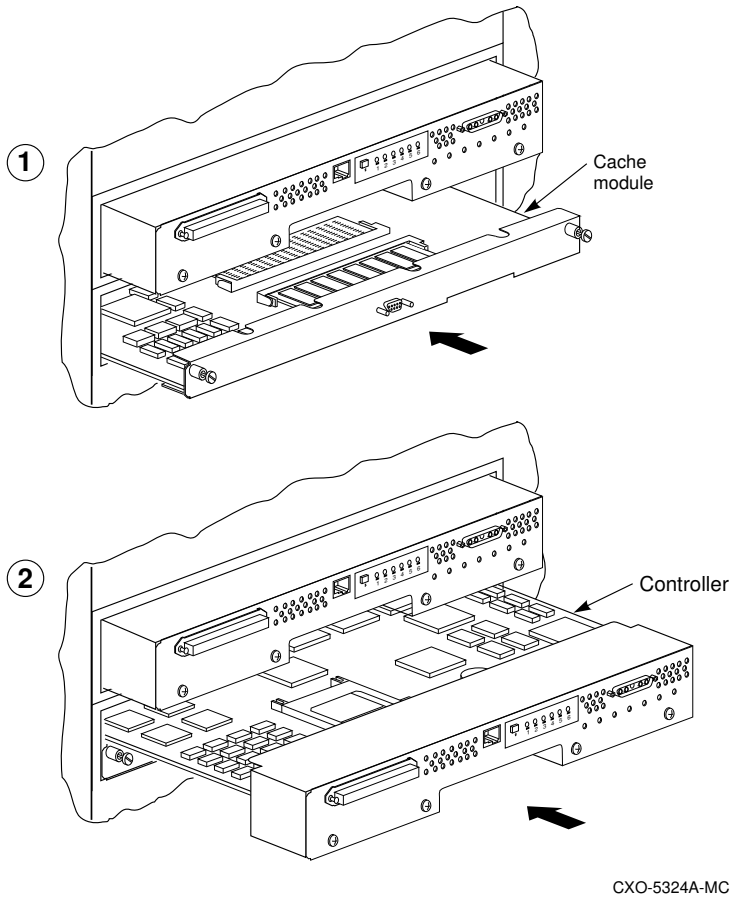
12. Slide the controller module out of the shelf, noting which rail it was seated in, and place it on an ESD mat (see Figure 18).

13. Slide the cache module out of the shelf (see Figure 18).

Installing the new cache module

1. Install the replacement cache module into the shelf using the same rails as the removed modules (see Figure 19).

Figure 19
Installing cache and controller module



2. Reinstall the controller module into the shelf using the same controllers rails and tighten the two captive retaining screws on the controller and cache modules (see Figure 19).

3. Reconnect the open end of the ECB cable to the new cache module.
4. Reconnect the power cords to the controller power supplies.
5. Initialize the controllers by pushing the front panel Reset (//) button.
6. If the controller reports an invalid cache error, enter the following command:

```
CLI> CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
DESTRY_UNFLUSHED_DATA
```

Replacing SBB battery modules (external cache batteries)

The batteries are installed in a 3 1/2-inch SBB storage building block (SBB) module. Digital does not recommend replacing individual ECBs. Therefore, when one ECB needs to be replaced, replace the entire SBB.

There are two ways to change the battery SBB: an online method (C_SWAP) in which one controller continues to process I/O, and an offline method in which both controllers are shut down. The following procedure describes the online method.

Required Tools

The tools listed in Table 12 are required for replacing the write-back cache batteries.

Table 12
Required tools

Required tools	Purpose
Maintenance terminal	To shut down controllers, restart controllers, execute CLI commands, and invoke utilities
ESD wrist strap and ESD mat	To protect all equipment against ESD
Small flat head screwdriver	To loosen CI connector, and front bezel captive screws
5/32-Allen wrench	To unlock the SW800 - Series cabinet

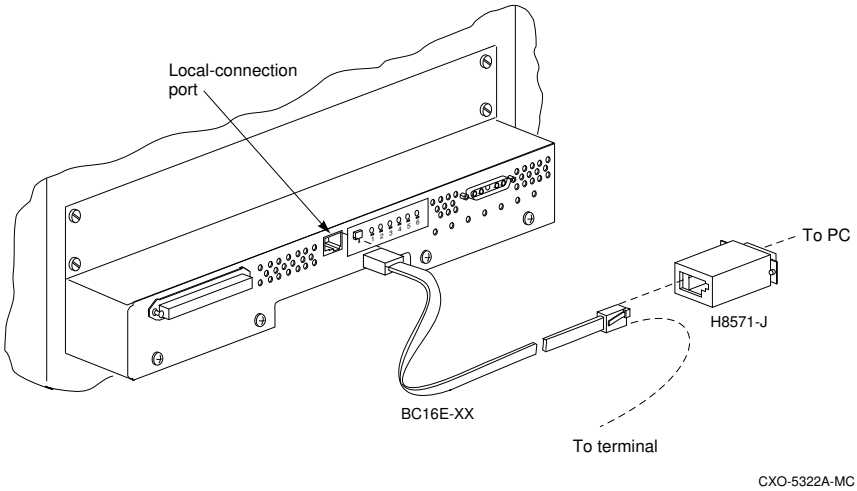
Replacing the SBB battery module

Use the following procedure to replace as SBB battery module in a dual-redundant controller configuration.

Preparing the subsystem

1. For the purpose of this procedure, mark one controller A and the other controller B.
2. Connect a maintenance terminal to controller B (see Figure 20).

Figure 20
Connecting a maintenance terminal to the controller



3. Loosen the captive screws of controller A CI connector and the front bezel of controller A and cache module A.
4. Shut down controller A:

   ```
   CLI> SHUTDOWN OTHER_CONTROLLER
   ```

   When the controller halts, the green Reset (//) LED stops flashing and stays lit.
5. Take the operating controller out of dual-redundant (failover) mode:

   ```
   CLI> SET NOFAILOVER
   ```

   You may see a Warning 600 at the terminal: you can safely ignore this warning.

6. Start the C_SWAP program:

```
CLI> RUN C_SWAP
```

Removing the ECB

1. When the controller prompts you, answer the question:

```
Do you wish to remove the other HSJ50 y/n [n] ?
```

2. Press "**Y**" for yes.

3. Answer the question:

```
Will its cache module also be removed Y/N [n] ?
```

4. Press "**Y**" for yes.

5. Wait for the following text to be displayed at the console:

```
Killing other controller
Attempting to quiesce all ports
Port 1 quiesced.
Port 2 quiesced.
Port 3 quiesced.
Port 4 quiesced.
Port 5 quiesced.
Port 6 quiesced.
All ports quiesced.
Remove the other controller (the one WITHOUT a blinking
green LED) within 5 minutes.
Time remaining 4 minutes 50 seconds.
```

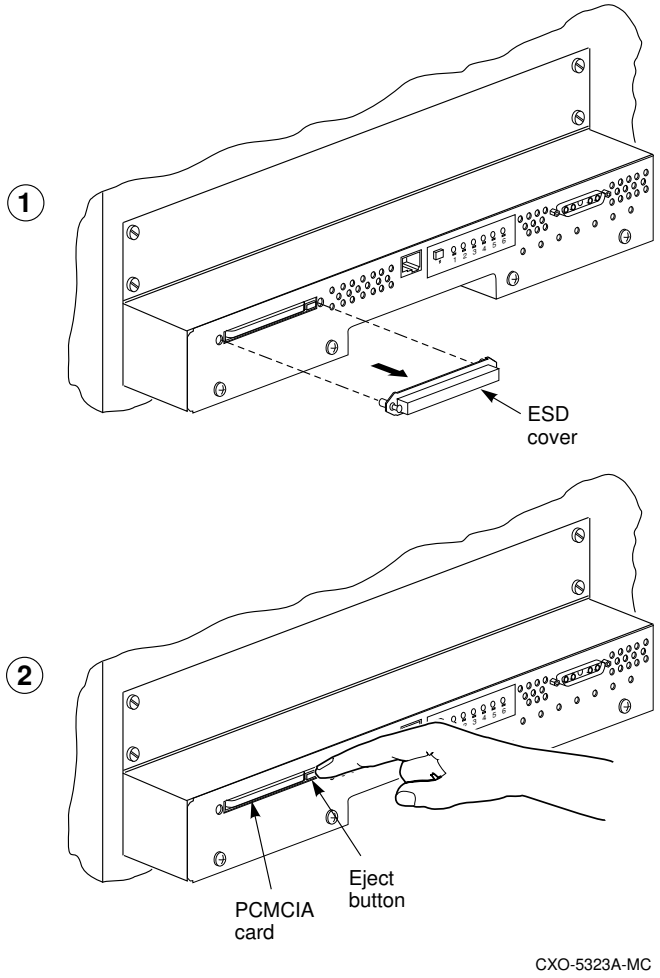
6. Place the ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.

7. Attach or clip the other end of the ESD wrist strap to the cabinet grounding stud or a convenient cabinet grounding point (nonpainted surface).

8. Unsnap and remove the program card ESD cover on the controller you are removing.

9. Remove the program card by pushing the eject button next to the card (see Figure 21).

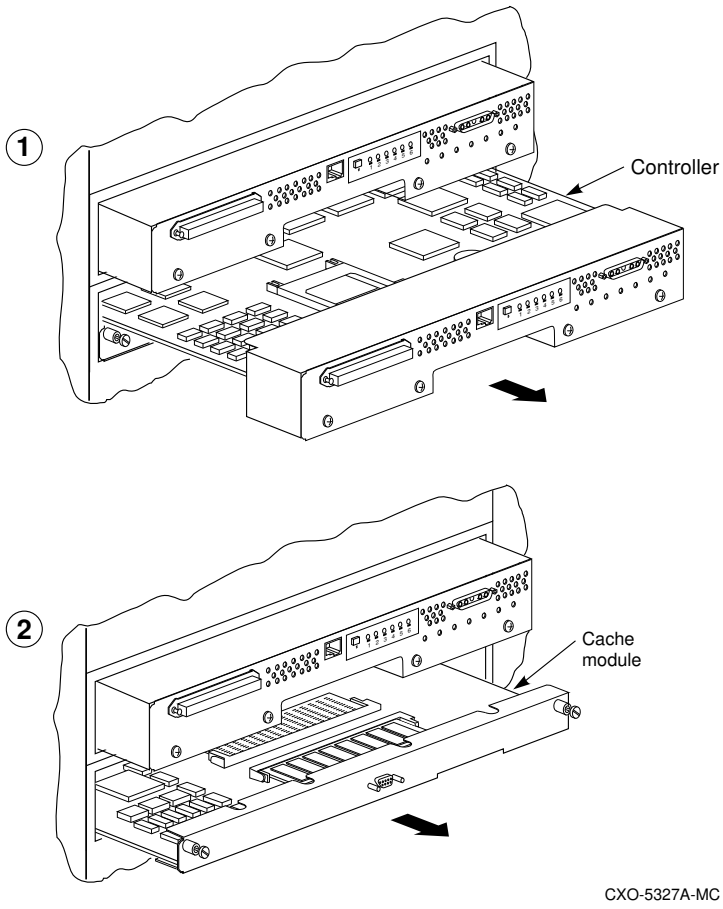
Figure 21
Removing the program card



10. Remove the CI cable from controller A.

11. Slide controller A out of the shelf and note the rails in which the module was seated. Place the module on an ESD mat. Do not remove the CI connector (see Figure 26).

Figure 22
Removing the controller and cache module



12. Wait for the following text to be displayed at the operating controller's console:

Note

You may remove the cache module before or after port activity has restarted.

```
Restarting all ports
Port 1 restarted.
Port 2 restarted.
Port 3 restarted.
Port 4 restarted.
Port 5 restarted.
Port 6 restarted.
```

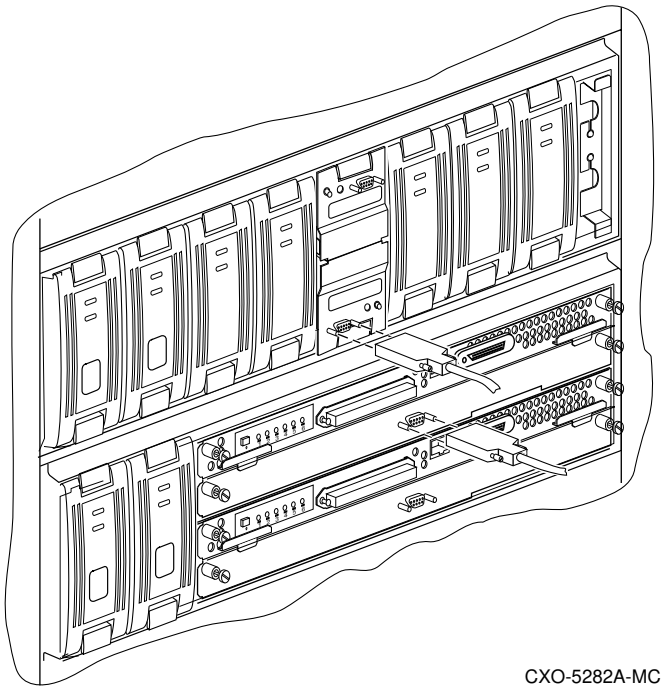
13. Pull the cache module for controller A partly out of the shelf. Leave the SBB battery module installed in the device shelf.

Caution

Do not disconnect the ECB cable from cache module B. Data may be lost if the battery cable is disconneted from the operating cache module.

14. Disconnect the ECB cable from controller A cache module and connect it to the new ECB. Tighten the battery cable connector mounting screws.(see Figure 23).

Figure 23
ECB Cable Connection



CXO-5282A-MC

Reinstalling the modules

1. When the controller prompts you, answer the question:

```
Do you have a replacement HSJ50 readily available? [N]
? y
```

2. Answer the question:

```
***Sequence to INSERT the other HSJ50 has begun.***

Do you wish to INSERT the other HSJ50 [N] ?
```

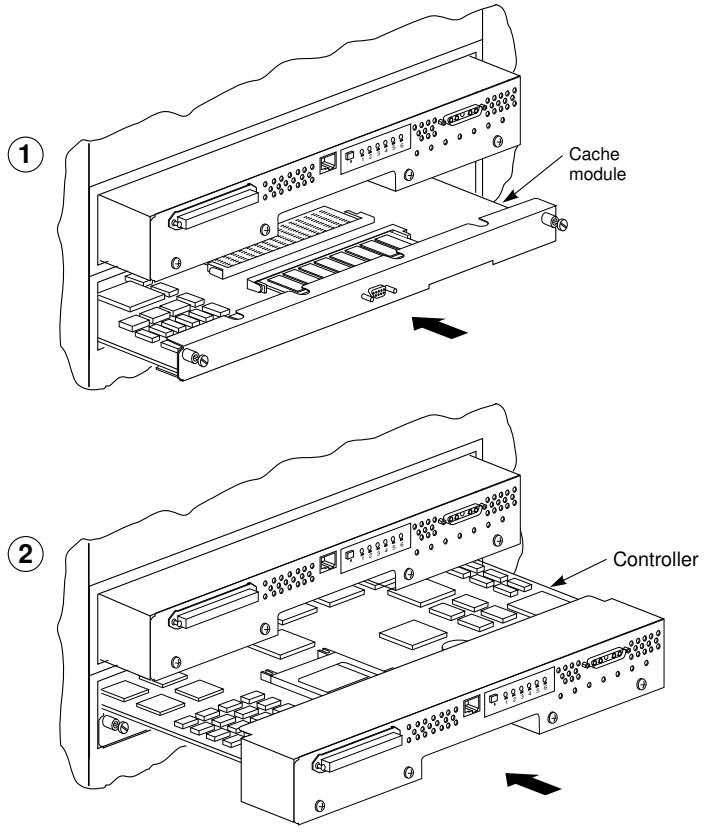
3. Press "**Y**" for yes.

4. Wait for the following text to appear on the operating controller's console:

```
Attempting to quiesce all ports.
Port 1 quiesced.
Port 2 quiesced.
Port 3 quiesced.
Port 4 quiesced.
Port 5 quiesced.
Port 6 quiesced.
All ports quiesced.
Insert the other HSJ50 WITHOUT its program card, and
press Return.
```

5. Slide the cache module for controller A along the rails and then push firmly to seat it in the backplane (see Figure 24).

Figure 24
Reinstalling the cache and controller module



6. Slide controller A along the rails and then push firmly to seat it in the backplane (see Figure 24).
7. Reinstall the CI connector on controller A and tighten the captive screws.

Caution

Do not overtighten the controller's front panel captive screws. Damage to the controller PC board or front panel may result.

8. Press **Return** on the operating controller's console.
9. Wait for the following text to be displayed on the operating controller's console:

```
Port 1 restarted.
Port 2 restarted.
Port 3 restarted.
Port 4 restarted.
Port 5 restarted.
Port 6 restarted.

Controller Warm Swap terminated.
The configuration has two controllers.
To restart the other HSJ50:
1) Enter the command RESTART OTHER_CONTROLLER.
2) Press and hold in the Reset (//) button while
inserting the program card.
3) Release Reset (//); the controller will initialize.
4) Configure new controller by referring to the
controller's configuration manual.
```

Restarting the subsystem

1. Restart controller A:

```
CLI> RESTART OTHER_CONTROLLER
```

2. Connect the maintenance terminal to controller A. (see Figure 20).
3. Press and hold the Reset (//) button on controller A while inserting the program card.
4. Release the Reset button to initialize the controller. Wait for the CLI prompt to appear at the terminal. You will see a "Controllers misconfigured" message, which you can ignore.
5. Enter the following command:

```
CLI> SET NOFAILOVER
```

6. Tighten the front bezel captive screws on controller A cache module.

Servicing the second cache module

1. Loosen the captive screws of controller B CI connector and the front bezel of controller B and cache module B.
2. At controller A, shut down controller B:

   ```
   CLI> SHUTDOWN OTHER_CONTROLLER
   ```

   When the controller halts, the green Reset (//) LED stops flashing and stays lit.
3. Take the operating controller out of dual-redundant (failover) mode:

   ```
   CLI> SET NOFAILOVER
   ```
4. Start the C_SWAP program:

   ```
   CLI> RUN C_SWAP
   ```

Removing the SBB battery module

1. When the controller prompts you, answer the question:

   ```
   Do you wish to remove the other HSJ50 y/n [n] ?
   ```
2. Press **Y** for yes.
3. Answer the question:

   ```
   Will its cache module also be removed Y/N [n] ?
   ```
4. Press **Y** for yes.

5. Wait for the following text to be displayed at the console:

```
Killing other controller
Attempting to quiesce all ports
Port 1 quiesced.
Port 2 quiesced.
Port 3 quiesced.
Port 4 quiesced.
Port 5 quiesced.
Port 6 quiesced.
All ports quiesced.
Remove the other controller (the one WITHOUT a blinking
green LED) within 5 minutes.
Time remaining 4 minutes 50 seconds.
```

6. Place the ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.
7. Attach or clip the other end of the ESD wrist strap to the cabinet grounding stud or a convenient cabinet grounding point (nonpainted surface).
8. Unsnap and remove the program card ESD cover on the controller you are removing (see Figure 21).
9. Remove the program card by pushing the eject button next to the card (see Figure 21).
10. Slide the controller module out of the shelf (noting which rails the module was seated in) and place it on an ESD mat (see Figure 22). Do not remove the CI connector.
11. Wait for the following text to be displayed at the operating controller's console:

```
Restarting all ports
Port 1 restarted.
Port 2 restarted.
Port 3 restarted.
Port 4 restarted.
Port 5 restarted.
Port 6 restarted.
```

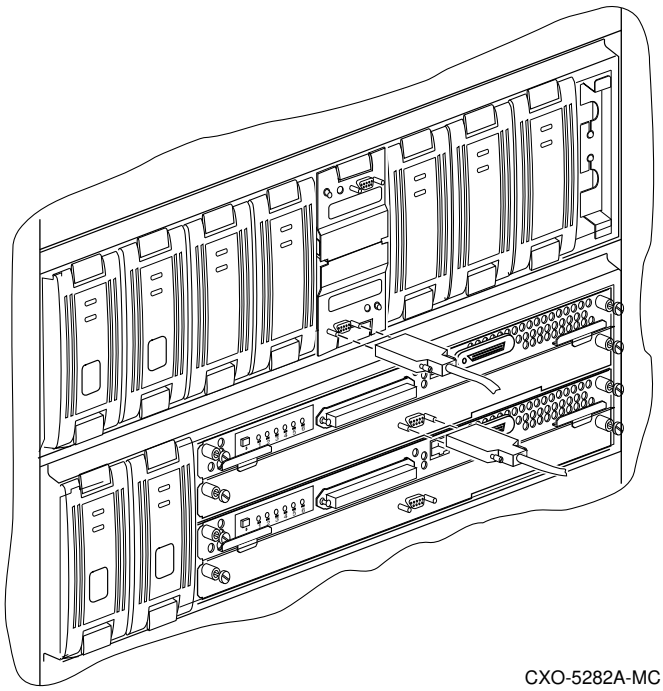
Note

You may remove the cache module before or after port activity has restarted.

12. Pull the cache module partly out of the shelf.

13. Disconnect the ECB cable and connect it to the new ECB (see Figure 25). Tighten the battery cable connector mounting screws on the new SBB battery module. Leave the old SBB battery module in the device shelf.

Figure 25
ECB Cable Connection



Reinstalling the modules

1. When the controller prompts you, answer the question:

```
Do you have a replacement HSJ50 readily available? [N]
? y
```

2. Press **Y** for yes.

3. Answer the question:

```
***Sequence to INSERT the other HSJ50 has begun.***

Do you wish to INSERT the other HSJ50 [N] ?
```

4. Press "**Y**" for yes.

5. Wait for the following text to appear on the operating controller's console:

```
Attempting to quiesce all ports.
Port 1 quiesced.
Port 2 quiesced.
Port 3 quiesced.
Port 4 quiesced.
Port 5 quiesced.
Port 6 quiesced.
All ports quiesced.
Insert the other HSJ50 WITHOUT its program card, and
press Return.
```

6. Slide the cache module along the rails and then push firmly to seat it in the backplane.
7. Install the controller module. Slide the controller module along the rails and then push firmly to seat it in the backplane (see Figure 24).

Caution

Do not overtighten the controller's front panel captive screws. Damage to the controller PC board or front panel may result.

8. Tighten the front bezel captive screws on the cache module and the controller module.
9. Press **Return** on the operating controller's console.
10. Wait for the following text to be displayed on the operating controller's console:

```
Port 1 restarted.
Port 2 restarted.
Port 3 restarted.
Port 4 restarted.
Port 5 restarted.
Port 6 restarted.

Controller Warm Swap terminated.
The configuration has two controllers.
To restart the other HSJ50.
1) Enter the command RESTART OTHER_CONTROLLER.
2) Press and hold in the Reset (//) button while
inserting the program card.
3) Release Reset (//); the controller will initialize.
4) Configure new controller by referring to the
controller's configuration manual.
```

Restarting the subsystem

1. Start the new controller by entering the following CLI command:

```
CLI> RESTART OTHER_CONTROLLER
```

2. Connect the maintenance terminal to controller B.

3. Press and hold the Reset (//) button on the new controller while inserting the program card.
4. Release the Reset (//) button to initialize the controller. Wait for the CLI prompt to appear at the terminal. You will see a “Controllers misconfigured” message, which you can ignore.
5. Enter the following command:

   ```
   CLI> SET NOFAILOVER
   ```

6. Enter the following command from the controller B CLI to put the controllers into dual-redundant mode.

   ```
   CLI> SET FAILOVER COPY=OTHER_CONTROLLER
   ```

   Controller B will restart.
7. Ensure that the ECB cable mounting are secure.
8. Remove the SBB battery module from the device shelf and replace it with the new operating SBB.

Replacing power supplies

There are two methods for replacing shelf and controller power supplies: asynchronous swap and cold swap.

Asynchronous swap allows you to remove a defective power supply while the other power supply provides power to the shelf or the controller.

Use asynchronous swap to replace a power supply only when there is a redundant power supply in the shelf and if one power supply is still operating.

When using the cold swap method, service to a device is interrupted for the duration of the service cycle. Use the cold-swap method when there are no redundant power supplies in the shelf.

Required tools

The tools listed in Table 13 are required for replacing power supplies.

Table 13
Required tools

Required tools	Purpose
Maintenance terminal	To shut down controllers, restart controllers, execute CLI commands, and invoke utilities
ESD wrist strap and ESD mat	To protect all equipment against ESD
Small flat head screwdriver	To loosen CI connector, and front bezel captive screws
5/32-Allen wrench	To unlock the SW800 - Series cabinet

Removing the power supply

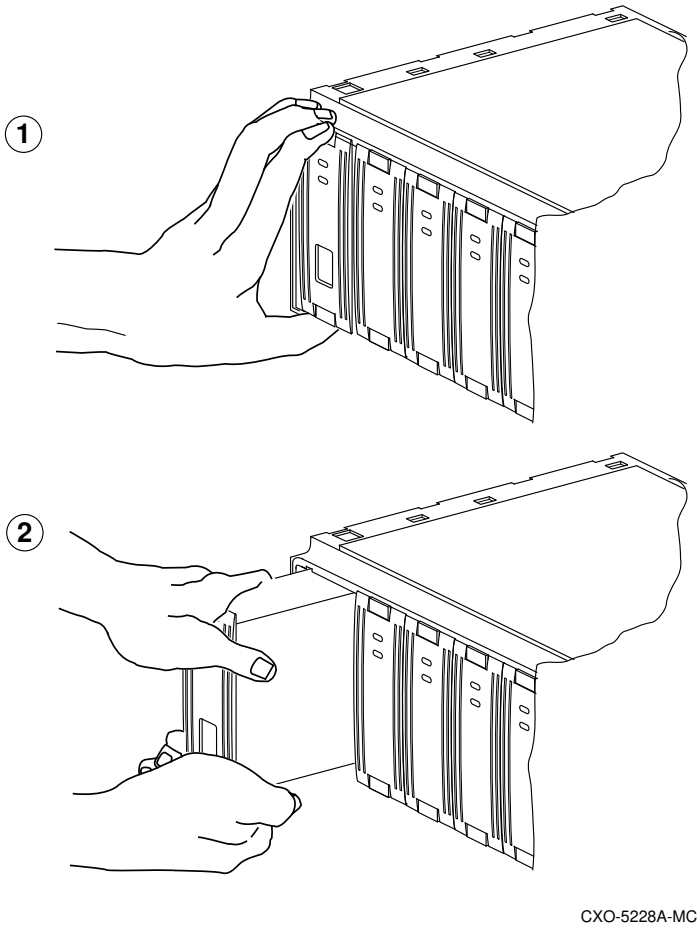
Use this procedure if you have only one power supply in the device shelf and the controller shelf.

1. If you are performing a cold swap, and the power supply is still operating, connect a maintenance terminal to one of the controllers.
2. At the CLI prompt, enter:

```
CLI> SHUTDOWN OTHER_CONTROLLER
CLI> SHUTDOWN THIS_CONTROLLER
```

3. Disconnect the power cords from the power supply.
4. Press the two mounting tabs together to release the power supply from the shelf and partially pull it out of the shelf (see Figure 26).
5. Use both hands to pull the power supply out of the shelf.

Figure 26 Removing the power supply

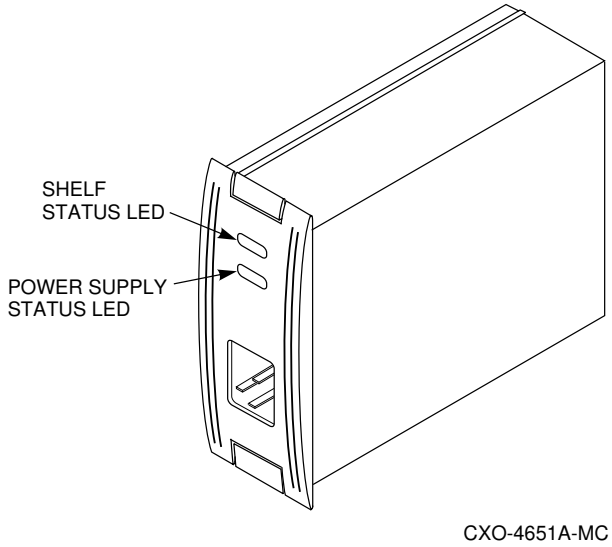


Installing the new power supply

1. Firmly push the power supply into the shelf until the mounting tabs snap into place.

2. Reconnect the power cord to the power supply.
3. Observe the power and shelf status indicators to make sure they are on (see Figure 27. If the status indicator are not on, refer to the installation section, tables 46 and 47 of this manual.

Figure 27
The power supply status indicator



Asynchronous swap method

Use this swap method only if you have redundant power supplies and if one of the supplies is still operating.

1. Remove the failed power supply using steps 4 and 5 in the preceeding procedure.
2. Follow the procedures for replacing a new power supply from the preceeding procedure.

Replacing storage devices

The asynchronous swap method may be used to replace disk drives.

Use the warm-swap method to replace tape drives.

Solid-state disks optical and CD-ROM drives can be replaced only using the cold-swap method. Disk drives.

Asynchronous disk drive swap

Software Version 5.0 supports asynchronous disk drive replacement, device removal, and device insertion without first quiescing the device bus. You can remove or insert devices at any time with the following restrictions:

- Do not remove or insert devices during failover.
- Do not remove or insert devices during failback.
- Do not remove or insert devices before the CLI prompt appears during controller initialization.
- Do not remove or insert devices while the controller is still recognizing a device removal (indicated by flashing LEDs).
- Do not remove or insert devices while the controller is running a local program such as DILX or HSUTIL.
- Wait 50 seconds after inserting one disk drive before inserting a second disk drive.

Required tools

The tools listed in Table 14 are required for replacing disk drives.

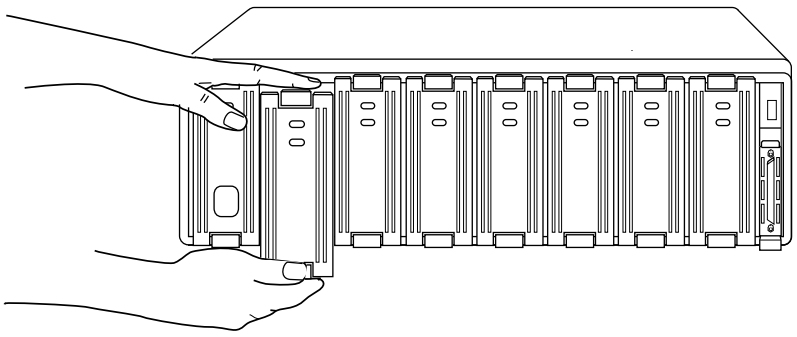
Table 14
Required tools for installing disk drives

Required tools	Purpose
5/32-inch Allen wrench	To unlock the SW800-series cabinet

Disk drive replacement procedure (3 1/2 and 5 1/4-inch drives)

1. Press the two mounting tabs together to release the disk drive from the shelf and partially pull it out of the shelf (see Figure 28).

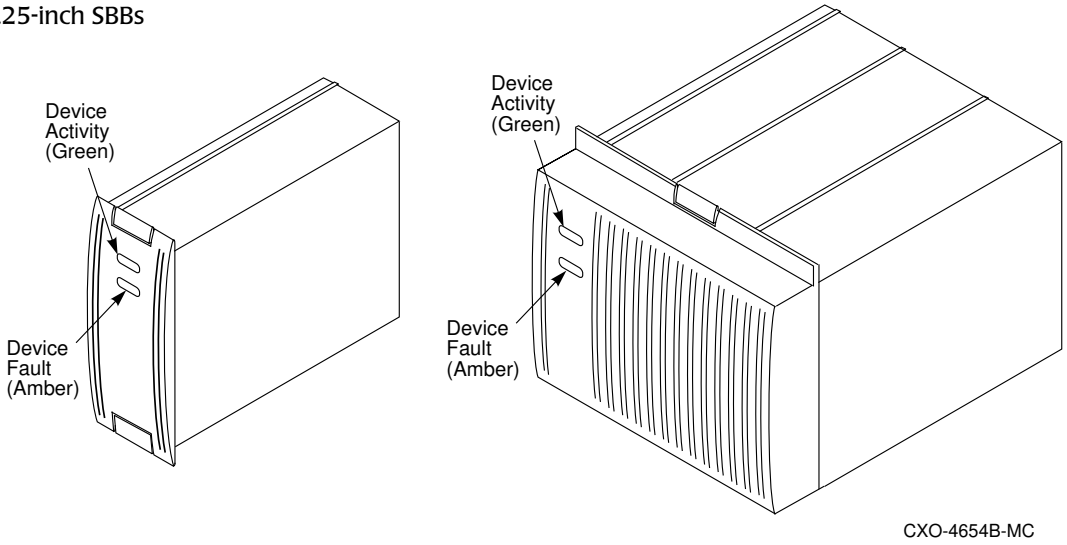
Figure 28
Removing a disk drive



2. Using both hands, pull the disk drive out of the shelf (see Figure 28). Notice that the corresponding port LED on the controller's OCP is flashing.
3. When the port LED stops flashing, align the replacement disk drive with the shelf rails.
4. Push the disk drive all the way into the shelf until the locking tabs snap into place.

5. Observe the device status LED for the following indications
(see Figure 29)
   - The device status indicator (amber) LED is off.

Figure 29
Status indicators for 3.5- and 5.25-inch SBBs



6. If the replaced disk was in the failedset before replacement, and the failedset is set to autospare, then the replacement disk will automatically place the new disk into the spareset.
7. Otherwise, you may use the replaced disk in creating or recreating an appropriate container type.
8. Restore the data from whatever backup method you use.

Replacing tape drives

Use the warm-swap method to replace tape drives. When using this method the OCP (operator control panel) buttons are used to quiesce the bus that corresponds to the replacement device.

Required tools

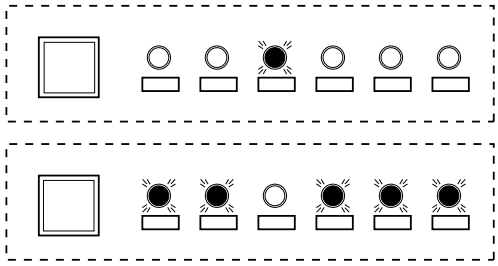
The tool listed in Table 15 is required for replacing tape, optical and CD–ROM drives.

Table 15 Required tools for SBB replacement

Required tools	Purpose
5/32-inch Allen wrench	To unlock the SW800-series cabinet

Tape drive replacement procedure

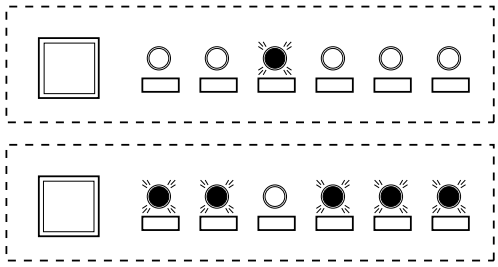
1. Quiesce the port by pressing the OCP button for that port.
2. When the OCP LEDs flash in an alternating pattern the device port is quiesce. For example, when you quiesce device port three and I/O has halted, the OCP LEDs are flashing in an alternating pattern as shown in the following illustration:



CXO-4824A-MC

3. At the tape drive to be replaced, press the two mounting tabs together to release the device from the shelf and partially pull it out of the shelf.

4. Use both hands to pull the device out of the shelf.
5. Quiesce the port again. Look for the following OCP indicators:



CXO-4824A-MC

6. Align the tape drive with the shelf rails and insert the new device.
7. When the controller recognizes the device, the port light will be turned off and the system will return to normal operation.

Replacing a solid-state disk drive, optical, or CD-ROM drives

Use the cold-swap method to replace a solid-state, optical, or CD-ROM drive. When using this method, you must shut down the controllers and remove power from the shelf.

Required tools

The tools listed in Table 16 are required for replacing solid-state disk drives opticalor CD-ROM drives.

Table 16 Required tools for Replacing solid-state disk drives

Required tools	Purpose
5/32-inch Allen wrench	To unlock the SW800-series cabinet

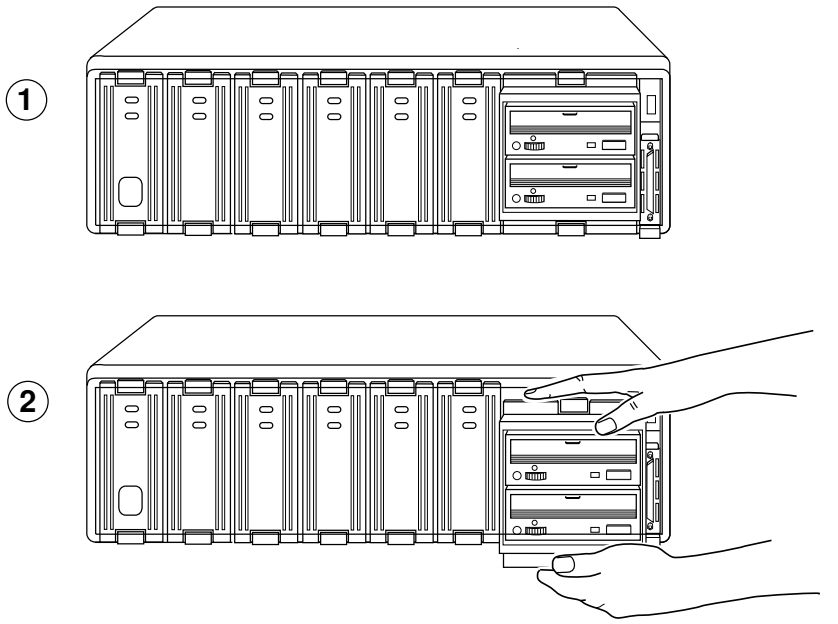
Solid-state, optical, and CD-ROM drive replacement procedure

1. Halt all host I/O activity using the appropriate procedures for your operating system.
2. Connect a maintenance terminal to one of the controllers.
3. At the CLI prompt, enter:

```
CLI> SHUTDOWN OTHER_CONTROLLER
CLI> SHUTDOWN THIS_CONTROLLER
```

4. Remove the power cords from the device shelf that contains the failed solid-state disk drive, optical or CD-ROM.
5. Press the two mounting tabs together to remove the starage building block device from the shelf (see Figure 30).

Figure 30
Removing a CD-ROM drive



CXO-5229A-MC

6. Align the replacement device with the shelf rails.
7. Push the device all the way into the shelf until the locking tabs snap into place.
8. Observe the status LED for the following indications:
   - The device fault (amber) LED is off.

Replacing internal CI cables

Servicing the internal CI cables will cause some system downtime, because the host path will be disconnected from at least one controller for the duration of the procedure. If you are using a dual-redundant configuration, you may want to shut down one controller and use the surviving controller to service devices while you replace the cables on the shut down controller.

Required tools

The tools listed in Table 17 are required for replacing CI host cables.

Table 17
Required tools for CI host cable replacement

Required tools	Purpose
Small flat-head screwdriver	To loosen captive screws
5/32-inch Allen wrench	To unlock the SW800-series cabinet

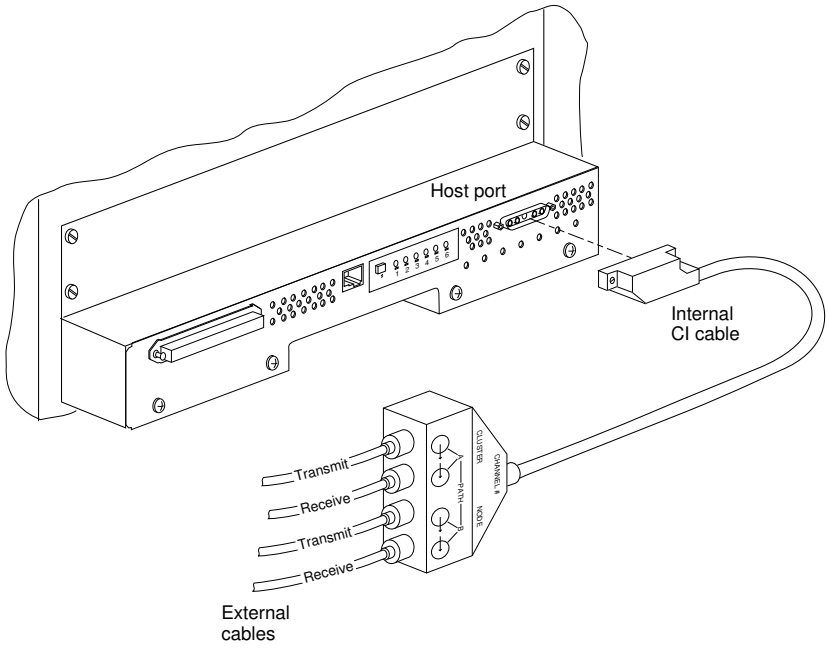
Replacing the internal CI cables

Caution

Never leave the active CI host buses unterminated during the service cycle.

1. Halt all I/O activity using the appropriate procedures for your operating system.
2. Dismount all units using the procedures for your operating system.
3. Disconnect the CI cable from the controller host port (see Figure 31).

