DIGITAL StorageWorks HSZ70 Array Controller HSOF Version 7.0

EK–HSZ70–SV. A01

Digital Equipment Corporation
Maynard, Massachusetts

Service Manual

July 1997

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, DIGITAL UNIX, DECconnect, HSZ, StorageWorks, VMS, OpenVMS, and the DIGITAL logo are trademarks of Digital Equipment Corporation.

UNIX is a registered trademark in the United States and other countries exclusively through X/Open Company Ltd. Windows NT is a trademark of the Microsoft Corporation. Sun is a registered trademark of Sun Microsystems, Inc. Hewlett-Packard and HP–UX are registered trademarks of the Hewlett-Packard Company. IBM and AIX are registered trademarks of International Business Machines Corporation. All other trademarks and registered trademarks are the property of their respective owners.

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 manuals, 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

Troubleshooting

Replacement Procedures

Upgrading the Subsystem

Appendix A: LED Codes

Appendix B: Event Codes

Figures

Tables

Preface

This book provides information and guidance for troubleshooting and servicing the HSZ70 array controller running HSOF Version 7.0. It also provides information and guidance for troubleshooting and servicing the cache module and external cache battery that support the controller's operation in a storage subsystem.

This book does not contain information about the operating environments to which the controller may be connected, nor does it contain detailed information about subsystem enclosures or their components. See the documentation that accompanied these peripherals for information about them.

Precautions

Follow these precautions when you're carrying out the procedures in this book.

Electrostatic Discharge Precautions

Static electricity collects on all nonconducting material, such as paper, cloth, and plastic. An electrostatic discharge (ESD) can easily damage a controller or other subsystem component even though you may not see or feel the discharge. Follow these precautions whenever you're servicing a subsystem or one of its components:

- Always use an ESD wrist strap when servicing the controller or other components in the subsystem. Make sure that the strap contacts bare skin and fits snugly, and that its grounding lead is attached to a bus that is a verified earth ground.
- Before touching any circuit board or component, always touch a verifiable earth ground to discharge any static electricity that may be present in your clothing.
- Always keep circuit boards and components away from nonconducting material.
- Always keep clothing away from circuit boards and components.
- Always use antistatic bags and grounding mats for storing circuit boards or components during replacement procedures.
- Always keep the ESD cover over the program card when the card is in the controller. If you remove the card, put it in its original carrying case. Never touch the contacts or twist or bend the card while you're handling it.
- Do not touch the connector pins of a cable when it is attached to a component or host.

VHDCI Cable Precautions

All of the cables to the controller, cache module, and external cache battery use very-high-density cable interconnect connectors (VHDCI). These connectors have extraordinarily small mating surfaces that can be adversely affected by dust and movement.

Use the following precautions when you’re connecting cables that use VHDCI connectors:

- Clean the mating surfaces with a blast of clean air.
- Mate the connectors by hand, then tighten the retaining screws to 1.5 inch-pounds—approximately 1/4 additional turn after the connectors have fully mated.
- Test the assembly by gently pulling on the cable, which should not produce visible separation.

Local Connection Port Precautions

The local connection port generates, uses, and radiates radio-frequency energy through cables that are connected to it. This energy may interfere with radio and television reception. Do not leave a cable connected to this port when you’re not communicating with the controller.

Conventions

This book uses the following typographical conventions and special notices to help you find what you're looking for.

Typographical Conventions

Convention	Meaning
ALLCAPS BOLD	Command syntax that must be entered exactly as shown, for example: **SET FAILOVER COPY=OTHER_CONTROLLER**
ALLCAPS	Command discussed within text, for example: "Use the SHOW SPARESET command to show the contents of the spareset."
`Monospaced`	Screen display.
Sans serif italic	Command variable or numeric value that you supply, for example: SHOW *RAIDset-name* or **SET THIS_CONTROLLER ID=***(n,n,n,n,)*
italic	Reference to other books, for example: "See *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for details."
. . .	Indicates that a portion of an example or figure has been omitted, for example: **ADD RAIDSET RAID1 DISK10000 DISK20000** **INITIALIZE RAID1** **.** **.** **.** **SHOW RAID1**
"this controller"	The controller serving your current CLI session through a local or remote terminal.
"other controller"	The controller in a dual-redundant pair that's connected to the controller serving your current CLI session.

Special Notices

This book doesn't contain detailed descriptions of standard safety procedures. However, it does contain warnings for procedures that could cause personal injury and cautions for procedures that could damage the controller or its related components. Look for these symbols when you're carrying out the procedures in this book:

Warning A warning indicates the presence of a hazard that can cause personal injury if you do not avoid the hazard.

Caution A caution indicates the presence of a hazard that might damage hardware, corrupt software, or cause a loss of data.

Tip A tip provides alternative methods or procedures that may not be immediately obvious. A tip may also alert prior customers that the controller's behavior being discussed is different from prior software or hardware versions.

Note A note provides additional information that's important to the completion of an instruction or procedure.

Required Tools

You'll need the following tools for servicing the controller, cache module, and external cache battery:

- A small screwdriver for loosening and tightening the cable-retaining screws.
- An antistatic wrist strap.
- An antistatic mat on which to place modules during servicing.
- An SBB Extractor for removing StorageWorks building blocks. This tool is not required, but it will enable you to provide more efficient service.

Related Publications

The following table lists some of the documents related to the use of the controller, cache module, and external cache battery.

Document Title	Part Number
HSZ70 Array Controller HSOF Version 7.0 CLI Reference Manual	EK–CLI70–RM. A01
HSZ70 Array Controller HSOF Version 7.0 Configuration Manual	EK–HSZ70–CG. A01
HSZ70 Array Controller HSOF Version 7.0 Service Manual	EK–HSZ70–SV. A01
HSZ70 Family Array Controller Operating Software (HSOF) Version 7.0 Software Product Description	SPD *xx.xx*. 00
Getting Started–HSZ70 Solutions Software Version 7.0 for...*platform*	AA–R60*xx*–TE. A01
Polycenter Console Manager	See the *Getting Started* guide for the platform-specific order number
StorageWorks Array Controller HSZ70 Array Controller Operating Software HSOF Version 7.0 Release Notes	EK–HSZ70–RN. A01
StorageWorks Getting Started with Command Console, Version 2.1	AA–R0HJC–TE
DIGITAL StorageWorks Ultra SCSI RAID Cabinet Subsystem (SW600) Installation and User's Guide	EK–SW600–UG
DIGITAL StorageWorks Ultra SCSI RAID Enclosure (BA370-Series) User's Guide	EK–BA370–UG
The RAIDBOOK—A Source for RAID Technology	RAID Advisory Board

Revision History

This is a new document.

CHAPTER 1

General Description

This chapter illustrates and describes in general terms the HSZ70 array controller, its cache module, and its external cache battery.