Figure 31
Disconnecting the internal CI cable



4. Disconnect the internal CI cable (17-03427-01) form the external CI cables (see Figure 31).
5. Remove the internal CI cable from the cabinet, cutting the tie wraps as necessary.
6. Position and route the new CI cable within the cabinet.
7. Connect the CI cable to the controller.
8. Install new tie wraps as necessary to hold the new CI cable in place.
9. Connect the other end of the internal CI cable to the external CI cable.

Replacing SCSI device port cables

Servicing SCSI device port cables will require some downtime, because you must remove devices to access SCSI connectors in the controller shelf and the device shelf.

Required tools

The tools listed in Table 18 are required for replacing SCSI device cables.

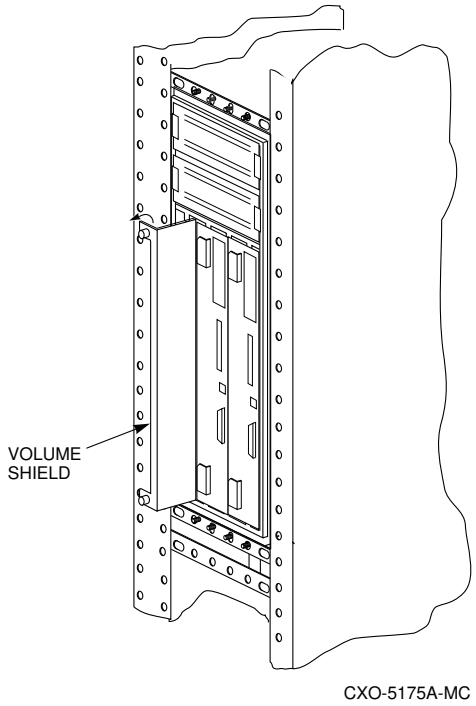
Table 18
Required tools for replacing SCSI device cables

Required tools	Purpose
Small flat-head screwdriver	To loosen captive screws
5/32-inch Allen wrench	To unlock the SW800-series cabinet

Replacing the device cables

1. Halt all I/O activity to the controller, using the appropriate procedure for your operating system.
2. Dismount all units using the appropriate procedures for your operating system.
3. Remove each controller and cache module using the Replacing Cache Module procedures.
4. Use a flat-head screwdriver to loosen the two captive screws on each side of the volume shield and remove the shield (see Figure 32).

Figure 32
Removing the volume shield



5. Remove the failed cable from the controller shelf backplane by pinching the cable connector side clips and disconnecting the cable.

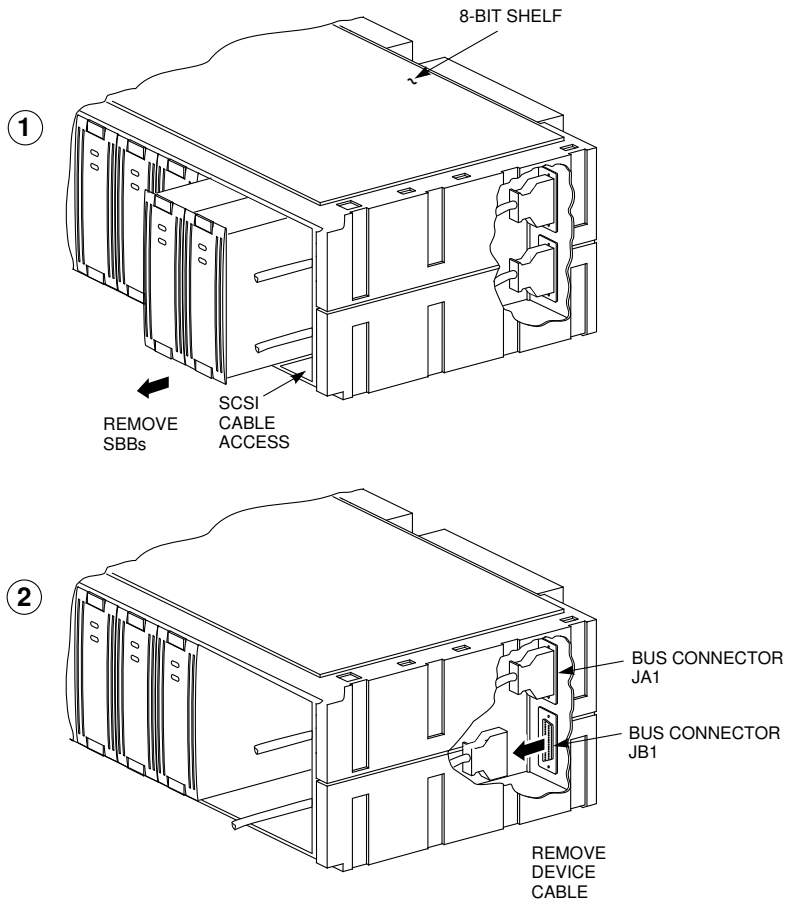
Caution

Digital recommends that you label all devices before you remove them from the device shelf.

6. Before removing the disk drives from the shelf, let the drive spin down for at least 30 seconds. Gyroscopic motion from a spinning disk may cause you to drop and damage the disk.

7. Remove any SBBs necessary to gain access the SCSI cable (see Figure 33).

Figure 33
Access to the SCSI cables



8. Remove the failed cable from the device shelf backplane by pinching the cable connector side clips and disconnecting the cable (see Figure 33).

9. To install the new SCSI device port cable at the device shelf, gently slide the cable connector in from one side to the other, and rock the connector to help seat it. Listen for the connector to snap into the place. Take care not to bend any connector pins.

10. To install the cable at the controller shelf, gently slide the cable connector on from one side to the other, and

rock the connector to help seat it. Listen for the connector to snap into place.

11. Reinstall the SBBs into the shelf. Ensure that you install all devices into the same slot that they were removed from.

12. Replace the volume shield in the controller shelf and lightly tighten the captive screws using a flat-head screwdriver.

13. Replace the cache modules and the controller modules using the Replace Cache Module section of this manual.

3 Installation

Patching controller software

Formatting disk drives

Installing new software on a device

Enabling a licensed option (FLS) Utility)

Installing a controller and cache module (single controller configuration)

Installing a second controller and cache module

Adding a second controller using C_SWAP

Installing a cache module

Adding cache memory

Installing power supplies

Installing storage building blocks

Precautions

Some of the procedures in this chapter involve handling program card, controller modules and cache modules. Use the following guidelines to prevent component damage while servicing your subsystem modules.

Electrostatic discharge protection

Electrostatic discharge (ESD) can damage system components. Use the following guidelines when handling your subsystem components:

Handling controllers or cache modules

Always wear a properly grounded ESD wrist strap whenever you remove or install a controller or cache module.

After removing a controller or cache module from the shelf, place the module into an approved antistatic bag or onto a grounded antistatic mat.

Write-back cache modules contain high-current battery cells that can cause injury to personnel if in contact with a conductive surface. Do not place write-back cache modules or battery cells on metal surfaces.

Handling the program card

Use the following guidelines when handling the program card:

- Cover the program card with the snap-on ESD cover when the card is installed in the controller.
- Keep the program card in its original carrying case when not in use.
- Do not twist or bend the program card.
- Do not touch the program card contacts.

Patching controller software

The Code Patch function of the CLCP utility allows you to enter small changes to the controller's software. The patches that you enter are placed directly into the controller's NVMEM, (non volatile memory) and become active after the next controller initialization. If the storage devices have been initialized with the SAVE_CONFIGURATION switch of the INITIALIZE command, the patches that you enter will be stored on each disk of the storage set.

The code patching utility allows more than one patch to be entered for a given software version. Each patch is associated with only one software version, and the code patch utility verifies the patch against the currently installed software version. Some patches require the installation of previous patches, *called dependent patches*, before they can be installed. Each patch has a unique patch number to identify it.

The Code Patch function also allows you to list patches already installed. You may want to list patches before you install a patch to see what has previously been loaded and to see how much free space is available.

You can run the Code Patch function of the CLCP utility from either a maintenance terminal or a virtual host terminal.

Code patch considerations

Be aware of the following characteristics when using the Code Patch function of the CLCP utility:

- The controller reserves enough nonvolatile memory for approximately 10 patches. However, this number varies according to the size of the patches you install.
- Each patch is associated with only one software version, and the Code Patch program verifies the patch against the currently installed software version.
- Patches are hierarchical. In other words, for any given software version, patch number one must be entered before you enter patch number two, and so on. Furthermore, there are no “zero” patches. Patches are always numbered sequentially beginning with the number one.
- Because of the hierarchical patch structure, removing any patch also removes all higher numbered patches. For example, deleting patch number two also removes patches three, four, and so on.
- Controllers in dual-redundant configurations must have the same patches applied. You must enter patches into each controller separately.

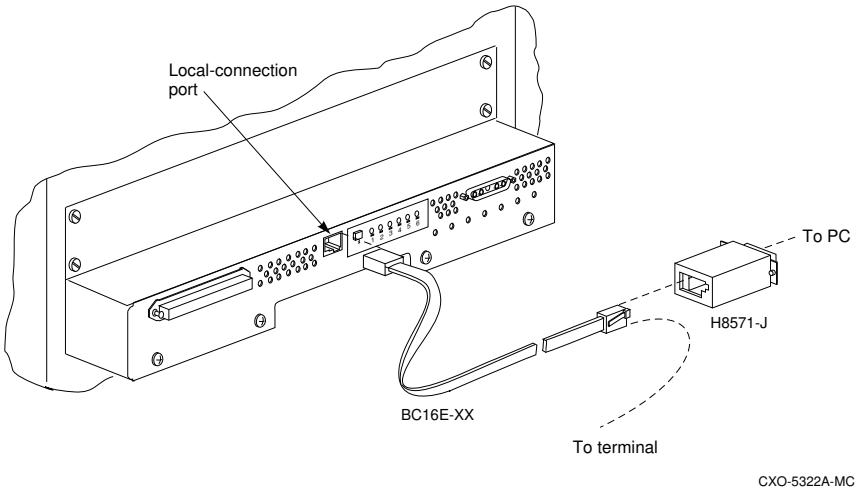
Listing patches

The List Patches option allows you to display a listing of controller software versions, and the currently installed patches that apply to them.

Following is an example of the List Patches option:

1. Connect a maintenance terminal to the controller (see Figure 34).

Figure 34
Connecting a maintenance terminal to the controller



2. Invoke the CLCP utility:

```
CLI> RUN CLCP
```

The CLCP main menu is displayed:

```
Select an option from the following list:

Code Load & Code Patch local program Main Menu

0: Exit
1: Enter Code LOAD local program
2: Enter Code PATCH local program
Enter option number  (0..2) [0] ?
-------------------------------------------------------
This controller module does not support code load
functionality. Exiting CLCP.
CLI>
```

3. Enter option "**2**" to enter the patch program:

```
You have selected the Code Patch local program. This
program is used to manage firmware code patches. Select
an option from the following list:

Type ^Y or ^C (then RETURN) at any time to abort Code
Patch.

Code Patch Main Menu

0: Exit
1: Enter a Patch
2: Delete Patches
3: List Patches

Enter option number (0..3) [0] ? 1
```

4. Enter option "**3**" to list patches.

```
The following patches are currently stored in the patch
area:

Firmware Version  -  Patch number(s)
     _______          _________

      V27J  -            2,1
      V30J  -          3,2,1

Currently, 91% of the patch area is free.
```

The SHOW THIS_CONTROLLER command also provides patch information. In the following example, software Version 3.0 has three patches applied to the current software.

5. At the CLI prompt, enter:

```
CLI> SHOW THIS_CONTROLLER

Controller:
HSJ50 ZG33400026 Firmware V30J-3,❶ Hardware 0000
.
.
.
```

Note at ❶, the bold number 3 shows that three patches have been installed for software version 30Z.

Installing a patch

This option allows you to enter a firmware program patch directly into the controller's NVMEM. You are prompted to enter the firmware version number to which the patch applies, the patch length, the patch type, the patch number, the count, the RAM address, the new contents of that address, and a patch verification number.

The code patch utility verifies that the patch you are entering is appropriate for the firmware version in the controller, and that there are no required dependent patches. It allows you to enter only one patch at a time. The utility prompts with error messages if you attempt to perform an illegal patch entry. Following is an example of the use of the patch entry option:

Note

The patch data in this example is provided only for the purpose of illustrating the code patch operation. Obtain actual code patch data for your controller's firmware version from your Digital representative.

1. Obtain the appropriate patch data for your controller's firmware version from your Digital Equipment Corporation representative.
2. Connect a maintenance terminal to the controller (see Figure 35).

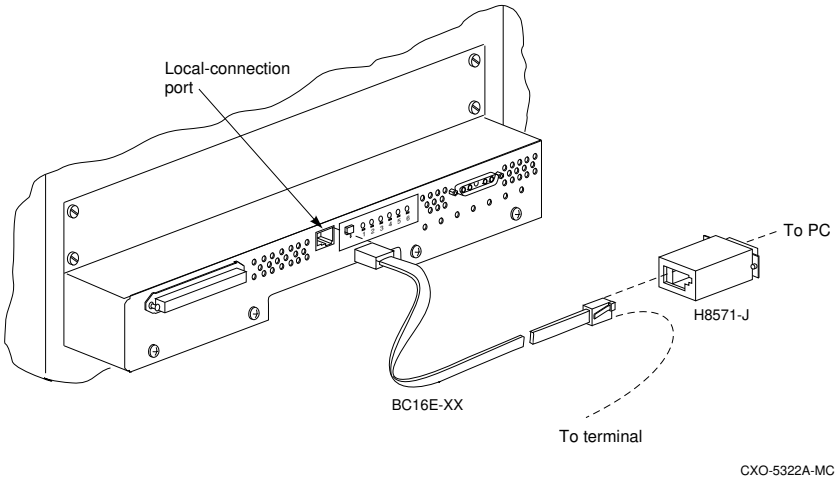


Figure 35 Connecting a maintenance terminal to the controller

3. Invoke the CLCP utility:

```
CLI> RUN CLCP
```

The CLCP main menu is displayed:

```
Select an option from the following list:

Code Load & Code Patch local program Main Menu

0: Exit
1: Enter Code LOAD local program
2: Enter Code PATCH local program
Enter option number  (0..2)?
-----------------------------------------------------
This controller module does not support code load
functionality. Exiting CLCP.
CLI>
```

4. Enter option "**2**" for the code patch menu:

```
You have selected the Code Patch program. This program
is used to manage firmware code patches. Select an
option from the following list:

Type ^Y or ^C (then RETURN) at any time to abort Code
Patch.

Code Patch Main Menu
0: Exit
1: Enter a Patch
2: Delete Patches
3: List Patches

Enter option number (0..3)?
```

5. Press **1** to select the Enter a Patch program.

```
This is the Enter a Code Patch option. The program
prompts you for the patch information, one line at
time. Be careful
to enter the information exactly as it appears on the
patch release.
Patches may be installed for any version of firmware;
however, patches entered for firmware versions other
than V30J are not applied until the matching version of
firmware is installed.

To enter any patch, you must first install all patches
with lower patch numbers, beginning with patch number
1, for the specific firmware version.
If you incorrectly enter the patch information, you are
given the option to review the patch one line at a
time.

Type ^Y or ^C (then RETURN) at any time to abort Code
Patch.

Do you wish to continue (y/n) [y] ?
```

6. Press **Y** to continue.

7. Enter the required information as shown:

```
Version:      ? V30J
Length:       ? 10
Patch Type:   ? 0
Patch Number: ? 1

Count:        ? 1
Address:      ? 10
Value[  0]    ? 0
Count:        ? 0

Verification: ? 18FG2118
The patch you just entered is not applied until
the controller is restarted.

Code Patch Main Menu

       0: Exit
       1: Enter a Patch
       2: Delete Patches
       3: List Patches

Enter option number (0..3) [0] ?

CLCP - Normal Termination
Restart of the controller required to apply new patch

CLI>
```

8. If you are using a dual-redundant controller configuration, repeat the Installing a Patch procedure for the second controller.

Code patch messages

The Code Patch utility does not allow you to incorrectly enter or delete patch information. The program provides messages to assist you with understanding any problems that you may encounter and suggests corrective actions.

Message:
`Software Version x does not have any patches to delete.`

Explanation: You cannot delete a patch because the software version entered does not have any patches entered.

Message:
`Firmware Version x does not have patch number x to delete.`

Explanation: You cannot delete this patch because the software version entered does not have the specified patch entered.

Message:
`The patch you entered is already installed on this controller.`

Explanation: The specified patch is already present in the patch area of controller memory. If you wish to reenter this patch, first use the Delete Patch option.

Message:
`The patch you are entering requires other patches to be entered.`

Explanation: You have attempted to enter a patch without first entering the lower numbered patches in the hierarchy. Enter all patches for this software version that have lower numbers than the current patch. Then enter the current patch.

Message:
`WARNING The patch you are entering is not for the current firmware version x.`

Explanation: The patch you are entering applies to a software version other than the one currently installed in the controller. Code Patch will allow you to enter the patch; however, the patch will not be applied until its correct software version is installed.

Message:
`You incorrectly entered the patch information.`

Explanation: The patch information was not entered exactly. The program prompts you for each line of the patch entry, with the default from your previous response. Verify that each entry is exactly the same as the patch release. If

you choose not to continue, or if you abort during this review procedure, the patch information you entered is lost and you must enter the entire patch again. You may enter Ctrl/Z followed by Return at any prompt to choose the default for the remaining entries.

Message:
`The patch you have just entered is not applied until the controller firmware is changed to Version x.`

Explanation: The patch entered applies to a software version other than the one currently installed in the controller. Code Patch will not apply the patch until its correct software version is installed.

Message:
`You have requested deletion of a patch number that another patch requires.`

Explanation: You are attempting to delete a patch in the hierarchy that has higher numbered patches entered. Code Patch will allow you to proceed; however, the program will delete all the higher numbered patches in the hierarchy (for this software version) along with the specified patch.

Formatting disk drives

Use HSUTIL's FORMAT_DISK option to format simultaneously up to seven disk drives attached to a single controller or up to six disk drives attached to a dual-redundant pair of controllers.

Caution

Suspend all I/O to the buses that service the target disk drives.

To format one or more disk drives:

1. Start HSUTIL.

   ```
   CLI> RUN HSUTIL
   ```

2. Press 1 to select the FORMAT function.

   HSUTIL finds and displays all of the unformatted disk drives attached to the controller.

3. Enter the name of each disk drive you want to format.

   ```
   Enter a device to format ? disk_name
   ```

4. Press "Y" to enter another disk drive name or "N" to begin the formatting operation.

   ```
   Select another device (y/n) [n] ? N
   ```

5. Read the cautionary information that HSUTIL displays, then confirm or cancel the formatting operation.

   ```
   Do you want to continue (y/n) [n] ? Y
   ```

Considerations for formatting disk drives

Keep the following points in mind for formatting disk drives with HSUTIL:

- HSUTIL cannot format disk drives that have been configured as single disk drive units or as members of a storageset, spareset, or failedset. If you want to format a disk drive that's previously been configured as such, you'll have to delete the unit number and storageset name associated with it.

- If the power fails or the bus is reset while HSUTIL is formatting a disk drive, the drive may become unusable until a successful format is completed. To minimize this possibility, Digital recommends that you secure a reliable power source and suspend all non HSUTIL activity to the bus that services the target disk drive.
- HSUTIL cannot control or affect the defect management for a disk drive. The drive's microcode controls the defect management during formatting.
- Don't invoke any CLI command or run any local program that might reference the target disk drive while HSUTIL is active. Also, don't initialize either controller in the dual-redundant configuration.

For example

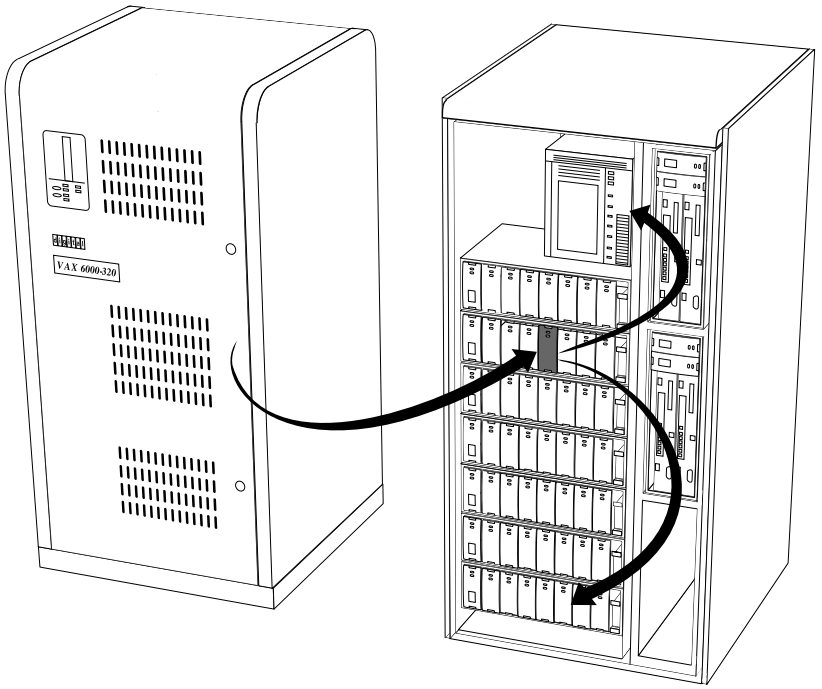
```
CLI> RUN HSUTIL

*** Available functions are:
0. EXIT
1. FORMAT
2. DEVICE_CODE_LOAD_DISK
3. DEVICE_CODE_LOAD_TAPE
Enter function number (0:3) [0] ? 1

Unattached devices on this controller include:
Device        SCSI Product ID    Current Device Rev
DISK100       RZ26   (C) DEC     T386
DISK200       RZ26   (C) DEC     T386
DISK210       RZ29B  (C) DEC     0006
DISK310       RZ25   (C) DEC     0900
DISK320       RZ26L  (C) DEC     X442

Enter a device to format ? disk100
Format DISK100 may take up to 40 minutes to format
Select another device (y/n) [n] Y

Enter a device to format ? disk200
Format DISK200 may take up to 40 minutes to format
Select another device (y/n) [n] Y

Enter a device to format ? disk210
Format DISK210 may take up to 15 minutes to format
Select another device (y/n) [n] N

^Y and ^C will be disabled while the format operation is in
progress.

CAUTION:
   When you format a device, it will destroy the data on
```

```
   the device. A backup of the device should have been
   done if the data is important.

NOTE:
   In order to minimize the possibility of a SCSI bus
   reset, it s recommended that you prevent non-HSUTIL IO
   operations to all other devices on the same port as the
   destination device(s). If a SCSI bus reset occurs, the
   format may be incomplete and you may have to re-invoke
   HSUTIL.

After you answer the next question, the format will start.
Do you want to continue (y/n) [n] ? Y

HSUTIL started at: 14-JUN-1996 15:00:31
Format of DISK100 finished at 14-JUN-1996 16:40:12
Format of DISK200 finished at 14-JUN-1996 17:15:31
Format of DISK210 finished at 14-JUN-1996 16:30:43

HSUTIL - Normal Termination at 14-JUN-1996 16:31:09
```

Installing new firmware on a device

Installing new firmware on a disk or tape drive is a two-step process as shown in Figure 36. First, you copy the new firmware from your host to a disk drive in your subsystem, then use HSUTIL to distribute the firmware to devices in your subsystem).

Figure 36
Copy the firmware to a disk drive in your subsystem, then distribute it to the devices you want to upgrade.



Considerations for installing new device firmware

Keep the following points in mind while using HSUTIL to install new firmware on a device:

- Installing new firmware with HSUTIL has been thoroughly tested with the qualified devices listed in the release notes. HSUTIL doesn't prevent you from

attempting to install new firmware on unsupported devices but, if the installation fails, the device may be rendered unusable and require the manufacturer's attention.

- If the power fails or the bus is reset while HSUTIL is installing the new firmware, the device may become unusable. To minimize this possibility, Digital recommends that you secure a reliable power source and suspend all non HSUTL activity to the bus that services the target device.
- HSUTIL cannot install firmware on devices that have been configured as single disk drive units or as members of a storageset, spareset, or failedset. If you want to install firmware on a device that's previously been configured as such, you'll have to delete the unit number and storageset name associated with it.
- The source disk drive that contains the new firmware to be downloaded must be configured as a single disk drive unit within your subsystem.
- During the installation, the source disk drive is not available for other subsystem operations.
- Some firmware releases require that you format the device after installing the new firmware. Refer to the documentation that accompanied the firmware to determine if you need to reformat the device after installing new firmware.
- Some devices may not reflect the new firmware version number, etc. when viewed from another controller (in dual-redundant configurations). If you experience this, simply re-initialize the device from either controller.

Copying the firmware to your subsystem

Before you can install new firmware on a device, you need to copy its image to a single disk drive unit in a StorageWorks subsystem. You can use this disk drive in other StorageWorks subsystems to install firmware on other devices in those subsystems.)

The single disk drive unit may be a raw disk drive with no file system or label, or it may be a normal file-system disk drive. In either case, the firmware must be copied in contiguous blocks beginning at a known logical block number (LBN). The steps for copying the firmware are specific to your host's operating system and are given below.

From OpenVMS...

To copy one or more firmware files from your OpenVMS host to a single disk drive unit in your subsystem:

1. Add a disk drive to your subsystem.

   ```
   CLI> ADD DISK disk-name PTL-location
   ```

2. Configure the disk drive as a single disk drive unit. See *Working with HSJ50 units in «Interface»* for the appropriate unit-number syntax.

   ```
   CLI> ADD UNIT unit-number disk-name
   ```

3. From a OpenVMS account, copy (contiguously) the firmware from your host to the single disk drive unit.

   ```
   $ COPY/CONTIGUOUS firmware unit-number:[000000]
   ```

   Repeat this step to copy more than one firmware image to the single disk drive unit. To find the starting LBN of each firmware image:

   ```
   $ DUMP/HEAD/BLOCK=COUNT=0 $2$DUA300:[000000]*.FUP
   ```

4. Copy the firmware onto the target devices in your subsystem.

For example

```
$ COPY/CONT BABAGI::LCA:[FIRMWARE.RZ2X]RZ29B_DEC_0014.LOD-
$2$DUA300:[000000]

$ COPY/CONT BABAGI::LCA:[FIRMWARE.RZ2X]RZ28P4_42C_DEC.FUP-
$2$DUA300:[000000]

$ DUMP/HEAD/BLOCK=COUNT=0 $2$DUA300:[000000]*.LOD
.
.
.
$2$DUA30:[000000] RZ29B_DEC_0014.LOD LBN: 8

$ DUMP/HEAD/BLOCK=COUNT=0 $2$DUA300:[000000]*.FUP
.
.
.
$2$DUA300:[000000]RZ28P4_42C_DEC.FUP LBN: 520
```

Installing the firmware onto a target device

Use HSUTIL's DEVICE_CODE_LOAD_DISK option to update a disk drive by installing new firmware. Use the DEVICE_CODE_LOAD_TAPE option to update a tape drive. In both cases, the disk drive that contains the new firmware and the device onto which you're installing it must be configured on the controller from which you're running HSUTIL.

Caution

Suspend all none HSUTIL I/O to the buses that service source disk drive and the target device.

To install new device firmware:

1. In dual-redundant configurations, you should shut down the controller that you won't be using for the installation and eject its program card. Reinstall the program card and restart the controller after you've finished installing the firmware.

2. Start HSUTIL.

   ```
   CLI> RUN HSUTIL
   ```

3. Press 2 to select DEVICE_CODE_LOAD_DISK or 3 to select the DEVICE_CODE_LOAD_TAPE . HSUTIL finds and displays all of the disk drives that may contain the new firmware for your device.

4. Enter the unit number of the disk drive that actually contains the firmware.

   ```
   Which unit is the code to be loaded from ? unit-number
   ```

5. Enter the starting LBN of the firmware. In most cases, you can accept the default (0).

   ```
   What is the starting LBN of the code on the unit where
   the code is to be loaded FROM [0] ? 0
   ```

6. Enter the product ID of the device that you're updating. Enter this information exactly as it appears in the SHOW command output.

   ```
   What is the SCSI PRODUCT ID of the device that you want
   code load TO ? Product-ID
   ```

7. Enter the name of the target device.

   ```
   Which device is the code to be loaded TO ? device-name
   ```

8. Read the cautionary information that HSUTIL displays, then confirm or cancel the load.

   ```
   Do you want to continue (y/n) [n] ? Y
   ```

9. When HSUTIL terminates, verify the new firmware revision level.

   ```
   CLI> SHOW device-name
   ```

For example

```
CLI> RUN HSUTIL

*** Available functions are:
0. EXIT
1. FORMAT
2. DEVICE_CODE_LOAD_DISK
3. DEVICE_CODE_LOAD_TAPE
Enter function number (0:3) [0] ? 3

Available single device units on this controller include:
Unit  Associated Device SCSI Product ID Current Device Rev
625   DISK250          RZ28(C) DEC     T436
613   DISK130          RZ25(C) DEC     0700
Which unit is the code to be loaded from ? 625

What is the starting LBN [0] ? 0
```

```
What is the SCSI PRODUCT ID of the device that you want
code load TO ? TZ867

Unattached devices on this controller include:
Device        SCSI Product ID    Current Device Rev
TAPE100       TZ867              4318
Which device is the code to be loaded TO ? tape100

The tape cartridge must be removed to update the tape drive
firmware. The cartridge is in the drive.
Please unload.
Is the cartridge loaded (y/n) [n] ? n

^Y and ^C will be disabled while the code load operation is
in progress.

CAUTION:
   Loading the incorrect firmware can disable the
   destination device. If a failure occurs while loading
   drive memory, the destination device could be disabled.

NOTE:
   In order to minimize the possibility of a SCSI bus
   reset, which could disable the destination device, it
   is recommended that you prevent non-HSUTIL IO
   operations to all other devices on the same port as the
   destination device.

After you answer the next question, the code load will
start. Do you want to continue (y/n) [n] ? Y

HSUTIL is doing code load. Please be patient.

Device code has been successfully downloaded to device
TAPE100

HSUTIL - Normal Termination at 14-JUN-1996 16:31:09
```

HSUTIL abort codes

If HSUTIL terminates before it formats a disk drive or installs new firmware, it reports one of the abort codes in Table 19.

Table 19
Abort codes

Abort code	Description
1	FAO returned either FAO_BAD_FORMAT or FAO_OVERFLOW
2	Bad return from TS$READ_TERMINAL_DATA
3	TS$READ_TERMINAL_DATA returned either an ABORTED or INVALID_BYTE_COUNT
4	User requested an abort via ^Y or ^C
5	An error occurred on a SCSI command
6	Can't find the PUB, device is probably missing

HSUTIL messages

HSUTIL may produce one or more of the following messages while you're formatting disk drives or installing new firmware. Many HSUTIL messages have been omitted from this section since they are self-explanatory.

Message:
```
Insufficient resources
```

Explanation: HSUTIL cannot find or perform the operation because internal controller resources are not available.

Message:
```
Unable to change operation mode to maintenance for unit
unit_number
```

Explanation: HSUTIL was unable to put the source single disk drive unit into maintenance mode to enable formatting or code load.

Message:
Unit *unit_number* successfully allocated

Explanation: HSUTIL has allocated the single disk drive unit for code load operation. At this point, the unit and its associated device are not available for other subsystem operations.

Message:
Unable to allocate unit

Explanation: HSUTIL could not allocate the single disk drive unit. An accompanying message explains the reason.

Message:
Unit is owned by another sysap

Explanation: Device cannot be allocated because it is being used by another subsystem function or local program.

Message:
Unit *unit_number* is in maintenance mode

Explanation: Device cannot be formatted or code loaded because it is being used by another subsystem function or local program.

Message:
Unit *unit_number* is allocated to other controller, please re-invoke HSUTIL from the other controller or make the unit allocated to this controller by one of the following commands:
SET THIS PREFERRED ID=(unit's target ID).
SET OTHER NOPREFERRED_ID.

Explanation: The device shown is still under the control of the companion controller. Follow the recommended steps to run HSUTIL.

Message:
CAUTION:
In order to minimize the possibility of a SCSI bus reset, which could disable the destination device, it is recommended that you prevent IO operations to all other devices on the same port as the destination device.

Explanation: (Displayed in code load only.) A SCSI bus reset can occur if the controller is manually initialized or if it detects an error during normal subsystem operation. The more active devices there are on the same port as the target device, the greater the chance that an error causing a SCSI bus reset may occur. By minimizing the level of activity on the device port being used for code loading, the user minimizes the chances of a SCSI bus reset that could render a target device unusable.

Message:
`Exclusive access is declared for unit` *`unit_number`*

Explanation: Another subsystem function has reserved the unit shown.

Message:
`The other controller has exclusive access declared for unit` *`unit_number`*

Explanation: The companion controller has locked out this controller from accessing the unit shown.

Message:
`The RUNSTOP_SWITCH is set to RUN_DISABLED for unit` *`unit_number`*

Explanation: The RUN\NORUN unit indicator for the unit shown is set to NORUN. The disk is not spun up.

Message:
`No available unattached devices.`

Explanation: The program could find no unattached devices to list.

Message:
`What BUFFER SIZE, (KB) 1024, does the drive require (2,4,8,16,32) [8] ?`

Explanation: This message is displayed if HSUTIL detects that an unsupported device has been selected as the target

device and if you're downloading the firmware image using more than one SCSI Write Buffer command. You must specify the number of bytes to be sent in each Write Buffer command. The default buffer size is 8192 bytes. A firmware image of 256 KB, for example, can be code loaded in 32 Write Buffer commands, each transferring 8192 bytes. In this example, the correct entry for the buffer size would be "8."

Message:

```
What is the TOTAL SIZE of the code image in 512 byte blocks
[MAX 512] ?
```

Explanation: This message is displayed if HSUTIL detects that an unsupported device has been selected as the target device. You must enter the total number of 512-byte blocks of data to be sent in the code load operation. For example, a firmware image that is 262,144 bytes long would require 512, 512-byte blocks.

Message:

```
Does the target device support only the download microcode
and SAVE (y/n) [y] ?
```

Explanation: This message is displayed if HSUTIL detects that an unsupported device has been selected as the target device. You must specify whether or not the device supports the SCSI Write Buffer command's DOWNLOAD AND SAVE function.

Message:

```
Should the code be downloaded with a single write buffer
command (y/n) [y] ?
```

Explanation: : This message is displayed if HSUTIL detects that an unsupported device has been selected as the target device. You must indicate whether to download the firmware image to the device in one or more contiguous blocks, each corresponding to one SCSI Write Buffer command.

Enabling a licensed option (FLS Utility)

The firmware licensing system (FLS) enables or disables the licensed value-added software features: (RAID, mirroring, and write-back cache. You may use the FLS utility to perform the following tasks:

- Enable or disable optional functions for your controller
- Try an optional feature before purchasing the license to use it
- Enter your license key for a licensed feature.

Start FLS from the CLI prompt. After starting the FLS utility, the display shows the current status of the value-added options for your controller and contains menu choices for each function of the utility.

Enabling options

You can turn on any option at any time using FLS, but if you enable an option for which you are not licensed, an error message appears on your CLI console and an error is logged in the host error log. These error indications are repeated once each hour while the unlicensed option remains enabled. Licensed value added software features may have their license keys preloaded at the factory.

License key

After you have installed a license key for a software option, you must run the FLS utility again to enable any licensed keys you have entered for your controller.

Also, you must run the FLS utility separately for each controller in a dual-redundant configuration. The FLS utility does not automatically load both controllers.

FLS operations

Table 20 shows all of the FLS operations. Enabling a software option and entering a licensed key are explained in this section. For disabling and clearing a licensed key, refer to the removal section of this manual.

Table 20
FLS operations

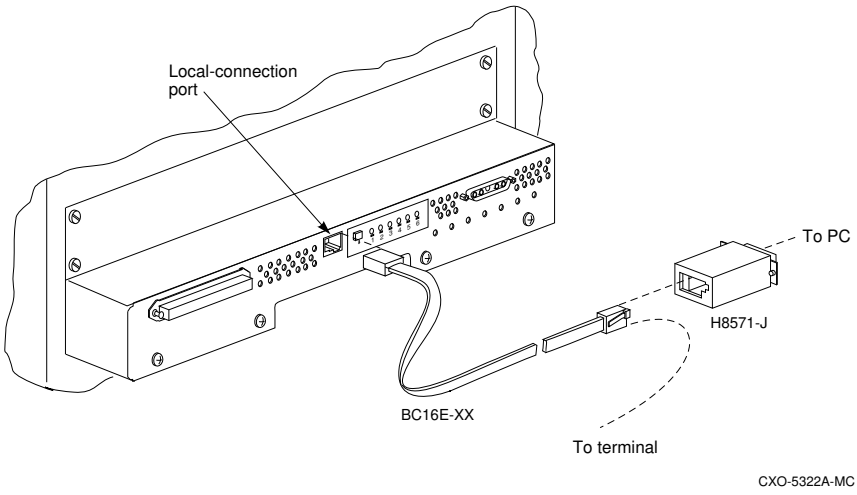
Action	Submenu choices	Result
Enable an option	List each option and its status	Option enabled
Disable an option	List each option and its status	Option disabled
Enter a license key	Prompt for new license key	Entered key becomes valid
Clear a license key	Prompt for license key to clear	Entered key becomes invalid

The FLS utility menu

The following example shows the FLS main menu:

1. Connect a maintenance terminal to a controller (see Figure 37).

Figure 37
Connecting a maintenance terminal to the controller



2. Start the FLS utility:

```
CLI> RUN FLS
```

The FLS menu will be displayed:

```
Firmware Licensing System (FLS) on node MASS
Option❶   State❷       License❸       Key❹
-------------------------------------------------
RAID      DISABLED      INVALID        *none*
WBCA      DISABLED      INVALID        *none*
MIRR      DISABLED      INVALID        *none*

               RAID = RAID Option❺
               WBCA = Writeback Cache Option
               MIRR = Disk Mirroring Option
-------------------------------------------------
    1   Enable a firmware option
    2.  Disable a firmware option
    3.  Enter a license key for a firmware option
    4.  Clear a license key for a firmware option
    0.  Exit FLS
Enter selection (0:4) [0] ?
```

- ❶**Option**–The RAID, write-back cache (WBCA), mirror (MIRR).
- ❷**State**–All three of the available options (RAID, WBCA, MIRR) are disabled. You may enable any option available, regardless of whether you have a valid license key.
- ❸**License**–None of the available license options are enabled.
- ❹**Key**–The company name that holds the valid license key (in this example no companies are listed).
- ❺**Description of Option**–A short description of each option is given.

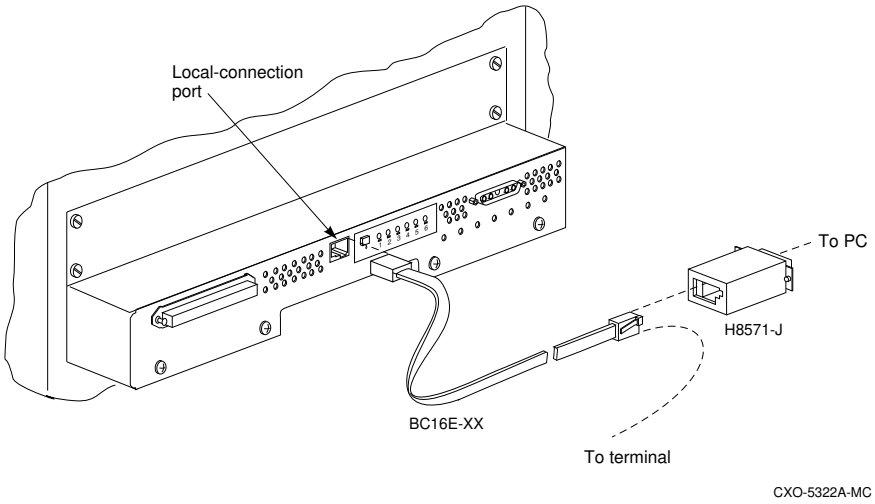
To perform an operation, enter the choice number and any information requested by the submenu or prompts.

The write-back cache example

The following example demonstrates how to enter a license key. The example will show how to enable the WBCA (write-back cache) key.

1. Connect a maintenance terminal to the controller (see Figure 38).

Figure 38
Connecting a maintenance terminal to the controller



2. At the CLI prompt, enter:

```
CLI> RUN FLS
```

The FLS menu is displayed:

```
-----------------------------------------------------
Firmware Licensing System (FLS) on node MASS
Option      State         License         Key
-----------------------------------------------------
RAID      DISABLED      INVALID         *none*
WBCA      DISABLED      INVALID         *none*
MIRR      DISABLED      INVALID         *none*
              RAID = RAID Option
              WBCA = Writeback Cache Option
              MIRR = Disk Mirroring Option
-----------------------------------------------------

1.  Enable a firmware option
2.  Disable a firmware option
3.  Enter a license key for a firmware option
4.  Clear a license key for a firmware option
```

```
0.  Exit FLS
Enter selection (0:4) [0] ?
```

3. Enter option "**3**" to enter a license key:

   The available options are displayed.

```
1. Enter new license key for RAID (current key is
invalid)
2. Enter new license key for WBCA (current key is
invalid)
3. Enter new license key for MIRR (current key is
invalid)
0. Return to main menu
Enter selection (0:5) [0] ?
```

4. Select option "**2**" to enter license key for WBCA:

```
Enter new WBCA key, or enter 0  to return to main menu:
```

5. Enter the license key for WBCA:

ACME_WIDGET_CORP2Z813AE7

6. Enter "**0**" to return to the FLS main menu.

   If the correct key has been entered, the controller will report:

```
*** License key verified ***
```

The FLS main menu will now be displayed:

```
-------------------------------------------------
Firmware Licensing System (FLS) on node MASS
Option      State        License        Key
-------------------------------------------------
RAID      DISABLED      INVALID        *none*
WBCA      DISABLED       VALID     ACME WIDGET_CORP
MIRR      DISABLED      INVALID        *none*

              RAID = RAID Option
              WBCA = Writeback Cache Option
              MIRR = Disk Mirroring Option
-------------------------------------------------

1. Enable a firmware option
2. Disable a firmware option
3. Enter a license key for a firmware option
4. Clear a license key for a firmware option
0. Exit FLS
Enter selection (0:4) [0] ?
```

7. Enter option "**1**" to enable the licensed option.

   The FLS main menu will now show the following license information:

```
-------------------------------------------------
Firmware Licensing System (FLS) on node MASS
Option      State        License        Key
-------------------------------------------------
RAID      DISABLED      INVALID        *none*
WBCA      ENABLED       VALID     ACME WIDGET CORP
MIRR      DISABLED      INVALID        *none*
               RAID = RAID Option
               WBCA = Writeback Cache Option
               MIRR = Disk Mirroring Option
-------------------------------------------------
```

Enabling a firmware option without a valid license key

You can turn on any firmware option at any time using the FLS utility. However, if you enable an option for which you are not licensed, an error message appears on your CLI console and an error is logged in the host error log. These host error indicators are repeated every hour while the unlicensed option remains enabled.

1. At the CLI prompt, enter:

   ```
   CLI> RUN FLS
   ```

   The FLS main menu will displayed:

   ```
   ------------------------------------------------
   Firmware Licensing System (FLS) on node MASS
   Option      State        License        Key
   ------------------------------------------------
   RAID      DISABLED      INVALID        *none*
   WBCA      DISABLED      INVALID        *none*
   MIRR      DISABLED      INVALID        *none*

               RAID = RAID Option
               WBCA = Writeback Cache Option
               MIRR = Disk Mirroring Option
   ------------------------------------------------

   1. Enable a firmware option
   2. Disable a firmware option
   3. Enter a license key for a firmware option
   4. Clear a license key for a firmware option
   0. Exit FLS
   Enter selection (0:4) [0] ?
   ```

2. Select option "**1**" to enable a firmware option.

3. Select the option you wish to enable (that is, RAID = RAID Option, WBCA = Write Back Cache Option, MIRR = Disk Mirroring Option.

   The controller will report that the option has been enabled.

4. Select "**0**" from the main menu to exit the FLS utility.

FLS messages

This section lists the messages that you may receive from FLS.

Message:
option has been turned on without a valid license

Explanation: You have activated the option named by *option* without entering a valid license key. You can evaluate this option for a time to determine its value, and you will receive a valid license key when you purchase the license for the option.

Message:
Error *nnnn*: *option* support is not enabled on this controller

Explanation: The *option* you are attempting to use is not enabled in FLS. For example, if you try to turn on write-back caching, you will receive this error if write-back caching is not enabled by FLS.

Message:
WARNING: This is an invalid license Key

Explanation: The license key you entered is not between 6 and 32 characters, or the customer license key is not valid. Verify that the key is correct and reenter.

Message:
Error: Disabling *option* is not possible at this time, option is in use

Explanation: You have attempted to disable the option named by *option* while it is in use.

Message:
`License different between the two controllers`

Explanation: You have installed your license key in only one of your dual-redundant controllers. Connect a maintenance terminal to the other controller, run FLS and enter the license key.

Installing a controller and cache module (single controller configuration)

Use the following procedure to install a controller and its power supplies into an empty controller shelf for the first time.

Required tools

The tools listed in Table 21 are required for the installation of controllers:

Table 21
Required tools for controller installation

Required tools	Purpose
Maintenance terminal	To set controller parameters
ESD wrist strap	To protect all equipment against electrostatic discharge
5/32-inch Allen wrench	To unlock the SW800 series cabinet
Flat-head screwdriver	To loosen controller mounting screws, and to disconnect the CI cable

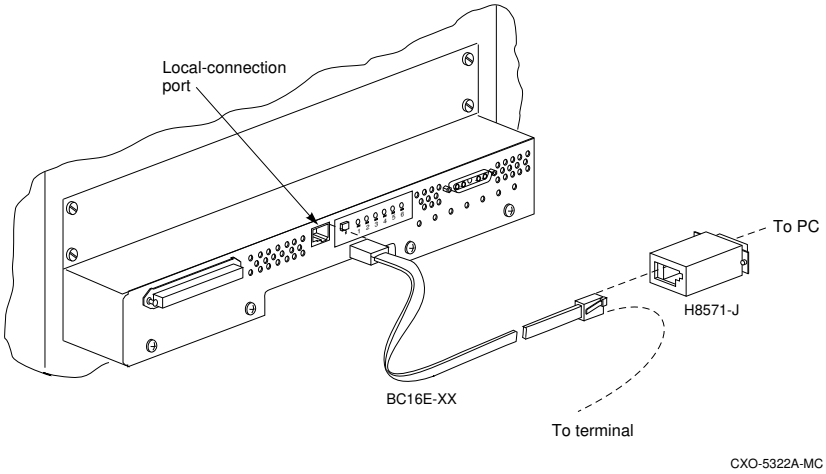
1. Using Table 22 as a guide, determine the slot and the SCSI ID into which the controller is to be installed. Note that the first controller should be installed in the slot that corresponds to SCSI ID 7.

Table 22
Controller installation guide

Controller	SW800 Front View	SW800 Rear View	SW500 Font & Rear View	SW300
First Controller	Right Side SCSI ID 7	Left Side SCSI ID 7	Top Slot SCSI ID 7	Bottom Slot SCSI ID 7
Second Controller	Left Side SCSI ID 6	Right Side SCSI ID 6	Bottom Slot SCSI ID 6	Top Slot SCSI ID 6

2. Connect a maintenance terminal to the controller (see Figure 39).

Figure 39
Connecting a maintenance terminal to the controller

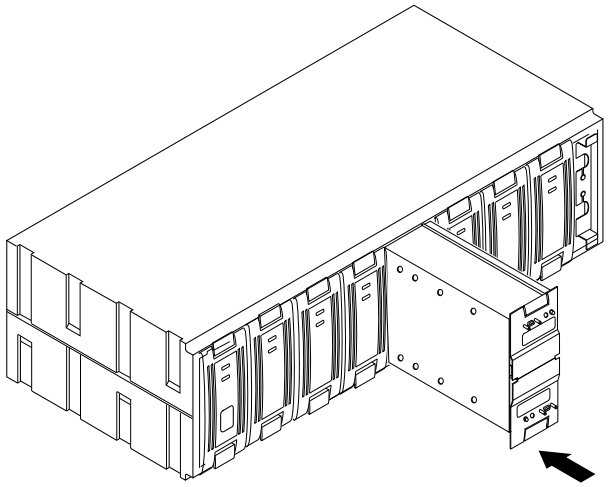


3. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around you wrist.

4. Attach or clip the other end of the ESD strap to the cabinet grounding stud or a convenient cabinet grounding point (nonpainted surface).

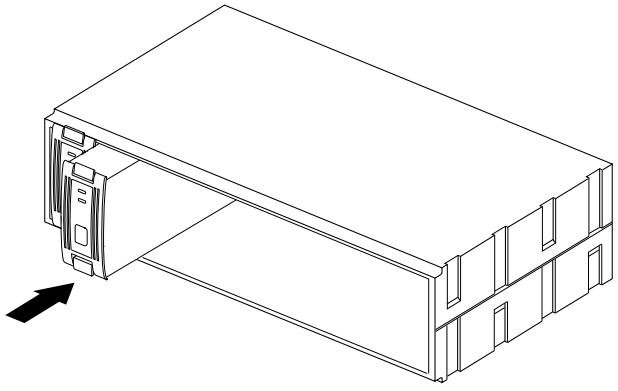
5. Install an SBB battery module into a convenient device slot (see Figure 40).

Figure 40
Installing an SBB battery module



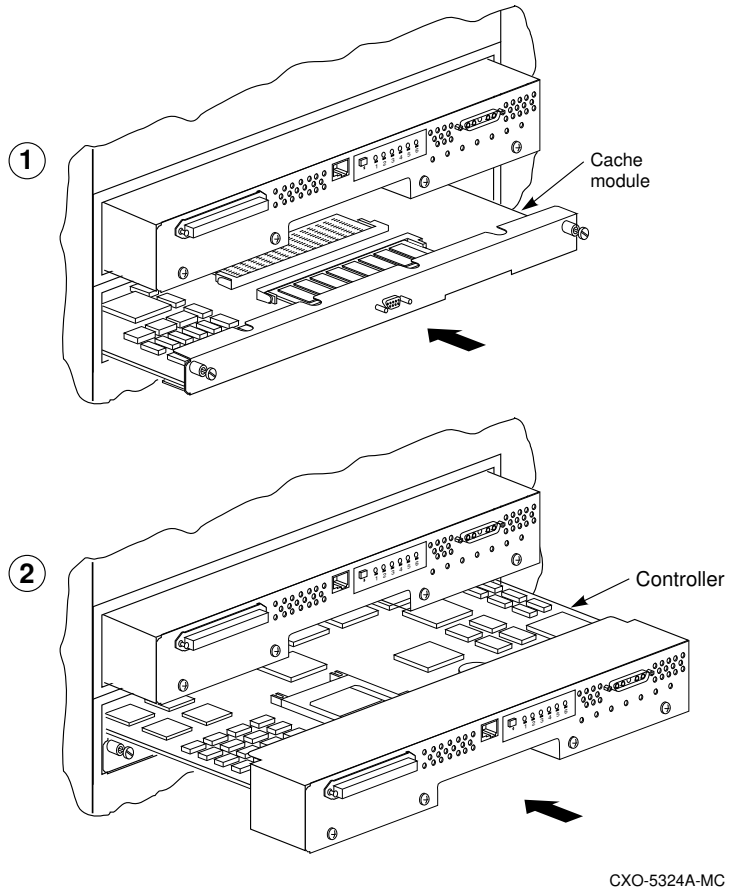
6. Install the controller power supplies into the controller shelf (see Figure 41).

Figure 41
Installing power supplies into the controller shelf



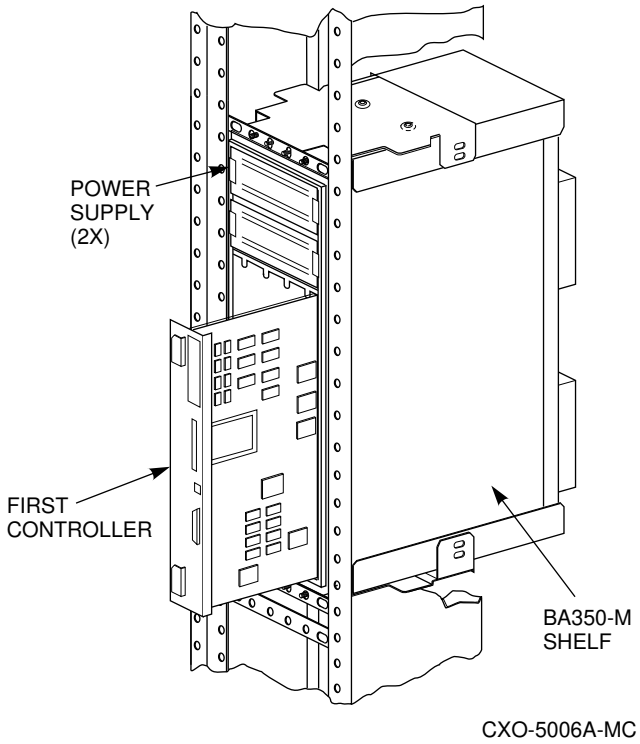
7. Slide the cache module into the controller shelf. Push the module firmly into the slot until it is seated. (see Figure 42).

Figure 42
Installing a single controller (SW500 cabinet)



8. Install the controller module into the shelf slot that corresponds to SCSI ID7 (see Figure 42 and Figure 43).

Figure 43
Installing a single controller
(SW800 cabinet)



9. Connect the battery cable to the cache module and then to the ECB
10. Remove the program card from the controller.
11. Connect the power cords to the controller power supplies.
12. Press and hold the Reset button (//) while inserting the program card. The controller will initialize and perform all internal self tests.
13. When the reset light flashes at a rate of once every second, the initialization process is complete.
14. Snap the ESD cover into place over the program card. Push the pins inward to lock the cover into place.
15. Connect the host CI connector to the controller.

16. Check the ECB status indicator for the appropriate indication (see Table 23).

Table 23
ECB status indications

LED status	Battery status
LED is on continuously	System power is on and the ECB is fully charged.
LED blinks rapidly	System power is on and the ECB is charging.
LED blinks slowly	System power is off and the ECB is supplying power to the cache.
LED is off	System power is off and the ECB is not supplying power to the cache.

17. Refer to the Enabling a license option (FLS utility) section to enable your valid license for write-back cache.

18. Enable the write-back cache at the CLI:

```
CLI> SET unit name WRITEBACK_CACHE
```

Installing a second controller and cache module

This procedure may be used to install a second controller and cache module for redundancy. Service to the subsystem during this procedure is halted. Use this procedure if you prefer not to use the C_Swap utility.

Required tools

The tools listed in Table 24 are required for the installation of a second controller and cache module:

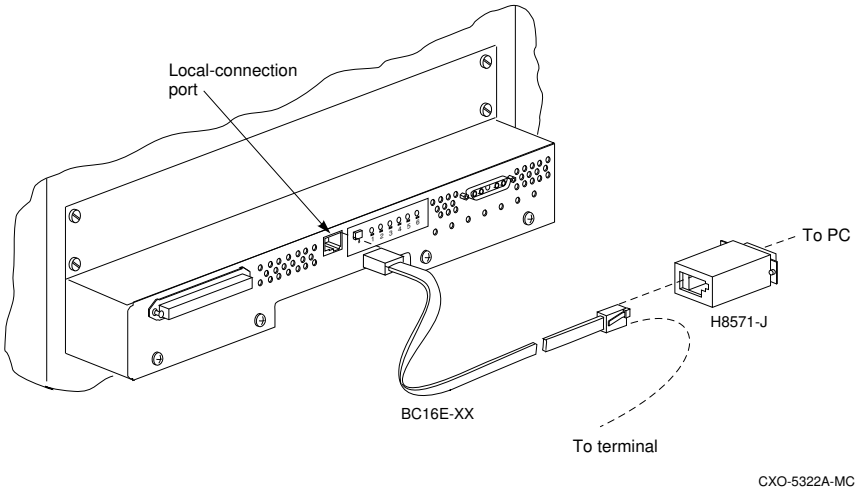
Table 24
Required tools

Required tools	Purpose
Maintenance terminal	To set controller parameters.
ESD wrist strap	To protect all equipment against electrostatic discharge
5/32-inch Allen wrench	To unlock the SW800 series cabinet
Flat-head screwdriver	To loosen controller mounting screws, and to disconnect SCSI cables

To add the second controller:

1. Connect a maintenance terminal to the operating controller (see Figure 44).

Figure 44
Connecting a maintenance terminal to the controller



2. At the operating controller's terminal enter:

```
CLI> SHOW THIS_CONTROLLER
```

   The controller will display the following information (this is a sample only):

```
Controller:
    HSJ50  ZG34901786 Firmware V03.0-0, Hardware BX11
    Not configured for dual-redundancy
    SCSI address 7
    Time: 15 JUN-1995 16:32:54
Host port:
    Node name: HSJA1, valid CI node 21, 32 max nodes
    Path A is on
    Path B is on
    MSCP allocation class  3
    TMSCP allocation class 3
    CI_ARBITRATION = SYNCHRONOUS
    MAXIMUM HOSTS =9
    NOCI_4K_PACKET _CAPABILITY
Cache:
    128 megabyte write cache, version 3
    Cache is GOOD
    Battery is good
    No unflushed data in cache
    CACHE_FLUSH TIMER = DEFAULT (10 seconds)
    CACHE_POLICY = B
    NOCACHE_UPS
```

3. Note the type, memory size and version of cache that is installed with the first controller.

4. If a cache module is present with the first controller, prepare another one of the same type, memory size and version for installation with the second controller. An ECB (external cache battery) must also be installed.

5. Use the procedures appropriate to your host operating system to halt *host* activity on your subsystem.

6. At the CLI prompt, enter:

```
CLI> SHUTDOWN THIS_CONTROLLER
```

   When you enter the SHUTDOWN command, do not specify any optional qualifiers. The default qualifiers do not allow the controller to shut down until data is

completely and successfully stored on the appropriate storage devices.

7. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around you wrist.
8. Attach or clip the other end of the ESD strap to the cabinet grounding stud or a convenient cabinet grounding point (nonpainted surface).
9. Disconnect power cords from controller power supplies.

   If you do not already have a second controller power supply, this may be the time to add one.

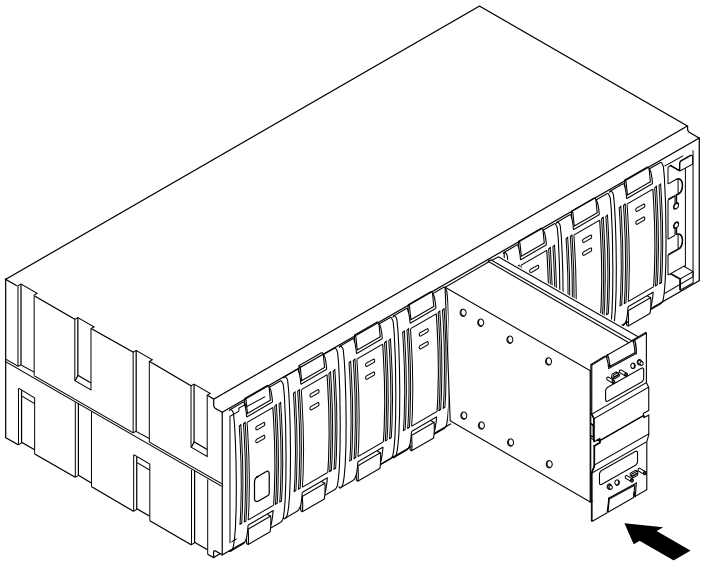
10. Using Table 25 as a guide, find the slot and the SCSI ID into which the controller is to be installed. Note that the second controller should be installed in the slot that corresponds to SCSI ID 6.

Table 25
Controller installation guide

Controller	SW800 Front View	SW800 Rear View	SW500 Front & Rear View	SW300
First Controller	Right Side SCSI ID 7	Left Side SCSI ID 7	Top Slot SCSI ID 7	Bottom Slot SCSI ID 7
Second Controller	Left Side SCSI ID 6	Right Side SCSI ID 6	Bottom Slot SCSI ID 6	Top Slot SCSI ID 6

11. Install an SBB battery module into a convenient device slot (see Figure 45).

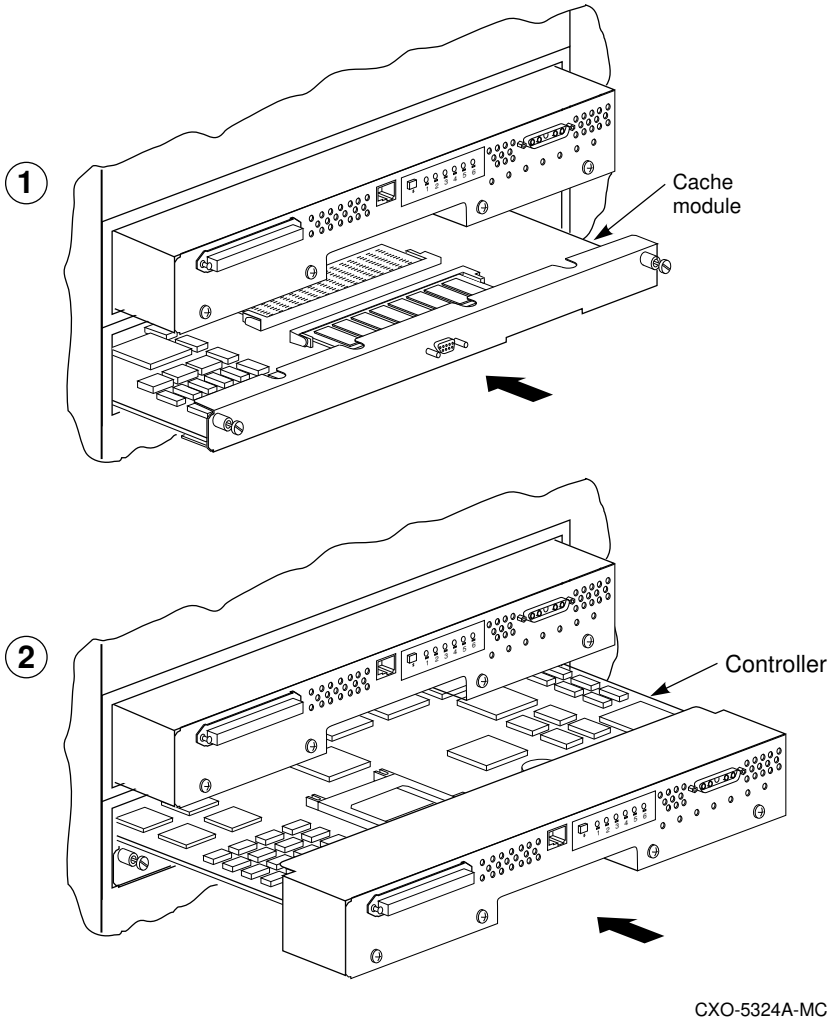
Figure 45
Installing an SBB Battery module



CXO-5306A-MC

12. Slide the cache module into the appropriate slot in the controller shelf. Push the module firmly into the slot until it is seated.(see Figure 46).

Figure 46
Installing the second controller and cache module



13. Slide the controller module into the appropriate slot. Push the module firmly into the slot until it is seated.

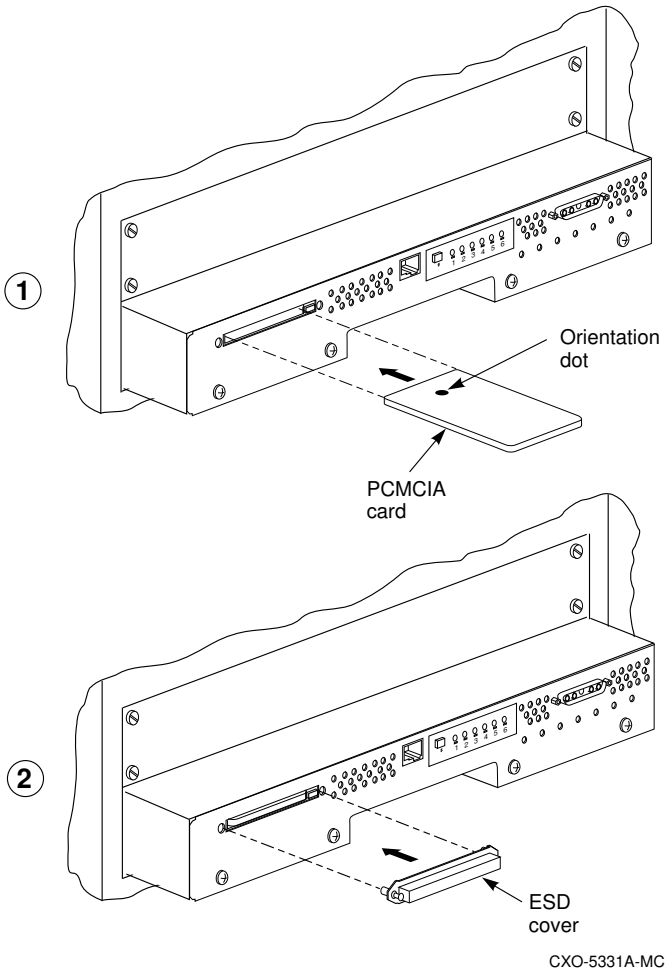
14. Tighten the front panel captive screws on the cache and the controller modules.

15. Connect the battery cable to the cache module and then the ECB.

16. Reconnect power cords to the controller power supplies.

17. Press and hold the Reset button (//) while inserting the program card. The controller will initialize and perform all internal self tests (see Figure 47).

Figure 47
Inserting the program card



18. Snap the ESD cover into place over the program card. Push the inward to lock the cover into place.

Note
Ensure the version level of the software in the program card is the same as that in the existing controller. A mismatch in the firmware levels may cause unpredictable controller operation.

19. Connect the CI cable to the controller.
20. At the maintenance terminal that is still connected to the first controller enter:

    ```
    CLI> SET FAILOVER COPY=THIS_CONTROLLER
    ```

    The two controllers are now configured in a dual-redundant configuration.
21. Check the front panel ECB status indicator for the Appropriate indication (see Table 26).

Table 26
ECB status indicators

LED Status	Battery Status
LED is on continuously	System power is on and the ECB is fully charged.
LED blinks rapidly	System power is on and the ECB is charging.
LED blinks slowly	System power is off and the ECB is supplying power to the cache.
LED is off	System power is off and the ECB is not supplying power to the cache.

Adding a second controller using C_SWAP

You can add a second controller to a single controller configuration to create a dual-redundant configuration. There are two procedures for adding a second controller: an online method using the C_SWAP utility in which the existing controller continues to process I/O, and an offline method in which you must shut down the existing controller (see previous procedure).

To add a controller module using the online (C_SWAP) method, your system must have two power supplies in the controller shelf of an SW500 or SW800 cabinet. If you are adding a second controller in an SW300 cabinet, your cabinet must have a minimum of five power supplies.

The following steps guide you through the online method using the C_SWAP utility.

Required tools

The tools listed in Table 27 are required for adding a second controller.

Table 27
Required tools for adding a second controller

Required tools	Purpose
Maintenance terminal and cable	To change controller parameters
ESD wrist strap and ESD mat	To protect all equipment against electrostatic discharge
3/32-inch Allen wrench	To loosen the controller mounting screws; to reinstall the controller
5/32-inch Allen wrench	To unlock the SW800-series cabinet

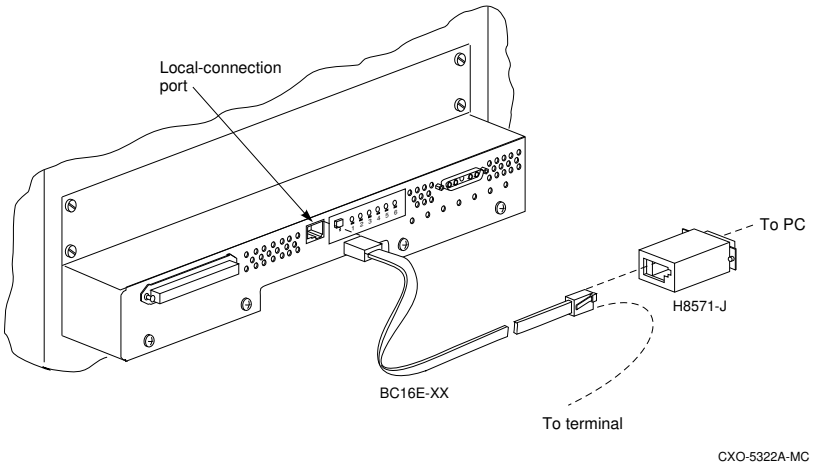
Caution

Before starting the C_SWAP utility, terminate all other running utilities and disable all other terminals.

Prepare the subsystem

1. Have the new module at hand. The module should be factory-fresh or should have been shut down cleanly (with the SHUTDOWN command) in its last application.
2. Connect a maintenance terminal to the existing controller (see Figure 48).

Figure 48 Connecting a maintenance terminal to the controller



3. Show the configuration of the existing controller:

```
CLI> SHOW THIS_CONTROLLER

Controller:
    HSJ50  ZG34901786 Firmware V03.0,❶(1) Hardware BX11
    Not configured for dual-redundancy
    SCSI address 7
    Time: 15 JUN-1995 16:32:54
Host port:
    Node name: HSJA1, valid CI node 21, 32 max nodes
    Path A is on
    Path B is on
    MSCP allocation class  3
    TMSCP allocation class 3
    CI_ARBITRATION = SYNCHRONOUS
    MAXIMUM HOSTS =9
    NOCI_4K_PACKET _CAPABILITY
Cache:
    128 megabyte write cache, version 3
    Cache is GOOD
    Battery is good
    No unflushed data in cache
    CACHE_FLUSH TIMER = DEFAULT (10 seconds)
    CACHE_POLICY = B
    NOCACHE_UPS
```

4. Note the size of the cache module that is installed with the first controller.
5. If a cache module is present at the first controller, prepare another one of the same size for installation with the second controller.
6. Insert the SBB battery module that was shipped your controller into an existing device slot.
7. Start the C_SWAP program:

```
CLI> RUN C_SWAP
```

8. When the controller prompts you, answer the question:

```
Do you have a replacement HSJ readily available?
[N] ? y
```

9. Press **Y** for Yes.
10. Answer the question:

```
***Sequence to INSERT the other HSJ has begun.***

Do you wish to INSERT the other HSJ y/n?
```

11. Press **Y** for yes.
12. Wait for the following text to appear on the operating controller's console:

```
Attempting to quiesce all ports.
Port 1 quiesced
Port 2 quiesced
Port 3 quiesced
Port 4 quiesced
Port 5 quiesced
Port 6 quiesced
All ports quiesced.
Insert the other HSJ50 WITHOUT its program card, and
press Return.
```

13. If you are installing a new cache module, slide it straight in along the rails and then push firmly to seat it in the backplane.

14. Check the new controller to make sure that the program card is not installed. If it is installed, take the card out by removing the ESD cover and then pressing the eject button next to the card.

15. Install the controller module. Slide the module straight in along the rails and then push firmly to seat it in the backplane.

16. Tighten the front panel captive screws on the cache and the controller modules.

Caution

Do not overtighten the controller's front panel captive screws. Damage to the controller PC board or front panel may result.

17. Connect the battery cable to the cache module and then the ECB.

18. Press **Return** on the operating controller's console.

19. Wait for the following text to be displayed on the operating controller's console:

```
Port 1 restarted
Port 2 restarted
Port 3 restarted
Port 4 restarted
Port 5 restarted
Port 6 restarted

Controller Warm Swap terminated.
The configuration has two controllers
To restart the other HSJ50
1) Enter the command RESTART OTHER_CONTROLLER
2) Press and hold in the Reset (//) button while
inserting the program card.
3) Release Reset (//); the controller will initialize.
4) Configure new controller by referring to
controller's user guide
```

Restarting the subsystem

1. Restart the new controller:

```
CLI> RESTART OTHER_CONTROLLER
```

2. Connect the maintenance terminal to the newly installed controller.

3. Press and hold the Reset button (//) on the new controller while inserting the program card from the new controller.

4. Release the Reset button to initialize the controller. Wait for the CLI prompt to appear at the terminal. You will see a "Controllers misconfigured" message, which you can ignore.

5. If the new controller reports an invalid cache error, enter the following CLI command to clear the error:

   ```
   CLI> CLEAR_ERRORS INVALID_CACHE THIS_CONTROLLER
   DESTROY_UNFLUSHED_DATA
   ```

6. Ensure that the new controller is not in dual-redundant mode by entering the following command on the new controller:

   ```
   CLI> SET NOFAILOVER
   ```

   If the controller was already in nonredundant mode, you will see a message indicating that.

7. Enter the following command from the *new* controller CLI to put the controllers into dual-redundant mode:

   ```
   CLI> SET FAILOVER COPY=OTHER_CONTROLLER
   ```

8. The new controller will initialize.

9. Verify that all host settings are correct:

   ```
   CLI> SHOW THIS_CONTROLLER
   ```

10. After the controller has initialized, connect the CI cable to the new controller and tighten the captive screws.

11. Enable the path by entering the following command:

    ```
    CLI> SET THIS_CONTROLLER PATH_A
    CLI> SET THIS_CONTROLLER PATH_B
    ```

Installing a cache module

This procedure contains information for installing cache modules. The controller modules are seated in front of the cache module. Any time you add a cache module, the controller module has to be removed first.

Service to the devices is interrupted during the installation procedure.

Required tools

The tools listed in Table 28 are required for the installation of a cache module:

Table 28 Required tools for cache module replacement

Required tools	Purpose
Maintenance terminal	To set controller parameters.
ESD wrist strap	To protect all equipment against electrostatic discharge
ESD Mat	To protect the controller and cache modules
5/32-inch Allen wrench	To unlock the SW800-series cabinet
Flat-head screwdriver	To loosen controller mounting screws, and to disconnect CI cable

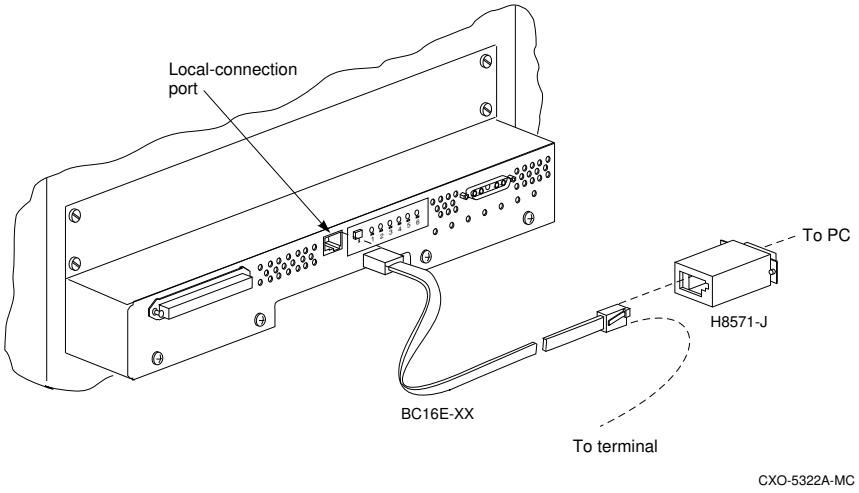
To install cache modules:

The following procedure describes how to install write-back cache modules in single controller configurations. For dual - redundant configurations, use the Adding a second controller using C_Swap procedure.

Removing the controllers

1. Connect a maintenance terminal to the controller (see Figure 49).
2. Use the FLS utility to install the firmware license key for write-back cache.

Figure 49
Connecting a maintenance terminal to the controller

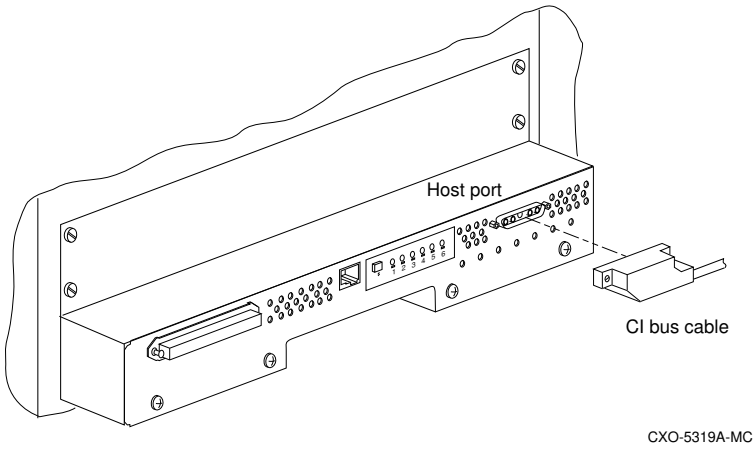


3. Halt all host I/O activity using the appropriate procedure for your operating system.
4. At the CLI prompt, enter:

   ```
   CLI> SHUTDOWN THIS_CONTROLLER
   ```

5. If you are in a dual redundant configuration, refer to the Adding a second controller using C_Swap procedure in this manual.
6. After the controller has shut down, remove the maintenance terminal cable and remove power cables from the controller shelf.
7. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.
8. Attach or clip the other end of the ESD strap to the cabinet grounding stud or a convenient cabinet grounding point (nonpainted surface).
9. With a small flat-head screw driver, loosen the captive screws on the CI cable of the controller (see Figure 50) and remove the cable.

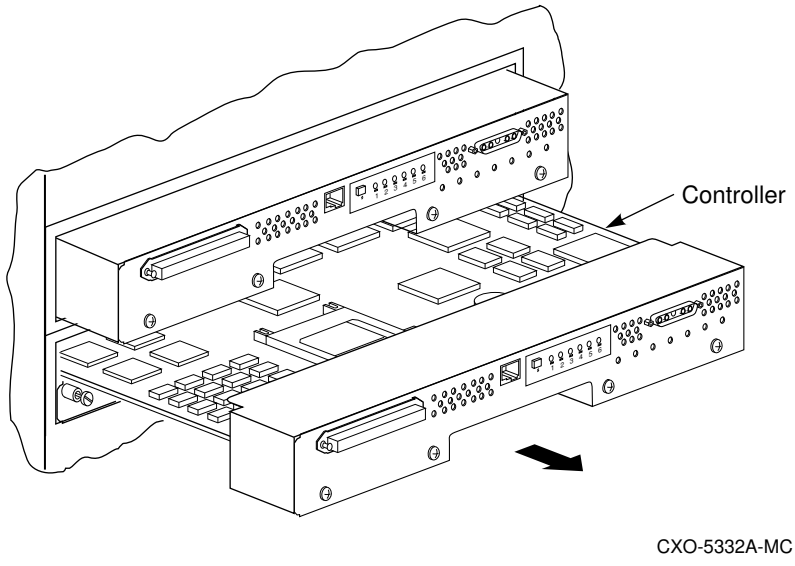
Figure 50
Disconnecting the CI cable adapter



10. Use a gentle rocking motion to loosen the controller modules.

11. Slide the controller modules out of the shelf (see Figure 51) and place them on a ESD mat.

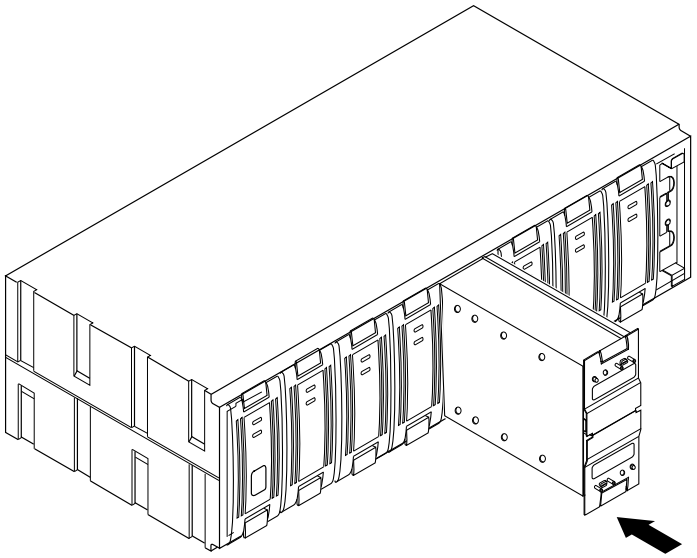
Figure 51
Removing controller modules



Installing a write-back cache module

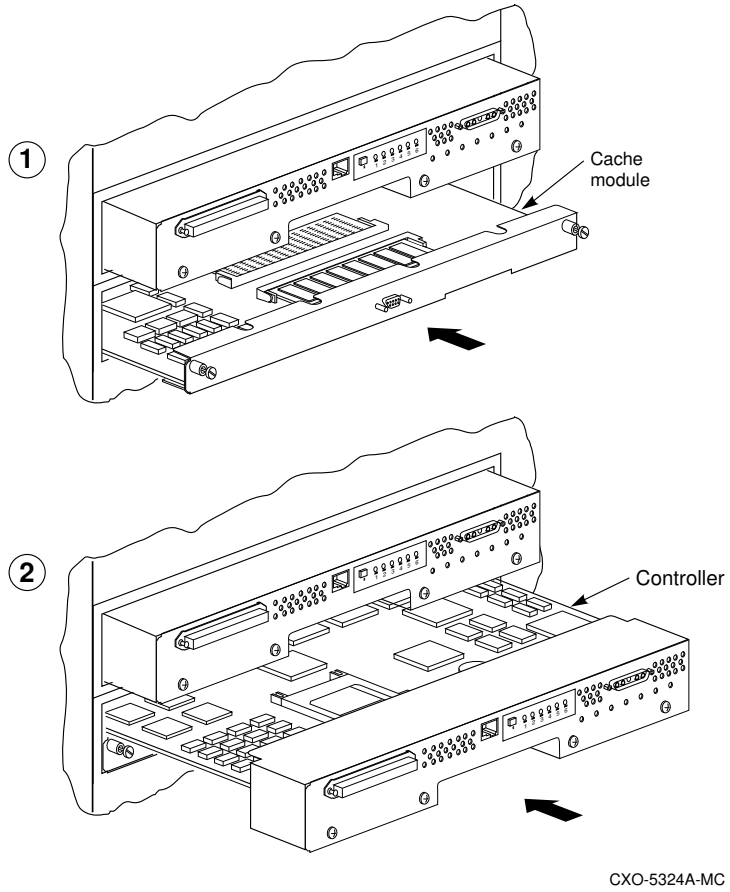
1. Install the SBB battery module into a convenient device slot (see Figure 52).