Typical Installation

A fully-populated BA370 rack-mountable enclosure is one of the typical building blocks for a storage subsystem. Figure 1–1 shows the components of this basic building block, which includes:

- One BA370 rack-mountable enclosure
- Two controllers, each supported by their own cache module
- One external cache battery (ECB), which provides backup power to the cache modules during a primary power failure
- One environmental monitoring unit (EMU) monitors the susbsystem's environment and alerts the controller of equipment failures that could cause an abnormal environment
- One power verification and addressing module (PVA) provides a unique address to each enclosure in an extended subsystem

Figure 1–1 Basic Building Block

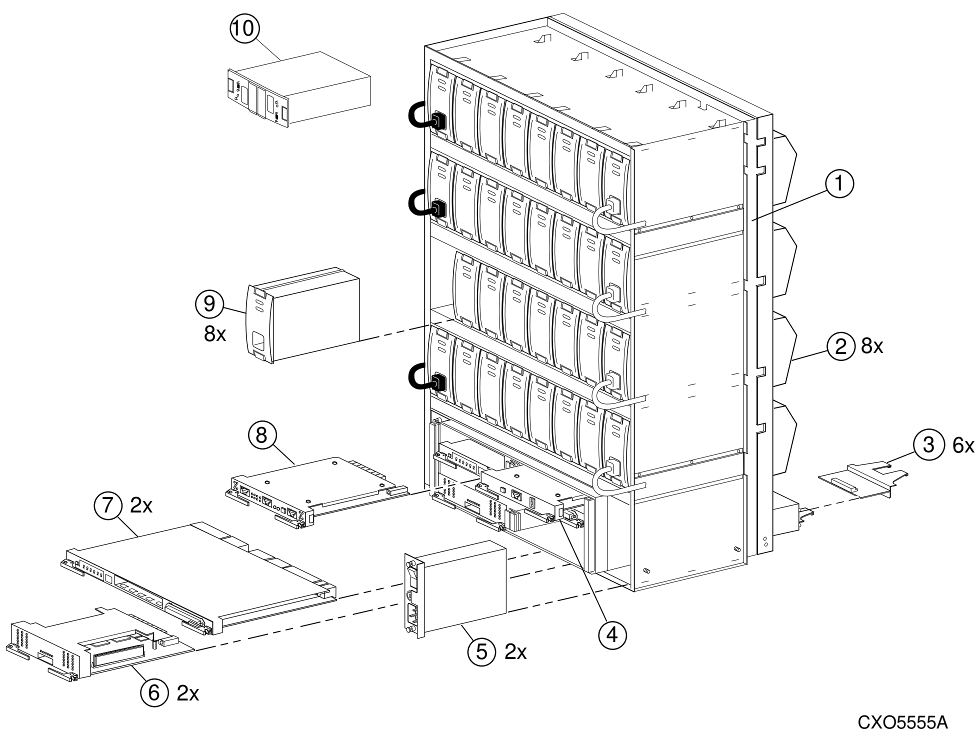


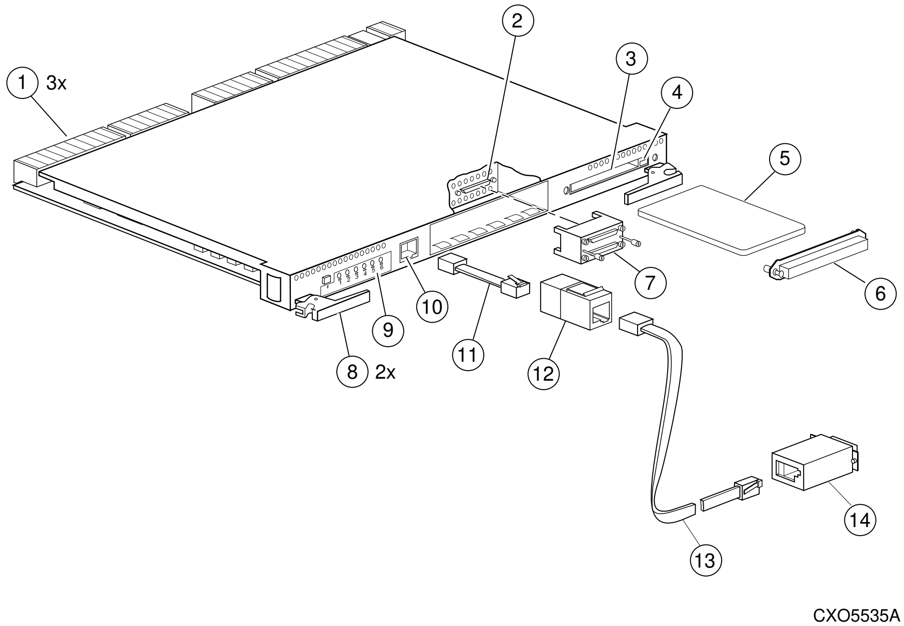
Table 1–1 Key to Figure 1–1 Basic Building Block

Item	Description	Part No.
1	BA370 rack-mountable enclosure	—
2	Cooling fan	DS–BA35X–MK
3	I/O module	70–32832–01
4	Power verification & addressing module (PVA)	DS–BA35X–EC
5	AC input module	DS–BA35X–HE
6	Cache module	70–32835–01
7	HSZ70 controller	DS–HSZ70–AH
8	Environmental monitoring unit (EMU)	DS–BA35X–EB
9	180-watt power supply	DS–BA35X–HH
10	External cache battery for dual-redundant configurations (ECB)	DS–HS35X–BD

HSZ70 Array Controller

The controller shown in Figure 1–2 is an integral part of any storage subsystem because it provides a host with high-performance and high-availability access to standard SCSI–2 storage devices. See the product-specific release notes that accompanied the software release for the most recent list of supported devices and operating systems.

Figure 1–2 HSZ70 Array Controller



The controller provides the ability to combine several ordinary disk drives into a single, high-performance storage unit called a storageset. Storagesets are implementations of RAID technology, which ensures that every unpartitioned storageset, whether it uses two disk drives or ten, looks like a single storage unit to the host. See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for more information about storagesets and how to configure them.

From the host’s perspective, the controller is simply another SCSI–2 device connected to one of its I/O buses. Consequently, the host sends its I/O requests to the controller just as it would to any SCSI–2 device. From the subsystem’s perspective, the controller receives the I/O requests and directs them to the devices in the subsystem. Because the controller processes the I/O requests, the host isn't burdened by the processing that's typically associated with reading and writing data to multiple storage devices.

Table 1–2 Key to Figure 1–2 HSZ70 Array Controller

Item	Description	Part No.
1	Backplane connectors	—
2	Host port	—
3	Program-card slot	—
4	Program-card ejection button	—
5	Program card	BG–*xxxxx–xx*
6	ESD cover	—
7	Trilink connector	H8861–AA
8	Lever for removing, installing, and retaining controller module.	—
9	Operator control panel (OCP)	—
10	Local connection port	—
11	DECconnect office cable	BC16E–XX
12	RJ-11 adapter	12–43346–01
13	RJ-11 extension cable	17–03511–04
14	PC serial-port adapter	H8571–J

Maintenance Features

Use these maintenance features to troubleshoot and service a controller:

- "Operator Control Panel," page 1-10
- "Local Connection Port," page 1-10
- "Initialization Diagnostics," page 1-14
- "Utilities and Exercisers," page 1-18

Table 1–3 summarizes the features of the controller.

Table 1–3 Summary of Controller Features

Feature	Supported
Host protocol	SCSI–2
Host bus interconnect	Wide Ultra Differential SCSI–2
Device protocol	SCSI–2
Device bus interconnect	Fast Wide Ultra Single-ended SCSI-2
Number of SCSI device ports	6
Number of SCSI device targets per port	12
Maximum number of SCSI devices (in an extended subsystem)	72
RAID levels	0, 1, 0+1, 3/5
Cache size	64 or 128 MB
Mirrored write-back cache sizes	32 or 64 MB
Maximum number of host target ID numbers per controller	8
Program card updates	Yes
Device warm swap	Yes
Exercisers for testing disks	Yes
Tape drives, loaders, and libraries	Yes
Number of configuration entities (devices + storagesets + partitions + units)	191
Maximum number of RAID 5 storagesets	20
Maximum number of RAID 5 and RAID 1 storagesets	30 (dual-redundant) 20 (single)
Maximum number of RAID 5, RAID 1, and RAID 0 storagesets	45

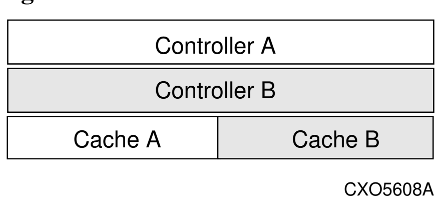
Table 1–3 Summary of Controller Features (Continued)

Feature	Supported
Maximum number of partitions per storageset or disk drive	8
Maximum number of units presented to host	64 (63 if you’re using the StorageWorks Command Console)
Maximum number of devices per unit	32
Maximum host port transfer speed	20 MHz
Largest device, storageset, or unit	120 GB

The components that you’ll use most often are conveniently located on the front panel, such as the local connection port and the operator control panel (OCP). The host port and program-card slot are also located on the front panel, making it easy to update the controller’s software or to connect the controller to a different host.