Figure 52
Installing an SBB battery module



2. Slide the cache module into the appropriate slot (see Figure 53).

Figure 53
Installing the cache
and controller modules

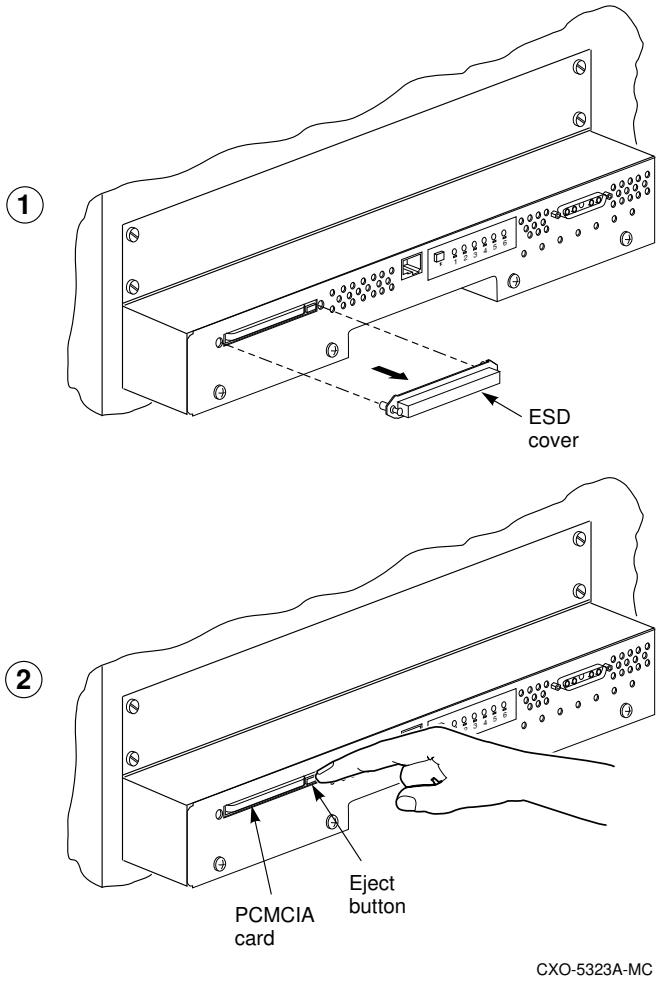


3. Install the controller module into the appropriate slot (see Figure 53).
4. Push the modules firmly into the slot until they are seated.
5. Tighten the front panel captive screws on the controller and cache module. Do not over tighten.
6. Connect the ECB battery cables starting at the cache modules.
7. Reinstall the CI cable at the controller's front bezel.

Restarting the subsystem

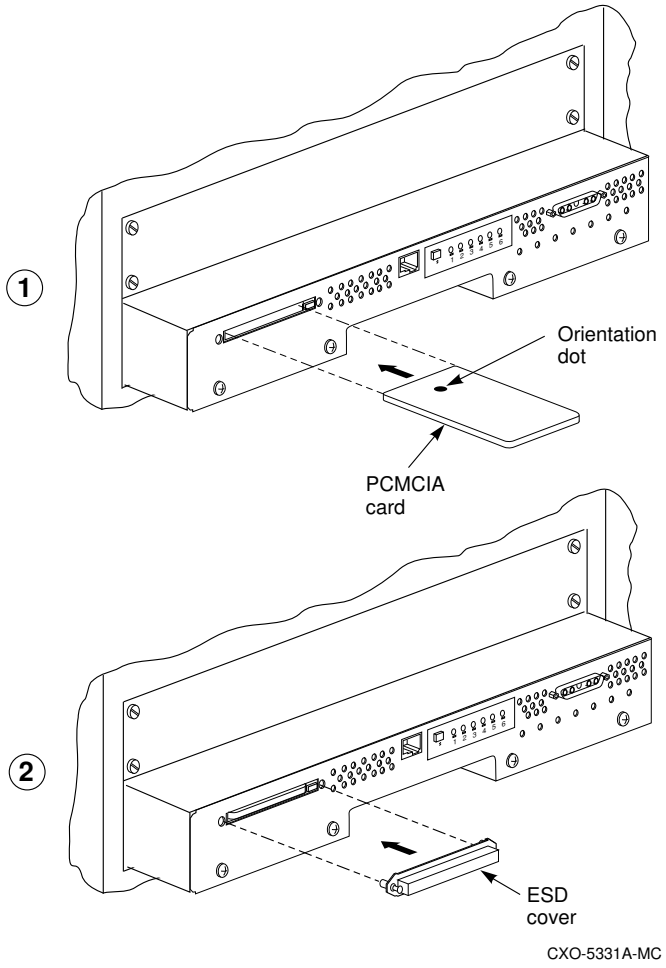
1. Remove the program card from the controller (see Figure 54).

Figure 54
Removing the program card



2. Reconnect power cords to the controller power supplies.
3. Press and hold the Reset button (//) on the controller while pushing in the program cards (see Figure 55).

Figure 55
Installing the program card



4. The controller will initialize.
5. When the reset light on each controller flashes at a rate of once every second, the initialization process is complete.
6. Snap the ESD covers into place over each program card. Push the pins inward to lock the covers in place.
7. At the maintenance terminal that is still connected to the controller invoke the FLS utility and install the new valid license keys for write-back cache.
8. At the controllers, check for the new write-back cache:

```
CLI> SHOW THIS_CONTROLLER
```

If you are in a dual-redundant configuration, the controller will report the following information:

```
Controller:
    HSJ50  ZG34901786 Firmware V05.0-0, Hardware BX11
    Configured for dual-redundancy with ZG61000012
       In dual-redundant configuration
    SCSI address 7
    Time: 15 JUN-1996 16:32:54
Host port:
    Node name: HSJA1, valid CI node 21, 32 max nodes
    Path A is on
    Path B is on
    MSCP allocation class  3
    TMSCP allocation class 3
    CI_ARBITRATION = SYNCHRONOUS
    MAXIMUM HOSTS =9
    NOCI_4K_PACKET _CAPABILITY
Cache:
    128 megabyte write cache, version 3
    Cache is GOOD
    Battery is good
    No unflushed data in cache
    CACHE_FLUSH TIMER = DEFAULT (10 seconds)
    CACHE_POLICY = B
    NOCACHE_UPS
```

Notice that the new write-back cache is reported on THIS_CONTROLLER.

9. Enable write-back cache on specific units using the command:

```
CLI> SET unit name WRITEBACK_CACHE
```

Adding Cache Memory

This procedure contains information for increasing cache memory. You may increase cache memory up to a maximum of 128 MB (in 4x32MB SIMM cards).

The controller module is seated in front of the cache module. Any time the cache module requires service, the controller module has to be removed first.

Service to the devices is interrupted during the upgrade procedures.

Required Tools

Table 29 Required tools

The tools listed in Table 29 are required for the upgrading of cache modules:

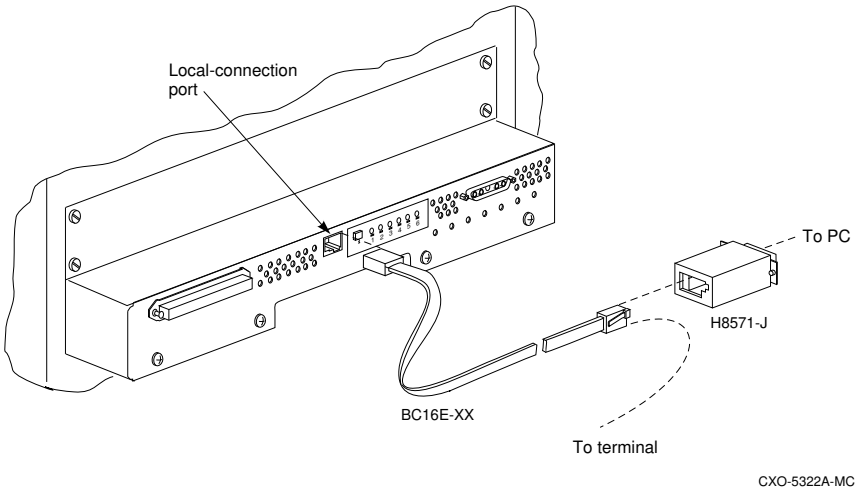
Required tools	Purpose
Maintenance terminal	To change controller parameters
ESD wrist strap and ESD mat	To protect all equipment against ESD
Small flat head screwdriver	To loosen CI cable, and front bezel captive screws
5/32-Allen wrench	To unlock the SW800 - Series cabinet

Installing SIMM Cards

The following procedure shows how to install SIMM cards to increase write-back cache capacity in single and dual-redundant controller configuration.

1. Connect a maintenance terminal to the controller (see Figure 56).

Figure 56
Connecting a maintenance terminal to the controller



2. Take the single controller out of service:

```
CLI> SHUTDOWN THIS_CONTROLLER
```

3. If you are working with a dual redundant configuration, take both controllers out of service.

```
CLI> SHUTDOWN OTHER_CONTROLLER
CLI> SHUTDOWN THIS_CONTROLLER
```

   To ensure that the controller has shut down cleanly, check the OCP for the following indications:

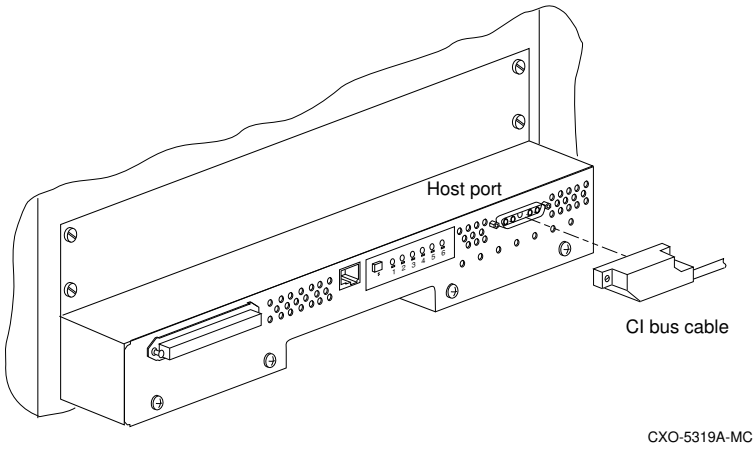
   - The Reset (//) LED is continuously lit.
   - Port LEDs 1, 2, 3, are also lit continuously.

4. After the controllers have shut down, remove the maintenance terminal cable and remove the power cords from the controller power supplies.

5. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around you wrist.

6. Attach or clip the other end of the ESD strap to the cabinet grounding stud or a convenient cabinet grounding point (nonpainted surface).
7. Loosen the captive screws on the controller's front bezel.
8. With a small flat-head screw driver, loosen the captive screws on the CI cable of each controller (see Figure 57) and remove the cable.

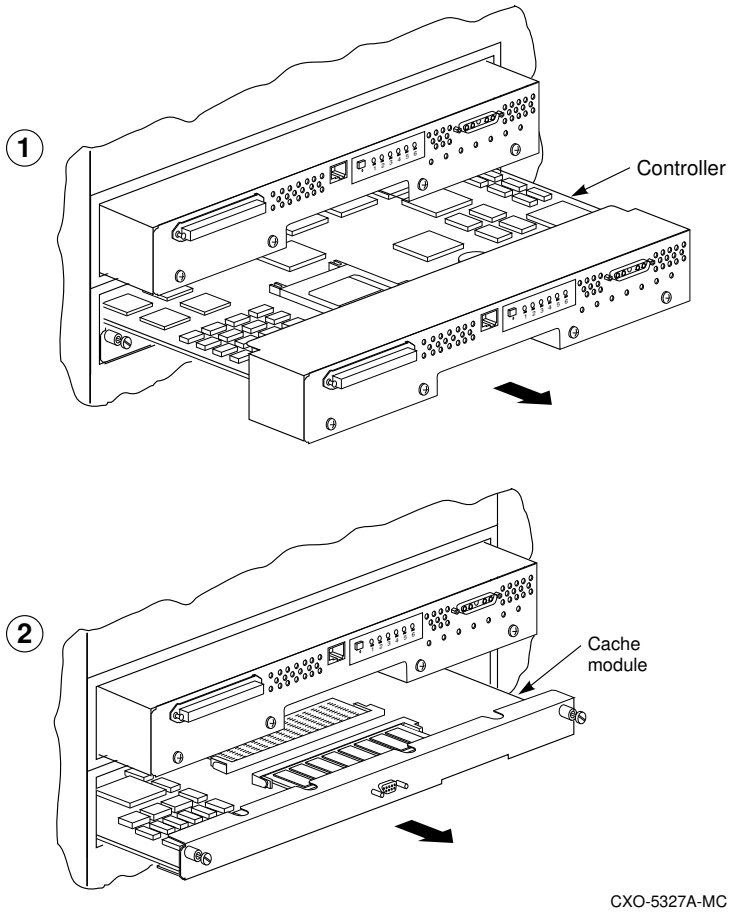
Figure 57
Disconnecting the CI cable



9. Use a gentle rocking motion to loosen the controller modules.

10. Slide the controller modules out of the shelf and place them on a ESD mat (see Figure 58).

Figure 58
Removing controller and cache modules



11. Remove the cache modules from the controller shelf.

12. Disconnect the battery cable from the SBB battery module.

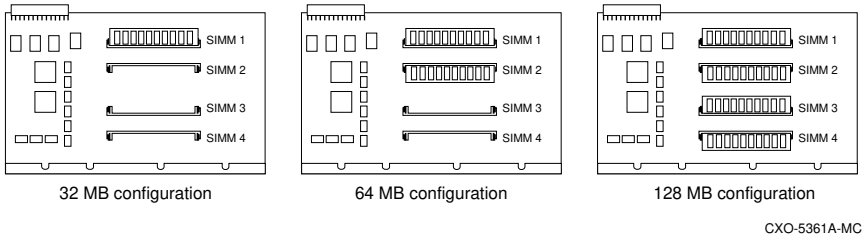
13. Refer to Table 30 and install as many SIMM cards into each cache modules as required (up to 4x32MB maximum).

Table 30
Adding cache memory capacity

Cache size	SIMM slot # occupied
32Mb	SIMM 1
64Mb	SIMM 1+2
128Mb	SIMM 1+2+3+4

Figure 59 shows all possible cache configurations.

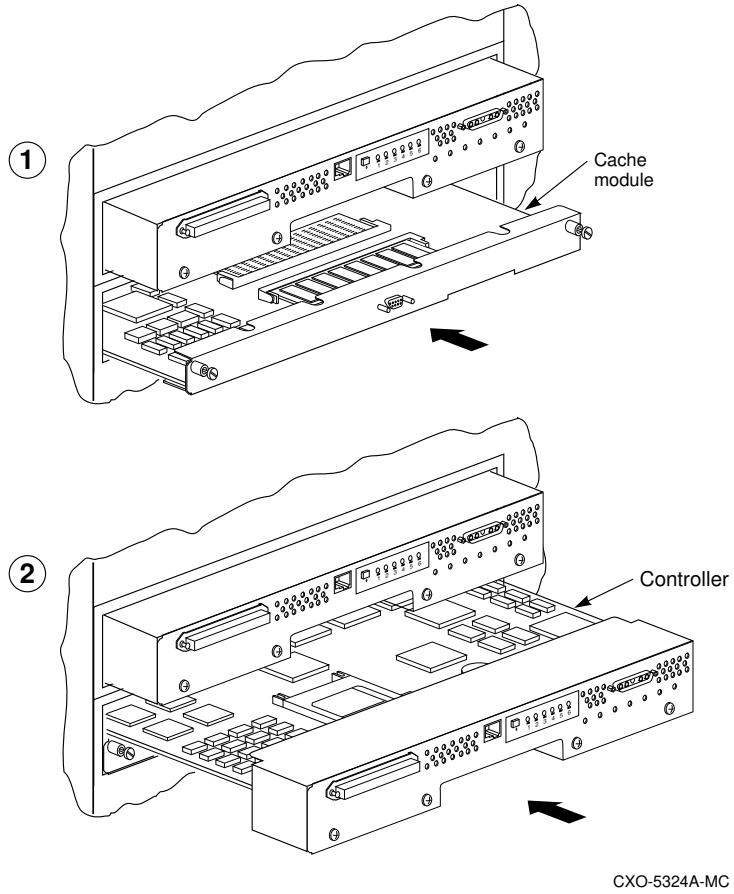
Figure 59
Cache configurations for cache version 3



14. Reinstall the cache modules into the controller shelf.

15. Reinstall the controller modules (see Figure 60) into their original slots. Use a gentle rocking motion to help seat the module. If you are using a single controller configuration, use the slot that is designated SCSI ID 7.

Figure 60
Installing the controller and cache module



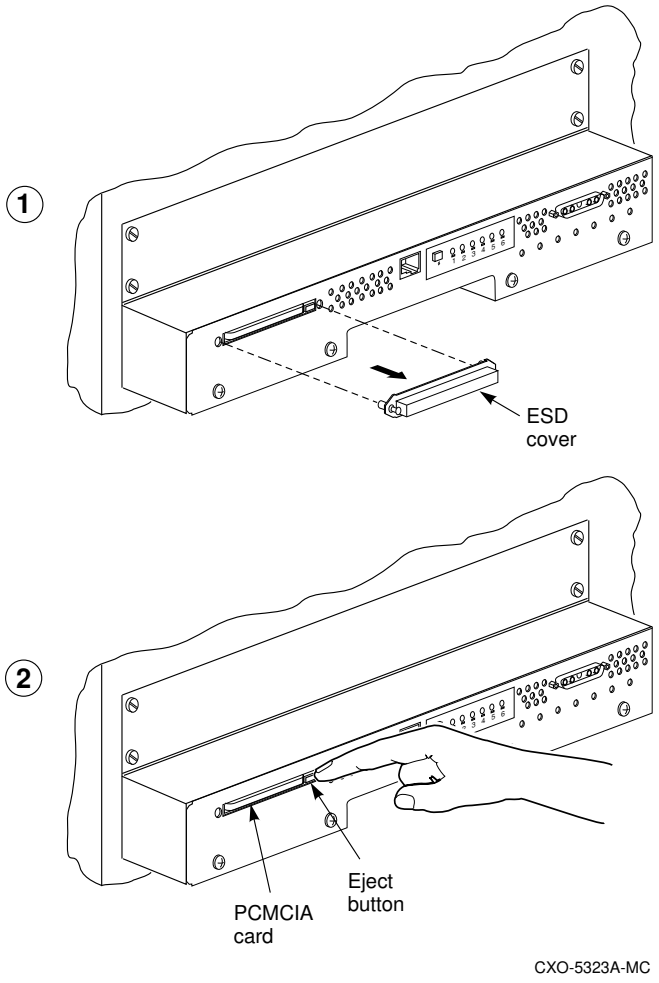
16. Connect one end of the battery cable to the cache module and the other end to the ECB.
17. Tighten the ECB cable mounting screws.

Caution

Do not overtighten the front panel captive screws. Damage to the controller PC board or front panel may result.

18. Tighten the two front panel captive screws on the cache module and the two captive screws on the controller module.
19. Remove the program cards from each controller (see Figure 61).

Figure 61
Removing the program card



20. Reconnect the power cords to the controller power supplies.
21. Press and hold the Reset button (//) on each controller while pushing in the program card.
22. The controllers will initialize.

    When the reset light on each controller flashes at a rate of once every second, the initialization process is complete.

23. Snap the ESD covers into place over each program card. Push the pins inward to lock the covers in place.

24. To check cache capacity of the modules, attach a maintenance terminal to one of the controllers. At the CLI prompt type:

```
CLI> SHOW THIS_CONTROLLER
```

The controller will report the following information:

```
Controller:
    HSJ50  ZG34901786 Firmware V05.0-0, Hardware BX11
    Configured for dual-redundancy with ZG61000012
       In dual-redundant configuration
    SCSI address 7
    Time: 15 JUN-1995 16:32:54
Host port:
    Node name: HSJA1, valid CI node 21, 32 max nodes
    Path A is on
    Path B is on
    MSCP allocation class  3
    TMSCP allocation class 3
    CI_ARBITRATION = SYNCHRONOUS
    MAXIMUM HOSTS =9
    NOCI_4K_PACKET _CAPABILITY
Cache:
    128 megabyte write cache, version 3
    Cache is GOOD
    Battery is good
    No unflushed data in cache
    CACHE_FLUSH TIMER = DEFAULT (10 seconds)
    CACHE_POLICY = B
    NOCACHE_UPS
```

25. Use the SHOW OTHER_COMMAND to check the capacity of the second cache module:

```
CLI>SHOW OTHER_CONTROLLER
```

The OTHER_CONTROLLER will report the same information.

Installing power supplies

This procedure may be used to install a power supply into a SBB shelf or into a controller shelf.

Power supply and shelf LED status indicators.

Each power supply has two LED indicators that display the power supply status. The upper LED is the common power supply status. The lower LED is the power supply status indicator.

Table 31 shows the possible fault indications for an SW300 cabinet.

Table 31
Power supply status indicators

When the LED Display is ...	The RAID Shelf Power Status is ...
■ ■	All the power supplies on the associated power bus are functioning
■ □	This power supply is functioning properly however one power supply on the associated bus has failed..
□ □	Either there is no AC power to this supply or this power supply should be replaced

LED on = ■

LED off = □

Table 32 shows all possible fault indications for the SW500 and the SW800 cabinet in a single power supply configuration.

Table 32
Shelf and single power supply status indicators

Status Indicator	State	Indication
Shelf LED Power supply LED		System is operating normally.
Shelf LED Power supply LED		There is a shelf fault; there is no power supply fault. Replace shelf blower.
Shelf LED Power supply LED		Shelf and power supply fault. Replace power supply Described in the Replace Section.

LED on =

LED off =

Table 33 shows all possible fault indications for the SW500 and the SW800 cabinets for a dual power supply configuration.

Table 33
Shelf and dual power supply status indicators

Status Indicator	PS 1	PS 2	Indication
Shelf LED Power supply LED	■ ■	■ ■	Normal. System is operating normally.
Shelf LED Power Supply LED	□ ■	□ ■	There is a shelf fault; there is no power supply fault Replace shelf blower.
Shelf LED Power supply LED	□ ■	□ □	PS 1 is operational. Replace PS 2.
Shelf LED Power supply LED	□ □	□ ■	PS 2 is operational. Replace PS 1.
Shelf LED Power supply LED	□ □	□ □	Possible PS 1 and PS 2 fault or input power problem

LED on = ■

LED off = □

Note

The status indicators will operate ONLY if the power supplies and the shelf blowers are present. The failure must be a electrical or mechanical failure.

Required tools

The tools listed in Table 34 are required for power supply installation.

Table 34
Required tools for power supply installation

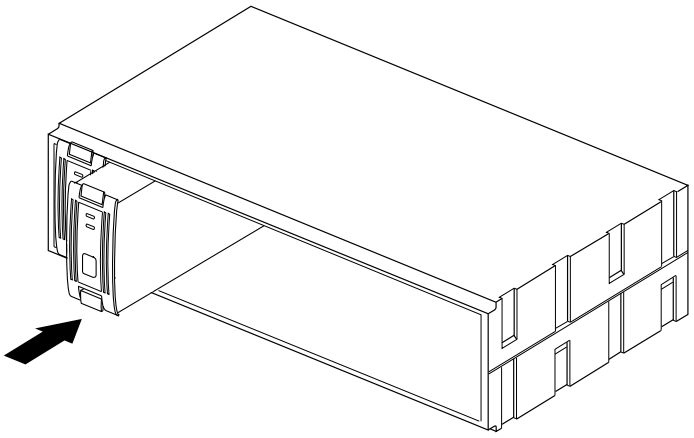
Required tools	Purpose
5/32-inch Allen wrench	To unlock the SW800 series cabinet

To install a power supply

Use the following procedure to install a power supply. For dual power supply configurations, repeat this procedure. For a single power supply configuration use slot 7 of the SBB shelf. Use lot 6 if you are adding a second power supply for redundancy.

1. Firmly push the power supply into the shelf until the mounting tabs snap into place (see Figure 62).

Figure 62
Installing a power supply SBB



2. Plug the power cord into the supply.
3. Observe the power and shelf status indicators and ensure they are both on. If the status indicators are not on, refer to the Status indicator tables and take appropriate service action.

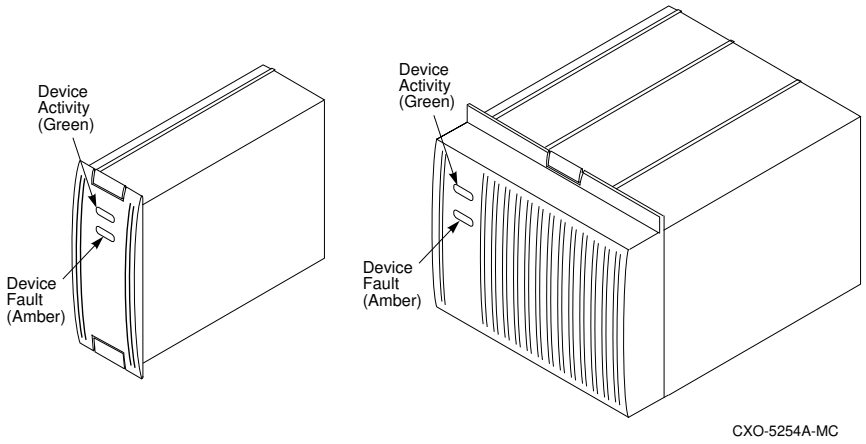
4. Repeat the above steps to add a second power supply for redundancy. After connecting the power cord, observe the status indicators and ensure that they are both on.

Installing storage building blocks

The storage device building blocks (SBBs) are in 3 1/2 inch or 5 1/4 inch form factors. The HSJ50 controller supports the following devices:

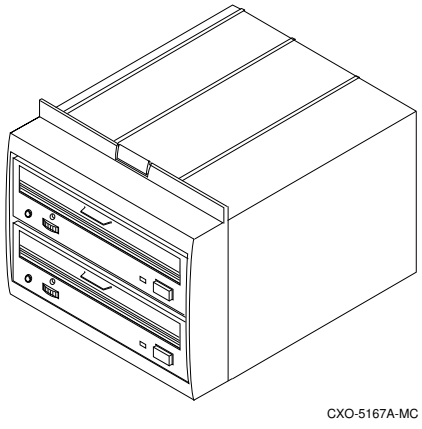
- 3.5-inch and 5.25-inch disk drives

Figure 63
Typical 3.5-inch and 5.25-inch disk drive or optical disk SBBs



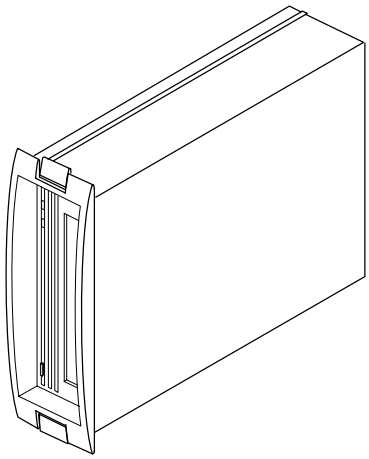
- CD ROM drives in 5 1/4 inch Storage Works building blocks

Figure 64
Typical 5.25-inch CD ROM SBB



- Solid state disks and tape drives

Figure 65
Typical 3.5-inch tape drive SBB



CXO-5168A-MC

Caution

Do not install solid state disk and CD-ROM drives when power is applied to the shelf.

SBB activity and status indicators

Most storage device have two LEDs that display SBB status. These LEDs have three states: on, off, and flashing.

The upper LED (green) is the device activity indicator and is on or flashing when the SBB is active.

The lower LED (amber) is the device status indicator and indicates an error condition or a configuration problem when it is on or flashing (see Table 35).

Table 35
Storage SBB Status Indicators

LED	Status	Indication
Device activity Device fault	■ □	SBB is operating normally.
Device activity Device fault	▒ □	SBB is operating normally.
Device activity Device fault	□ □	SBB is operating normally. The SBB is inactive, and there is no fault.

LED	Status	Indication
Device activity	■	Fault status SBB is probably not responding to control signals.
Device fault	■	Replace the SBB.
Device activity	□	Fault status SBB is inactive and spun down.
Device fault	■	Replace the SBB.
Device activity	■	Fault status SBB is active and is spinning down because of a fault
Device fault	▭	
Device activity	□	Fault status SBB has been identified by the controller as failed.
Device fault	▭	Replace the SBB.

LED on = ■
LED off = □
LED flashing = ▭

When using the LOCATE command, the lower LED is used to locate or identify units, storagesets, and devices in a cabinet.

For example:

To locate or identify device DISK100, enter:

```
CLI> LOCATE DISK100
```

The lower LED (amber) of DISK100 will flash a rate of once every second. To turn off the lower LED use the LOCATE CANCEL command.

Note

If a device has been placed into a failedset, the lower LED will flash at a rapid rate. In this case, the LOCATE command cannot identify the device.

The lower LED of each configured device can be tested using the LOCATE command with the ALL qualifier.

For example:

To test the fault LED of each configured device, enter:

```
CLI> LOCATE ALL
```

The lower LED of each configured device will flash at rate of once every second. To turn off the lower LED use the LOCATE CANCEL command.

Refer to the *CLI Reference Manual* for further details of the LOCATE command.

Asynchronous device installation

The controller supports asynchronous device swapping on the device bus. Asynchronous swapping is defined as removal or insertion of a device while the controller is running, without halting bus activity using port quiesce buttons or CLI commands.

Asynchronous device swapping is supported on the HSJ50 controller subject to the following restrictions:

- Asynchronous device swapping is not supported during failover.
- Asynchronous device swapping is not supported during failback.
- Asynchronous device swapping is not supported from the time the controller is initialized, until the CLI prompt appears.
- Asynchronous device swapping is not supported if the controller is in the process of recognizing or processing one or more asynchronous device removals.

- Asynchronous device swapping is not supported while local programs such as DILX or VTDPY are running.

Installing SBBs

Use the following procedure to install SBBs.

1. Insert the SBB into the shelf guide slots and push it in until it is fully seated and the mounting tabs engage the shelf.
2. Observe the activity indicator (upper LED) and the status indicator (lower LED). The activity indicator is either on, flashing, or off. The status indicator is off.

Installing a solid state disk CD-ROM and optical drives

Use the following procedure to install a solid state disk, CD-ROM and optical drives. To install the device, power must be removed from the shelf.

1. Halt all I/O activity using the appropriate procedures for your operating system.
2. Connect a maintenance terminal to one of the controllers.
3. At the CLI prompt, enter:

```
CLI> SHUTDOWN OTHER_CONTROLLER
CLI> SHUTDOWN THIS_CONTROLLER
```

4. To ensure that the controller has shut down cleanly, check for the following indications on the controller's OPC (operator control panel).
   - The Reset (//) light is on continuously.
   - Port lights 1, 2, 3, are also on continuously.
5. Remove the power cords from the shelf power supplies in which you will install the solid state drive.

6. Insert the device into the shelf.
7. Reconnect the power cord to the shelf power supply.
8. Reinitialize the controllers by pressing the Reset (//) button on both controllers.
9. Observe the status indicators for the following conditions:
10. Ensure that the amber status indicator is off.

4 Moving storagesets and devices

Moving storagesets

Moving storageset members

Moving single disk-drive units

Moving devices

Precautions

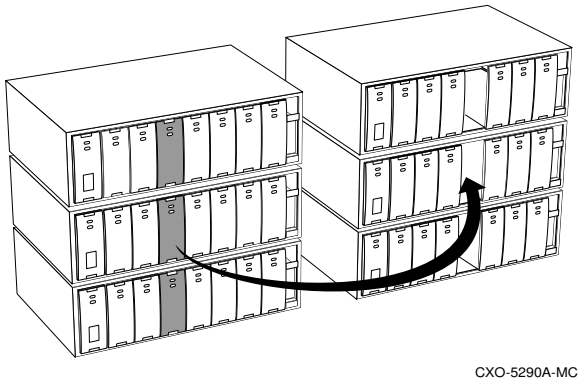
If you're moving a storageset or device that contains data you want to keep:

- Make sure that the controller is functioning properly—its green LED should be flashing on and off about one time per second.
- Exit any local programs that you may be running, such as CSWAP, CFMENU, or CHVSN.
- Wait until the CLI prompt appears on your local or remote terminal before inserting or removing any device.
- Wait about one minute after inserting each device before you insert another.
- Don't insert or remove a device during failover or failback.

Moving storagesets

You can move a storageset from one subsystem to another without destroying its data. You can also follow these steps to move a storageset to a new location within the same subsystem.

Figure 66
Moving a storageset from one subsystem to another



To move a storageset while maintaining the data it contains:

1. Show the details for the storageset that you want to move.

   CLI> **SHOW *storageset-name***

2. Label each member with its name and PTL location. (If you don't have a storageset map for your subsystem, you can LOCATE each member to find its PTL location.)

   CLI> **LOCATE *disk-name***

   To cancel the locate command:

   CLI> **LOCATE CANCEL**

3. Delete the unit-number shown in the "Used by" column of the SHOW *storageset-name* command.

   CLI> **DELETE *unit-number***

4. Delete the storageset shown in the "Name" column of the SHOW *storageset-name* command.

   CLI> **DELETE *storageset-name***

5. Delete each disk drive—one at a time—that was contained by the storageset.

```
CLI> DELETE disk-name
CLI> DELETE disk-name
CLI> DELETE disk-name
```

6. Remove the disk drives and move them to their new PTL locations.

7. Re-add each disk drive to the controller's list of valid devices.

```
CLI> ADD DISK disk-name PTL-location
CLI> ADD DISK disk-name PTL-location
CLI> ADD DISK disk-name PTL-location
```

8. Re-create the storageset by adding it's name to the controller's list of valid storagesets and specifying the disk drives it contains. (Although you have to re-create the storageset from its original disks, you don't have to add them in their original order.)

```
CLI> ADD STORAGESET storageset-name disk-name disk-name
disk-name
```

9. Re-present the storageset to the host by giving it a unit number that the host can recognize. You can use the original unit number or create a new one.

```
CLI> ADD UNIT unit-number storageset-name
```

For example

The following example moves unit D100 to another cabinet. D100 is the RAIDset "RAID99" that comprises members 200, 300, and 400.

```
CLI> SHOW Raid99

Name     Storageset        Uses        Used by
-------------------------------------------
RAID99    raidset          disk100     D100
                           disk200
                           disk300
CLI> DELETE D100
CLI> DELETE RAID99
CLI> DELETE DISK200 DISK300 DISK400
```

(...move the disk drives to their new location...)

```
CLI> ADD DISK DISK200 2 0 0
CLI> ADD DISK DISK300 3 0 0
CLI> ADD DISK DISK400 4 0 0
CLI> ADD RAIDSET RAID99 DISK200 DISK300 DISK400
CLI> ADD UNIT D100 RAID99
```

For example

The following example moves the reduced RAIDset, "R3," to another cabinet. (R3 used to contain disk200, which failed before the RAIDset was moved. At the beginning of this example, it contains disk100, disk300, and disk400.)

```
CLI> DELETE D100
CLI> DELETE R3
CLI> DELETE DISK100 DISK300 DISK400
```

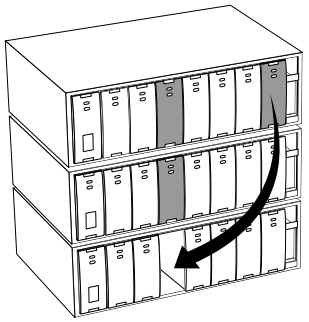
(...move disk drives to their new location...)

```
CLI> ADD DISK DISK100 1 0 0
CLI> ADD DISK DISK300 3 0 0
CLI> ADD DISK DISK400 4 0 0
CLI> ADD RAIDSET R3 DISK100 DISK300 DISK400 REDUCED
CLI> ADD UNIT D100 R3
```

Moving storageset members

You may want to move a storageset member—and its data—from one PTL location to another to maintain the symmetry in your subsystem. For example, if a RAIDset member fails and is replaced by a disk drive in the spareset, you could move the replacement member into the column that contains the RAIDset.

Figure 67 Maintaining symmetry in your subsystem makes it easier to keep track of your storagesets and their members



CXO-5291A-MC

To move a storageset member while maintaining the data it contains:

1. Delete the unit-number of the storageset that contains the disk drive you want to move.

   ```
   CLI> DELETE unit-number
   ```

2. Delete the storagesest that contains the disk drive you want to move.

   ```
   CLI> DELETE storageset-name
   ```

3. Delete each disk drive—one at a time—that was contained by the storageset.

   ```
   CLI> DELETE disk-name_1
   CLI> DELETE disk-name_2
   CLI> DELETE disk-name_n
   ```

4. Move the desired disk drive to its new PTL location.

5. Re-add each member to the controller's list of valid devices.

```
CLI> ADD DISK disk-name PTL-location
CLI> ADD DISK disk-name PTL-location
CLI> ADD DISK disk-name PTL-location
```

6. Re-create the storageset by adding it's name to the controller's list of valid storagesets and specifying the disk drives it contains. (Although you have to re-create the storageset from its original members, you don't have to add them in their original order.)

```
CLI> ADD STORAGESET storageset-name disk_1 disk_n
```

7. Re-present the storageset to the host by giving it a unit number that the host can recognize. You can use the original unit number or create a new one.

```
CLI> ADD UNIT unit-number storageset-name
```

For example

The following example moves disk210 to PTL location 300. (Its new name will be disk300 to correspond to its new PTL location.) Disk210 was a spare that was pulled into unit D100 when its disk300 failed. (D100 is the RAIDset "RAID99" that comprises members 200, 210, and 400.)

```
CLI> DELETE D100
CLI> DELETE RAID99
CLI> DELETE DISK210
```

(...move disk210 to PTL location 300...)

```
CLI> ADD DISK DISK300 3 0 0
CLI> ADD RAIDSET RAID99 DISK200 DISK300 DISK400
CLI> ADD UNIT D100 RAID99
```

Moving a single disk-drive unit

You can move a single disk-drive unit from one subsystem to another without destroying its data. You can also use the procedure given below to move a unit to a new location within the same subsystem.

To move a single disk-drive unit while maintaining the data it contains:

1. Show the details for the unit that you want to move.

   ```
   CLI> SHOW unit-number
   ```

2. Delete the unit-number shown in the "Used by" column of the SHOW *unit-number* command.

   ```
   CLI> DELETE unit-number
   ```

3. Delete the disk drive.

   ```
   CLI> DELETE disk-name
   ```

4. Remove the disk drive and move it to its new PTL location.

5. If you're moving disk drives from an HSC subsystem, run CHVSN to generate a unique volume serial number for each disk, otherwise skip this step.

   ```
   CLI> RUN CHVSN
   Device (port target lun) [EXIT] ? PTL-location
   CHVSN: Volume Serial Number is 00000000 00000000
   Update CHVSN (Y/N) ? Y
   ```

   HSC controllers accept duplicate volume serial numbers, whereas «Model» controllers do not. If CHVSN reports a volume serial number of zero for a disk drive, press "Y" when prompted to "Update CHVSN."

6. Re-add the disk drive to the controller's list of valid devices.

   ```
   CLI> ADD DISK disk-name PTL-location
   ```

7. Re-present the disk drive to the host by giving it a unit number that the host can recognize. You can use the original unit number or create a new one.

```
CLI> ADD UNIT unit-number disk-name
```

For example

The following example moves Disk507 to PTL location 100. (Its new name will be Disk100 to correspond to its new PTL location.)

```
CLI> Show D507
CLI> Delete D507
CLI> Delete Disk100
CLI> Add Disk100 1 0 0
CLI> Add D507 Disk100
```

Moving devices

Follow these steps to move a device, such as a disk drive, tape drive, CDROM drive, or tape loader:

1. Quiesce the bus that services the device you want to move.
2. Show the details for the device that you want to move. (If you're moving a tape loader, show the details for the passthrough device that's associated with it.)

   ```
   CLI> SHOW device-name
   ```

3. If the device has a unit number associated with it, delete the unit-number that's shown in the "Used by" column.

   ```
   CLI> DELETE unit-number
   ```

4. Delete the device name shown in the "Name" column.

   ```
   CLI> DELETE device-name
   ```

5. Remove the device and move it to its new PTL location.
6. Re-add the device to the controller's list of valid devices.

   ```
   CLI> ADD DEVICE device-name PTL-location
   ```

7. If you're moving a tape loader, re-create the passthrough device that represents the loader.

   ```
   CLI> ADD PASSTHROUGH passthrough_name PTL-location
   ```

8. Re-present the device to the host by giving it a unit number that the host can recognize. You can use the original unit number or create a new one.

   ```
   CLI> ADD UNIT unit-number device-name
   ```

9. You might have to reconfigure the host-based software that controls the loader. Refer to the documentation that accompanied the loader and its software.

For example

The following example moves TAPE100 (unit T108) from PTL 1 0 0 to PTL 6 0 0.

```
CLI> SHOW tape100

NAME TypePort TargLunUsed by
-------------------------------------------------
TAPE100tape100T108

CLI> DELETE T108
CLI> DELETE TAPE100
```

(...move tape100 to its new location...)

```
CLI> ADD TAPE TAPE600 6 0 0
CLI> ADD UNIT T600 TAPE600
```

The following example moves tape LOADER120 from p3 to p1:

```
CLI> SHOW PASSTHROUGH LOADER

NAME       Type                Port   TargLunUsed by
-------------------------------------------------
LOADER120  passthrough loader     4      2  0  P3
TAPE430    passthrough tape       4      3  0  P0


CLI> DELETE P3
CLI> DELETE P0
CLI> DELETE TAPE430

(...move passthrough loader120 to new location)

CLI> ADD PASSTHROUGH LOADER120 1 2 0
CLI> ADD UNIT P0 TAPE430
CLI> ADD UNIT P3 LOADER LOADER 120
```

5 Removing

Removing a patch

Disabling a licensed option

Removing a license key

Removing a controller and cache module

Removing storage devices

Precautions

Some of the procedures in this chapter involve handling program cards, controller modules and cache modules. Use the following guidelines to prevent component damage while servicing subsystem modules.

- After removing a controller or cache module from the shelf, place the module into an approved antistatic bag or onto a grounded antistatic mat.
- Cover the program card with the snap-on ESD cover when the card is installed in the controller.
- Keep the program card in its original carrying case when not in use.
- Do not twist or bend the program card.
- Do not touch the program card contacts.

Removing a patch

Use the delete patch program to free memory space for patches that need to be added to the current software version. When patches are removed from controller memory, they will also be removed from storagesets that have been initialized with the INITIALIZE *container name* SAVE CONFIGURATION command.

The version numbers and patch numbers in this procedure are only examples. The Patch Code program will not allow you enter any of these numbers used in these examples.

Required tools

The tools listed in Table 36 are required for removing a patch:

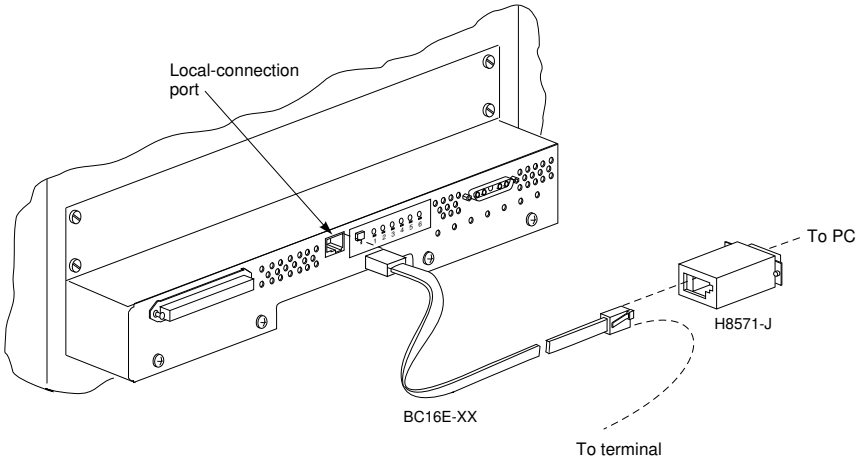
Table 36
Required tools

Required tools	Purpose
Maintenance terminal	To start the CLCP utility
5/32-inch Allen wrench	To unlock the SW800 cabinet

To remove a patch:

1. Connect a maintenance terminal to one of the controllers (see Figure 68).

Figure 68
Connecting a maintenance terminal to the controller



2. Start the CLCP utility:

```
CLI> RUN CLCP
```

The CLCP main menu is displayed.

```
Select an option from the following list:

Code Load & Code Patch Utility Main Menu

0: Exit
1: Enter Code LOAD utility
2: Enter Code PATCH utility
Enter option number  (0..2) [0] ?

This controller module does not support code load
functionality. Exiting CLCP
CLI>
```

3. Press **2** to select the code patch program.

The code patch menu is displayed.

```
You have selected the Code Patch local program. This
program is used to manage firmware code patches. Select
an option from the following list:

Type ^Y or ^C (then RETURN) at any time to abort Code
Patch.
Code Patch Main Menu

0: Exit
1: Enter a Patch
2: Delete Patches
3: List Patches
Enter option number (0..3) [0] ?
```

4. Select option **2** to delete a patch.

```
This is the Delete Patches option. The program prompts
you for the firmware version and patch number you wish
to delete. If you select a patch for deletion that is
required for an other patch, all dependent patches are
also selected for deletion. The program lists your
deletion selections and asks if you wish to continue.

Type ^Y or ^C (then RETURN) at any time to abort Code
Patch.

The following patches are currently stored in the patch
area:

Firmware Version - Patch number(s)

     V123               1,2
     V456               1

Currently 90% of the patch area is free.

Firmware Version of patch to delete?
```

5. Enter the firmware version **V456**

6. Patch Number to delete?

```
The following patches have been selected for deletion:

Firmware Version - Patch number(s)

    V456               1

Do you wish to continue (y/n) [y]  ?
```

7. Press **Y** to continue.

```
The patch you have just deleted is currently applied,
but will not be applied when the controller is
restarted.

Code Patch Main Men

0: Exit
1: Enter a Patch
2: Delete Patches
3: List Patches

Enter option number (0..3) [0]  ?

The following patches are currently stored in the patch
area:

Firmware Version - Patch number(s)
```

```
V123                1,2
Currently, 95% of the patch area is free.
```

Disabling a licensed option

Once you have tested a licensed option and have decided not to purchase a valid license key, you need to disable this option. You cannot disable an option if that option is currently in use. Table 37 lists the conditions under which you can disable an FLS option.

Table 37
Disabling FLS options

Option	Condition required to disable
RAID	No RAIDsets configured
WBCA	Write-back caching not in use on any unit
MIRR	No mirrorsets configured

Required tools

The tools listed in Table 38 are required for disabling a licensed option:

Table 38
Required tools

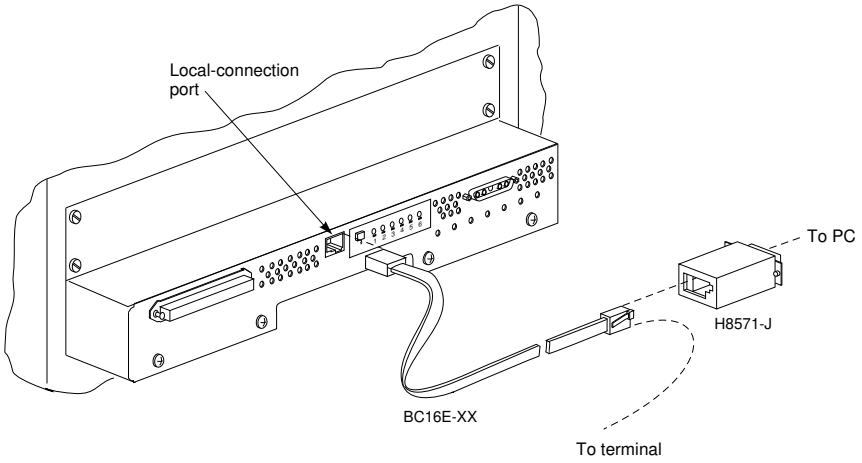
Required tools	Purpose
Maintenance terminal	To start the FLS utility
5/32-inch Allen wrench	To unlock the SW800 cabinet

To disable a licensed option:

Use the following procedure to disable a licensed option. In the following example, the MIRR (disk mirroring option) option is disabled.

1. Connect a maintenance terminal to one of the controllers (see Figure 68).

Figure 69
Connecting a maintenance terminal to the controller



2. Start the FLS utility:

```
CLI> RUN FLS
```

The FLS Main menu and all enabled options are displayed.

```
Firmware Licensing System (FLS) on node MASS
Option      State       License          Key
-------------------------------------------------
RAID      DISABLED      INVALID         *none*
WBCA      DISABLED      INVALID         *none*
MIRR      ENABLED       INVALID         *none*

               RAID = RAID Option
               WBCA = Writeback Cache Option
               MIRR = Disk Mirroring Option
-------------------------------------------------
1. Enable a firmware option
2. Disable a firmware option
3. Enter a license key for a firmware option
4. Clear a license key for a firmware option
0. Exit FLS
Enter selection (0:4) [0] ?
```

3. Press **2** to select the disable firmware option. All of the license option are displayed.

```
1. Disable RAID  (already disabled)
2. Disable WBCA  (already disabled)
3. Disable MIRR
0. Return to main menu

Enter selection (0:4)  {0}  ?
```

4. Press **3** to disable the MIRR firmware option.

Note

The warning at the top of the FLS main menu is displayed only if there is a dual-redundant controller in the subsystem with the same license enabled.

```
***Warning: other controller's MIRR option is enabled
at this time.***

-------------------------------------------------------
Firmware Licensing System (FLS) on node MASS
Option      State        License        Key
-------------------------------------------------------
RAID      DISABLED       INVALID      * none *
WBCA      DISABLED       INVALID      * none *
MIRR      DISABLED       INVALID      * none *

              RAID = RAID Option
              WBCA = Writeback Cache Option
              MIRR = Disk Mirroring Option
-------------------------------------------------------

    1.  Enable a firmware option
    2.  Disable a firmware option
    3.  Enter a license key for a firmware option
    4.  Clear a license key for a firmware option
    0.  Exit FLS
Enter selection (0:4) [0] ?
```

Notice that the MIRR option is disabled.

Press **0** to exit the FLS utility.

Removing a license key

You may wish to move a specific license key to a different controller. Use the following procedure to remove a license key.

Required tools

The tools listed in Table 39 are required for removing a license key.

Table 39
Required tools

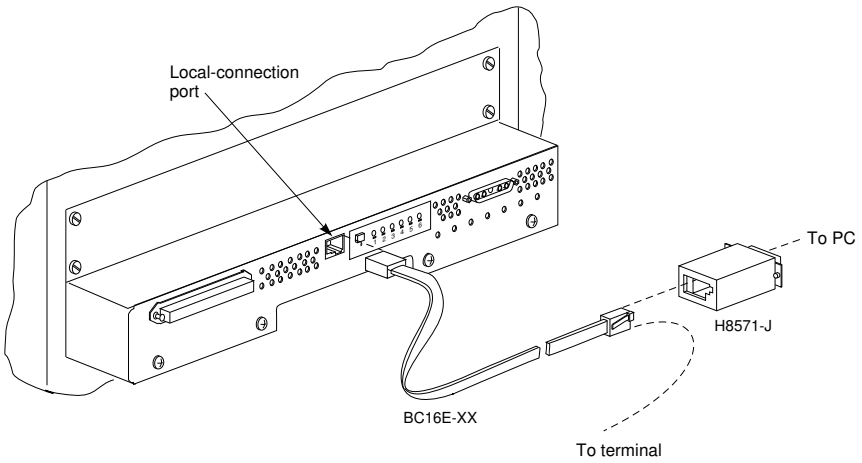
Required tools	Purpose
Maintenance Terminal	To start the FLS utility
5/32-inch Allen wrench	To unlock the SW800 cabinet

To remove a license key:

In this example the license key for MIRR option is removed.

1. Connect a maintenance terminal to controller that has the valid license key installed (see Figure 70).

Figure 70
Connecting a maintenance terminal to the controller



2. Start the FLS utility:

```
CLI>RUN FLS
```

The FLS main menu is displayed.

```
------------------------------------------------------
Firmware Licensing System (FLS) on node MASS
Option      State        License        Key
------------------------------------------------------
RAID      ENABLED        VALID    * ACME WIDGIT CO
WBCA      ENABLED        VALID    * ACME WIDGIT CO
MIRR      ENABLED        VALID    * ACME WIDGIT CO

             RAID = RAID Option
             WBCA = Writeback Cache Option
             MIRR = Disk Mirroring Option
------------------------------------------------------

1. Enable a firmware option
2. Disable a firmware option
3. Enter a license key for a firmware option
4. Clear a license key for a firmware option
0. Exit FLS
Enter selection (0:4) [0] ?
```

3. Press **4** to select the clear a license key option.

The program is showing all valid license keys that may be cleared.

```
1. Clear license key for RAID (current key is valid)
2. Clear license key for WBCA (current key is valid)
3. Cleat license key for MIRR (current key is valid)
0 Return to main menu

Enter selection (0..3)  [0]  ?
*CAUTION*  You are about to erase a valid license key
Continue (y/n {n} ?
```

4. Press **3** to clear the license key for the MIRR option.

   The FLS utility main menu is displayed.

```
-----------------------------------------------------
Firmware Licensing System (FLS) on node MASS
Option      State        License        Key
-----------------------------------------------------
RAID      ENABLED        VALID    * ACME WIDGIT CO *
WBCA      ENABLED        VALID    * ACME WIDGIT CO *
MIRR      DISABLED      INVALID        *none*

              RAID = RAID Option
              WBCA = Writeback Cache Option
              MIRR = Disk Mirroring Option
-----------------------------------------------------

    1.  Enable a firmware option
    2.  Disable a firmware option
    3.  Enter a license key for a firmware option
    4.  Clear a license key for a firmware option
    0.  Exit FLS
Enter selection (0:4) [0] ?
```

Notice that the license key for the MIRR option is cleared.

Removing a controller and cache module

A controller and a cache module may be removed so they it can be used in another subsystem.

Required tools

The tools listed in Table 40 are required for removing a controller.

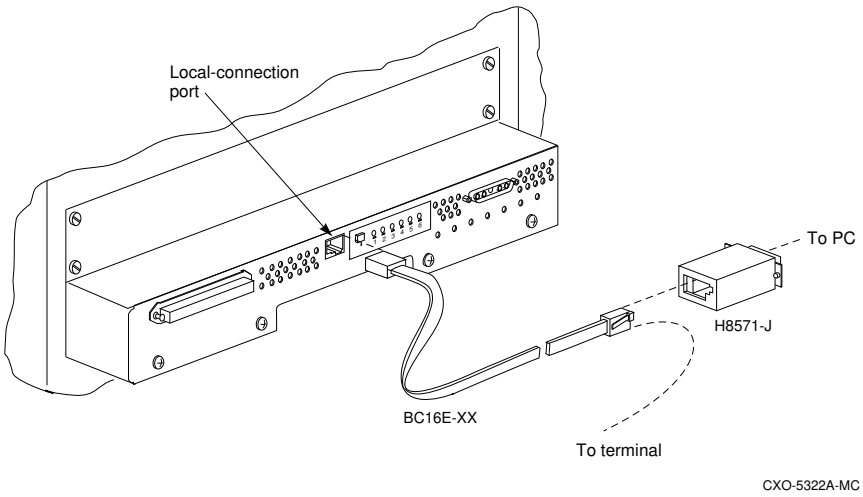
Table 40
Required tools

Required tools	Purpose
Maintenance terminal	To shutdown controllers.
Small flat-head screwdriver	To loosen captive screws
ESD wrist strap	To protect all equipment against electrostatic discharge
5/32-inch Allen wrench	To unlock the SW800 series cabinet

To remove a controller and its cache module:

1. Connect a maintenance terminal to the controller to be removed (see Figure 71).

Figure 71
Connecting a maintenance terminal to the controller



2. Take the controller to be removed out of service:

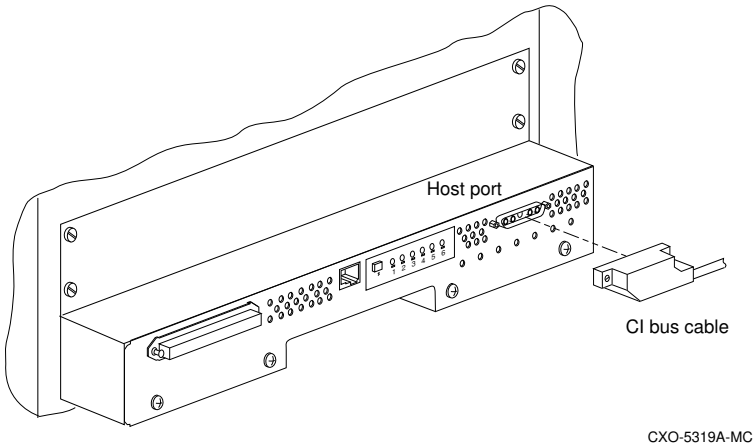
   CLI **> SHUTDOWN THIS_CONTROLLER**

3. Ensure that the controller has shutdown cleanly. Check for the following indications on the controller's OCP (operator control panel).

   - The Reset (//) light is on.
   - Port lights 1, 2, 3 are continuously lit.

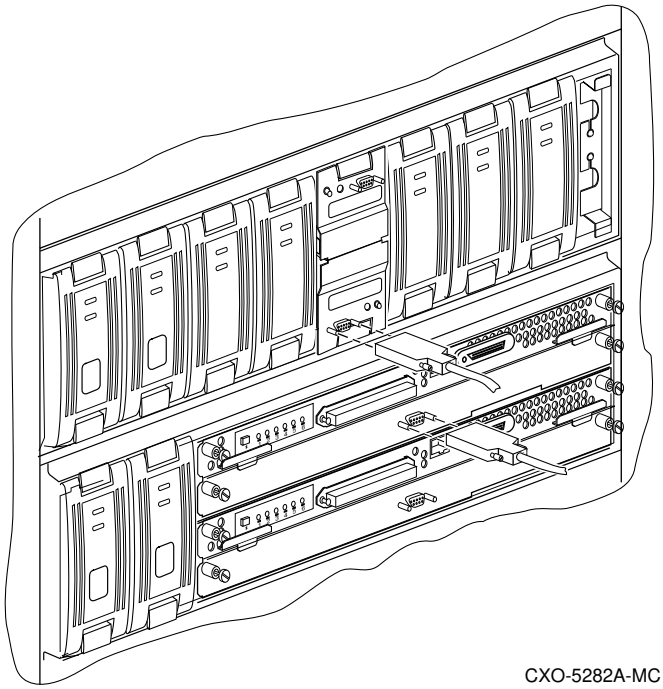
4. With a small flat-head screwdriver, loosen the captive screws that secure the CI cable to the controller (see Figure 72).

Figure 72
Disconnecting the CI cable connector



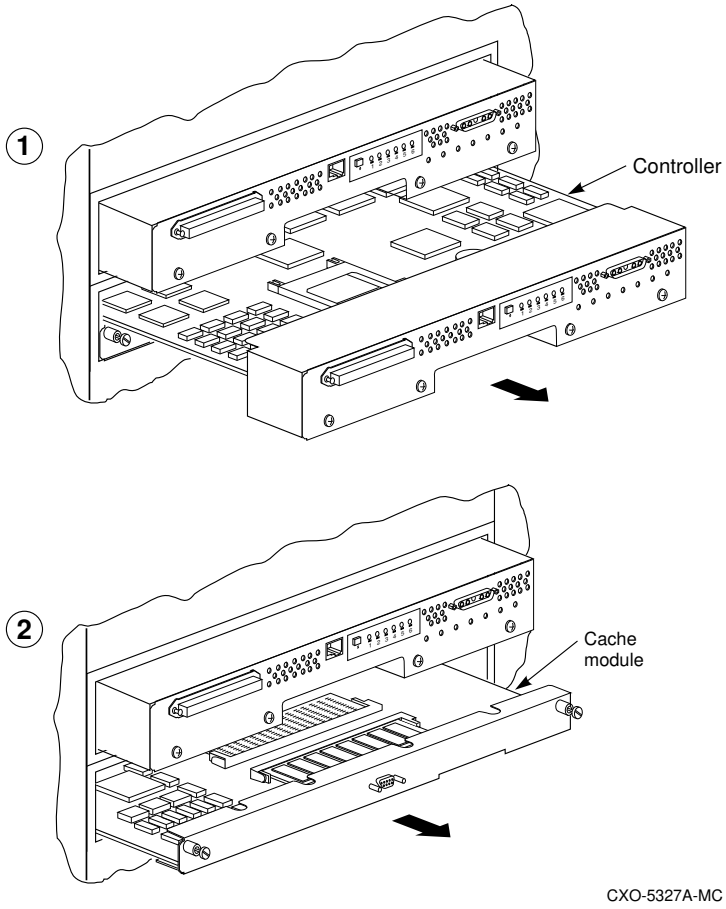
5. Remove the CI cable from the controller's front bezel.
6. Disconnect the ECB cables (see Figure 73).

Figure 73
Removing the ECB cables



7. Loosen the captive screws on the controller and cache module's front bezel.
8. Obtain and place an ESD wrist strap around your wrist. Ensure that the strap fits snugly around your wrist.
9. Attach the other end of the ESD strap to the cabinet grounding stud or a convenient cabinet grounding point (non-painted surface).
10. Slide the controller out of the shelf (see Figure 74) and place it in an ESD bag.

Figure 74
Removing the controller and cache module



11. If required, slide the cache module out of the shelf (see Figure 74) and place it in an ESD bag.

12. Remove the ECB and store it with the cache module.

Removing storage devices

Remove storage devices so they can be used in other subsystems.

Removing disk drives

Disk drives may be removed without having to quiesce the device bus or remove power from the shelf with the following restrictions:

- Do not remove devices during failover.
- Do not remove devices during failback.
- Do not remove devices before the CLI prompt appears during controller initialization.
- Do not remove devices while the controller is running a local program such as DILX or VTDPY.

Required tools

The tools listed in Table 41 are required for removing SBBs.

Table 41
Required tools

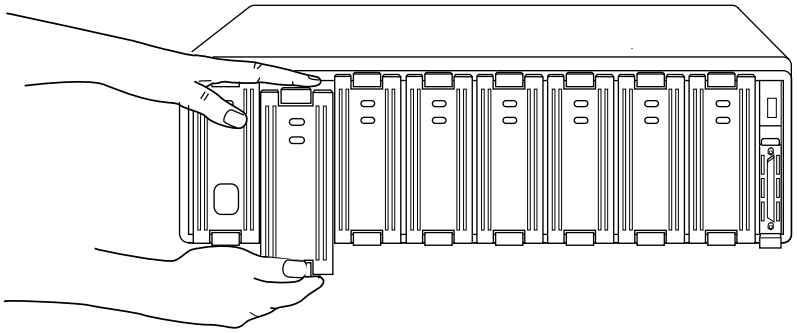
Required tools	Purpose
5/32-inch Allen wrench	To unlock the SW800 series cabinet

To remove storage devices:

Use the following procedure to remove 3 1/2 - inch and 5 1/4 - inch disk drives

1. Determine the disk drive you wish to remove.
2. Press the two mounting tabs together to release the disk drive from the shelf and partially pull the disk drive out of the shelf. Allow the disk drive to spin down.

Figure 75
Removing a 3.5-inch disk drive



CXO-4439A-MC

3. Using both hands, slide the disk drive out of the shelf and place it on flat surface (see Figure 75).

Removing solid state disks, read/write optical devices and CD-ROM drives

When removing solid state disk drives or read/write optical devices, the controller needs to be shutdown and power must be removed from the device shelf.

Required tools

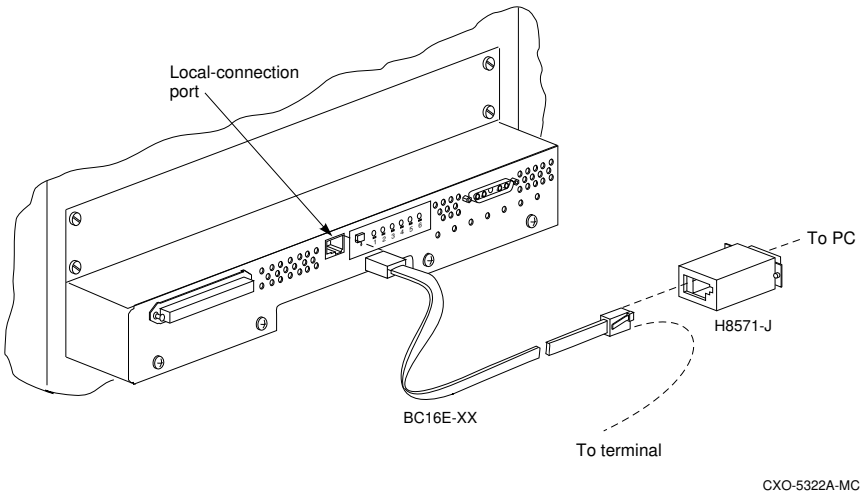
The tools listed in Table 42 are required for removing solid state disk drives, tape drives CD-ROM readers and optical devices.

Table 42
Required tools

Required tools	Purpose
Maintenance terminal	To shut down the controller
5/32-inch Allen wrench	To unlock the SW800 series cabinet

1. Connect a maintenance terminal to the controller (see Figure 76).

Figure 76
Connecting a maintenance terminal to the controller



2. Halt all host I/O activity using the appropriate procedures for your operating system.
3. Take the controllers out of service:

```
CLI> SHUTDOWN OTHER_CONTROLLER
CLI> SHUTDOWN OTHER_CONTROLLER
```

4. Remove the power cords from the shelf power supplies.
5. Remove the device by pressing the two mounting tabs together to release it from the shelf. Using both hands, remove the device from the shelf.
6. Restart the system.

Removing tape drives

Use the following procedure to remove tape drives.

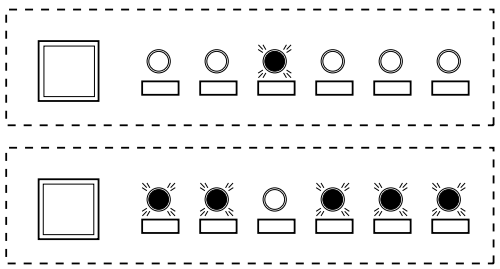
Required tools

The tools listed in Table 43 are required for removing tape drives.

Table 43
Required tools

Required tools	Purpose
5/32-inch Allen wrench	To unlock the SW800 series cabinet

1. Halt all I/O activity to the tape drive using the appropriate procedures for your operating system.
2. Quiesce the appropriate device port by pushing the device port button on the controller's OCP (operator control panel).
3. When the OCP LEDs flash in an alternating pattern the device port is quiesced. For example when you quiesce device port 3 and I/O has halted, the OCP LEDs are flashing in an alternating pattern as shown below:



CXO-4824A-MC

4. When the port has quiesced, remove the tape drive by pressing the two mounting tabs together to release it from the shelf.
5. Using both hands, pull the tape drive out of the device shelf.

Appendix

Instance codes

Last failure codes

Repair action codes

Instance codes and definitions

The following table contains instance codes and their definitions. Use these tables to identify instance code definitions and the suggested repair action. *Repair action codes* on page 329 contains the repair action codes and actions.

Table 44
Instance codes

Instance Code	Explanation	Repair Action Code
01010302	An unrecoverable hardware detected fault occurred.	03
0102030A	An unrecoverable firmware inconsistency was detected or an intentional restart or shutdown of controller operation was requested.	03
01032002	Nonvolatile parameter memory component EDC check failed. The content of the component was reset to default settings.	20
0121370A	Memory System Error Analysis is indicated in the information preserved during a previous last failure but no error conditions are indicated in the available DRAB registers. The Master DRAB registers content is supplied.	37
0122330A	An error condition detected by one of the CACHE DRABs that requires supplemental information has been reported in another event report. This event report contains the Master DRAB and Diagnostic registers content associated with that initial event report.	33
01292602	The Master DRAB detected a Cache Time-out condition during an access attempt to a CACHEA0, CACHEA1, CACHEB0, or CACHEB1 DRAB registers region or memory region. The addressed region failed to respond.	26
012A3702	The CACHEA0 DRAB unexpectedly reported a Cache Time-out condition.	37
012B3702	The CACHEA1 DRAB unexpectedly reported a Cache Time-out condition.	37
012C3702	The CACHEB0 DRAB unexpectedly reported a Cache Time-out condition.	37
012D3702	The CACHEB1 DRAB unexpectedly reported a Cache Time-out condition.	37
012E2702	The Master DRAB detected an Nbus Transfer Error Acknowledge (TEA) condition. This means the TEA signal was asserted by an Nbus device during an I960 to Nbus device transaction.	37
012F3702	The Master DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	37
01303702	The CACHEA0 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	37

Instance Code	Explanation	Repair Action Code
01313702	The CACHEA1 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	37
01323702	The CACHEB0 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	37
01333702	The CACHEB1 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	37
01342802	A Multiple Bit ECC error was detected during a memory refresh attempt by the Master DRAB.	28
01352902	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEA0 DRAB.	29
01362902	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEA1 DRAB.	29
01372A02	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEB0 DRAB.	2A
01382A02	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEB1 DRAB.	2A
01392802	The Master DRAB detected a Multiple Bit ECC error during an FX attempt to read buffer memory.	28
013A2802	The Master DRAB detected a Multiple Bit ECC error during a Host Port attempt to read buffer memory.	28
013B2802	The Master DRAB detected a Multiple Bit ECC error during a Device Port attempt to read buffer memory.	28
013C2802	The Master DRAB detected a Multiple Bit ECC error during an I960 attempt to read buffer memory.	28
013D2902	The CACHEA0 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEA0 memory.	29
013E2902	The CACHEA0 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEA0 memory.	29
013F2902	The CACHEA0 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEA0 memory.	29
01402902	The CACHEA0 DRAB detected a Multiple Bit ECC error during an I960 attempt to read CACHEA0 memory.	29
01412902	The CACHEA1 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEA1 memory.	29
01422902	The CACHEA1 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEA1 memory.	29
01432902	The CACHEA1 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEA1 memory.	29
01442902	The CACHEA1 DRAB detected a Multiple Bit ECC error during an I960 attempt to read CACHEA1 memory.	29
01452A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEB0 memory.	2A

Instance Code	Explanation	Repair Action Code
01462A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEB0 memory.	2A
01472A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEB0 memory.	2A
01482A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during an I960 attempt to read CACHEB0 memory.	2A
01492A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEB1 memory.	2A
014A2A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEB1 memory.	2A
014B2A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEB1 memory.	2A
014C2A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during an I960 attempt to read CACHEB1 memory.	2A
014D3702	The Master DRAB unexpectedly reported a Multiple Bit ECC error.	37
014E3702	The CACHEA0 DRAB unexpectedly reported a Multiple Bit ECC error.	37
014F3702	The CACHEA1 DRAB unexpectedly reported a Multiple Bit ECC error.	37
01503702	The CACHEB0 DRAB unexpectedly reported a Multiple Bit ECC error.	37
01513702	The CACHEB1 DRAB unexpectedly reported a Multiple Bit ECC error.	37
01522B02	The Master DRAB detected an Ibus to Nbus Time-out condition during an I960 to Nbus device transaction. The Nbus device failed to respond.	2B
01533702	The CACHEA0 DRAB unexpectedly reported an Ibus to Nbus Time-out condition.	37
01543702	The CACHEA1 DRAB unexpectedly reported an Ibus to Nbus Time-out condition.	37
01553702	The CACHEB0 DRAB unexpectedly reported an Ibus to Nbus Time-out condition.	37
01563702	The CACHEB1 DRAB unexpectedly reported an Ibus to Nbus Time-out condition.	37
01572C02	The Master DRAB detected a Nonexistent Memory Error condition during an FX attempt to write buffer memory.	2C
01582C02	The Master DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to buffer memory.	2C
01592C02	The Master DRAB detected a Nonexistent Memory Error condition during an FX attempt to read buffer memory.	2C

Instance Code	Explanation	Repair Action Code
015A2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write buffer memory.	2C
015B2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to buffer memory.	2C
015C2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read buffer memory.	2C
015D2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write buffer memory.	2C
015E2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to buffer memory.	2C
015F2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read buffer memory.	2C
01602C02	The Master DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write buffer memory.	2C
01612C02	The Master DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write a byte to buffer memory.	2C
01622C02	The Master DRAB detected a Nonexistent Memory Error condition during an I960 attempt to read buffer memory.	2C
01632D02	The CACHEAO DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEAO memory.	2D
01642D02	The CACHEAO DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEAO memory.	2D
01652D02	The CACHEAO DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEAO memory.	2D
01662D02	The CACHEAO DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEAO memory.	2D
01672D02	The CACHEAO DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEAO memory.	2D
01682D02	The CACHEAO DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEAO memory.	2D
01692D02	The CACHEAO DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEAO memory.	2D

Instance Code	Explanation	Repair Action Code
016A2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEA0 memory.	2D
016B2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEA0 memory.	2D
016C2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write CACHEA0 memory.	2D
016D2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write a byte to CACHEA0 memory.	2D
016E2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to read CACHEA0 memory.	2D
016F2D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEA1 memory.	2D
01702D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEA1 memory.	2D
01712D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEA1 memory.	2D
01722D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEA1 memory.	2D
01732D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEA1 memory.	2D
01742D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEA1 memory.	2D
01752D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEA1 memory.	2D
01762D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEA1 memory.	2D
01772D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEA1 memory.	2D
01782D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write CACHEA1 memory.	2D

Instance Code	Explanation	Repair Action Code
01792D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write a byte to CACHEA1 memory.	2D
017A2D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to read CACHEA1 memory.	2D
017B2E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEBO memory.	2E
017C2E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEBO memory.	2E
017D2E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEBO memory.	2E
017E2E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEBO memory.	2E
017F2E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEBO memory.	2E
01802E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEBO memory.	2E
01812E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEBO memory.	2E
01822E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEBO memory.	2E
01832E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEBO memory.	2E
01842E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write CACHEBO memory.	2E
01852E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write a byte to CACHEBO memory.	2E
01862E02	The CACHEBO DRAB detected a Nonexistent Memory Error condition during an I960 attempt to read CACHEBO memory.	2E
01872E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEB1 memory.	2E

Instance Code	Explanation	Repair Action Code
01882E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEB1 memory.	2E
01892E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEB1 memory.	2E
018A2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEB1 memory.	2E
018B2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEB1 memory.	2E
018C2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEB1 memory.	2E
018D2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEB1 memory.	2E
018E2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEB1 memory.	2E
018F2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEB1 memory.	2E
01902E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write CACHEB1 memory.	2E
01912E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to write a byte to CACHEB1 memory.	2E
01922E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an I960 attempt to read CACHEB1 memory.	2E
01933702	The Master DRAB unexpectedly reported a Nonexistent Memory Error condition.	37
01943702	The CACHEA0 DRAB unexpectedly reported a Nonexistent Memory Error condition.	37
01953702	The CACHEA1 DRAB unexpectedly reported a Nonexistent Memory Error condition.	37
01963702	The CACHEB0 DRAB unexpectedly reported a Nonexistent Memory Error condition.	37
01973702	The CACHEB1 DRAB unexpectedly reported a Nonexistent Memory Error condition.	37
01982F02	An Address Parity error was detected during a memory refresh attempt by the Master DRAB.	2F

Instance Code	Explanation	Repair Action Code
01993002	An Address Parity error was detected during a memory refresh attempt by the CACHEA0 DRAB.	30
019A3002	An Address Parity error was detected during a memory refresh attempt by the CACHEA1 DRAB.	30
019B3102	An Address Parity error was detected during a memory refresh attempt by the CACHEB0 DRAB.	31
019C3102	An Address Parity error was detected during a memory refresh attempt by the CACHEB1 DRAB.	31
019D2F02	The Master DRAB detected an Address Parity error during an FX attempt to read buffer memory.	2F
019E2F02	The Master DRAB detected an Address Parity error during a Host Port attempt to read buffer memory.	2F
019F2F02	The Master DRAB detected an Address Parity error during a Device Port attempt to read buffer memory.	2F
01A02F02	The Master DRAB detected an Address Parity error during an I960 attempt to read buffer memory.	2F
01A13002	The CACHEA0 DRAB detected an Address Parity error during an FX attempt to read CACHEA0 memory.	30
01A23002	The CACHEA0 DRAB detected an Address Parity error during a Host Port attempt to read CACHEA0 memory.	30
01A33002	The CACHEA0 DRAB detected an Address Parity error during a Device Port attempt to read CACHEA0 memory.	30
01A43002	The CACHEA0 DRAB detected an Address Parity error during an I960 attempt to read CACHEA0 memory.	30
01A53002	The CACHEA1 DRAB detected an Address Parity error during an FX attempt to read CACHEA1 memory.	30
01A63002	The CACHEA1 DRAB detected an Address Parity error during a Host Port attempt to read CACHEA1 memory.	30
01A73002	The CACHEA1 DRAB detected an Address Parity error during a Device Port attempt to read CACHEA1 memory.	30
01A83002	The CACHEA1 DRAB detected an Address Parity error during an I960 attempt to read CACHEA1 memory.	30
01A93102	The CACHEB0 DRAB detected an Address Parity error during an FX attempt to read CACHEB0 memory.	31
01AA3102	The CACHEB0 DRAB detected an Address Parity error during a Host Port attempt to read CACHEB0 memory.	31
01AB3102	The CACHEB0 DRAB detected an Address Parity error during a Device Port attempt to read CACHEB0 memory.	31
01AC3102	The CACHEB0 DRAB detected an Address Parity error during an I960 attempt to read CACHEB0 memory.	31
01AD3102	The CACHEB1 DRAB detected an Address Parity error during an FX attempt to read CACHEB1 memory.	31

Instance Code	Explanation	Repair Action Code
01AE3102	The CACHEB1 DRAB detected an Address Parity error during a Host Port attempt to read CACHEB1 memory.	31
01AF3102	The CACHEB1 DRAB detected an Address Parity error during a Device Port attempt to read CACHEB1 memory.	31
01B03102	The CACHEB1 DRAB detected an Address Parity error during an I960 attempt to read CACHEB1 memory.	31
01B13702	The Master DRAB unexpectedly reported an Address Parity error.	37
01B23702	The CACHEA0 DRAB unexpectedly reported an Address Parity error.	37
01B33702	The CACHEA1 DRAB unexpectedly reported an Address Parity error.	37
01B43702	The CACHEB0 DRAB unexpectedly reported an Address Parity error.	37
01B53702	The CACHEB1 DRAB unexpectedly reported an Address Parity error.	37
01B63202	The Master DRAB detected an Ibus Parity Error during an I960 ID/Cache access attempt.	32
01B73202	The Master DRAB detected an Ibus Parity Error during an I960 buffer memory access attempt.	32
01B83202	The Master DRAB detected an Ibus Parity Error during an I960 buffer memory access attempt with a simultaneous, but unrelated, CACHExn memory access.	32
01B93202	The Master DRAB detected an Ibus Parity Error during an I960 CACHEA memory access with a simultaneous, but unrelated, buffer memory access.	32
01BA3202	The Master DRAB detected an Ibus Parity Error during an I960 CACHEB memory access with a simultaneous, but unrelated, buffer memory access.	32
01BB3202	The Master DRAB detected an Ibus Parity Error during an I960 CACHEA Control and Status Register access with a simultaneous, but unrelated, buffer memory access.	32
01BC3202	The Master DRAB detected an Ibus Parity Error during an I960 CACHEB Control and Status Register access with a simultaneous, but unrelated, buffer memory access.	32
01BD3702	The Master DRAB unexpectedly reported an Ibus Parity error.	37
01BE3702	The CACHEA0 DRAB unexpectedly reported an Ibus Parity error.	37
01BF3702	The CACHEA1 DRAB unexpectedly reported an Ibus Parity error.	37
01C03702	The CACHEB0 DRAB unexpectedly reported an Ibus Parity error.	37

Instance Code	Explanation	Repair Action Code
01C13702	The CACHEB1 DRAB unexpectedly reported an Ibus Parity error.	37
01C22F02	The Master DRAB detected a Write Data Parity error during an FX attempt to write buffer memory.	2F
01C32F02	The Master DRAB detected a Write Data Parity error during an FX attempt to write a byte to buffer memory.	2F
01C42F02	The Master DRAB detected a Write Data Parity error during a Host Port attempt to write buffer memory.	2F
01C52F02	The Master DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to buffer memory.	2F
01C62F02	The Master DRAB detected a Write Data Parity error during a Device Port attempt to write buffer memory.	2F
01C72F02	The Master DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to buffer memory.	2F
01C82F02	The Master DRAB detected a Write Data Parity error during an I960 attempt to write buffer memory.	2F
01C92F02	The Master DRAB detected a Write Data Parity error during an I960 attempt to write a byte to buffer memory.	2F
01CA3002	The CACHEA0 DRAB detected a Write Data Parity error during an FX attempt to write CACHEA0 memory.	30
01CB3002	The CACHEA0 DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEA0 memory.	30
01CC3002	The CACHEA0 DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEA0 memory.	30
01CD3002	The CACHEA0 DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEA0 memory.	30
01CE3002	The CACHEA0 DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEA0 memory.	30
01CF3002	The CACHEA0 DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEA0 memory.	30
01D03002	The CACHEA0 DRAB detected a Write Data Parity error during an I960 attempt to write CACHEA0 memory.	30
01D13002	The CACHEA0 DRAB detected a Write Data Parity error during an I960 attempt to write a byte to CACHEA0 memory.	30
01D23002	The CACHEA1 DRAB detected a Write Data Parity error during an FX attempt to write CACHEA1 memory.	30
01D33002	The CACHEA1 DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEA1 memory.	30