Each controller is supported by its own cache module. Figure 1–3 shows which cache module supports which controller in a dual-redundant configuration in a BA370 rack-mountable enclosure.

Figure 1–3 Location of Controllers and Cache Modules

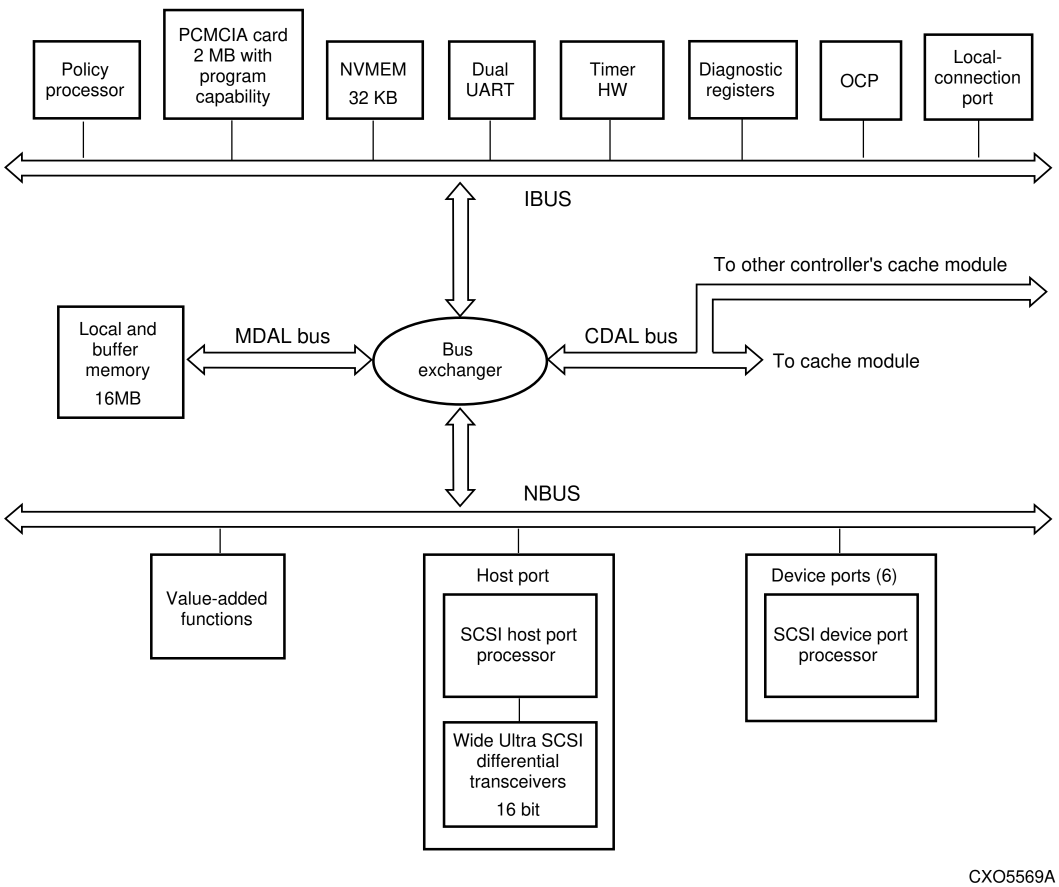


Tip DIGITAL recommends that you use the slots for controller “A” and cache module “A” for single configurations. Slot “A” responds to SCSI target ID number 7; slot “B” responds to SCSI target ID number 6.

Architecture

The controller’s architecture includes the components shown in Figure 1–4.

Figure 1–4 Controller Architecture



Policy Processor

The policy processor coordinates, controls and executes the software on the controller. The heart of the policy processor is an Intel® 80960CF i960 microprocessor. The i960 executes the software from the program card and has a 25 MHz input clock. The i960 controls all but low-level device and host-port operations.

The i960's internal cache is augmented by a separate 32 KB instruction/ data (I/D) cache. This static RAM cache provides the i960 nearly immediate access to the instructions and variables that it needs to operate.

Program Card

The controller's software is stored on a 2 MB PCMCIA program card. The policy processor loads the software from the program card into the local memory when the controller initializes.

Nonvolatile Memory

The controller has 32 KB of nonvolatile memory (NVMEM) to store the following kinds of data:

- Controller's configuration, such as its SCSI target IDs, preferred IDs, prompt text, transfer rate, and failover status.
- Subsystem's configuration, such as the name and location of disk drives, the way in which they're combined into storagesets or used in the spareset, and the unit numbers assigned to the storagesets.
- Last failure and memory-system failure entries received from the fault-management software.

Dual UART

One half of the dual UART supports serial communication for the local connection port. The other half provides serial communication between two controllers in a dual-redundant configuration. This failover link allows the controllers to communicate information about their respective status and configuration independently of their CDAL buses.

Timer

The timer is controlled by and interrupts the i960 at programmed intervals to track timeouts, interrupts, LED flashing frequencies, and so forth.

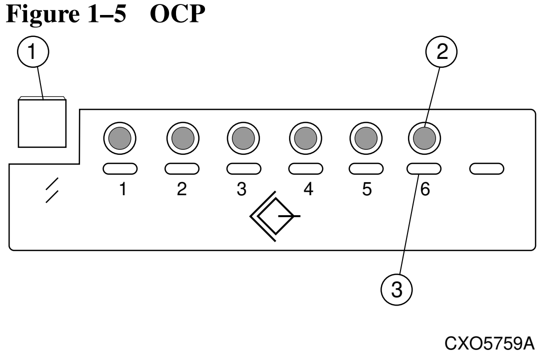
Diagnostic Registers

The controller has two write- and two read-diagnostic registers. Diagnostic and functional software use the write-diagnostic registers to control the devices and the controller. For example, some bits in the registers activate test modes for forcing errors in the controller, other bits control the OCP LEDs. The policy processor uses the read-diagnostic registers to determine the cause of interrupts when they occur.

Operator Control Panel

The operator control panel (OCP) contains a reset button (1) and six device-port LEDs (3) as shown in Figure 1–5. The reset button flashes about once per second to indicate that the controller is operating normally. The LEDs correspond to the controller's device ports and remain off during normal operation. If an error occurs, the reset button and LEDs will illuminate in a solid or flashing pattern to help you diagnose the problem.

Figure 1–5 OCP



The OCP also contains six port-quiesce buttons (2) that you can use to turn off the controller's device ports. To quiesce a device port, push its port button until the port's LED is lit continuously. Push the button again to resume I/O activity to the port.

See Figure 1–2 on page 1-4 for the location of the OCP. See "Operator Control Panel LED Codes," page A-2 for an explanation of the LED codes that may appear on the OCP.

Local Connection Port

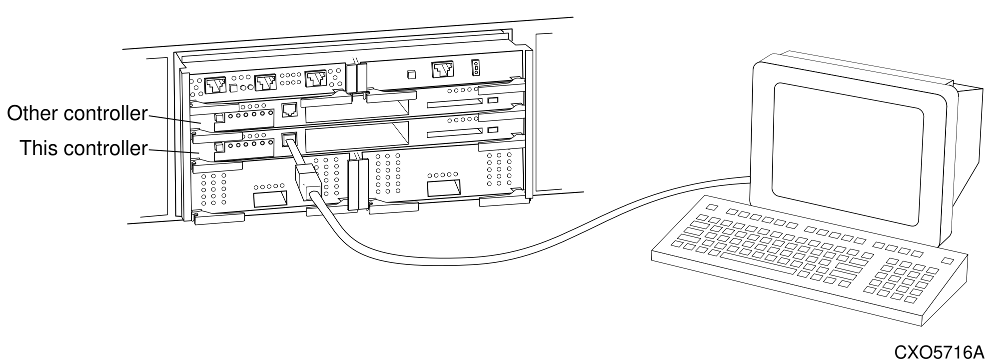
You can access the controller in two ways: through a local terminal via the local connection port, or through a remote terminal—sometimes called a virtual terminal or host console—via the host. DIGITAL recommends that you use a local terminal to carry out the troubleshooting and servicing procedures in this manual.

The local connection port provides a convenient way to connect a terminal to the controller so that you can troubleshoot and configure it. This port accepts a standard RS-232 jack from any EIA-423 compatible terminal or a PC with a terminal-emulation program. The port supports serial communications up to 19200 baud using 8 data bits, 1 stop bit, and no parity.

To connect a local terminal to a controller:

1. Turn off the terminal and connect it to the controller via the DECconnect office cable shown in Figure 1–2 on page 1-4. When you're entering CLI commands in a dual-redundant configuration, remember that the controller to which you're connected is "this controller" and the other controller is the "other controller." This relationship is shown in Figure 1–6.
2. Turn on the terminal and configure it for 19200 baud, 8 data bits, 1 stop bit, and no parity.
3. Press Enter (or Return) until the CLI prompt appears.

Figure 1–6 "This Controller" and "Other Controller"



Buses

The controller's architecture includes the following buses:

- The IBUS enables the policy processor to read, write, and control all of the IBUS components. For example, the IBUS transfers code and text from the program card, code and data from the policy processor's I/D cache, and configuration information to the controller's nonvolatile memory.
- During failover, the CDAL bus conveys data to the surviving controller, including data to and from addresses in the cache modules. Addresses may originate from the IBUS or NBUS of either controller in a dual-redundant configuration.
- The MDAL bus conveys data to and from addresses in the local buffer memory that originate from the IBUS or NBUS.
- The NBUS transfers data to and from addresses in any of the NBUS components: host ports, device ports, and the value-added functions chip. These components may access each other, the local buffer memory, and either cache module in a dual-redundant configuration.
- The bus exchanger facilitates high-speed communication between the local memory and the devices on the IBUS, MDAL, CDAL, and NBUS buses. The exchanger is as a four-way cross-point switch that coordinates addresses and data between any two ports on the exchanger.

Local Memory

When the controller initializes, the policy processor loads and stores the controller's software from the program card into the local memory. Therefore, after the controller initializes, the local memory contains instructions for the policy processor, the software variables, and the data structures, which includes the look-up table for the i960. This single-point of storage ensures that the data structures and buffers remain consistent during the controller's operation.

The local memory consists of a dynamic RAM controller, an arbitration engine, a gate array controller, and 16 MB of dynamic RAM. Seven-bit error detection and correction code improves error detection and data recovery. All of the controller's buses have access to the local memory through the bus exchanger and the MDAL bus.

Value-Added Functions Chip

The value-added function chip generates the parity for RAIDsets when data is written to them. If a RAIDset member fails, this chip also regenerates the parity to recover the data that was stored on the failed member—the controller performs an XOR of the parity data on the surviving members to reconstruct the data that was stored on the failed member. The value-added functions chip acts as an accelerator for this XOR operation. This chip also assists with device-compare operations, and is programmed to conduct large-block reads and writes from a failed controller's cache module to the surviving controller's cache module in event of a failover.

Host Port

The host port comprises a Wide Ultra SCSI processor, a Wide Ultra SCSI differential transceiver, and a VHDCI SCSI connector. The controller connects to a host bus through a SCSI–2 trilink connector attached to the VHDCI SCSI connector (external terminators are required if the controller is at the end of the host bus). The Wide Ultra processor reads and executes scripts from the local memory to perform command and DMA operations. The policy processor sets and maintains the operation of the Wide Ultra processor.

Device Ports

The controller communicates with the devices and modules in the subsystem through three backplane connectors. Each connector contains two ports to give the controller access to the six SCSI–2 buses in the enclosure's backplane. Each device port comprises a Wide Ultra SCSI processor to support Wide Ultra, single-ended SCSI communication to the devices in the subsystem. As with the host port, the policy processor sets and maintains the operation of the Wide Ultra processor.

Each device port can support up to 16 targets, including initiators.

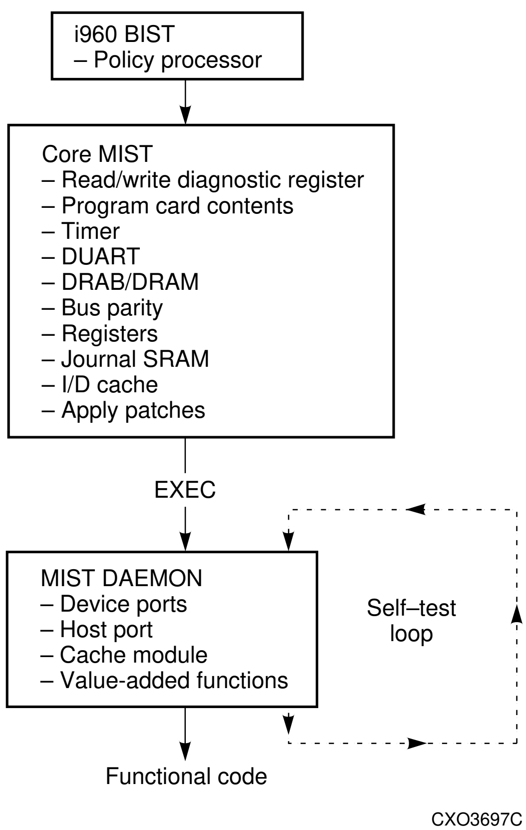
The Controller's Software

The controller's software, which is loaded from the program card into local memory when the controller initializes, provides the functions described in this section.

Initialization Diagnostics

When the controller initializes, it performs the "go/no go" tests shown in Figure 1–7 to detect hardware and software faults. These tests verify the integrity of the controller's architecture as well as many of the components that support the controller in its enclosure.

Figure 1–7 Initialization Diagnostics



Policy Processor Built-In Self-Test
The controller begins initialization by executing its policy processor's internal built-in self-test (BIST), an integral test of the i960 microprocessor. If BIST fails, the controller’s reset button will light continuously while the rest of the port LEDs will be turned off. Successful completion of BIST means the i960 is functioning properly.

Tip One of the more common causes of a BIST failure is a faulty or improperly seated program card.

Core Module Integrity Self-Test
If BIST completes successfully, the controller reads the initial boot record (IBR) to determine the address of hardware setup parameters and process-control information. The software on the program card is initialized to the IBR parameters and the initialization routines and diagnostics begin to test the controller module itself. The tests are part of the controller’s software and are collectively known as the core module integrity self-tests (core MIST). If a fault occurs during core MIST, the OCP displays an LED code and the register contents are displayed on a local terminal, if one is connected to the controller.

Core MIST performs the following functions in order:

1. Sets the initial state of the read and write diagnostic register.
2. Validates the contents of the program card by reading each memory location, computing an error detection code (EDC), then comparing the EDCs against preset EDCs.
3. Checks the controller’s internal buses and the components attached to them: the IBUS parity, the policy processor’s I/D cache, the diagnostic registers, the DUART, the local memory, and so forth.

   To check these components, the core MIST selects a device, then checks whether the bus has selected that device; verifies that legal transfer sizes work and illegal sizes don’t; writes to and reads from all legal addresses, then checks boundaries by attempting to access nonexistent addresses.
4. Loads the software into the first two megabytes of local memory. Core MIST uses the EDC compare method to validate the memory contents with the program card to confirm a successful download.
5. Applies memory-resident code patches and updates the free memory list accordingly.

6. Initializes the i960 microprocessor with the IBR parameters.
7. Passes control to EXEC when the core MIST tests are complete.

DAEMON Tests
EXEC calls the diagnostic and execution monitor (DAEMON) to test the following components: device ports, host port, cache module, and value-added functions.