Instance Code	Explanation	Repair Action Code
01D43002	The CACHEA1 DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEA1 memory.	30
01D53002	The CACHEA1 DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEA1 memory.	30
01D63002	The CACHEA1 DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEA1 memory.	30
01D73002	The CACHEA1 DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEA1 memory.	30
01D83002	The CACHEA1 DRAB detected a Write Data Parity error during an I960 attempt to write CACHEA1 memory.	30
01D93002	The CACHEA1 DRAB detected a Write Data Parity error during an I960 attempt to write a byte to CACHEA1 memory.	30
01DA3102	The CACHEBO DRAB detected a Write Data Parity error during an FX attempt to write CACHEBO memory.	31
01DB3102	The CACHEBO DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEBO memory.	31
01DC3102	The CACHEBO DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEBO memory.	31
01DD3102	The CACHEBO DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEBO memory.	31
01DE3102	The CACHEBO DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEBO memory.	31
01DF3102	The CACHEBO DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEBO memory.	31
01E03102	The CACHEBO DRAB detected a Write Data Parity error during an I960 attempt to write CACHEBO memory.	31
01E13102	The CACHEBO DRAB detected a Write Data Parity error during an I960 attempt to write a byte to CACHEBO memory.	31
01E23102	The CACHEB1 DRAB detected a Write Data Parity error during an FX attempt to write CACHEB1 memory.	31
01E33102	The CACHEB1 DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEB1 memory.	31
01E43102	The CACHEB1 DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEB1 memory.	31
01E53102	The CACHEB1 DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEB1 memory.	31

Instance Code	Explanation	Repair Action Code
01E63102	The CACHEB1 DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEB1 memory.	31
01E73102	The CACHEB1 DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEB1 memory.	31
01E83102	The CACHEB1 DRAB detected a Write Data Parity error during an I960 attempt to write CACHEB1 memory.	31
01E93102	The CACHEB1 DRAB detected a Write Data Parity error during an I960 attempt to write a byte to CACHEB1 memory.	31
01EA3702	The Master DRAB unexpectedly reported a Write Data Parity error.	37
01EB3702	The CACHEAO DRAB unexpectedly reported a Write Data Parity error.	37
01EC3702	The CACHEA1 DRAB unexpectedly reported a Write Data Parity error.	37
01ED3702	The CACHEBO DRAB unexpectedly reported a Write Data Parity error.	37
01EE3702	The CACHEB1 DRAB unexpectedly reported a Write Data Parity error.	37
02020064	Disk Bad Block Replacement attempt completed for a write within the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	00
02032001	Journal SRAM backup battery failure; detected during system restart. The Memory Address field contains the starting physical address of the Journal SRAM.	20
02042001	Journal SRAM backup battery failure; detected during periodic check. The Memory Address field contains the starting physical address of the Journal SRAM.	20
02052301	A processor interrupt was generated by the CACHE Dynamic Ram controller and ArBitration engine (DRAB) with an indication that the CACHE backup battery has failed or is low (needs charging). The Memory Address field contains the starting physical address of the CACHEAO memory.	23
02062301	The CACHE backup battery has been declared bad. Either it failed testing performed by the Cache Diagnostics during system startup or it was too low (insufficiently charged) for the expected duration. The Memory Address field contains the starting physical address of the CACHEAO memory.	23

Instance Code	Explanation	Repair Action Code
02072201	The CACHE Dynamic Ram controller and ArBitration engine 0 (DRABO) failed testing performed by the Cache Diagnostics. The Memory Address field contains the starting physical address of the CACHEAO memory.	22
02082201	The CACHE Dynamic Ram controller and ArBitration engine 1 (DRAB1) failed testing performed by the Cache Diagnostics. The Memory Address field contains the starting physical address of the CACHEA1 memory.	22
02090064	A data compare error was detected during the execution of a compare modified READ or WRITE command.	00
020A0064	A data compare error was detected during the execution of a compare modified READ or WRITE command. Note that in this instance the SCSI Device Sense Data fields, cmdopcd through keyspec, are undefined.	00
020B2201	A failed read test of a write-back metadata page residing in cache occurred. Dirty write-back cached data exists and cannot be flushed to media. The dirty data is lost. The Memory Address field contains the starting physical address of the CACHEAO memory.	22
020C2201	Cache Diagnostics have declared the cache bad during testing. The Memory Address field contains the starting physical address of the CACHEAO memory.	22
020D2401	The wrong write cache module is configured. The serial numbers do not match. Either the existing or the expected cache contains dirty write-back cached data. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	24
020E2401	The write cache module is missing. A cache is expected to be configured and contains dirty write-back cached data. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	24
020F2401	The write cache modules are not configured properly for a dual-redundant configuration. One of the write cache modules is not present to perform cache failover of dirty write-back cached data. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	24
02102401	The write cache modules are not configured properly for a dual-redundant configuration. One of the cache modules is not the same size to perform cache failover of dirty write-back cached data. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	24
02110064	Disk Bad Block Replacement attempt completed for a read within the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	00

Instance Code	Explanation	Repair Action Code
02120064	There are insufficient resources to complete operation in a SCSI environment. Insufficient resources returned from HIS$CREATE_RECEIVE_DATA.	00
02130064	The tape device does not contain any medium.	00
02140064	The unit has been marked inoperative or UNKNOWN. In either case,. the unit is not available.	00
02150064	The Unit State Block unit status, associated with this I/O has changed to the UNKNOWN state. Therefore, the I/O was aborted.	00
02160064	A request was received to abort this command.	00
0217000A	Raid support is enabled but not licensed on this controller. Any use of this feature requires licensing. Continued use does not comply with the terms and conditions of licensing for this product.	00
0218000A	Write-back Cache support is enabled but not licensed on this controller. Any use of this feature requires licensing. Continued use does not comply with the terms and conditions of licensing for this product.	00
02192401	The cache modules are not configured properly for a dual-redundant configuration. One of the cache modules is not the same type (both write cache) which is necessary to perform cache failover of dirty write-back cached data. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	24
021A0064	Disk Bad Block Replacement attempt completed for a write of controller metadata to a location outside the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	00
021B0064	Disk Bad Block Replacement attempt completed for a read of controller metadata from a location outside the user data area of the disk. Note that due to the way Bad Block Replacement is performed on SCSI disk drives, information on the actual replacement blocks is not available to the controller and is therefore not included in the event report.	00
021D0064	Unable to lock the other controller's cache in a write-cache failover attempt. Either a latent error could not be cleared on the cache or the other controller did not release its cache. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	00
021E0064	The device specified in the Device Locator field has been added to the RAIDset associated with the logical unit. The RAIDset is now in Reconstructing state.	00

Instance Code	Explanation	Repair Action Code
021F0064	The device specified in the Device Locator field has been removed from the RAIDset associated with the logical unit. The removed device is now in the Failedset. The RAIDset is now in Reduced state.	00
02200064	The device specified in the Device Locator field failed to be added to the RAIDset associated with the logical unit. The device will remain in the spareset.	00
02210064	The device specified in the Device Locator field failed to be added to the RAIDset associated with the logical unit. The failed device has been moved to the Failedset.	00
02220064	The RAID set associated with the logical unit has transitioned from Reconstructing state to Normal state. Note that in this instance information supplied in the Device Locator, Device Firmware Revision Level, Device Product ID, and Device Type fields is for the first device in the RAID set.	00
02230064	The RAIDset associated with the logical unit has gone inoperative. Note that in this instance information supplied in the Device Locator, Device Firmware Revision Level, Device Product ID, and Device Type fields is for the first device in the RAIDset.	00
02240064	The RAIDset associated with the logical unit has transitioned from Normal state to Reconstructing state. Note that in this instance information supplied in the Device Locator, Device Firmware Revision Level, Device Product ID, and Device Type fields is for the first device in the RAIDset.	00
0227000A	Mirroring support is enabled but not licensed on this controller. Any use of this feature requires licensing. Continued use does not comply with the terms and conditions of licensing for this product.	00
02280064	The device specified in the Device Locator field has been added to the mirrorset associated with the logical unit. The new mirrorset member is now in the Copying state.	00
02290064	The device specified in the Device Locator field has been removed from the mirrorset associated with the logical unit. The removed device is now in the Failedset.	00
022A0064	The device specified in the Device Locator field failed to be added to the mirrorset associated with the logical unit. The device will remain in the Spareset.	00
022B0064	The device specified in the Device Locator field failed to be added to the mirrorset associated with the logical unit. The failed device has been moved to the Failedset.	00
022C0064	The device specified in the Device Locator has transitioned from Copying or Normalizing state to Normal state.	00

Instance Code	Explanation	Repair Action Code
022D0064	The mirrorset associated with the logical unit has gone inoperative. Note that in this instance information supplied in the Device Locator, Device Firmware Revision Level Device Product ID, and Device Type fields is for the first device in the mirrorset .	00
022E0064	The device specified in the Device Locator field has been converted to a mirrorset unit.	00
022F0064	The mirrored device specified in the Device Locator field has been converted to a single device associated with the logical unit.	00
02300064	The device specified in the Device Locator field has been reduced from its associated mirrorset. The nominal number of members in the mirrorset has been decreased by one. The reduced device is now available for use.	00
02310064	The mirrorset associated with the logical unit has had its nominal membership changed. The new nominal number of members for the mirrorset is specified in the Associated Port field. Note that in this instance information supplied in the Device Locator, Device Firmware Revision Level, Device Product ID, and Device Type fields is for the first device in the mirrorset . This Instance code has been removed from the HSOF version 2.7 release.	00
023B0064	The device specified in the Device Locator field had a read error which has been repaired with data from another mirrorset member.	00
023C0064	The device specified in the Device Locator field had a read error. Attempts to repair the error with data from another mirrorset member failed due to lack of alternate error-free data source.	00
023D0064	The device specified in the Device Locator field had a read error. Attempts to repair the error with data from another mirrorset member failed due to a write error on the original device. The original device will be removed from the mirrorset.	00
02422464	Cache failover attempt failed because the other cache was illegally configured with SIMMs. Note that in this instance the memory address, byte count, DRAB register, and Diagnostic register fields are undefined.	24
02432201	The CACHE Dynamic Ram controller and ArBitration engine 0 (DRAB0) failed Cache Diagnostics testing performed on Cache B (other cache) during a cache failover attempt. The memory address field contains the starting physical address of the CACHEB0 memory.	22
02442201	The CACHE Dynamic Ram controller and ArBitration engine 1 (DRAB1) failed Cache Diagnostics testing performed on Cache B (other cache) during a cache failover attempt. The memory address field contains the starting physical address of the CACHEB1 memory.	22

Instance Code	Explanation	Repair Action Code
02452201	The CACHE Dynamic Ram controller and ArBitration engine 0 and 1 (DRABO and DRAB1) failed Cache Diagnostics testing performed on Cache B (other cache) during a cache failover attempt. The memory address field contains the starting physical address of the CACHEB1 memory.	22
02460064	The A Write Append Position Error occurred during a tape write but no recovery was attempted because the attempted transfer did not meet the parameters for a recoverable Write Append Position Error.	00
02470064	When attempting to recover a Write Append Position Error on a tape unit, the recovery failed to start because resources required for the recovery were not available.	00
02480064	When attempting to recover a Write Append Position Error on a tape unit, an error occurred during the recovery	00
024B2401	The Write-back caching has been disabled either due to a cache or battery related problem. The exact nature of the problem is reported by other instance codes. Note that in this instance the memory address, byte count, DRAB register, and Diagnostic register fields are undefined.	24
024F2401	This cache module is populated with SIMMs incorrectly. Cache metadata resident in the cache module indicates that unflushed write cache data exists for a cache size different than what is found present. Note that in this instance the memory address, byte count, DRAB register and Diagnostic register fields are undefined.	24
02502401	The cache module has memory SIMMs populated in an unsupported configuration. Note that in this instance the memory address, byte count, DRAB register, and Diagnostic register fields are undefined.	24
0251000A	The command failed because the target unit is not online to the controller. The Information field of the Device Sense Data contains the block number of the first block in error.	00
0252000A	The last block of data returned contains a forced error. A forced error occurs when a disk block is successfully reassigned, but the data in that block is lost. Re-writing the disk block will clear the forced error condition. The Information field of the Device Sense Data contains the block number of the first block in error.	00
0253000A	The data supplied from the host for a data compare operation differs from the data on the disk in the specified block. The Information field of the Device Sense Data contains the block number of the first block in error.	00
0254000A	The command failed due to a host data transfer failure. The information field of the Device Sense Data contains the block number of the first block in error.	00
0255000A	The controller was unable to successfully transfer data to target unit.	00

Instance Code	Explanation	Repair Action Code
0256000A	The write operation failed because the unit is Data Safety Write Protected.	00
0257000A	An attempt to reassign a bad disk block failed. The contents of the disk block is lost. The Information field of the Device Sense Data contains the block number of the first block in error.	00
0258000A	The command was aborted prior to completion. The Information field of the Device Sense Data contains the block number of the first block in error.	00
0259000A	The write operation failed because the unit is hardware write protected. The Information field of the Device Sense Data contains the block number of the first block in error.	00
025A000A	The command failed because the unit became inoperative prior to command completion. The Information field of the Device Sense Data contains the block number of the first block in error.	00
025B000A	The command failed because the unit became unknown to the controller prior to command completion. The Information field of the Device Sense Data contains the block number of the first block in error.	00
025C000A	The command failed because of a unit media format error. The Information field of the Device Sense Data contains the block number of the first block in error.	00
025D000A	The command failed for an unknown reason. The Information field of the Device Sense Data contains the block number of the first block in error.	00
025E0064	The mirrorset unit associated with the logical unit has had its nominal membership changed. The information provided in the device locator, device type , device identification, and the device serial number fields is for the first device in the mirrorset.	00
03010101	No command control structures available for disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03022002	A SCSI interface chip command time-out occurred during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03034002	Byte transfer time-out during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	40
03044402	SCSI bus errors during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	44

Instance Code	Explanation	Repair Action Code
03052002	Device port SCSI chip reported gross error during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03062002	Non-SCSI bus parity error during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03070101	Source driver programming error encountered during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03080101	Miscellaneous SCSI Port Driver coding error detected during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03094002	An unrecoverable disk drive error was encountered while performing work related to disk unit operations.	40
030C4002	A Drive failed because a Test Unit Ready command or a Read Capacity command failed.	40
030D000A	Drive was failed by a Mode Select command received from the host.	00
030E4002	Drive failed due to a deferred error reported by drive.	40
030F4002	Unrecovered Read or Write error.	40
03104002	No response from one or more drives.	40
0311430A	Nonvolatile memory and drive metadata indicate conflicting drive configurations.	43
0312430A	The Synchronous Transfer Value differs between drives in the same storageset.	43
03134002	Maximum number of errors for this data transfer operation exceeded.	40
03144002	Drive reported recovered error without transferring all data.	40
03154002	Data returned from drive is invalid.	40
03164002	Request Sense command to drive failed.	40
03170064	Illegal command for pass through mode.	00
03180064	Data transfer request error.	00
03194002	Premature completion of a drive command.	40
031A4002	Command time-out.	40
031B0101	Watchdog timer time-out.	01
031C4002	Disconnect time-out.	40

Instance Code	Explanation	Repair Action Code
031D4002	Unexpected bus phase.	40
031E4002	Disconnect expected.	40
031F4002	ID message not sent by drive.	40
03204002	Synchronous negotiation error.	40
03214002	The drive unexpectedly disconnected from the SCSI bus.	40
03224002	Unexpected message.	40
03234002	Unexpected Tag message.	40
03244002	Channel busy.	40
03254002	Message Reject received on a valid message.	40
0326450A	The disk device reported Vendor Unique SCSI Sense Data.	45
03270101	A disk related error code was reported which was unknown to the Fault Management firmware. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
0328450A	The disk device reported standard SCSI Sense Data.	45
03324002	SCSI bus selection time-out.	40
03330002	Device power on reset.	00
03344002	Target assertion of REQ after WAIT DISCONNECT.	40
03354002	During device initialization a Test Unit Ready command or a Read Capacity command to the drive failed.	40
03364002	During device initialization the device reported a deferred error.	40
03374002	During device initialization the maximum number of errors for a data transfer operation was exceeded.	40
03384002	Request Sense command to the device failed.	40
03394002	Command time-out.	40
033A4002	Disconnect time-out.	40
033B4002	Unexpected bus phase.	40
033C4002	The device unexpectedly disconnected from the SCSI bus.	40
033D4002	Unexpected message	40
033E4002	Message Reject received on a valid message.	40
033F0101	No command control structures available for pass-through device operation.	01
03402002	Device port SCSI chip reported gross error.	20
03410101	Miscellaneous SCSI Port Driver coding error.	01

Instance Code	Explanation	Repair Action Code
03420101	A pass-through device related internal error code was reported which is not recognized by the Fault Management firmware of the Hsxxx controller.	01
03434002	During device initialization the device reported unexpected standard SCSI Sense Data.	40
03644002	An unrecoverable tape drive error was encountered while performing work related to tape unit operations.	01
03674002	A Drive failed because a Test Unit Ready command or a Read Capacity command failed.	40
0368000A	Drive was failed by a Mode Select command received from the host.	00
03694002	Drive failed due to a deferred error reported by drive.	40
036A4002	Unrecovered Read or Write error.	40
036B4002	No response from one or more drives.	40
036C430A	Nonvolatile memory and drive metadata indicate conflicting drive configurations.	43
036D430A	The Synchronous Transfer Value differs between drives in the same storageset.	43
036E4002	Maximum number of errors for this data transfer operation exceeded.	40
036F4002	Drive reported recovered error without transferring all data.	40
03704002	Data returned from drive is invalid.	40
03714002	Request Sense command to drive failed.	40
03720064	Illegal command for pass through mode.	00
03730064	Data transfer request error.	00
03744002	Premature completion of a drive command.	40
03754002	Command time-out.	40
03760101	Watchdog timer time-out.	01
03774002	Disconnect time-out.	40
03784002	Unexpected bus phase.	40
03794002	Disconnect expected.	40
037A4002	Message not sent by drive.	40
037B4002	Synchronous negotiation error.	40
037C4002	The drive unexpectedly disconnected from the SCSI bus.	40
037D4002	Unexpected message.	40
037E4002	Unexpected Tag message.	40

Instance Code	Explanation	Repair Action Code
037F4002	Channel busy.	40
03804002	Message Reject received on a valid message.	40
0381450A	The tape device reported Vendor Unique SCSI Sense Data.	45
03820101	No command control structures available for tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03832002	A SCSI interface chip command time-out occurred during tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03844002	Byte transfer time-out during tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	40
03854402	SCSI bus errors occurred during tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	44
03862002	Device port SCSI chip reported gross error during tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03872002	A non-SCSI bus parity error occurred during tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03880101	A source driver programming error was encountered during tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03890101	A miscellaneous SCSI Port Driver coding error was encountered during tape operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
038A0101	A tape-related error code was reported which was unknown to the Fault Management firmware. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
038B450A	The tape device reported standard SCSI Sense Data.	45
03964002	An unrecoverable media loader error was encountered while performing work related to media loader operations.	40
03994002	A Drive failed because a Test Unit Ready command or a Read Capacity command failed.	40

Instance Code	Explanation	Repair Action Code
039A000A	The drive was failed by a Mode Select command received from the host.	00
039B4002	The drive failed due to a deferred error reported by drive.	40
039C4002	Unrecovered Read or Write error.	40
039D4002	No response from one or more drives.	40
039E430A	Nonvolatile memory and drive metadata indicate conflicting drive configurations.	43
039F430A	The Synchronous Transfer Value differs between drives in the same storageset.	43
03A04002	Maximum number of errors for this data transfer operation exceeded.	40
03A14002	The drive reported recovered error without transferring all data.	40
03A24002	Data returned from drive is invalid.	40
03A34002	Request Sense command to drive failed.	40
03A40064	Illegal command for pass through mode.	00
03A50064	Data transfer request error.	00
03A64002	Premature completion of a drive command.	40
03A74002	Command time-out.	40
03A80101	Watchdog timer time-out.	01
03A94002	Disconnect time-out.	40
03AA4002	Unexpected bus phase.	40
03AB4002	Disconnect expected.	40
03AC4002	ID message not sent by drive.	40
03AD4002	Synchronous negotiation error.	40
03AE4002	The drive unexpectedly disconnected from the SCSI bus.	40
03AF4002	Unexpected message.	40
03B04002	Unexpected Tag message.	40
03B14002	Channel busy.	40
03B24002	Message Reject received on a valid message.	40
03B3450A	SCSI Sense Data.	44
03B40101	No command control structures available for media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01

Instance Code	Explanation	Repair Action Code
03B52002	SCSI interface chip command time-out during media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03B64002	Byte transfer time-out during media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	40
03B74402	SCSI bus errors during media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	44
03B82002	Device port SCSI chip reported gross error during media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03B92002	Non-SCSI bus parity error during media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03BA0101	Source driver programming error encountered during media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03BB0101	Miscellaneous SCSI Port Driver coding error detected during media loader operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03BC0101	A media loader related error code was reported which was unknown to the Fault Management firmware. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03BD450A	The media changer device reported standard SCSI Sense Data.	45
03C80101	No command control structures available for operation to a device which is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03C92002	SCSI interface chip command time-out during operation to a device which is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03CA4002	Byte transfer time-out during operation to a device which is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	40

Instance Code	Explanation	Repair Action Code
03CB0101	Miscellaneous SCSI Port Driver coding error detected during operation to a device which is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03CC0101	An error code was reported which was unknown to the Fault Management firmware. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03CD2002	Device port SCSI chip reported gross error during operation to a device which is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	??
03CE2002	Non-SCSI bus parity error during operation to a device which is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	20
03CF0101	Source driver programming error encountered during operation to a device which is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	01
03D04002	A failure occurred while attempting a SCSI Test Unit Ready or Read Capacity command to a device. The device type is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	40
03D24402	SCSI bus errors during device operation. The device type is unknown to the controller. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	44
03D3450A	During device initialization, the device reported the SCSI Sense Key NO SENSE. This indicates that there is no specific sense key information to be reported for the designated logical unit. This would be the case for a successful command or a command that received CHECK CONDITION or COMMAND TERMINATED status because one of the FM, EOM, or ILI bits is set to one in the sense data flags field.	45
03D4450A	During device initialization, the device reported the SCSI Sense Key RECOVERED ERROR. This indicates the last command completed successfully with some recovery action performed by the target.	45
03D5450A	During device initialization, the device reported the SCSI Sense Key NOT READY. This indicates that the logical unit addressed cannot be accessed. Operator intervention may be required to correct this condition.	45

Instance Code	Explanation	Repair Action Code
03D6450A	During device initialization, the device reported the SCSI Sense Key MEDIUM ERROR. This indicates that the command terminated with a non-recovered error condition that was probably caused by a flaw in the medium or an error in the recorded data. This sense key may also be returned if the target is unable to distinguish between a flaw in the medium and a specific hardware failure (HARDWARE ERROR sense key).	45
03D7450A	During device initialization, the device reported the SCSI Sense Key HARDWARE ERROR. This indicates that the target detected a non-recoverable hardware failure (for example, controller failure, device failure, parity error, etc.) while performing the command or during a self test.	45
03D8450A	During device initialization, the device reported the SCSI Sense Key ILLEGAL REQUEST. This indicates that there was an illegal parameter in the command descriptor block or in the additional parameters supplied as data for some commands (FORMAT UNIT, SEARCH DATA, etc.). If the target detects an invalid parameter in the command descriptor block, then it will terminate the command without altering the medium. If the target detects an invalid parameter in the additional parameters supplied as data, then the target may have already altered the medium. This sense key may also indicate that an invalid IDENTIFY message was received.	45
03D9450A	During device initialization, the device reported the SCSI Sense Key UNIT ATTENTION. This indicates that the removable medium may have been changed or the target has been reset.	45
03DA450A	During device initialization, the device reported the SCSI Sense Key DATA PROTECT. This indicates that a command that reads or writes the medium was attempted on a block that is protected from this operation. The read or write operation is not performed.	45
03DB450A	During device initialization, the device reported the SCSI Sense Key BLANK CHECK. This indicates that a write-once device encountered blank medium or format-defined end-of-data indication while reading or a write-once device encountered a non-blank medium while writing.	45
03DC450A	During device initialization, the device reported a SCSI Vendor Specific Sense Key. This sense key is available for reporting vendor specific conditions.	45
03DD450A	During device initialization, the device reported the SCSI Sense Key COPY ABORTED. This indicates a COPY, COMPARE, or COPY AND VERIFY command was aborted due to an error condition on the source device, the destination device, or both.	45

Instance Code	Explanation	Repair Action Code
03DE450A	During device initialization, the device reported the SCSI Sense Key ABORTED COMMAND. This indicates the target aborted the command. The initiator may be able to recover by trying the command again.	45
03DF450A	During device initialization, the device reported the SCSI Sense Key EQUAL. This indicates a SEARCH DATA command has satisfied an equal comparison.	45
03E0450A	During device initialization, the device reported the SCSI Sense Key VOLUME OVERFLOW. This indicates a buffered peripheral device has reached the end-of-partition and data may remain in the buffer that has not been written to the medium. A RECOVER BUFFERED DATA command(s) may be issued to read the unwritten data from the buffer.	45
03E1450A	During device initialization, the device reported the SCSI Sense Key MISCOMPARE. This indicates the source data did not match the data read from the medium.	45
03E2450A	During device initialization, the device reported a reserved SCSI Sense Key.	45
03E60702	The EMU has detected one or more bad power supplies. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	07
03E70602	The EMU has detected one or more bad fans. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	06
03E80D02	The EMU has detected an elevated temperature condition. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	0D
03E90E02	The EMU has detected an external air sense fault Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	0E
03EA0F02	The EMU-detected power supply fault is now fixed. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	0F
03EB0F02	The EMU-detected bad fan fault is now fixed. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	0F
03EC0F02	The EMU-detected elevated temperature fault is now fixed. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	0F

Instance Code	Explanation	Repair Action Code
03ED0F02	The EMU-detected external air sense fault is now fixed. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	0F
03F00402	The shelf indicated by the port field is reporting a problem. This could mean one or both of the following: If the shelf is using dual power supplies, one power supply has failed. One of the shelf cooling fans has failed. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	04
03F10502	The SWAP interrupt from the shelf indicated by the port field can not be cleared. All SWAP interrupts from all ports will be disabled until corrective action is taken. When SWAP interrupts are disabled, neither controller front panel button presses nor removal/insertion of devices are detected by the controller. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	05
03F20064	The SWAP interrupts have been cleared and re-enabled for all shelves. Note that in this instance the Associated Port, Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	00
03F30064	An asynchronous SWAP interrupt was detected by the controller for the shelf indicated by the port field. Possible reasons for this occurrence include device insertion/removal shelf power failure SWAP interrupts re-enabled Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	00
03F40064	Device services had to reset the port to clear a bad condition. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	00

Instance Code	Explanation	Repair Action Code
03F50402	The controller shelf is reporting a problem. This could mean one or both of the following: If the shelf is using dual power supplies, one power supply has failed. One of the shelf cooling fans has failed. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	04
07030B0A	Failover Control detected a receive packet sequence number mismatch. The controllers are out of synchronization with each other and are unable to communicate. Note that in this instance the Last Failure Code and Last Failure Parameters fields are undefined.	0B
07040B0A	Failover Control detected a transmit packet sequence number mismatch. The controllers are out of synchronization with each other and are unable to communicate. Note that in this instance the Last Failure Code and Last Failure Parameters fields are undefined.	0B
07050064	Failover Control received a Last Gasp message from the other controller. The other controller is expected to restart itself within a given time period. If it does not, it will be held reset with the Kill line.	40
07060C01	Failover Control detected that both controllers are acting as SCSI ID 6. Since IDs are determined by hardware, it is unknown which controller is the real SCSI ID 6. Note that in this instance the Last Failure Code and Last Failure Parameters fields are undefined.	0C
07070C01	Failover Control detected that both controllers are acting as SCSI ID 7. Since IDs are determined by hardware, it is unknown which controller is the real SCSI ID 7. Note that in this instance the Last Failure Code and Last Failure Parameters fields are undefined.	0C
07080B0A	Failover Control was unable to send keep alive communication to the other controller. It is assumed that the other controller is hung or not started. Note that in this instance the Last Failure Code and Last Failure Parameters fields are undefined.	0B
40016001	CI A/B transmit cables are crossed.	60
40026001	CI A/B receive cables are crossed.	60
4003640A	CI Port detected a Dual Receive condition that resulted in the closure of the Virtual Circuit. This error condition will be eliminated in a future CI interface chip.	64
4004020A	Host Interconnect Services detected protocol error upon validating a received packet.	02
4007640A	CI Port detected error upon attempting to transmit a packet. This resulted in the closure of the Virtual Circuit.	64

Instance Code	Explanation	Repair Action Code
4009640A	CI Port detected bad path A upon attempting to transmit a packet.	64
400A640A	CI Port detected bad path B upon attempting to transmit a packet.	64
400D640A	CI Port detected bad path A upon attempting to transmit a packet.	64
400E640A	CI Port detected bad path B upon attempting to transmit a packet.	64
400F640A	Host Interconnect Services detected packet sequence number mismatch.	64
4015020A	Remote SYSAP sent an SCS APPL_MSG but no receive credit was available.	02
4029010A	Illegal connection state. Not in CONNECT_REC connection state when an SCS ACCEPT_REQ is pending.	01
402A010A	Illegal connection state. Not in CONNECT_REC connection state when an SCS REJECT_REQ is pending.	01
402B010A	Illegal connection state. Not in CLOSED connection state when an SCS CONNECT_REQ is pending.	01
402C010A	Illegal connection state. Not in OPEN or DISCONNECT_REC connection state when an SCS DISCONNECT_REQ is pending.	01
403D020A	Received packet with an unrecognized PPD opcode. Note that the content of the vcstate field is undefined in this instance.	02
40440064	Received a PPD NODE_STOP and closed virtual circuit.	00
4051020A	Received SCS CONNECT_RSP when not in CONNECT_SENT connection state.	02
4052020A	Received SCS CONNECT_RSP when the connection is no longer valid.	02
4053020A	Received SCS ACCEPT_REQ when not in CONNECT_ACK connection state.	02
4054020A	Received SCS ACCEPT_RSP when not in the ACCEPT_SENT connection state.	02
4055020A	Received SCS REJECT_REQ when not in the CONNECT_ACK connection state.	02
4056020A	Received SCS REJECT_RSP when not in the REJECT_SENT connection state.	02
4057020A	Received SCS DISCONNECT_REQ when not in the OPEN, DISCONNECT_SENT or DISCONNECT_ACK connection state.	02
4058020A	Received SCS DISCONNECT_RSP when not in the DISCONNECT_SENT or DISCONNECT_MATCH connection state.	02

Instance Code	Explanation	Repair Action Code
4059020A	Received SCS CREDIT_REQ when in the DISCONNECT_REC or DISCONNECT_MATCH connection state.	02
405A020A	Received SCS APPL_MSG when in the DISCONNECT_SENT or DISCONNECT_ACK connection state.	02
405B020A	Received SCS ACCEPT_REQ on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the "vcstate," "remote node name," "remote connection id" and "connection state" fields are undefined.	02
405C020A	Received SCS ACCEPT_RSP on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
405D020A	Received SCS REJECT_REQ on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
405E020A	Received SCS REJECT_RSP on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
405F020A	Received SCS DISCONNECT_REQ on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
4060020A	Received SCS DISCONNECT_RSP on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
4061020A	Received SCS CREDIT_REQ on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
4062020A	Received SCS CREDIT_RSP on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
4063020A	Received SCS APPL_MSG on a connection that is no longer valid. Note that in this instance, if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02

Instance Code	Explanation	Repair Action Code
4064020A	Received an unrecognized SCS message. Note that in this instance if the connection id field is zero, the content of the vcstate, remote node name, remote connection id and connection state fields are undefined.	02
4065020A	Received SCS CONNECT_RSP with an unrecognized status. Connection is broken by Host Interconnect Services.	02
4066020A	Received SCS REJECT_REQ with an invalid reason.	02
4067020A	Received SCS APPL_MSG with no receive credit available.	02
41010064	SCSI Host Interconnect Services has detected that the other controller, identified in the Failed Controller Target Number and Other Controller Board Serial Number sense data fields, has failed and that the controller reporting the event has assumed control of the units identified in the Affected LUNs sense data field.	00
41020064	SCSI Host Interconnect Services has detected that the other controller, identified in the Failed Controller Target Number and Other Controller Board Serial Number sense data fields, is again operational and that the controller reporting the event is willing to relinquish control of the units identified in the affected LUNs sense data field.	00
82012002	An unrecoverable error was detected during execution of the Device Port Subsystem Built-In Self Test. One or more of the device ports on the controller module has failed; some/all of the attached storage is no longer accessible via this controller.	20
82042002	A spurious interrupt was detected during the execution of a Subsystem Built-In Self Test.	20
82052002	An unrecoverable error was detected during execution of the HOST PORT Subsystem Test. The system will not be able to communicate with the host.	20
82062002	An unrecoverable error was detected during execution of the UART/DUART Subsystem Test. This will cause the console to be unusable. This will cause failover communications to fail.	20
82072002	An unrecoverable error was detected during execution of the FX Subsystem Test.	20
82082002	An unrecoverable error was detected during execution of the nbuss init Test.	20

Last fail codes

The following tables contain last fail codes and their definitions. Use these tables if your subsystem or controller is out of service due to some type of failure and you cannot use FMU to translate the last fail code.

These codes are presented in tables according to the software component that was the source of the error. However, they are also sorted numerically, so you can scan down the list until you find the code you're looking for.

Table 45
Executive services last failure codes

Last Fail Code	Explanation	Repair Action Code
01000100	Memory allocation failure during executive initialization.	01
01010100	An interrupt without any handler was triggered.	01
01020100	Entry on timer queue was not of type AQ or BQ.	01
01030100	Memory allocation for a facility lock failed.	01
01040100	Memory initialization called with invalid memory type.	01
01050104	The I960 reported a fault. Last Failure Parameter[0] contains the PC value. Last Failure Parameter[1] contains the AC value. Last Failure Parameter[2] contains the fault type and subtype values. Last Failure Parameter[3] contains the address of the faulting instruction.	01
01070100	Timer chip setup failed.	01
01082004	The core diagnostics reported a fault. Last Failure Parameter[0] contains the error code value (same as blinking OCP LEDs error code). Last Failure Parameter[1] contains the address of the fault. Last Failure Parameter[2] contains the actual data value. Last Failure Parameter[3] contains the expected data value.	20

Last Fail Code	Explanation	Repair Action Code
01090105	An NMI occurred during EXEC$BUGCHECK processing. Last Failure Parameter[0] contains the executive flags value. Last Failure Parameter[1] contains the RIP from the NMI stack. Last Failure Parameter[2] contains the read diagnostic register 0 value. Last Failure Parameter[3] contains the Master DRAB CSR value. Last Failure Parameter[4] contains the SIP last failure code value.	01
010A2080	A single bit or a multi-single bit ECC error was detected. To prevent data corruption, the controller was reset. If this event occurs frequently, the controller module should be replaced.	20
010B2380	A processor interrupt was generated by the CACHEA Dynamic Ram controller and ArBitration engine (DRAB) with an indication that the CACHE backup battery has failed or is low (needs charging).	23
010C2380	A processor interrupt was generated by the CACHEB Dynamic Ram controller and ArBitration engine (DRAB) with an indication that the CACHE backup battery has failed or is low (needs charging).	23
010D0110	The System Information structure within the System Information Page has been reset to default settings. The only known cause for this event is an I960 processor hang caused by an unimplemented memory region reference. When such a hang occurs, controller modules equipped with inactivity watchdog timer circuitry will spontaneously reboot after the watchdog timer expires (within seconds of the hang). Controller modules not so equipped will just hang as indicated by the green LED on the OCP remaining in a steady state.	01
010E0110	All structures contained in the System Information Page (SIP) and the Last Failure entries have been reset to their default settings. This is a normal occurrence in the following situations: For the first boot following manufacture of the controller module During the transition from one firmware version to another if the format of the SIP is different between the two versions. If this event is reported at any other time, follow the recommended repair action associated with this Last Failure code.	01

Last Fail Code	Explanation	Repair Action Code
010F0110	All structures contained in the System Information Page and the Last Failure entries have been reset to their default settings as the result of certain controller manufacturing configuration activities. If this event is reported at any other time, follow the recommended repair action associated with this Last Failure code.	01
01100100	Non-maskable interrupt entered but no Non-maskable interrupt pending. This is typically caused by an indirect call to address 0.	01
01110106	A bugcheck occurred during EXEC$BUGCHECK processing. Last Failure Parameter [0] contains the executive flags value. Last Failure Parameter [1] contains the RIP from the bugcheck call stack. Last Failure Parameter [2] contains the first SIP last failure parameter value. Last Failure Parameter [3] contains the second SIP last failure parameter value. Last Failure Parameter [4] contains the SIP last failure code value Last Failure Parameter [5] contains the EXEC$BUGCHECK call last failure code value.	01
01126880	A processor interrupt was generated by the CACHA Dynamic Ram controller and ArBitration engine (DRAB) with an indication that the CACHE backup battery has been disconnected.	68
01136880	A processor interrupt was generated by the CACHB Dynamic Ram controller and ArBitration engine (DRAB) with an indication that the CACHE backup battery has been disconnected.	68
01150106	A bugcheck occurred before subsystem initialization completed. Last Failure Parameter [0] contains the executive flags value. Last Failure Parameter [1] contains the RIP from the bugcheck call stack. Last Failure Parameter [2] contains the first SIP last failure parameter value. Last Failure Parameter [3] contains the second SIP last failure parameter value. Last Failure Parameter [4] contains the SIP last failure code value Last Failure Parameter [5] contains the EXEC$BUGCHECK call last failure code value.	01
018000A0	A powerfail interrupt occurred.	00

Last Fail Code	Explanation	Repair Action Code
018600A0	A processor interrupt was generated with an indication that the other controller in a dual controller configuration asserted the KILL line to disable this controller.	00
018700A0	A processor interrupt was generated with an indication that the (//) RESET button on the controller module was depressed.	00
018800A0	A processor interrupt was generated with an indication that the program card was removed.	00
018900A0	A processor interrupt was generated with an indication that the controller inactivity watchdog timer expired.	00
018B2580	A NMI interrupt was generated with an indication that a memory system problem occurred.	25
018C2580	A DRAB_INT interrupt was generated with an indication that a memory system problem occurred.	25
018D2580	The memory address range for which buffer SYSCOM was linked is not available.	25

Table 46
Value-added services last failure codes

Last Fail Code	Explanation	Repair Action Code
02000100	Initialization code was unable to allocate enough memory to setup the receive data descriptors.	01
02010100	Initialization code was unable to allocate enough memory to setup the send data descriptors.	01
02040100	Unable to allocate memory necessary for data buffers.	01
02050100	Unable to allocate memory for the Free Buffer Array.	01
02080100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the disk read DWD stack.	01
02090100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the disk write DWD stack.	01
020A0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the tape read DWD stack.	01
020B0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the tape write DWD stack.	01
020C0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the miscellaneous DWD stack.	01
02100100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when creating the device services state table.	01
02170100	Unable to allocate memory for the Free Node Array.	01
02180100	Unable to allocate memory for the Free Buffer Descriptor Array.	01

Last Fail Code	Explanation	Repair Action Code
021D0100	Unable to allocate memory for the Free Buffer Array.	01
021E0100	Unable to allocate memory for the Free Strip Node Array.	01
021F0100	Unable to allocate memory for WARPs and RMDs.	01
02210100	Invalid parameters in CACHE$OFFER_META call.	01
02220100	No buffer found for CACHE$MARK_META_DIRTY call.	01
02270104	A callback from DS on a transfer request has returned a bad or illegal DWD status. Last Failure Parameter[0] contains the DWD Status. Last Failure Parameter[1] contains the DWD address. Last Failure Parameter[2] contains the PUB Address. Last Failure Parameter[3] contains the Device Port.	01
022C0100	A READ_LONG operation was requested for a Local Buffer Transfer. READ_LONG is not supported for Local Buffer Transfers.	01
022D0100	A WRITE_LONG operation was requested for a Local Buffer Transfer. WRTE_LONG is not supported for Local Buffer Transfers.	01
022E0102	An invalid mapping type was specified for a logical unit. Last Failure Parameter[0] contains the USB address. Last Failure Parameter[1] contains the Unit Mapping Type.	01
02360101	Unrecognized state supplied to FOC$SEND callback routine va_dap_snd_cmd_complete. Last Failure Parameter[0] contains the unrecognized value.	01
02370102	Unsupported return from HIS$GET_CONN_INFO routine Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
02392084	A processor interrupt was generated by the controller's XOR engine (FX), with no bits set in the CSR to indicate a reason for the interrupt. Last Failure Parameter[0] contains the FX Control and Status Register (CSR). Last Failure Parameter[1] contains the FX DMA Indirect List Pointer register (DILP). Last Failure Parameter[2] contains the FX DMA Page Address register (DADDR). Last Failure Parameter[3] contains the FX DMA Command and control register (DCMD).	20