Tip You may re-run the controller's DAEMON tests—also called the self test loop—as a troubleshooting aid. See "Running a Self Test," page 2-31, for help on running the self test.

- To test the host and device ports, the DAEMON checks each port's microprocessor. The DAEMON passes the hardware if at least one device port is OK; the DAEMON fails the hardware if all device ports fail or if the DUART fails the core MIST and the host port fails the DAEMON test.
- To test the cache module, the DAEMON checks for unwritten data in the cache. If the cache contains data, the controller immediately restricts itself to accept a limited set of CLI commands until you clear the error with the CLEAR_ERRORS INVALID_CACHE command. This prevents commands from being entered that may worsen the situation.

  If the cache memory doesn't contain unwritten data, the DAEMON tests the DRAB memory controller and the ECB batteries. If they pass, the DAEMON passes control to the functional code. The cache manager continues to test the cache memory; at least the first megabyte of the memory must test OK, or the cache module is failed. If unwritten data exists, the DAEMON tests only the batteries, and postpones other tests. The cache manager flushes the unwritten data after testing the DRAB and memory.

  If the cache is locked by the other controller in a dual-redundant configuration, then all cache DAEMON diagnostics are postponed. During functional code, when the cache manager determines that the cache is unlocked, the cache manager tests the DRAB, batteries, and memory.

  The DAEMON handles all interrupts and errors received during cache module testing. If the DAEMON receives an interrupt, it stops initialization. The DAEMON displays errors as an LED code on the OCP.

- Finally, to ensure RAIDset functionality, the DAEMON evaluates the XOR operations of the value-added hardware and its associated buffer memory. Initialization stops if the XOR operation test fails.

Executive Functions

The executive functions (EXEC) act as the operating system kernel for the controller. EXEC controls the interrupts, thread, queuing support, timers, and so forth to ensure a nonpreemptive, interrupt-driven environment.

Host Interconnect Functions

The host interconnect functions support the SCSI–2 protocol with the following features:

- SCSI passthrough software to the CLI
- Tagged-command queuing on the host and device side
- Mode select and mode sense support for SCSI

User-Interface Functions

The command-line interpreter (CLI) provides a direct, command-line interface to the controller. You can enter CLI commands through a local terminal connected to the controller or through a remote terminal running on the host. The CLI provides the following kinds of commands:

- ADD commands for adding devices, storagesets, and logical units to the subsystem.
- DELETE commands for deleting devices, storagesets, and logical units.
- SET commands for setting the configuration parameters for the subsystem, as well as its storagesets and controllers.
- SHOW commands for showing the configuration parameters for the subsystem, as well as its storagesets and controllers.

See the *HSZ70 Array Controller HSOF Version 7.0 CLI Reference Manual* for more information about the CLI commands and how to use them.

Utilities and Exercisers

The controller's software includes the following utilities and exercisers to assist in troubleshooting and maintaining the controller and the other modules that support its operation:

Fault Management Utility

The Fault Management Utility (FMU) provides a limited interface to the controller's fault-management system. As a troubleshooting tool, you can use FMU to:

- Display the last-failure and memory-system-failure entries that the fault-management software stores in the controller's nonvolatile memory.
- Translate many of the event messages that are contained in the entries related to the significant events and failures. For example, entries may contain codes that indicate the cause of the event, the software component that reported the event, the repair action, and so on.
- Set the display characteristics of spontaneous events and failures that the fault-management system sends to the local terminal or host.

See "Checking Failure Entries," page 2-11, for more information about using this utility.

Virtual Terminal Display

Use the virtual terminal display utility (VTDPY) to aid in troubleshooting the following issues:

- Communication between the controller and its hosts
- Communication between the controller and the devices in the subsystem
- The state and I/O activity of the logical units, devices, and device ports in the subsystem

See "Checking for Communication Problems," page 2-17, for more information about using this utility.

Disk Inline Exerciser

Use the disk inline exerciser (DILX) to investigate the data-transfer capabilities of disk drives. Disk inline exerciser (DILX) tests and verifies operation of the controller and the SCSI–2 disk drives to which it's attached. DILX generates intense read and write loads to the disk drive while monitoring the drive's performance and status. See "Checking for Disk-Drive Problems," page 2-26, for more information about this exerciser.

Field Replacement Utility
Use the field replacement utility (FRUTIL) to replace a failed controller (in a dual-redundant configuration) without shutting down the subsystem. You can also use this menu-driven utility to replace cache modules and external cache batteries. Most of the procedures beginning on "Replacing Modules in a Dual-Redundant Configuration," page 3-8, explain how to use FRUTIL.

Configuration Utility
Use the configuration utility (CONFIG) to add one or more storage devices to the subsystem. This utility checks the device ports for new disk or tape drives, then adds them to the controller's configuration and automatically names them. See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for more information about using the CONFIG utility.

HSUTIL
Use HSUTIL to upgrade the firmware on disk drives and tape drives in the subsystem. See "Upgrading Firmware on a Device," page 4-6, for more information about this utility.

Code Load/Code Patch Utility
Use Code Load/Code Patch utility (CLCP) to upgrade and patch the controller's software. See "Upgrading Controller Software," page 4-2, for more information about using this utility.

Configuration Menu
Use the configuration menu (CFMENU) to configure the storagesets in the subsystem. See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for more information about using CFMENU.

Clone
Use the Clone utility to duplicate the data on any unpartitioned single-disk unit, stripeset, or mirrorset. Backup the cloned data while the actual storageset remains online. See the *HSZ70 Array*

Controller HSOF Version 7.0 Configuration Manual for more information about using the Clone utility.

Device Services

The SCSI–2 device service software provides the following functions:

- Device port drivers
- Addressing, access, and tagged-command queuing for qualified SCSI–2 devices
- Device warm swap
- Enclosure and SBB observation and control
- Device error recovery

Value-Added Functions

The controller's software provides the following value-added functions to enhance the availability, performance, subsystem management, and connectivity features of the controller:

- RAID functions support the creation and operation of RAIDsets, stripesets, mirrorsets, and striped mirrorsets. See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for more information about storagesets.
- Failover functions support dual-redundant and multiple-bus failover configurations. In either of these configurations, two controllers exchange status signals and configuration information. If one controller fails, the surviving controller takes over the failed controller's devices and units. See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for more information about these redundant configurations.
- The cache manager controls the caching techniques for up to 128 MB data in each cache module to enhance the subsystem's performance. See "Caching Techniques," page 1-22 for more information about the caching techniques that can be enabled.

Cache Module

The controller requires a companion cache module as shown in Figure 1–8. (Figure 1–3 on page 1-7 shows the location of a controller's companion cache module.) The cache module, which contains 64 MB or 128 MB of memory, increases the subsystem's
I/O performance by providing read, write-through, and write-back caching. These caching techniques are described below.

Figure 1–8 Cache Module

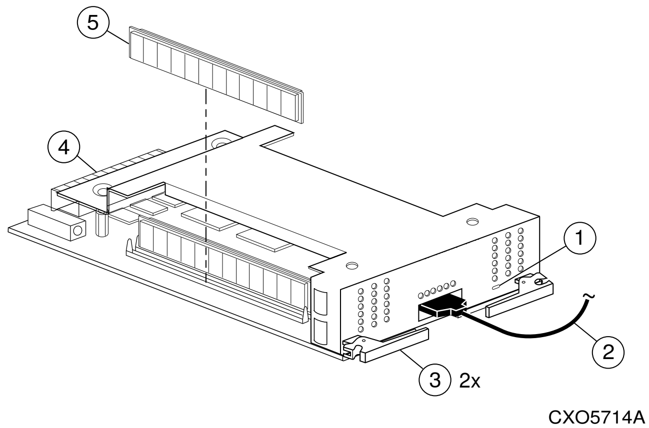


Table 1–4 Key to Figure 1–8 Cache Module

Item	Description	Part No.
1	Cache-memory power LED	—
2	ECB cable	70–33268–01
3	Retaining lever	—
4	Backplane connector	—
5	SIMM (2 or 4) (64 MB SIMM pack)	54–23391–01 (DS–HSSIM–AB)

Caching Techniques

The cache module supports read, write-through, and write-back caching techniques to increase the subsystem’s read and write performance.