Last Fail Code	Explanation	Repair Action Code
023A2084	A processor interrupt was generated by the controller's XOR engine (FX), indicating an unrecoverable error condition. Last Failure Parameter[0] contains the FX Control and Status Register (CSR). Last Failure Parameter[1] contains the FX DMA Indirect List Pointer register (DILP). Last Failure Parameter[2] contains the FX DMA Page Address register (DADDR). Last Failure Parameter[3] contains the FX DMA Command and control register (DCMD).	20
02440100	The logical unit mapping type was detected invalid in va_set_disk_geometry()	01
02530102	An invalid status was returned from CACHE$LOOKUP_LOCK(). Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
02560102	An invalid status was returned from CACHE$LOOKUP_LOCK(). Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
02570102	An invalid status was returned from VA$XFER() during a operation. Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
025A0102	An invalid status was returned from CACHE$LOOKUP_LOCK(). Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
025B0102	An invalid mapping type was specified for a logical unit. Last Failure Parameter[0] contains the USB address. Last Failure Parameter[1] contains the Unit Mapping Type.	01
025C0102	An invalid mapping type was specified for a logical unit. Last Failure Parameter[0] contains the USB address. Last Failure Parameter[1] contains the Unit Mapping Type.	01
02620102	An invalid status was returned from CACHE$LOOKUP_LOCK(). Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01

Last Fail Code	Explanation	Repair Action Code
02690102	An invalid status was returned from CACHE$OFFER_WRITE_DATA(). Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
02730100	A request was made to write a device metadata block with an invalid block type.	01
02790102	An invalid status was returned from VA$XFER() in a complex read operation. Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
027B0102	An invalid status was returned from VA$XFER() in a complex ACCESS operation. Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
027D0100	Unable to allocate memory for a Failover Control Block.	01
027E0100	Unable to allocate memory for a Failover Control Block.	01
027F0100	Unable to allocate memory for a Failover Control Block.	01
02800100	Unable to allocate memory for a Failover Control Block.	01
02820100	Unable to allocate memory for the Dirty Count Array.	01
02830100	Unable to allocate memory for the Cache Buffer Index Array.	01
02840100	Unable to allocate memory for the XNode Array.	01
02850100	Cache was declared bad by the Cache Diagnostics after first Meg was tested. Can't recover and use local memory because cannot get those initial buffers back.	01
02860100	Unable to allocate memory for the Fault Management Event Information Packet used by the Cache Manager in generating error logs to the host.	01
02880100	Invalid FOC Message in cmfoc_snd_cmd.	01
02890100	Invalid FOC Message in cmfoc_rcv_cmd.	01
028A0100	Invalid return status from DIAG$CACHE_MEMORY_TEST.	01
028B0100	Invalid return status from DIAG$CACHE_MEMORY_TEST.	01
028C0100	Invalid error status given to cache_fail.	01
028E0100	Invalid DCA state detected in init_crashover.	01
028F0100	Invalid status returned from CACHE$CHECK_METADATA.	01
02900100	Unable to allocate memory for the First Cache Buffer Index Array.	01
02910100	Invalid metadata combination detected in build_raid_node.	01

Last Fail Code	Explanation	Repair Action Code
02920100	Unable to handle that many bad dirty pages (exceeded MAX_BAD_DIRTY). Cache memory is bad.	01
02930100	There was no free or freeable buffer to convert bad metadata or to borrow a buffer during failover of bad dirty.	01
02940100	A free Device Correlation Array entry could not be found during write-back cache failover.	01
02950100	Invalid DCA state detected in start_crashover.	01
02960100	Invalid DCA state detected in start_failover.	01
02970100	Invalid DCA state detected in init_failover.	01
02980100	This bugcheck was created for testing purposes only, specifically testing write-back cache failover. It should not be seen in the field.	01
02990100	A free RAID Correlation Array entry could not be found during write-back cache failover.	01
029A0100	Invalid cache buffer metadata detected while scanning the Buffer Metadata Array. Found a page containing dirty data but the corresponding Device Correlation Array entry does exist.	01
029D0100	Invalid metadata combination detected in build_bad_raid_node.	01
029E0100	Distinguished member is not null_pub. This last_fail code was removed from HSOF firmware at Version 2.5.	01
029F0100	The Cache Manager software has insufficient resources to handle a buffer request pending.	01
02A00100	VA change state is trying to change device affinity and the cache has data for this device.	01
02A10100	Pubs not one when transportable.	01
02A20100	Pubs not one when transportable.	01
02A30100	No available data buffers. If the cache module exists then this is true after testing the whole cache. Otherwise, there were no buffers allocated from BUFFER memory on the controller module.	01
02A40100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating VAXDs.	01
02A50100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating DILPs.	01
02A60100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating Change State Work Items.	01
02A70100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating VA Request Items.	01

Last Fail Code	Explanation	Repair Action Code
02A80000	Controller is being rebooted as a result of a CLI CLEAR INVALID_CACHE command being issued on the other controller.	00
02A90100	Too many pending FOC$SEND requests by the Cache Manager. Code is not designed to handle more than one FOC$SEND to be pending because there's no reason to expect more than one pending.	01
02AA0100	An invalid call was made to CACHE$DEALLOCATE_CLD. Either that device had dirty data or it was bound to a RAIDset.	01
02AB0100	An invalid call was made to CACHE$DEALLOCATE_SLD. A RAIDset member either had dirty data or write-back already turned on.	01
02AC0100	An invalid call was made to CACHE$DEALLOCATE_SLD. The RAIDset still has data (strip nodes).	01
02AD0180	The FX detected a compare error for data that was identical. This error has always previously occurred due to a hardware problem.	01
02AE0100	The mirrorset member count and individual member states are inconsistent. Discovered during a mirrorset write or erase.	01
02AF0102	An invalid status was returned from VA$XFER() in a write operation. Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
02B00102	An invalid status was returned from VA$XFER() in an erase operation. Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
02B10100	A mirrorset read operation was received and the round robin selection algorithm found no normal members in the mirrorset. Internal inconsistency.	01
02B20102	An invalid status was returned from CACHE$LOCK_READ during a mirror copy operation Last Failure Parameter[0] contains the DD address. Last Failure Parameter[1] contains the invalid status.	01
02B80100	Invalid Cache Policy parameter to CACHE$POLICY_CHANGE.	01
02B90100	Invalid code loop counter attempting to find the Cache ID Blocks.	01
02BC0100	A mirrorset read operation was received and the preferred member selection algorithm found no normal members in the mirrorset. Internal inconsistency.	01

Last Fail Code	Explanation	Repair Action Code
02BD0100	A mirrorset metadata online operation found no normal members in the mirrorset. Internal inconsistency.	01
02BF0100	Report_error routine encountered an unexpected failure status returned from DIAG$LOCK_AND_TEST_CACHE_B.	01
02C00100	Copy_buff_on_this routine expected the given page to be marked bad and it wasn't.	01
02C10100	Copy_buff_on_other routine expected the given page to be marked bad and it wasn't.	01
02C60100	Mirroring transfer found CLD with writeback state OFF.	01
02C70100	Bad BBR offsets for active shadowset, detected on write.	01
02C80100	Bad BBR offsets for active shadowset, detected on read.	01
02C90100	Illegal call made to CACHE$PURGE_META when the storageset was not quiesced.	01
02CA0100	Illegal call made to VA$RAID5_META_READ when another read (of metadata) is already in progress on the same strip.	01
02CB0000	A restore of the configuration has been done. This cleans up and restarts with the new configuration	00
02CC0100	On an attempt, which is not allowed to fail, to allocate a cache node, no freeable cache node was found.	01
02CD0100	On an attempt, which is not allowed to fail, to allocate a strip node, no freeable strip node was found.	01
02CE1010	Serial number mismatch was detected during an attempt to restore saved configuration information.	10
02CF0100	An unsupported message type or terminal request was received by the VA_SAVE_Config virtual terminal code from the CLI.	01
02D00100	Not all alter_device requests from VA_SAVE_CONFIG completed within the time-out interval.	01
02D10102	Failed to read or write metadata while UNMIRRORING a mirrorset to a disk unit.	01
02D30100	The controller has insufficient memory to allocate enough data structures used to manage metadata operations.	01
02D50100	No resources are available to handle a new metadata work request.	01
02D60100	An invalid storage set type was specified for metadata initialization.	01
02D72390	Forced failover of devices due to a cache battery failure. This was initiated because the dual partner was operational with a good battery and there is no host failover assistance.	23
02D80100	Unable to allocate memory for Fast Buffers. Code bug suspected rather than low buffer memory, because the code just checked for sufficient buffer memory.	01

Table 47
Device services last failure codes

Last Fail Code	Explanation	Repair Action Code
03010100	Failed request for port-specific scripts memory allocation.	01
03020101	Invalid SCSI direct-access device opcode in misc command DWD. Last Failure Parameter[0] contains the SCSI command opcode.	01
03030101	Invalid SCSI sequential-access device opcode in misc cmd DWD. Last Failure Parameter[0] contains the SCSI command opcode.	01
03040101	Invalid SCSI CDROM device opcode in misc command DWD. Last Failure Parameter[0] contains the SCSI command opcode.	01
03050101	Invalid SCSI medium changer device opcode in misc command DWD. Last Failure Parameter[0] contains the SCSI command opcode.	01
03060101	Invalid SCSI device type in PUB. Last Failure Parameter[0] contains the SCSI device type.	01
03070101	Invalid CDB Group Code detected during create of misc cmd DWD Last Failure Parameter[0] contains the SCSI command opcode.	01
03080101	Invalid SCSI OPTICAL MEMORY device opcode in misc command DWD. Last Failure Parameter[0] contains the SCSI command opcode.	01
030A0100	Error DWD not found in port in_proc_q.	01

Last Fail Code	Explanation	Repair Action Code
030B0188	A dip error was detected when pcb_busy was set. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the new info NULL - SSTAT0 - DSTAT - ISTAT. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03150100	More DBDs than allowed for in mask	01
031E0100	Can't find in_error dwd on in-process queue	01
031F0100	Either DWD_ptr is null or bad value in dsps	01
03280100	SCSI CDB contains an invalid group code for a transfer command	01
03290100	The required error information packet (EIP) or device work descriptor (DWD) were not supplied to the Device Services error logging code.	01
032A0100	HIS$GET_CONN_INFO() returned an unexpected completion code.	01
032B0100	A Device Work Descriptor (DWD) was supplied with a NULL Physical Unit Block (PUB) pointer	01
03320101	An invalid code was passed to the error recovery thread in the error_stat field of the PCB. Last Failure Parameter[0] contains the PCB error_stat code.	01

Last Fail Code	Explanation	Repair Action Code
03330188	A parity error was detected by a device port while sending data out onto the SCSI bus. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03350188	The TEA (bus fault) signal was asserted into a device port. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port BC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01

Last Fail Code	Explanation	Repair Action Code
03360188	A device port's host bus watchdog timer expired. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03370108	A device port detected an illegal script instruction. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01

Last Fail Code	Explanation	Repair Action Code
03380188	A device port's DSTAT register contains multiple asserted bits, or an invalidity asserted bit, or both. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03390108	An unknown interrupt code was found in a device port's DSPS register. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
033C0101	An invalid code was seen by the error recovery thread in the er_funct_step field of the PCB. Last Failure Parameter[0] contains the PCB er_funct_step code.	01

Last Fail Code	Explanation	Repair Action Code
033E0108	An attempt was made to restart a device port at the SDP DBD. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
033F0108	An EDC error was detected on a read of a soft-sectored device-path not yet implemented. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03410101	Invalid SCSI device type in PUB. Last Failure Parameter[0] contains the PUB SCSI device type.	01

Last Fail Code	Explanation	Repair Action Code
03420188	A UDC interrupt could not be associated with either a DWD or the non-callable scripts. Last Failure Parameter[0] contains the PCB port_ptr value. Last Failure Parameter[1] contains the PCB copy of the device port TEMP register. Last Failure Parameter[2] contains the PCB copy of the device port DBC register. Last Failure Parameter[3] contains the PCB copy of the device port DNAD register. Last Failure Parameter[4] contains the PCB copy of the device port DSP register. Last Failure Parameter[5] contains the PCB copy of the device port DSPS register. Last Failure Parameter[6] contains the PCB copies of the device port SSTAT2/SSTAT1/SSTAT0/DSTAT registers. Last Failure Parameter[7] contains the PCB copies of the device port LCRC/RESERVED/ISTAT/DFIFO registers.	01
03470100	Insufficient memory available for target block allocation.	01
03480100	Insufficient memory available for device port info block allocation.	01
03490100	Insufficient memory available for autoconfig buffer allocation.	01
034A0100	Insufficient memory available for PUB allocation.	01
034B0100	Insufficient memory available for DS init buffer allocation.	01
034C0100	Insufficient memory available for static structure allocation.	01
034D0100	DS init DWDs exhausted.	01
034E2080	Diagnostics report all device ports are broken.	20
03500100	Insufficient memory available for command disk allocation.	01
03510100	Insufficient resources available for command disk data region.	01
03520100	A failure resulted when an attempt was made to allocate a DWD for use by DS CDI.	01
035A0100	Invalid SCSI message byte passed to DS.	01
035B0100	Insufficient DWD resources available for SCSI message pass-through.	01
03640100	Processing run_switch disabled for LOGDISK associated with the other controller.	01

Last Fail Code	Explanation	Repair Action Code
03650100	Processing pub unblock for LOGDISK associated with the other controller	01
03660100	No memory available to allocate pub to tell the other controller of reset to one if its LUNs.	01
03670100	No memory available to allocate pub to tell the other controller of a bdr to one if its LUNs.	01

Table 48
Fault manager last failure codes

Last Fail Code	Explanation	Repair Action Code
04010101	The requester id component of the instance code passed to FM$REPORT_EVENT is larger than the maximum allowed for this environment. Last Failure Parameter[0] contains the instance code value.	01
04020102	The requester's error table index passed to FM$REPORT_EVENT is larger than the maximum allowed for this requester. Last Failure Parameter[0] contains the instance code value. Last Failure Parameter[1] contains the requester error table index value.	01
04030102	The USB index supplied in the EIP is larger than the maximum number of USBs. Last Failure Parameter[0] contains the instance code value. Last Failure Parameter[1] contains the USB index value.	01
04040103	The event log format found in V_fm_template_table is not supported by the Fault Manager. The bad format was discovered while trying to fill in a supplied eip. Last Failure Parameter[0] contains the instance code value. Last Failure Parameter[1] contains the format code value. Last Failure Parameter[2] contains the requester error table index value.	01
04050100	The Fault Manager could not allocate memory for his Event Information Packet (EIP) buffers.	01
04060100	The Fault Manager could not allocate a Datagram HTB in his initialization routine.	01

Last Fail Code	Explanation	Repair Action Code
04070103	There is more EIP information than will fit into a datagram. The requester specific size is probably too large. Last Failure Parameter[0] contains the instance code value. Last Failure Parameter[1] contains the format code value. Last Failure Parameter[2] contains the requester error table index value.	01
04080102	The event log format found in the already built eip is not supported by the Fault Manager. The bad format was discovered while trying to copy the eip information into a datagram HTB. Last Failure Parameter[0] contains the format code value. Last Failure Parameter[1] contains the instance code value.	01
04090100	The caller of FM$CANCEL_EVENT_NOTIFICATION passed an address of an event notification routine which does not match the address of any routines for which event notification is enabled.	01
040A0100	The caller of FM$CANCEL_SCSI_DE_NOTIFICATION passed an address of a deferred error notification routine which doesn't match the address of any routines for which deferred error notification is enabled.	01
040B0100	An error which is not related to an I/O request(htb_ptr) has an unsupported template type.	01
040D0100	FM$ENABLE_EVENT_NOTIFICATION was called to enable eip notification but the specified routine was already enabled to receive eip notification.	01
040E0100	FM$ENABLE_DE_NOTIFICATION was called to enable deferred error notification but the specified routine was already enabled to receive deferred error notification.	01
040F0102	The eip->generic.mscp1.flgs field of the EIP passed to FM$REPORT_EVENT contains an invalid flag. Last Failure Parameter[0] contains the instance code value. Last Failure Parameter[1] contains the value supplied in the eip->generic.mscp1.flgs field.	01
04100101	Unexpected template type found during fmu_display_errlog processing. Last Failure Parameter[0] contains the unexpected template value.	01
04110101	Unexpected instance code found during fmu_memerr_report processing. Last Failure Parameter[0] contains the unexpected instance code value.	01

Last Fail Code	Explanation	Repair Action Code
04120101	CLIB$SDD_FAO call failed. Last Failure Parameter[0] contains the failure status code value.	01
04130103	The event log format found in the eip is not supported by the Fault Manager. The bad format was discovered while trying to fill in the DLI of the supplied eip. Last Failure Parameters[0] contains the instance code value Last Failure Parameters[1] contains the format code value. Last Failure Parameters[2] contains the requester error table index value.	01
04140103	The template value found in the eip is not supported by the Fault Manager. The bad template value was discovered while trying to build an esd. Last Failure Parameters[0] contains the instance code value Last Failure Parameters[1] contains the template code value. Last Failure Parameters[2] contains the requester error table index value.	01

Table 49
Common library last failure codes

Last Fail Code	Explanation	Repair Action Code
05010100	In recursive_nonconflict could not get enough memory for scanning the keyword tables for configuration name conflicts.	01
05030100	In clib$scan_for_nonconflict could not get enough memory for scanning the keyword tables for configuration name conflicts.	01

Table 50
DUART services last failure codes

Last Fail Code	Explanation	Repair Action Code
06010100	The DUART was unable to allocate enough memory to establish a connection to the CLI.	01
06020100	A port other than terminal port A was referred to by a set terminal characteristics command. This is illegal.	01
06030100	A DUP question or default question message type was passed to the DUART driver, but the pointer to the input area to receive the response to the question was NULL.	01
06040100	Attempted to detach unattached maintenance terminal.	01

Last Fail Code	Explanation	Repair Action Code
06050100	Attempted output to unattached maintenance terminal.	01
06060100	Attempted input from output only maintenance terminal service.	01
06070100	The DUART was unable to allocate enough memory for its input buffers.	01
06080000	Controller was forced to restart due to entry of a CONTROL-K character on the maintenance terminal.	00

Table 51
Failover control last failure codes

Last Fail Code	Explanation	Repair Action Code
07010100	All available slots in the FOC notify table are filled	01
07020100	FOC$CANCEL_NOTIFY() was called to disable notification for a rtn that did not have notification enabled	01
07030100	Unable to start the Failover Control Timer before main loop	01
07040100	Unable to restart the Failover Control Timer	01
07050100	Unable to allocate flush buffer	01
07060100	Unable to allocate active receive fcb	01
07070100	The other controller killed this controller, but could not assert the kill line because nindy was on or in debug. It killed this controller now.	01
07080000	The other controller crashed, so this one must crash too.	00

Table 52
Nonvolatile parameter memory failover control last failure codes

Last Fail Code	Explanation	Repair Action Code
08010101	A remote state change was received from the FOC thread that NVFOC does not recognize. Last Failure Parameter[0] contains the unrecognized state value.	01
08020100	No memory could be allocated for a NVFOC information packet.	01
08030101	Work received on the S_nvfoc_bque did not have a NVFOC work id. Last Failure Parameter[0] contains the id type value that was received on the NVFOC work queue.	01
08040101	Unknown work value received by the S_nvfoc_bque. Last Failure Parameter[0] contains the unknown work value.	01

Last Fail Code	Explanation	Repair Action Code
08050100	An unlock was received and the controller was not locked by the other controller. This last_failure code was removed from HSOF firmware at Version 2.7.	01
08060100	A really write command was received when the NV memory was not locked.	01
08070100	A write to NV memory was received while not locked.	01
08080000	The other controller requested this controller to restart.	00
08090010	The other controller requested this controller to shutdown.	00
080A0000	The other controller requested this controller to selftest.	00
080B0100	Could not get enough memory to build a FCB to send to the remote routines on the other controller.	01
080C0100	Could not get enough memory for FCBs to receive information from the other controller.	01
080D0100	Could not get enough memory to build a FCB to reply to a request from the other controller.	01
080E0101	An out-of-range receiver ID was received by the NVFOC communication utility (master send to slave send ACK). Last Failure Parameter[0] contains the bad id value.	01
080F0101	An out-of-range receiver ID was received by the NVFOC communication utility (received by master). Last Failure Parameter[0] contains the bad id value.	01
08100101	A call to NVFOC$TRANSACTION had a from field (id) that was out of range for the NVFOC communication utility. Last Failure Parameter[0] contains the bad id value.	01
08110101	NVFOC tried to defer more than one FOC send. Last Failure Parameter[0] contains the master ID of the connection that had the multiple delays.	01
08120100	Unable to lock other controller's NVmemory despite the fact that the running and handshake_complete flags are set.	01
08130100	Could not allocate memory to build a callback context block on an unlock NVmemory call.	01
08140100	Could not allocate memory to build a workblock to queue to the NVFOC thread.	01
08150100	A lock was requested by the other controller but the memory is already locked by the other controller.	01
08160100	A request to clear the remote configuration was received but the memory was not locked.	01
08170100	A request to read the next configuration was received but the memory was not locked.	01

Last Fail Code	Explanation	Repair Action Code
08180100	Could not get enough memory for FLS FCBs to receive information from the other controller.	01
08190100	An unlock command was received when the NV memory was not locked. Removed from HSOF firmware at Version 2.7.	01
081A0100	Unable to allocate memory for remote work.	01
081B0101	Bad remote work received on remote work queue. Last Failure Parameter[0] contains the id type value that was received on the NVFOC remote work queue.	01
081C0101	Bad member management work received. Last Failure Parameter[0] contains the bad member management value that was detected.	01
081F0000	An FLM$INSUFFICIENT_RESOURCES error was returned from a FLM lock or unlock call.	01
08200000	Expected restart so the write_instance may recover from a configuration mismatch.	01
08210100	Unable to allocate memory to setup NVFOC lock/unlock notification routines.	01

Table 53
Facility lock manager last failure codes

Last Fail Code	Explanation	Repair Action Code
09010100	Unable to acquire memory to initialize the FLM structures.	01
09640101	Work that was not FLM work was found on the FLM queue. Bad format is detected or the formatted string overflows the output buffer. Last Failure Parameter[0] contains the work found.	01
09650101	Work that was not FLM work was found on the FLM queue. Last Failure Parameter[0] contains the structure found.	01
09670101	Local FLM detected an invalid facility to act upon. Last Failure Parameter[0] contains the facility found.	01
09680101	Remote FLM detected an error and requested the local controller to restart. Last Failure Parameter[0] contains the reason for the request.	01
09C80101	Remote FLM detected an invalid facility to act upon. Last Failure Parameter[0] contains the facility found.	01
09C90101	Remote FLM detected an invalid work type. Last Failure Parameter[0] contains the work type found.	01
09CA0101	Remote FLM detected an invalid work type. Last Failure Parameter[0] contains the work type found.	01

Last Fail Code	Explanation	Repair Action Code
09CB0012	Remote FLM detected that the other controller has a facility lock manager at an incompatible revision level with this controller. Last Failure Parameter[0] contains this controller's FLM revision. Last Failure Parameter[1] contains the other controller's FLM revision.	01

Table 54
Integrated logging facility last failure codes

Last Fail Code	Explanation	Repair Action Code
0A010100	CACHE$FIND_LOG_BUFFERS returned continuation handle >0.	01
0A020100	ILF$CACHE_READY unable to allocate necessary DWDs.	01
0A030100	ILF$CACHE_READY buffers_obtained > non-zero stack entry count.	01
0A040100	ILF$CACHE_READY DWD overrun.	01
0A050100	IFL$CACHE_READY DWD underrun.	01

Table 55
CLI last failure codes

Last Fail Code	Explanation	Repair Action Code
20010100	The action for work on the CLI queue should be CLI_CONNECT, CLI_COMMAND_IN or CLI_PROMPT. If it isn't one of these three, this bugcheck will result.	01
20020100	The FAO returned a non-successful response. This will only happen if a bad format is detected or the formatted string overflows the output buffer.	01
20030100	The type of work received on the CLI work queue wasn't of type CLI.	01
20060100	A work item of an unknown type was placed on the CLI's SCSI Virtual Terminal thread's work queue by the CLI.	01
20070100	A work item of an unknown type was placed on the CLI's DUP Virtual Terminal thread's work queue by the CLI.	01
20080000	This controller requested this controller to restart.	00
20090010	This controller requested this controller to shutdown.	00
200A0000	This controller requested this controller to selftest.	00
200B0100	Could not get enough memory for FCBs to receive information from the other controller.	01

Last Fail Code	Explanation	Repair Action Code
200C0100	After a CLI command the NV memory was still locked. The CLI should always unlock NV memory when the command is complete (if it had an error or not). Removed from HSOF firmware at Version 2.7.	01
200D0101	After many calls to DS$PORT_BLOCKED, we never got a FALSE status back (which signals that nothing is blocked). Last Failure Parameter[0] contains the port number (1 - n) that we were waiting on to be unblocked.	01
200E0101	While traversing the structure of a unit, a config_info node was discovered with an unrecognized structure type. Last Failure Parameter[0] contains the structure type number that was unrecognized.	01
200F0101	A config_info node was discovered with an unrecognized structure type. Last Failure Parameter[0] contains the structure type number that was unrecognized.	01
20100101	A config_node of type VA_MA_DEVICE had an unrecognized SCSI device type. Last Failure Parameter[0] contains the SCSI device type number that was unrecognized.	01
20110100	An attempt to allocate memory so the CLI prompt messages could be deleted failed.	01
20120101	While traversing the structure of a unit, a config_info node was discovered with an unrecognized structure type. Last Failure Parameter[0] contains the structure type number that was unrecognized.	01
20130101	While traversing the structure of a unit, the device was of a unrecognized type. Last Failure Parameter[0] contains the SCSI device type that was unrecognized.	01
20150100	On SCSI failover, both controllers must be restarted for failover to take effect. This is how this controller is restarted in COPY=OTHER.	01
20160100	Unable to allocate resources needed for the CLI local program.	01
20180010	User requested this controller's parameters to be set to initial configuration state.	00
20190010	A cache state of a unit remains WRITE_CACHE_UNWRITTEN_DATA. The unit is not ONLINE, thus this state would only be valid for a very short period of time.	00
201A0100	An attempt to allocate memory so a CLI prompt message could be reformatted has failed.	01

Last Fail Code	Explanation	Repair Action Code
201B0100	Insufficient resources to get memory to lock CLI.	01
201C0100	Insufficient resources to get memory to unlock CLI.	01
20640000	Nindy was turned on.	00
20650000	Nindy was turned off.	00
20692010	To enter dual-redundant mode both controllers must be of the same type.	20
206A0000	Controller restart forced by DEBUG CRASH REBOOT command.	01
206B0010	Controller restart forced by DEBUG CRASH NOREBOOT command.	01

Table 56
Host interconnect services last failure codes

Last Fail Code	Explanation	Repair Action Code
40000101	HSJ3x/4x: An unrecognized DSSI opcode was received by HIS. These packets are packets with CI opcodes recognized by the port but not by HIS. Last Failure Parameter[0] contains the CI opcode value. HSD3x/4x/HS1CP: An unrecognized DSSI opcode was received by HIS. These packets are packets with DSSI opcodes recognized by the port but not by HIS. Last Failure Parameter[0] contains the DSSI opcode value.	01
4007640A	HSD3x/4x/HS1CP: DSSI Port detected error upon attempting to transmit a packet. This resulted in the closure of the Virtual Circuit.	64
40150100	LOCAL VC Timer in unexpected state.	01
40280100	Failed to allocate Buffer Name Table.	01
40290100	Failed to allocate ACB.	01
402A0100	Failed to allocate ID member template.	01
402B0100	Failed to allocate DG HTBs.	01
402C0100	Failed to allocate message HTBs.	01
402D0101	S_max_node greater than MAX_VC_ENTRIES. Last Failure Parameter[0] contains the S_ci_max_nodes value.	01
402E0101	S_max_node not set to valid value (8, 16, 32, 64, 128, 256). Last Failure Parameter[0] contains the S_ci_max_nodes value.	01
402F0100	Failure to allocate a HIS EIP structure.	01

Last Fail Code	Explanation	Repair Action Code
40300100	Failure in memory allocation.	01
40510100	htb_id type not DG, when attempting to deallocate DG HTB.	01
40520100	htb_id type not RCV_SND, when attempting to dealloc recv queue HTB.	01
40530100	htb_id type not RCV_SND, when attempting to dealloc SCS queue HTB.	01
40560100	Failed to find a vc entry for ccb during his_close_connection routine.	01
407B0100	SCS command timeout unexpectedly inactive during SCS Accept Request.	01
407C0100	SCS command timeout unexpectedly inactive during SCS Reject Request.	01
408E0100	Message receive queue count disagrees with # HTBs on the queue.	01
408F0100	Unrecognized HTB id type.	01
40900100	htb_id type not DG, when attempting to xmit DG HTB.	01
40930100	Message receive queue count disagrees with # HTBs on the queue.	01
40950100	Create xfer request with 0-byte count	01
40960100	Create xfer request with 0-byte count	01
40970100	Create xfer request with 0-byte count	01
40980100	Create xfer request with 0-byte count	01
409D0100	Illegal return value from HIS$MAP.	01
40B40101	Invalid value in max_nodes field of se_params structure. Last Failure Parameter[0] contains the max_nodes field value.	01

Table 57
SCSI host interconnect services last failure codes

Last Failure Code	Explanation	Repair Action Code
41000100	Encountered an unexpected structure type on S_shis_ctl.scsi_q.	01
41020100	Unable to allocate the necessary number of HTBS in shis_init().	01
41030100	Unable to allocate the necessary number of large Sense Data buckets in shis_init().	01
41060100	Unable to locate the IDENTIFY msg in HTB.	01

Last Failure Code	Explanation	Repair Action Code
41070100	Encountered an unknown MESSAGE OUT message.	01
41080100	Encountered an unknown MESSAGE OUT message.	01
41090100	Encountered an unknown structure on the host port queue. During SCSI ABORT message.	01
410A0100	Encountered an unknown structure on the host port queue. During SCSI ABORT TAG message.	01
410B0100	Encountered an unknown structure on the host port queue. During SCSI CLEAR QUEUE message.	01
410E0100	Encountered an unrecognized queue tag message.	01
41100100	Encountered a NULL completion routine pointer in a DD.	01
41130100	Could not allocate a large sense bucket.	01
41160100	A sense data bucket of unknown type (neither LARGE or SMALL) was passed to deallocate_SDB().	01
41170100	Call to VA$ENABLE_NOTIFICATION() failed due to INSUFFICIENT_RESOURCES.	01
41180100	Encountered a NULL completion routine pointer in a Work q entry.	01

Table 58
Host interconnect port services last failure codes

Last Fail Code	Explanation	Repair Action Code
42000100	Cmpl_main routine found invalid port xmt status.	01
42020100	Cannot start timer.	01
42030100	Cannot restart work timer.	01
42040100	Host port buffer allocation macro found an error allocating free buffers. The free buffer was NULLPTR. $DEBUG conditional.	01
42060100	HP_INIT could not allocate initial buffers.	01
420B0100	HP_INIT could not allocate initial buffs for Path A dl_ctl table.	01
420C0100	HP_INIT could not allocate initial htb for Path A.	01
420D0100	HP_INIT could not allocate HPHW structure.	01
42120100	Host Port polling HTB failed to complete in time. This last_failure code was removed from HSOF firmware at Version 2.7.	01
42126500	Host Port polling HTB failed to complete in time.	65
42130100	Host Port detected a inconsistency in the HW transmit status.	01

Last Fail Code	Explanation	Repair Action Code
42316601	Host Port found that the controller has exceeded the maximum number of user specified host VCS. Last Failure Parameter[0] is a 32-bit MASK of OPEN VCS the controller sees to host nodes.	66
42332080	Receive_main found destination address in the rcv packet does not match node address.	20
42340100	HP could not allocate buffers for I/O rundown in VC Close.	01
42350100	HP found a negative offset in a Host Data transfer Operation.	01
42382080	Ci_isr found that the yaci hardware had invalid xmt status on Path A, no bits set.	20
42392080	Ci_isr found that the yaci hardware had invalid xmt status on Path B, no bits set.	20
423A2080	CI_ISR found the abort bit set with out any valid reason. Path A.	20
423B2080	CI_ISR found transmit parity error without abort bit set. Path A.	20
423C2080	CI_ISR found buffer underflow without abort bit set. Path A.	20
423D2080	CI_ISR found the abort bit set with out any valid reason. Path B.	20
423E2080	CI_ISR found transmit parity error without abort bit set. Path B.	20
423F2080	CI_ISR found buffer underflow without abort bit set. Path B.	20
42442080	Ci_isr found that yaci hardware had a parity error.	20
42452080	Ci_isr found that yaci hardware had a bus timeout error.	20
42472080	Ci_isr found Data parity on Transmit Path A.	20
42482080	Ci_isr found Data parity on Transmit Path B.	20
424B0001	Ci_isr found Host Reset on Path A. Last Failure Parameter[0] contains the node number of the resetting node.	00
424C0001	Ci_isr found Host Reset on Path B. Last Failure Parameter[0] contains the node number of the resetting node.	00
424D2080	Ci_isr found Fetch parity on Transmit Path A.	20
424E2080	Ci_isr found Fetch parity on Transmit Path B.	20
424F0100	HP could not allocate buffers to repopulate dds when we close path.	01

Last Fail Code	Explanation	Repair Action Code
42506700	CI Host Port detected an arbitration timeout on path A. Persistent Hardware faults generating an arbitration timeout will cause the controller to repeatedly reboot.	67
42516700	CI Host Port detected an arbitration timeout on path b. Persistent Hardware faults generating an arbitration timeout will cause the controller to repeatedly reboot.	67
42590001	Ci_isr found Host Reset on Path A. Last Failure Parameter[0] contains the node number of the resetting node.	00
425A0001	Ci_isr found Host Reset on Path B. Last Failure Parameter[0] contains the node number of the resetting node.	00
425B2080	CI_ISR found the abort bit set with out any valid reason. Path A.	20
425C2080	CI_ISR found transmit parity error without abort bit set. Path A.	20
425D2080	CI_ISR found buffer underflow without abort bit set. Path A.	20
425E2080	Ci_isr found that the yaci hardware had invalid xmt status on path a, no bits set.	20
425F2080	CI_ISR found the abort bit set with out any valid reason. Path B.	20
42602080	CI_ISR found transmit parity error without abort bit set. Path B.	20
42612080	CI_ISR found buffer underflow without abort bit set. Path B.	20
42622080	Ci_isr found that the yaci hardware had invalid xmt status on Path B, no bits set.	20
42632080	Receive_main found destination address in the rcv packet does not match node address.	20
42640100	Scan packet que found bad path select case for DSSI	01
42680102	Dssi_wait_isr routine found that 720 report unexpected interrupt status for target mode. Last Fail Parameter[0] contains the 720 chip sist0 register value. Last Failure Parameter[1] contains the 720 chip sist1 register value.	01
42690101	Dssi_wait_isr routine found that the 720 script reported an invalid rcv status. Last Failure Parameter[0] contains the receive interrupt status N720)_dsps value.	01

Last Fail Code	Explanation	Repair Action Code
426B0101	Dssi_wait_isr routine found that 720 interrupted without status. Last Failure Parameter[0] contains the 720 chip istat register value.	01
42752002	Dssi_wait_isr routine found that 720 reported a bus error on the controller's internal bus. Last Failure Parameter[0] contains the 720 chip dstat register value. Last Failure Parameter[1] contains the 720 chip dcmd register value.	20
42760102	Dssi_wait_isr routine found that 720 reported an unexpected status for initiator mode. Last Failure Parameter[0] contains the 720 chip dstat register value. Last Failure Parameter[1] contains the 720 chip dcmd register value.	01
42770102	Dssi_wait_isr routine found that 720 reported an unexpected status for initiator mode. Last Failure Parameter[0] contains the 720 chip dstat register value. Last Failure Parameter[1] contains the 720 chip dcmd register value.	01
42790103	Dssi_wait_isr routine found that 720 reported an unexpected status in initiator mode causes stacked interrupters too many. Last Failure Parameter[0] contains the 720 chip dstat register value. Last Failure Parameter[1] contains the 720 chip dcmd register value.	01
427A6601	Host port found that the controller has exceeded the maximum number of user specified host VCs Last Failure Parameter[0] is a 32-bit MASK of OPEN VCs the controller sees to host nodes.	66

Table 59
Disk and tape MSCP server last failure codes

Last Fail Code	Explanation	Repair Action Code
60030100	Unable to fine free DCD_CMDCORL_BLOCK.	01
60050100	Invalid return value from routine HIS$CONNECT, while DCD attempting to establish connection to a remote subsystem.	01
60070100	Invalid return value from routine HIS$MAP, while dmscp_dcd_allocate_bh attempting to map a buffer.	01

Last Fail Code	Explanation	Repair Action Code
60090100	Invalid return value from routine HIS$DISCONNECT, while dmscp_dcd_comm_path_event attempting to disconnect a remote source connection.	01
600C0100	Invalid return value from routine RESMGR$ALLOCATE_DATA_SEGMENT.	01
600D0100	Opcode field in command being aborted is not valid.	01
60120100	Opcode of TMSCP command to be aborted is invalid.	01
60130100	tmscp_clear_sex_cdl_cmpl_rtn detected an unexpected opcode.	01
60140100	tmscp_clear_sex_cdl_cmpl_rtn detected an unexpected opcode.	01
60150100	VA$CHANGE_STATE failed to change the SW Write protect when requested to do so as part of the Disk Set Unit Characteristics command.	01
60160100	VA$CHANGE_STATE failed to change the SW Write protect when requested to do so as part of the Tape Set Unit Characteristics command.	01
60170100	Invalid type in entry of long interval work queue.	01
60180100	mscp_short_interval found an Invalid type in entry of long interval work queue.	01
60190100	dmscp_dcd_send_cmd found that the SIWI Work Item code supplied is unrecognized or invalid in this context during DCD inhibited processing.	01
601B0100	Invalid EVENT_CODE parameter in call to dmscp_connection_event.	01
601C0100	Invalid EVENT_CODE parameter in call to tmscp_connection_event.	01
601D0100	Invalid EVENT_CODE parameter in call to dmscp_dcd_comm_path_event.	01
601E0100	Invalid EVENT_CODE parameter in call to dmscp_dcd_comm_path_event.	01
60250100	An attempt was about to be made to return a progress indicator to the host that was OxFFFFFFFF, the only invalid value.	01
60260100	An WH_DAF command was requested to be performed by the wrong process.	01
60270100	A nonimmediate WHM operation was passed to the dmscp_exec_whm_immediate routine.	01
60280100	This routine found an invalid xfer_state so cannot continue.	01
60290100	HIS did not allocate an HTB when there should have been one reserved for this connection as determined by mscp_rcv_listen.	01

Last Fail Code	Explanation	Repair Action Code
602A0100	HIS did not allocate an HTB when there should have been one reserved for this connection as determined by dmscp_dcd_src_gcs_send.	01
602B0100	HIS did not allocate an HTB when there should have been one reserved for this connection as determined by dmscp_dcd_comm_path_event.	01
602C0100	When trying to put THE extra send-HTB on the connections send_htb_list there was already one on the queue.	01
602D0100	The VA$CHANGE_STATE service did not set the Software write protect as requested (for disk).	01
602E0100	The VA$CHANGE_STATE service did not set the Software write protect as requested (for tape).	01
603B0100	Initial HIS$LISTEN call for MSCP$DISK was unsuccessful.	01
603C0100	Initial HIS$LISTEN call for MSCP$TAPE was unsuccessful.	01
60400100	Unrecognized or invalid in this context return value from routine RESMGR$ALLOCATE_DATA_SEGMENT, while dmscp_dcd_allocate_dseg attempting to allocate a data segment.	01
60410100	Unrecognized or invalid in this context return value from routine RESMGR$ALLOCATE_DATA_BUFFERS, while dmscp_dcd_allocate_dbuf attempting to allocate a data buffer.	01
60420100	dmscp_dcd_rmte_end_msg was unable to find a command message that corresponds to end message it is currently processing.	01
60440100	dmscp_dcd_src_gcs_cmpl found the command being GCSed is no longer at the head of the remote connection's queue.	01
60450100	dmscp_dcd_errlog_rvc found that an error log is not associated with a command, internal miscellaneous error logs are assumed to not be associated with a connection and remote miscellaneous error logs generation was not requested.	01
60460100	dmscp_dcd_elrt_scc_send was entered to issue a remote source connection SCC but was unable to find an available HTB on the connection's htb_list. With no active DCDs the connection should always have HTBs available.	01
60480100	tmscp_suc_avl_cmpl_rtn found the unit not in the available state.	01
60490100	tmscp_clear_sex_cdl_cmpl_rtn found the state change failed.	01
604A0100	tmscp_clear_sex_cdl_cmpl_rtn found the state change failed.	01