Read Caching

By caching read data, this caching technique decreases the subsystem’s response time to a read request by allowing the controller to satisfy the request from the cache memory rather than from the disk drives.

When the controller receives a read request from the host, it reads the data from the disk drives, delivers it to the host, and also stores it in the cache memory. If the host requests the same data again, the controller can satisfy the read request from the cached data rather than re-reading it from the disk drives.

By default, read caching is enabled for all storage units.

Write-Through Caching

By caching write data, this caching technique also decreases the subsystem’s response time to a read request by allowing the controller to satisfy the request from the cache memory rather than from the disk drives.

This caching technique is called write-through caching because the write data passes through—and is stored in—the cache memory on its way to the target disk drives. When the controller receives a write request from the host, it stores the data in its cache memory, writes the data to the disk drives, then notifies the host when write operation is complete. If the host requests the recently written data, the controller satisfies the read request from its cache memory rather than from the disk drives.

If read caching is enabled for a storage unit, write-through caching is also enabled. Also, because both caching techniques enhance the controller’s read performance, if you disable read caching, write-through caching is automatically disabled.

Write-Back Caching

This caching technique decreases the subsystem's response time to write requests by allowing the controller to declare the write operation "complete" as soon as the data reaches its cache memory. The controller performs the slower operation of writing the data to the disk drives at a later time.

By default, write-back caching is disabled for all storagesets. In either case, the controller will not provide write-back caching to a unit unless you ensure that the cache memory is non-volatile as described below.

Fault-Tolerance for Write-Back Caching

The cache module supports the non-volatile memory, mirrored caching, and dynamic caching policies to protect the availability of its unwritten (write-back) data.

Non-Volatile Memory

The controller cannot provide write-back caching to a unit unless its cache memory is non-volatile. In other words, you must provide a back up power source to the cache module to preserve the unwritten cache data in the event of a power failure. If the cache memory were volatile—that is, if it didn't have a back up power supply—the unwritten cache data would be lost during a power failure.

By default, the controller expects to use an ECB as its cache module's back up power source. See "External Cache Battery," page 1-29, for more information about the ECB. If the subsystem is backed up by a UPS, see the *HSZ70 Array Controller HSOF Version 7.0 CLI Reference Manual* for instructions on using the SET THIS CONTROLLER CACHE_UPS command.

Note The controller executes multiple write operations to satisfy a single write request for a RAIDset or mirrorset. For this reason, a RAIDset or mirrorset requires non-volatile cache memory to ensure data redundancy until the write request is satisfied.

Regardless of the backup power source you choose, the cache-memory power LED shown in Figure 1–8 flashes about once every three seconds to indicate that the cache module is receiving power from the subsystem.

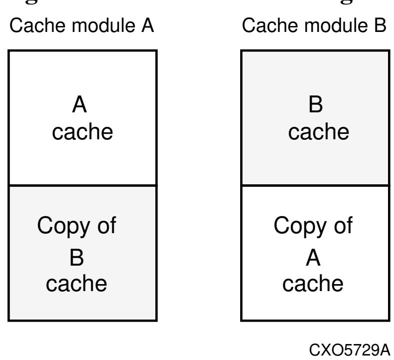
Mirrored Caching

To further ensure the availability of unwritten cache data, you can use a portion of each cache module's memory to mirror the other cache module's write-back data in a dual-redundant configuration.

Figure 1–9 shows the principle of mirrored caching: half of cache "A" mirrors cache "B's" write-back data and vice versa. This arrangement ensures that the write-back data will be preserved if a cache module or any of its components fail.

See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for instructions on configuring mirrored caching.

Figure 1–9 Mirrored Caching



Cache Policies Resulting from Cache Module Failtures

If the controller detects a full or partial failure of its cache module, it automatically reacts to preserve the cached write-back data. Then, depending upon the severity of the failure, the controller chooses an interim caching technique—also called the cache policy—which it uses until you repair or replace the cache module.

Table 1–5 shows the consequences of a full or partial failure of cache module A in a dual-redundant configuration. The consequences shown in this table are reciprocal for a failure of cache module B.

Table 1–5 Cache Policies Resulting from Cache Module Failures

Cache Module Status		Cache Policy	
Cache A	**Cache B**	**Unmirrored Cache**	**Mirrored Cache**
Good	Good	**Data loss:** No. **Cache policy:** Both controllers support write-back caching. **Failover:** No.	**Data loss:** No. **Cache policy:** Both controllers support write-back caching. **Failover:** No.
Multibit cache memory failure	Good	**Data loss:** forced error and loss of write-back data for which multibit error occurred. Controller A detects and reports the lost blocks. **Cache policy:** Both controllers support write-back caching. **Failover:** No.	**Data loss:** no. Controller A recovers its lost write-back data from the mirrored copy on cache B. **Cache policy:** Both controllers support write-back caching. **Failover:** No.
SIMM or cache memory controller failure	Good	**Data loss:** loss of write-back data that wasn't written to media when failure occurred. **Cache policy:** Controller A supports write-through caching only; controller B supports write-back caching. **Failover:** In dual-redundant failover, all units failover to controller B. In multiple-bus failover, RAIDsets, mirrorsets, and storagesets that use write-back caching failover to controller B. All units with lost data become inoperative until you clear them with the CLEAR LOST_DATA command. Units that didn't lose data operate normally on controller B. In single configurations, RAIDsets, mirrorsets, and all units with lost data become inoperative. Although you can clear the lost data errors on some units, RAIDsets and mirrorsets remain inoperative until you repair or replace the non-volatile memory on cache A.	**Data loss: No.** Controller A recovers all of its write-back data from the mirrored copy on cache B. **Cache policy:** Controller A supports write-through caching only; controller B supports write-back caching. **Failover:** In dual-redundant failover, all units failover to controller B and operate normally. In multiple-bus failover, RAIDsets, mirrorsets, and storagesets that use write-back caching failover to controller B.

Table 1–5 Cache Policies Resulting from Cache Module Failures (Continued)

Cache Module Status		Cache Policy	
Cache A	Cache B	Unmirrored Cache	Mirrored Cache
Cache board failure	Good	Same as for SIMM failure.	**Data loss: No.** Controller A recovers all of its write-back data from the mirrored copy on cache B. **Cache policy:** Both controllers support write-through caching only. Controller B cannot execute mirrored writes because cache module A cannot mirror controller B's unwritten data. **Failover:** No.

Cache Policies Resulting from ECB Failures

When the controller detects a full or partial failure of its ECB, it automatically reacts to preserve some or all of the write-back data in its cache module. Then, depending upon the severity of the failure, the controller chooses a caching method—also called the cache policy—which it uses until you replace the cache module's ECB.

Table 1–6 shows the consequences of a full or partial failure of cache module A's ECB in a dual-redundant configuration. The consequences shown in this table are reciprocal for a failure of cache module B's ECB.

Table 1–6 Cache Policies Resulting from ECB Failures

ECB Status		Cache Policy	
ECB Cache A	ECB Cache B	Unmirrored Cache	Mirrored Cache
Good	Good	**Data loss:** No. **Cache policy:** Both controllers continue to support write-back caching. **Failover:** No.	**Data loss:** No. **Cache policy:** Both controllers continue to support write-back caching. **Failover:** No.

Table 1–6 Cache Policies Resulting from ECB Failures (Continued)

ECB Status		Cache Policy	
ECB Cache A	ECB Cache B	Unmirrored Cache	Mirrored Cache
Low	Good	**Data loss:** No. **Cache policy:** Controller A supports write-through caching only; controller B supports write-back caching. **Failover:** In dual-redundant failover, all units failover to controller B and operate normally. In multiple-bus failover, RAIDsets, mirrorsets, and storagesets that use write-back caching failover to controller B. In single configurations, the controller only provides write-through caching to its units.	**Data loss:** No. **Cache policy:** Both controllers continue to support write-back caching. **Failover:** No.
Failed	Good	**Data loss:** No. **Cache policy:** Controller A supports write-through caching only; controller B supports write-back caching. **Failover:** In dual-redundant failover, all units failover to controller B and operate normally. In multiple-bus failover, RAIDsets, mirrorsets, and storagesets that use write-back caching failover to controller B. In single configurations, RAIDsets and mirrorsets become inoperative.	**Data loss:** No. **Cache policy:** Both controllers continue to support write-back caching. **Failover:** No.
Low	Low	**Data loss:** No. **Cache policy:** Both controllers support write-through caching only. **Failover:** No.	**Data loss:** No. **Cache policy:** Both controllers support write-through caching only. **Failover:** No.

Table 1–6 Cache Policies Resulting from ECB Failures (Continued)

ECB Status		Cache Policy	
ECB Cache A	**ECB Cache B**	**Unmirrored Cache**	**Mirrored Cache**
Failed	Low	**Data loss:** No. **Cache policy:** Both controllers support write-through caching only. **Failover:** In dual-redundant failover, all units failover to controller B and operate normally. In multiple-bus failover, RAIDsets, mirrorsets, and storagesets that use write-back caching failover to controller B. In single configurations, RAIDsets and mirrorsets become inoperative.	**Data loss:** No. **Cache policy:** Both controllers support write-through caching only. **Failover:** No.
Failed	Failed	**Data loss:** No. **Cache policy:** Both controllers support write-through caching only. **Failover:** No. RAIDsets and mirrorsets become inoperative. Other units that use write-back caching operate with write-through caching only.	**Data loss:** No. **Cache policy:** Both controllers support write-through caching only. **Failover:** No. RAIDsets and mirrorsets become inoperative. Other units that use write-back caching operate with write-through caching only.

External Cache Battery

To preserve the write-back cache data in the event of a primary power failure, a cache module must be connected to an external cache battery (ECB) or an uninterruptable power supply (UPS).

DIGITAL supplies two versions of ECBs: a single-battery ECB for single configurations, and a dual-battery ECB for dual-redundant configurations, which is shown in Figure 1–10. When the batteries are fully charged, an ECB can preserve 128 MB of cache memory for 24 hours and 64 MB for 48 hours.

Figure 1–10 ECB for Dual-Redundant Configurations

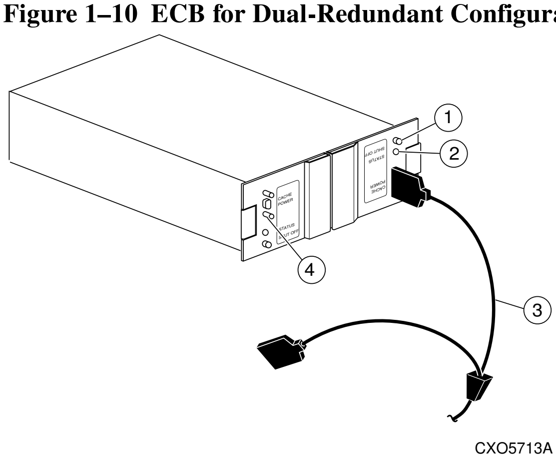


Table 1–7 Key to Figure 1–10 ECB for Dual-Redundant Configurations

Item	Description	Part No.
	ECB for dual-redundant configurations	DS–HS35X–BD
	ECB for single configurations	DS–HS35X–BC
1	Shut off button	—
2	Status LED	—
3	ECB cable	70–33268–01
4	VHDCI male port for second battery	—

Charging Diagnostics

Whenever you restart the controller, its diagnostic routines automatically check the charge in the ECB's batteries. If the batteries are fully charged, the controller reports them as "good" and rechecks them every 24 hours. If the batteries are low, the controller reports them as "low" and rechecks them every 4 minutes.

This 4-minute polling continues for up to 10 hours—the maximum time it should take to recharge fully discharged batteries. If the batteries have not been charged sufficiently after 10 hours, the controller declares them to be "failed."

Caution DIGITAL recommends that you replace the ECB every two years to prevent battery failure.

Note If a UPS is used for backup power, the controller does not check for battery charge. See the *HSZ70 Array Controller HSOF Version 7.0 CLI Reference Manual* for information about the CACHE_UPS and NOCACHE_UPS commands. Use these commands to set the backup power source for the cache module.

Host Cabling

Figures 1–11 through 1–13 show how to connect a controller to a host for single, dual-redundant, and multiple-bus failover configurations. See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for instructions about configuring a controller.

Figure 1–11 Cabling for Single Configuration

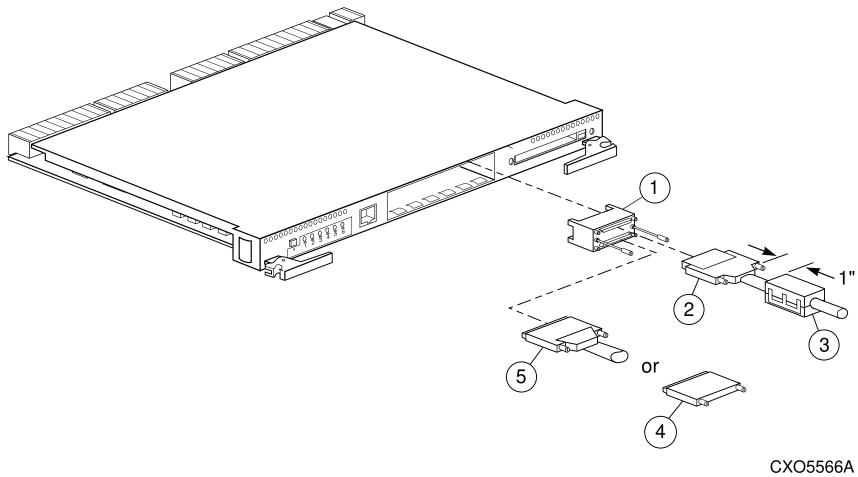


Table 1–8 Key to Figure 1–11 Cabling for Single Configuration

Item	Description	Part No.
1	Trilink connector	H8861–AA
2	Cable from host to controller The last two digits represent the cable's length in meters. "E" indicates one-half meter. For example, "02" represents a 2 m cable; "2E" represents a 2.5 m cable.	DS–BN37A–1 DS–BN37A–1E DS–BN37A–02 DS–BN37A–2E DS–BN37A–03 DS–BN37A–05 DS–BN37A–10 DS–BN37A–15 DS–BN37A–20 DS–BN37A–25
3	Ferrite bead	16–25105–18
4	Terminator	H8865–AA
5	Cable to other devices on host bus	Same as item 2