Last Fail Code	Explanation	Repair Action Code
604B0100	Subroutine process_event returned a value to dmscp_dcd_comm_path_event that indicates that an internal disconnect request occurred while processing an immediate communications event.	01
604D0100	Subroutine process_event returned a value to dmscp_dcd_comm_path_event that indicates that a connection established event occurred while no DCD commands were active.	01
604F0100	tmscp_set_sex_cmpl_rtn found the state change failed.	01
60500100	dmscp_dcd_op_cmpl found an unrecognized P_STS value in a DCD HTB status field.	01
60550100	mscp_initialize unable to get LOCAL STATIC memory from exec for use as a local connection ITB.	01
60560100	mscp_initialize unable to get LOCAL STATIC memory from exec for use as an AVAILABLE ITB.	01
60570100	mscp_initialize unable to get LOCAL STATIC memory from exec for use as an AVAILABLE state change ITB.	01
60580100	mscp_initialize unable to get LOCAL STATIC memory from exec for use as a state change ITB.	01
605D0100	tmscp_onl_cleanup_rtn detected a failure in enabling variable speed mode suppression.	01
605E0100	tmscp_suc_cmpl_rtn detected a failure in enabling variable speed mode suppression.	01
605F0100	tmscp_suc_cmpl_rtn detected a failure in enabling variable speed mode suppression.	01
60610100	mscp_initialize unable to get BUFFER STATIC memory from exec for use as Write History Logs.	01
60620100	mscp_initialize unable to get LOCAL STATIC memory from exec for use as Write History Log Allocation Failure Lists.	01
60640100	Invalid condition when there exists no unused Write History Log Entries.	01
60650100	Attempting to block incoming requests for the tape/loader when it was unexpectedly found already blocked.	01
60660100	Loader boundary block request to stall incoming requests to the tape/loader unit was not setup as expected.	01
60670100	The controller has insufficient memory available for allocating context blocks needed for Disk_Copy_Data commands.	01
60680100	VA$ENABLE_NOTIFICATION failed with insufficient resources at init time.	01
606B0100	mscp_foc_receive_cmd detected that the message sent from the other controller had an illegal usb index.	01

Last Fail Code	Explanation	Repair Action Code
606C0100	mscp_foc_receive_cmd detected that the message sent from the other controller had an illegal exclusive access state.	01
606D0100	FOC provided mscp_foc_send_cmpl_rtn with an invalid status for the FOC$SEND transmit command completion.	01
606E0100	FOC provided mscp_foc_send_rsp_done with an invalid transmit status for the FOC$SEND transmit response completion.	01

Table 60
Diagnostics and utilities protocol server last failure codes

Last Fail Code	Explanation	Repair Action Code
61010000	Controller crash was intentionally caused by the execution of the CRASH program. This bugcheck does not indicate the occurrence of a controller failure. Removed from HSOF firmware at Version 2.7	00
61020100	HIS$LISTEN call failed with INSUFFICIENT_RESOURCES.	01
61090100	LISTEN_CONNECTION_ESTABLISHED event from HIS specified a connection ID for a connection we already know about.	01
610B0100	Code Load or Code Patch utility in CLCP local program forced controller restart to force new code or patch to take effect. This last_failure code was removed from HSOF firmware at Version 2.7	01
610C0100	HIS has reported a connection event that should not be possible.	01

Table 61
System communication services directory last failure code

Last Fail Code	Explanation	Repair Action Code
62000100	HIS$LISTEN call failed with INSUFFICIENT_RESOURCES.	01
62020100	Failure to allocate associated timer queue.	01
62030100	Failure to allocate connection id timers.	01

Table 62
SCSI host value-added services last failure codes

Last Fail Code	Explanation	Repair Action Code
64000100	Insufficient buffer memory to allocate data structures needed to propagate SCSI Mode Select changes to other controller.	01
64010100	During initialization of LUN specific mode pages, an unexpected device type was encountered.	01

Table 63
Disk inline exerciser (DILX) last failure codes

Last Fail Code	Explanation	Repair Action Code
80010100	An HTB was not available to issue an I/O when it should have been	01
80020100	A unit could not be dropped from testing because an available cmd failed.	01
80030100	DILX tried to release a facility that wasn't reserved by DILX	01
80040100	DILX tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources	01
80050100	DILX tried to change the usb unit state from MAINTENANCE_MODE to NORMAL but DILX never received notification of a successful state change	01
80060100	DILX tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was not successful	01
80070100	DILX aborted all cmds via va$d_abort() but the HTBS haven't been returned	01
80080100	While DILX was deallocating his eip buffers, at least one could not be found.	01
80090100	DILX received an end msg which corresponds to an op code not supported by DILX	01
800A0100	DILX was not able to restart his timer	01
800B0100	DILX tried to issue an I/O for an opcode not supported	01
800C0100	DILX tried to issue a oneshot I/O for an opcode not supported	01
800D0100	A DILX device control block contains an unsupported unit_state	01
800E0100	While trying to print an Event Information Packet, DILX discovered an unsupported MSCP error log format.	01
800F0100	A DILX cmd completed with a sense key that DILX does not support	01
80100100	DILX could not compare buffers because no memory was available from EXEC$ALLOCATE_MEM_ZEROED	01
80110100	While DILX was deallocating his deferred error buffers, at least one could not be found	01
80120100	DILX expected an eip to be on the receive eip q but no eips were there.	01
80130100	DILX was asked to fill a data buffer with an unsupported data pattern.	01
80140100	DILX could not process an unsupported answer in dx$reuse_params().	01

Last Fail Code	Explanation	Repair Action Code
80150100	A deferred error was received with an unsupported template.	01

Table 64
Tape inline exerciser (TILX) last failure codes

Last Fail Code	Explanation	Repair Action Code
81010100	An HTB was not available to issue an I/O when it should have been	01
81020100	A unit could not be dropped from testing because an available cmd failed	01
81030100	TILX tried to release a facility that wasn't reserved by TILX	01
81040100	TILX tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources	01
81050100	TILX tried to change the usb unit state from MAINTENANCE_MODE to NORMAL but TILX never received notification of a successful state change	01
81060100	TILX tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was not successful	01
81070100	TILX aborted all cmds via va$d_abort() but the htbs haven't been returned	01
81080100	While TILX was deallocating his eip buffers, at least one could not be found	01
81090100	TILX received an end msg which corresponds to an opcode not supported by TILX	01
810A0100	TILX was not able to restart his timer	01
810B0100	TILX tried to issue an I/O for an opcode not supported	01
810D0100	A TILX device control block contains an unsupported unit_state	01
810E0100	TILX received an unsupported Value Added status in a Value added completion message.	01
810F0100	TILX found an unsupported device control block substate while trying to build a cmd for the Basic Function test	01
81100100	TILX found an unsupported device control block substate while trying to build a cmd for the Read Only test	01
81110100	TILX found an unsupported device control block substate while trying to build a cmd for the User Defined test	01
81120100	TILX received an EOT encountered while in a substate where EOT encountered should not occur	01

Last Fail Code	Explanation	Repair Action Code
81130100	TILX calculated an illegal position type value while trying to generate a cmd for the position intensive phase of the Basic Function test	01
81140100	While trying to print an Event Information Packet, TILX discovered an unsupported MSCP error log format	01
81150100	A cmd which TILX issued was terminated with a sense key of SCSI_SENSEKEY_ILLEGAL_REQUEST	01
81160100	A cmd which TILX issued was terminated with a sense key of SCSI_SENSEKEY_VOLUME_OVERFLOW but the End of Medium bit is not set	01
81170100	A TILX cmd completed with a sense key that TILX does not support	01
81180100	TILX found an unsupported device control block substate while trying to build a SCSI cmd for the Basic Function test	01
81190100	While TILX was deallocating his deferred error buffers, at least one could not be found	01
811A0100	TILX expected a deferred error to be on the receive deferred error q but no deferred errors were there.	01
811B0100	TILX was asked to fill a data buffer with an unsupported data pattern.	01
811C0100	TILX could not process an unsupported answer in tx$reuse_params().	01
811D0100	TILX received a SCSI deferred error with a template which is not supported	01

Table 65
Device configuration utilities (CONFIG/CFMENU) last failure codes

Last Fail Code	Explanation	Repair Action Code
83020100	An unsupported message type or terminal request was received by the CONFIG virtual terminal code from the CLI	01
83030100	Not all alter_device requests from the CONFIG utility completed within the timeout interval	01
83050100	An unsupported message type or terminal request was received by the CFMENU utility code from the CLI	01
83060100	Not all alter_device requests from the CFMENU utility completed within the timeout interval	01

Table 66
Clone unit utility (CLONE) last failure codes

Last Fail Code	Explanation	Repair Action Code
84010100	An unsupported message type or terminal request was received by the CLONE virtual terminal code from the CLI	01

Last Fail Code	Explanation	Repair Action Code
84020100	VA$GET_MEMBER_INFO returned a bad status for a member 10 times in a row.	01
84030100	VA$GET_MEMBER_INFO returned a bad status for a container 10 times in a row.	01

Table 67
Format and device code load utility (HSUTIL) last failure codes

Last Fail Code	Explanation	Repair Action Code
85010100	HSUTIL tried to release a facility that wasn't reserved by HSUTIL.	01
85020100	HSUTIL tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources.	01
85030100	HSUTIL tried to change the usb unit state from MAINTENANCE_MODE to NORMAL but HSUTIL never received notification of a successful state change	01
85040100	HSUTIL tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was not successful.	01

Table 68
Code load/code patch utility (CLCP) last failure codes

Last Fail Code	Explanation	Repair Action Code
86000020	Controller was forced to restart in order for new code load or patch to take effect.	00
86010010	The controller code load function is about to update the program card. This requires controller activity to cease. This code is used to inform the other controller this controller will stop responding to inter-controller communications during card update. An automatic restart of the controller at the end of the program card update will cause normal controller activity to resume.	00

Table 69
Induce controller crash utility (CRASH) last failure codes

Last Fail Code	Explanation	Repair Action Code
88000000	Controller was forced to restart due to the execution of the CRASH utility.	00

Repair action codes

This section contains the repair action codes you will reference from Instance Codes and Last Fail codes.

Table 70
Repair action codes

Repair Action Code	Action to take
00	No action necessary
01	An unrecoverable hardware detected fault occurred or an unrecoverable firmware inconsistency was detected, proceed with controller support avenues.
02	Inconsistent or erroneous information was received from the operating system. Proceed with operating system software support avenues.
03	Follow the recommended repair action contained in the Last Failure Code.
04	There are two possible problem sources: 1. In the case of a shelf with dual power supplies, one of the power supplies has failed. Follow repair action 07 for the power supply with the power LED out. 2. One of the shelf blowers has failed. Follow repair action 06.
05	There are four possible problem sources: 1. Total power supply failure on a shelf. Follow repair action 09. 2. A device inserted into a shelf that has a broken internal SBB connector. Follow repair action 0A. 3. A standalone device is connected to the controller with an incorrect cable. Follow repair action 08. 4. A controller hardware failure. Follow repair action 20.
06	Determine which blower failed and replace it.
07	Replace the power supply.
08	Replace the cable. Refer to the specific device documentation.
09	Determine power failure cause.
10	Restore on-disk configuration information to original state.
0A	Determine which SBB has a failed connector and replace it.
0B	The other controller in a dual-redundant configuration has been reset with the Kill line by the controller that reported the event. To restart the Killed controller enter the CLI command RESTART OTHER on the Surviving controller and then depress the (//) RESET button on the Killed controller. If the other controller is repeatedly being Killed for the same or a similar reason, follow repair action 20.

Repair Action Code	Action to take
0C	Both controllers in a dual-redundant configuration are attempting to use the same SCSI ID (either 6 or 7, as indicated in the event report). Note: The other controller of the dual-redundant pair has been reset with the Kill line by the controller that reported the event. Two possible problem sources are indicated: 1. A controller hardware failure. 2. A controller backplane failure. First, follow repair action 20 for the Killed controller. If the problem persists, then follow repair action 20 for the Surviving controller. If the problem still persists, then replace the controller backplane.
0D	The Environmental Monitor Unit (EMU) has detected an elevated temperature condition. Check the shelf and its components for the cause of the fault.
0E	The Environmental Monitor Unit (EMU) has detected an external air-sense fault. Check components outside of the shelf for the cause of the fault.
0F	An environmental fault previously detected by the EMU is now fixed. The EIP is used to notify that the repair was successful.
20	Replace the controller module.
22	Replace the indicated cache module, or the appropriate memory SIMMs located on the indicated cache module.
23	Replace the indicated write cache battery. Caution: BATTERY REPLACEMENT MAY CAUSE INJURY.
24	Check for the following invalid write cache configurations: If it is the wrong write cache module, replace with the matching module or clear the invalid cache error via the CLI. See the *CLI Reference Manual* for details. If the write cache module is missing, re-seat cache if it is actually present, or add the missing cache module or clear the invalid cache error via the CLI. See the *CLI Reference Manual* for details. If this is a dual-redundant configuration and one of the write cache modules is missing, match write cache boards with both controllers. If this is a dual-redundant configuration and both caches are not of the same type, for example both write cache, replace a cache module to assure both are compatible. If this is a dual-redundant configuration and both write caches are not of the same size, replace a cache module to assure both are compatible. If the cache module is populated with memory SIMMs in an illegal configuration, reconfigure according to guidelines.
25	An unrecoverable Memory System failure occurred. Upon restart the controller will generate one or more Memory System Failure Event Sense Data Responses. Follow the repair actions contained in the responses.

Repair Action Code	Action to take
26	The Master DRAB detected a Cache Time-out condition. The cache regions in effect are identified in the Master DRAB RSR register as follows. Bits 8 through 11 identify the CACHEA memory region Bits 12 through 15 identify the CACHEB memory region Bits 20 through 23 the CACHEA DRAB registers region Bits 24 through 27 identify the CACHEB DRAB registers region If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 36.
27	The Master DRAB detected an Nbus Transfer Error Acknowledge (TEA) condition. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 36.
28	A Multiple Bit ECC error was detected by the Master DRAB. Use the following register information to locate additional details. The Master DRAB DER register bits 0 through 6 contain the syndrome value. The Master DRAB EAR register combined with Master DRAB ERR bits 0 through 3 (address region) yields the affected memory address. The Master DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 34.

Repair Action Code	Action to take
29	A Multiple Bit ECC error was detected by the CACHEA0 or CACHEA1 DRAB. Use the following register information to locate additional details. The CACHEAn DRAB DER register bits 0 through 6 contain the syndrome value. The CACHEAn DRAB EAR register combined with the Master DRAB RSR register bits 8 through 11 (CACHEA memory region) yields the affected memory address. The CACHEAn DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 34.
2A	A Multiple Bit ECC error was detected by the CACHEB0 or CACHEB1 DRAB. Use the following register information to locate additional details. The CACHEBn DRAB DER register bits 0 through 6 contain the syndrome value. The CACHEBn DRAB EAR register combined with the Master DRAB RSR register bits 12 through 15 (CACHEB memory region) yields the affected memory address. The CACHEBn DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 34.

Repair Action Code	Action to take
2B	The Master DRAB detected an Ibus to Nbus Time-out condition. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. If any of the following is true, a firmware fault is indicated; follow repair action 01. Master DRAB CSR register bits 10 through 12 contains the value 1 and WDR1 register bit 26 is clear. Master DRAB CSR register bits 10 through 12 contains the value 2 and WDR1 register bit 27 is clear. Master DRAB CSR register bits 10 through 12 contains the value 3 and WDR1 register bit 28 is clear. Master DRAB CSR register bits 10 through 12 contains the value 4 and WDR1 register bit 29 is clear. Master DRAB CSR register bits 10 through 12 contains the value 5 and WDR1 register bit 30 is clear. Master DRAB CSR register bits 10 through 12 contains the value 6 and WDR1 register bit 31 is clear. If none of the above conditions were true, follow repair action 36.
2C	The Master DRAB detected a Nonexistent Memory Error condition. Use the following register information to locate additional details. The Master DRAB EAR register combined with Master DRAB ERR bits 0 through 3 (address region) yields the affected memory address. The Master DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 36.

Repair Action Code	Action to take
2D	The CACHEA0 or CACHEA1 DRAB detected a Nonexistent Memory Error condition. The CACHEAn DRAB EAR register combined with the Master DRAB RSR register bits 8 through 11 (CACHEA memory region) yields the affected memory address. The CACHEAn DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 36.
2E	The CACHEB0 or CACHEB1 DRAB detected a Nonexistent Memory Error condition. Use the following register information to locate additional details. The CACHEBn DRAB EAR register combined with the Master DRAB RSR register bits 12 through 15 (CACHEB memory region) yields the affected memory address. The CACHEBn DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. Follow repair action 36.
2F	The Master DRAB detected an Address Parity Error or a Write Data Parity Error condition. Use the following register information to locate additional details. The Master DRAB EAR register combined with Master DRAB ERR bits 0 through 3 (address region) yields the affected memory address. The Master DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. For Write Data Parity Error conditions Bits 0 through 3 of the Master DRAB CSR register identify the byte in error. For Address Parity Error conditions follow repair action 34. For Write Data Parity Error conditions follow repair action 35.

Repair Action Code	Action to take
30	The CACHEA0 or CACHEA1 DRAB detected an Address Parity Error or a Write Data Parity Error condition. Use the following register informtion to locate additional details about the error. If the failure occurred during a memory refresh attempt, the CACHEAn DRAB EAR register combined with the Master DRAB RSR register bits 8 through 11 (CACHEA memory region) yields the affected memory address. If the failure occurred during a memory access attempt, the CACHEA0 DRAB EAR register combined with the Master DRAB RSR register bits 8 through 11 (CACHEA memory region) or bits 20 through 23 (CACHEA DRAB register region) yields the affected memory address. Unfortunately, no other information is available to distinguish a memory region access from a DRAB register region access. The CACHEAn DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. For Write Data Parity Error conditions bits 0 through 3 of the CACHEAn DRAB CSR register identify the byte in error. For Address Parity Error conditions follow repair action 34. For Write Data Parity Error conditions follow repair action 35.
31	The CACHEB0 or CACHEB1 DRAB detected an Address Parity Error or a Write Data Parity Error condition. Use the following register information to location additional details about the error. If the failure occurred during a memory refresh attempt, the CACHEBn DRAB EAR register combined with the Master DRAB RSR register bits 8 through 11 (CACHEB memory region) yields the affected memory address. If the failure occurred during a memory access attempt, the CACHEB0 DRAB EAR register combined with the Master DRAB RSR register bits 8 through 11 (CACHEB memory region) or bits 20 through 23 (CACHEB DRAB register region) yields the affected memory address. Unfortunately, no other information is available to distinguish a memory region access from a DRAB register region access. The CACHEBn DRAB EDR register contains the error data. If the failure involved a Device Port, the Master DRAB CSR register bits 10 through 12 identify that Device Port. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. For Write Data Parity Error conditions bits 0 through 3 of the CACHEBn DRAB CSR register identify the byte in error. For Address Parity Error conditions follow repair action 34. For Write Data Parity Error conditions follow repair action 35.

Repair Action Code	Action to take
32	The Master DRAB detected an Ibus Parity Error condition. Use the following register information to locate additional details about the error. The Master DRAB EAR register combined with the Master DRAB ERR bits 4 through 7 (address region) yields the affected memory address. The Master DRAB EDR register contains the error data. If Master DRAB DSR register bit 14 is set, the failure was reported via the NMI. If Master DRAB DSR register bit 14 is clear, the failure was reported via the DRAB_INT. If bits 20 through 23 of the Master DRAB DCSR register contain a non-zero value, a firmware fault is indicated; follow repair action 01, otherwise, follow repair action 36.
33	This event report contains supplemental information related to a Memory System Failure event report delivered earlier. Use the instance code contained in the memory address field of this event report to correlate this event report with the other event report.
34	If bit 31 of the DCSR register of the DRAB that detected the failure is set, it indicate a firmware fault; follow repair action 01. If bit 31 is not set, follow repair action 36.
35	If bits 20 through 23 of the WDR1 register contain a non-zero value, it indicates a firmware fault; follow repair action 01. If bits 20 through 23 contain zero, follow repair action 36.
36	No other information is available to aid in diagnosing the cause of the failure. If the Master DRAB detected the failure, follow repair action 20. If the CACHEAn or CACHEBn DRAM detected the failure, follow repair action 22. If the problem persists, follow repair action 01.
37	The Memory System Failure translator could not determine the failure cause. Follow repair action 01.
40	If the Sense Data FRU field is non-zero, follow repair action 41. If the Sense Data FRU field is zero, replace the appropriate FRU associated with the device's SCSI interface or the entire device.
41	Consult the device's maintenance manual for guidance on replacing the indicated device FRU.
43	Update the configuration data to correct the problem.
44	Replace the SCSI cable for the failing SCSI bus. If the problem persists, replace the controller backplane, drive backplane, or controller module.
45	Interpreting the device supplied Sense Data is beyond the scope of the controller's firmware. See the device's service manual to determine the appropriate repair action, if any.
60	Swap the transmit and receive cables for the indicated path.
61	Check the indicated path cables for proper installation.
63	For HSHJ3x/4x: Check the CI adapter on the host system identified in the Remote Node Name field for proper operation. For HSD3x/HS1CP: Check the DSSI adapter on the host system identified in the Remote Node Name field for proper operation.

Repair Action Code	Action to take
64	Excessive VC closures are occurring. Perform repair action 61 on both sets of path cables. If the problem persists, perform repair action 63.
65	Polling failed to complete in a timely manner. Perform repair action 61 on all path cables.
66	The number of hosts forming virtual circuits with the controller exceeds the current user specified maximum. Increase the maximum number of hosts allowed value.
67	Perform repair action 61. If the problem persists, perform repair action 20.
68	The external cache battery cable might have been disconnected.

Glossary

Adapter
A device that converts the protocol and hardware interface of one bus type into that of another without changing the functionality of the bus.

Allocation class
A numerical value assigned to a controller to identify units across multiple, independent controllers. (Controllers in a dual-redundant configuration must have the same allocation class.)

Array controller
A hardware/software device that facilitates communications between a host and one or more devices organized in an array. HS family controllers are examples of array controllers.

BBR
Bad block replacement. The procedure used to locate a replacement block, mark the bad block as replaced, and move the data from the bad block to the replacement block.

BBU
Battery backup unit. A StorageWorks SBB option that extends power availability after the loss of primary ac power or a power supply to protect against the corruption or loss of data.

Block
The smallest data unit addressable on a disk. Also called a sector. In integrated storage elements, a block contains 512 bytes of data, EDC, ECC, flags, and the block's address header.

CDU
Cable distribution unit. The power entry device for StorageWorks cabinets. The unit provides the connections necessary to distribute ac power to cabinet shelves and fans.

CI bus
Computer interconnect bus. Uses two serial paths, each with a transfer rate of 70 Mb/s (8.75 MB/s).

CLI
Command line interpreter. Operator command line interface for the HS family controller firmware.

Controller shelf
A StorageWorks shelf designed to contain controller and cache memory modules.

CRC
An 8-character cyclic redundancy check string used in conjunction with the customer identification string for turning on licensed features such as write-back caching.

Data center cabinet
A generic reference to the large cabinets, such as the SW800-series, in which StorageWorks components can be mounted.

DDL
Dual data link. The ability to operate on the CI bus using both paths simultaneously to the same remote node.

Differential SCSI bus
A signal's level is determined by the potential difference between two wires. A differential bus is more robust and less subject to electrical noise than is a single-ended bus.

DILX
Disk inline exerciser. Diagnostic firmware used to test the data transfer capabilities of disk drives in a way that simulates a high level of user activity.

DSA
Digital storage architecture. A set of specifications and interfaces describing standards for designing mass storage products. DSA defines the functions performed by host computers, controllers, and disk drives. It also specifies how they interact to accomplish mass storage management.

DSSI
Digital storage system interconnect. A Digital-specific data bus with an 8-bit data transfer rate of 4 MB/s.

Dual-redundant configuration
Two controllers in one controller shelf providing the ability for one controller to take over the work of the other controller in the event of a failure of the other controller.

DUART
Dual universal asynchronous receiver/transmitter. An integrated circuit containing two serial, asynchronous transceiver circuits.

DUP
Diagnostic and utility protocol. Host application software that allows a host terminal to be connected to the controller's command line interpreter.

DWZZA
The StorageWorks compatible SCSI bus signal converter.

ECB
External cache battery.

ECC
Error correction code. One or more cyclic redundancy check (CRC) words that allow detection of a mismatch between transmitted and received data in a communications system, or between stored and retrieved data in a storage system. The ECC allows for location and correction of an error in the received/retrieved data. All ECCs have limited correction power.

EDC
Error detection code. One or more checksum words that allow detection of a mismatch between transmitted and received data in a communications system, or between stored and retrieved data in a storage system. The EDC has no data correction capability.

ESD
Electrostatic discharge. The discharge of a potentially harmful static electric voltage as a result of improper grounding.

Failedset
A group of disk drives that have been removed from RAIDsets due to a failure or a manual removal. Disk drives in the failedset should be considered defective and should be tested, repaired, and then placed into the spareset.

Failover
The process that takes place when one controller in a dual-redundant configuration assumes the workload of a failed controller.

Flush
The act of writing data from the cache module to the media.

FRU
Field replaceable unit. A hardware component that can be replaced.

FWD SCSI
Fast, wide, differential SCSI. The differential SCSI bus with a 16-bit parallel data path that yields a transfer rate of up to 20 MB/s.

Half-height device
A device that occupies half of a 5.25 inch SBB carrier. Two half-height devices can be mounted in a 5.25 inch SBB carrier. The first half-height device is normally mounted in the lower part of the carrier. The second device is normally mounted in the upper part of the carrier.

HBVS
Host-based volume shadowing. Also known as Phase 2 volume shadowing.

HSOF
Hierarchical storage operating firmware. Software contained on a program card that provides the logic for the HS array controllers.

HIS
Host interconnect services. The firmware in the HS array controller that communicates with the host.

Host
Any computer to which a storage subsystem can be attached.

Hot swap
A method of replacing a device whereby the system that contains the device remains online and active during replacement. The device being replaced is the only device that cannot perform operations during a hot swap.

Initiator
A SCSI device that requests an I/O process to be performed by another SCSI device (a target). This is always the controller.

Local terminal
A terminal plugged into the EIA-423 maintenance port on the front bezel of the HS array controller. Also called a maintenance terminal.

Logical unit
The physical device or storage unit seen by the host. Often these logical units are spread across more than one physical device, especially in RAID implementations. This is *not* a LUN.

Logical Unit Number
See LUN.

LRU
Least recently used. This is cache terminology for the block replacement policy for the read cache.

LUN
A logical unit number is a physical or virtual peripheral device addressable through a target. LUNs use their target's bus connection to communicate on the SCSI bus.

Maintenance terminal
Any EIA-423 compatible terminal to be plugged into the HS controller. This terminal is used to identify the controller, enable host paths, define the configuration, and check controller status. It is not required for normal operations. It is sometimes referred to as a local terminal.

Metadata
Data written on the physical disk that is not visible to the host/customer that allows the HS array controller to maintain a high integrity of customer data.

Mirrorset
Two or more physical disks configured to present one highly reliable virtual unit to the host.

MSCP
Mass storage control protocol. The protocol by which blocks of information are transferred between the host and the controller.

Non-redundant configuration
A single controller configuration. A controller configuration which does not include an second backup controller permitting failover in the event of a failure.

Normal member
A mirrorset member whose entire contents is guaranteed to be the same as all other NORMAL members. All NORMAL members are exactly equivalent.

Normalizing member
A mirrorset member whose contents is the same as all other NORMAL and NORMALIZING members for data that has been written since the mirrorset was created or lost cache data was cleared. Data that has never been written may differ among NORMALIZING members.

NV
Nonvolatile. A term used to describe memory that can retain data during a power loss to the controller.

Partition
A percentage of a storageset or single-disk unit that may be presented to the host as a storage unit.

PPort
The hardware and software used to connect a host controller to a communication bus, such as CI, DSSI, or SCSI bus. This term also is used to describe the connection between the controller and its SCSI storage devices.

PTL
Port-target-LUN. A method of device notation where **P** designates the controller's device port (1-6), **T** designates the target ID of the device (0-6), and **L** designates the LUN of the device (0-7).

Qualified device
A device that has been fully tested in an approved StorageWorks configuration, (that is, shelf, cabinet, power supply, cabling, and so forth) and is in complete compliance with country-specific standards (for example, FCC, TUV, and so forth) and with all Digital standards.

Quiesce
To make a bus inactive or dormant. The operator must quiesce SCSI bus operations, for example, during a device warm swap.

RAID
Redundant array of independent disks. The multiple storage access methods devised for performance (RAID 0, striping) and/or various cost levels of availability (RAID 1 through RAID 5).

RAIDset
Three or more physical disks that are configured to present an array of disks as a single virtual unit to the host.

Read cache
The cache used to accelerate read operations by retaining data which has been previously read, written, or erased, based on a prediction that it will be reread.

Replacement policy
The method by which a spare disk is selected to replace a disk that has failed in a RAIDset.

SBB
StorageWorks building block. A modular carrier plus the individual mechanical and electromechanical interface required to

mount it into a standard StorageWorks shelf. Any device conforming to shelf mechanical and electrical standards is considered an SBB.

SBB shelf
StorageWorks building block shelf. A StorageWorks shelf, such as the BA350--Sx, designed to house plug-in SBB modules.

SCS
System communication services. A delivery protocol for packets of information (commands or data) to or from the host.

SCSI
Small computer system interface. An ANSI interface defining the physical and electrical parameters of a parallel I/O bus used to connect initiators to a maximum of seven devices. The StorageWorks device interface is implemented according to SCSI--2 standard, allowing the synchronous transfer of 8-bit data at rates of up to 10 MB/s.

SCSI device
A host computer adapter, a peripheral controller, or a storage element that can be attached to the SCSI bus.

SCSI device ID
The bit-significant representation of the SCSI addressing that refers to one of the signal lines numbered 0 through 7. Also referred to as a *target* ID.

SCSI--A cable
A 50-conductor (25 twisted pair cable used for single-ended, SCSI bus connections.

SCSI--P cable
A 68-conductor (34 twisted pair cable used for differential bus connections.

Small Computer System Interface
See SCSI.

Spareset
A pool of disk drives used by the controller to replace failed members of a RAIDset.

SPD
Software product description. A document that contains the legal description of a product.

Storageset
Any collection of containers, such as stripesets, RAIDsets, the spareset, and the failedset, that make up a container.

Storage unit
The general term that refers to storagesets, single disk units, and all other storage devices that can be installed in your subsystem and accessed by a host. A storage unit can be any entity that is capable of storing data, whether it is a physical device or a group of physical devices.

StorageWorks
Digital's family of modular data storage products that allows customers to design and configure their own storage subsystems. Components include power, packaging, cabling, devices, controllers, and software. Customers can integrate devices and array controllers in StorageWorks enclosure to form storage subsystems.

StorageWorks building block
See SBB.

Stripeset
A virtual disk drive with its physical data spread across multiple physical disks. Stripeset configurations do not include a data recovery mechanism.

Striped mirrorset
Stripesets whose members have been mirrored.

Tagged command queuing
A SCSI feature that allows a device to have multiple I/O requests outstanding to it at one time.

Target
A SCSI device that performs an operation requested by an initiator. The target number is determined by the device's address on its SCSI bus.

TILX
Tape inline exerciser. Diagnostic firmware used to test the data transfer capabilities of tape drives in a way that simulates a high level of user activity.

TMSCP
Tape mass storage control protocol. The protocol by which blocks of information are transferred between the host and the controller.

Unit
The host's view of a container on an HS array controller. A unit may be made up of simply a physical disk or tape drive, or a more complex container such as a RAIDset.

Unwritten cached data
Data in the write-back cache which has not yet been written to the physical device, but the user has been notified that the data has been written.

VCS
VAXcluster console system.

Virtual terminal
A software path from an operator terminal on the host to the controller's CLI. The path can be established via the host port on the controller (using DUP) or via the maintenance port through on intermediary host (VCS). A virtual terminal is also sometimes called a host console.

Warm swap
A method for adding or replacing a device whereby the system remains online, but all activity on the device's bus must be halted for the duration of the swap.

Write-back caching
A caching strategy that writes data to the cache memory, then flushes the data to the intended device at some future time. From the user's perspective, the write operation is complete when the data is stored in the cache memory. This strategy avoids unnecessary access of the devices.

Write hole
Undetectable RAID level 1 or 5 data corruption. A write hole is caused by the successful writing of some, but not all, of the storageset members. Write holes occur under conditions such as power outages, where the writing of multiple members can be abruptly interrupted. A battery backed-up cache design eliminates the write hole, because data is preserved and writes can be retried.

Write-through cache

A cache write strategy in which the destination of the write data is the primary storage media. This operation may update, invalidate, or delete data from the cache memory accordingly, to ensure that the cache does not contain obsolete data. The user sees the operation as complete only after the backup storage device has been updated.

Index

A

Abort codes, 165
Adapter, 340
Adding disk drives to configuration, 161
Allocation class, 340
Array controller, 340
Asynchronous device swap, 220
Asynchronous swap, 129
  power supplies, 129
  storage devices, 132

B

BBR, 340
BBU, 340
Block, 340

C

C_SWAP, 191
  adding second controller, 191
  offline method, 191
  online method, 191
Cables
  handling for ESD, 83
  replacing CI host cables, 139
  replacing SCSI device port cables, 141
Cache memory
  procedure for adding, 204
  SIMM cards, 204
Cache modules
  handling for ESD, 82
  installing into HSJ50 controller, 196
  removing, 247
  replacing, 111
  replacing battery cells, 116
CD ROM, installing, 221
CDROM drive, moving, 232
CDU, 340
CFMENU, 224
CI bus, 340
CI host cables
  replacing, 139
CI performance display, 60
CI/DSSI connection status, 62
CI/DSSI host path status, 64
CI/DSSI host port characteristics, 57
CLCP
  code patch, 147
CLI, 340
code patch
  error messages, 153
  installing patches, 151
  listing patches, 147, 148
  special considerations, 148
Cold swap
  power supplies, 129
  solid state disks, 132
Configuring disk drives, 161
control keys, 53
Controller shelf, 340
Controllers
  handling for ESD, 82, 146
  installing patches for, 147
  LED codes, 7
  removing, 247
  replacing controllers, 84
  replacing in a dual-redundant configuration, 103
  replacing in a single configuration, 95
  warm swap, 84
Copying
  firmware from host to subsystem, 161
CRC, 341
Creating the firmware source in your subsystem, 161

D

Data center cabinet, 341
DDL, 341
DECevent, 16
Delete patch program, 237
Deleting
  cache modules, 247
  controllers, 247
  license keys, 244
  licensed options, 241
  patches, 237
  storage devices, 252
Device code load function, 159
Device SCSI port performance, 79

device SCSI status, 66
Device status, 76
Devices
  installing new firmware on, 159
  moving, 224, 232
  removing, 252
Differential SCSI bus, 341
DILX, 24, 341
Disk drive
  move between subsystems, 230
  move within subsystem, 230
Disk drives
  configuring, 161
  formating, 156
  installing new firmware on, 159
  removing, 252
Disk In-line Exerciser. *See* DILX
Drives
  formatting, 156
  installing new firmware on, 159
  removing, 252
DSA, 341
DSSI, 341
DSSI performance display, 61
Dual-redundant configuration, 341
DUART, 341
DUP, 341
DWZZA, 342

E

ECB, 342
ECC, 342
EDC, 342
Electrostatic discharge. *See ESD*. *See* ESD
ERF, 12
Error
  controller not operating, 3
  foreign disk drive not usable, 6
  unable to see units from host, 3
  units host unavailable, 5
  VMS shadowsets go into mount verify, 4
Error logging, 12
  HSJ-series, 16
ESD, 342
  guidelines, 82, 146
  handling components, 146
  precautions, 146
  protection from, 82, 146
  wrist strap, 146

F

Failedset, 342
Failover, 342
Fault indications
  SW300 cabinet, 212
  SW500 and SW800, single power supply, 213
Fault indicators
  SW500 and SW800, dual power supply, 214
fault isolation, 3
Fault management utility. *See* FMU
Field replaceable units. *See* FRU
Firmware
  copying from host to subsystem, 161
  installing on devices, 159
  upgrading for devices, 159
Firmware licensing system. *See* FLS
FLS
  enabling a license, 169
  enter license example, 172
  error for invalid license key, 175
  error messages, 176
  license key, 169
  menu, 170
  operations, 170
  overview, 169
Flush, 342
FMU
  describe event log codes, 20
  describe last fail codes, 22
  describe memory system codes, 22
Formatting a disk drive, 156
FRU, 342
  dual-redundant configuration, 103
  replacing, 82
  single configuration, 95
FWD SCSI, 342

G

Guidelines
  ESD protection, 82

H

Half-height device, 343
HBVS, 343
HIS, 343
Host, 343
Host copy script, OpenVMS, 161
host event log message, 12
Host port cables and ESD, 83
host port characteristics, 57, 58
Hot swap, 343
HSOF, 343
HSUTIL
  abort codes, 165
  device code load function, 159
  error messages, 165
  formatting a disk drive with, 156

I

Initiator, 343
Installation
  controller into a shelf, 178
  firmware on target device, 162
  installing a cache module, 196
  power supplies into shelf, 212
  precautions, 146
  SBBs, 217
  second controller, 184
  SIMM cards, 204
Installing new device firmware, 159
Instance codes
  finding in event message, 12
  tables and definitions, 258

L

Last fail codes
  CLI, 313
  clone unit utility (CLONE), 327
  code load/code patch utility (CLCP), 328
  common library, 309
  device configuration utilities (CONFIG/CFMENU), 327
  device services, 300
  Diagnostics and utilities protocol server, 324
  Disk and tape MSCP server, 320
  disk inline exerciser (DILX), 325
  DUART services, 309

  executive services, 290
  facility lock manager, 312
  failover control, 310
  fault manager, 307
  host interconnect port services, 317
  host interconnect services, 315
  induce controller crash utility (CRASH), 328
  integrated logging facility, 313
  load utility (HSUTIL), 328
  nonvolatile parameter memory failover, 310
  overview, 290
  SCSI host interconnect services, 316
  SCSI host value added services, 324
  system communication services directory, 324
  tape inline exerciser (TILX), 326
  value-added services, 293
LED code
  flashing, 8
  overview, 7
  solid, 7
LED status indicators, 212
License keys
  enabling, 169
  removing, 244
Licensed options, removing, 241
Local terminal, 343
Logical unit, 343
LRU, 343
LUN, 344

M

Maintenance terminal, 344
Metadata, 344
Move
  device, 224
  precautions, 224
  storageset, 224
MSCP, 344

N

Non-redundant configuration, 344
Normal member, 344

NV, 344

O

OpenVMS host copy script, 161
optical drives
  installing, 221

P

Patches
  installing for controllers, 147
  removing, 237
Patching controller software, 147
Performance monitoring, 52
Port, 345
Power supplies
  installing into shelf, 212
  replacing, 129
Precautions
  electrostatic discharge, 146
  moving storageset or device, 224
  removing components, 236
Program cards
  guidelines, 146
  handling for ESD, 82, 146
Protection
  ESD, 82

Q

Qualified device, 345
Quiesce, 345

R

Read cache, 345
Removing
  cache modules, 247
  controllers, 247
  license keys, 244
  licensed options, 241
  patches, 237
  storage devices, 252
Repair action codes, 329
Replacement procedures
  battery cells, 116
  cache modules, 111
  CD–ROM drives, 135
  CI host cables, 139
  controllers, 84

  optical drives, 135
  power supplies, 129
  SCSI device port cables, 141
  solid state disk drives, 137
  storage devices, 132
  tape drives, 135
  write-back cache battery cells, 116
Replacing units (FRUs)
  C_swap, 84
  dual-redundant configuration, 103
  precautions, 82
  single configuration, 95

S

SBB, 345
SBBs, 217
  installing SBBs, 217
  installing, procedure, 221
  status indicators, 218
SCS, 346
SCSI, 346
SCSI device port cables
  replacing, 141
SCSI host port characteristics, 58
SIMM card
  installing, 204
  precaution, 209
Software patching, 147
SPD, 346
Storage device building blocks. *See* SBBs
Storage devices, 132
Storage unit, 347
Storageset
  move between subsystems, 225
  move members, 228
  move within same subsystem, 225
  moving, 224

T

Tagged command queuing, 347
Tape drives

installing new firmware on, 159
moving, 232
removing, 252
Tape In-line Exerciser. *See TILX*
Tape loader, moving, 232
Target, 347
TILX, 37, 347
TMSCP, 348
Troubleshooting
DILX, 24
fault isolation, 3
FMU, 20
host event log message, 12
LED code, 7
overview, 2
TILX, 37

U

Unit, 348
Unit status, abbreviated, 68
Unit status, full, 72
Upgrading device firmware, 159

V

VCS, 348
Virtual terminal, 348
VTDPY
CI performance display, 60
CI/DSSI connection status, 62
CI/DSSI host path status, 64
CI/DSSI host port characteristics, 57
command line interpreter, 53
commands, 53
control keys, 53
default display, 54
device SCSI port performance, 79
device SCSI status, 66
device status, 76
DSSI performance display, 61
help, 80
overview, 52
running, 52
SCSI host port characteristics, 58
unit status, abbreviated, 68
unit status, full, 72

W

Warm swap, 348
controllers, 84
Write hole, 348
Write-back cache
handling for ESD, 82
replacing battery cells, 116
Write-through cache, 349