Figure 1–12 Cabling for Dual-Redundant Configuration

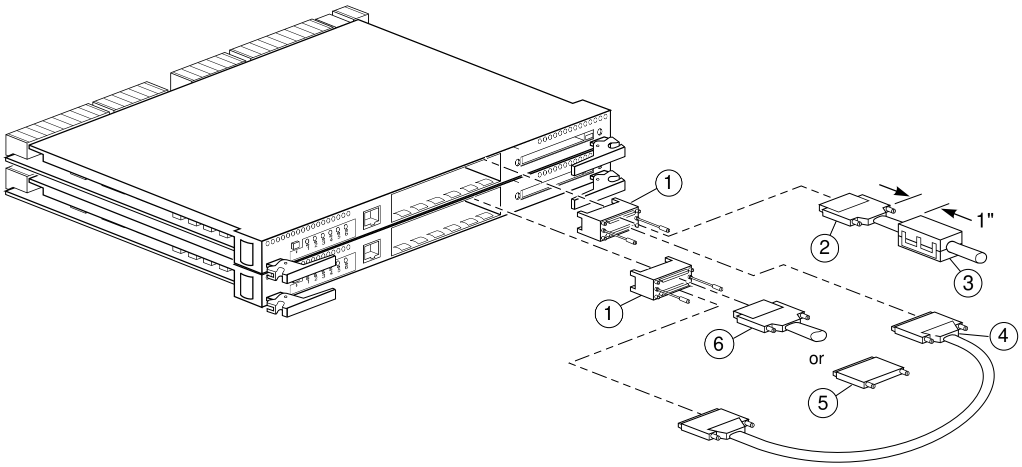


Table 1–9 Key to Figure 1–12 Cabling for Dual-Redundant Configuration

Item	Description	Part No.
1	Trilink connector	H8861–AA
2	Cable from host to controller "A" The last two digits represent cable length in meters. "E" indicates one-half meter. For example, "02" represents a 2 m cable; "2E" represents a 2.5 m cable.	DS–BN37A–1 DS–BN37A–1E DS–BN37A–02 DS–BN37A–2E DS–BN37A–03 DS–BN37A–05 DS–BN37A–10 DS–BN37A–15 DS–BN37A–20 DS–BN37A–25
3	Ferrite bead	16–25105–18
4	Dual-controller cable from "A" to "B"	DS–BN37A–0E
5	Terminator	H8865–AA
6	Cable from controller "B" to other devices on host bus	Same as item 2

Figure 1–13 Cabling for Multiple-Bus Failover Configuration

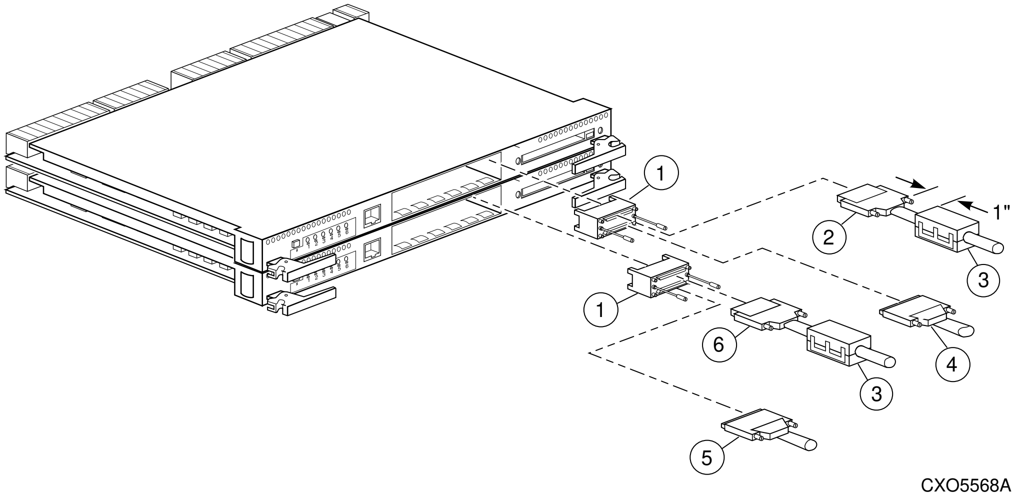


Table 1–10 Key to Figure 1–13 Cabling for Multiple-Bus Failover Configuration

Part	Description	Part No.
1	Trilink connector	H8861–AA
2	Cable from host to controller “A” The last two digits represent cable length in meters. “E” indicates one-half meter. For example, “02” represents a 2 m cable; “2E” represents a 2.5 m cable.	DS–BN37A–1 DS–BN37A–1E DS–BN37A–02 DS–BN37A–2E DS–BN37A–03 DS–BN37A–05 DS–BN37A–10 DS–BN37A–15 DS–BN37A–20 DS–BN37A–25
3	Ferrite bead	16–25105–18
4	Terminator or cable to other devices on host bus	H8865–AA or same as item 2
5	Terminator or cable to other devices on host bus	H8865–AA or same as item 2
6	Cable from host to controller “B”	Same as item 2

CHAPTER 2

Troubleshooting

This chapter provides guidelines for troubleshooting the controller, cache module, and external cache battery. It also describes the utilities and exercisers that you can use to aid in troubleshooting these components. See the appendixes for a list of LEDs and event codes. See the documentation that accompanied the enclosure for troubleshooting its hardware, such as the power supplies, cooling fans, and environmental monitoring unit.

Troubleshooting Checklist

The following checklist provides a general procedure for diagnosing the controller and its supporting modules. If you follow this checklist, you'll be able to identify many of the problems that occur in a typical installation. When you've identified the problem, use Table 2–1 to confirm your diagnosis and fix the problem.

If your initial diagnosis points to several possible causes, use the tools described later in this chapter to further refine your diagnosis. If the problem can't be diagnosed in the field, call customer service for additional support.

To troubleshoot the controller and its supporting modules:

1. Check the power to the cabinet and its components. Are the cords connected properly? Is the power within specifications?
2. Check the component cables. Are the bus cables to the controllers connected properly? Are the external cache battery (ECB) cables connected properly?
3. Check the program cards to ensure they're fully seated.
4. Check the operator control panel and devices for LED codes. See Appendix A to interpret the LED codes.
5. Connect a local terminal to the controller and check its configuration with the following command:

   SHOW THIS_CONTROLLER FULL

   Ensure that the HSOF software version is correct and that pertinent patches have been installed. Also, check the status of the cache module and its ECB.
6. Using FMU, check for last failure or memory-system failure entries. Show these codes and translate the last failure codes they contain. See page 2-11, Checking Failure Entries.

   If the controller has failed to the extent it cannot support a local terminal for FMU, check the host's error log for the instance or last-failure codes. See Appendix B to interpret the event codes.
7. Check the status of the devices with the following command:

   SHOW DEVICES FULL

Look for errors such as “misconfigured device” or “No device at this PTL.” If a device reports misconfigured or missing, check its status with the following command:

SHOW *device-name*

8. Check the status of the storagesets with the following command:

   SHOW STORAGESETS FULL

   Ensure that all storagesets are “normal” (or “normalizing” if it’s a RAIDset or mirrorset). Check again for misconfigured or missing devices.

9. Check the status of the units with the following command:

   SHOW UNITS FULL

   Ensure that all of the units are “available” or “online.” If the controller reports that a unit is unavailable or offline, re-check the storageset it belongs to with the following command:

   SHOW *storageset-name*

   If the controller reports that a unit has “lost data” or is “unwriteable,” re-check the status of the devices that make up the storageset. If the devices are OK, re-check the status of the cache module. If the unit reports a “media format error,” re-check the status of the storageset and its devices.

Troubleshooting Table

Use the troubleshooting checklist that begins on page 2–2 to find a symptom, then use this table to verify and fix the problem.

Table 2–1 Troubleshooting Table

Symptom	**Possible Cause**	**Investigation**	**Remedy**
Reset button not lit	No power to subsystem	Check power to subsystem and power supplies on controller's shelf	Replace cord or AC input power module
		Ensure that all cooling fans are installed. If one fan is missing or inoperative for more than 8 minutes, or if all fans have failed for more than 8 minutes, the EMU shuts down the subsystem.	Turn off power switch on AC input power module. Replace cooling fan. Restore power to subsystem.
	Failed controller	If the foregoing check fails to produce a remedy	Replace controller
Reset button lit steadily; other LEDs also lit	Various	See "Operator Control Panel LED Codes," page A-2	Follow repair action
Can't set failover to create dual-redundant configuration	Incorrect command syntax	See the *HSZ70 Array Controller HSOF Version 7.0 CLI Reference Manual* for the SET FAILOVER command	Use correct command syntax
	Different software versions on controllers	Check software versions on both controllers	Update one or both controllers so that both controllers are using the same software version
	Incompatible hardware	Check hardware versions	Upgrade controllers so that they're using compatible hardware

Table 2–1 Troubleshooting Table (Continued)

Symptom	Possible Cause	Investigation	Remedy
Can’t set failover to create dual-redundant configuration (Continued)	Controller previously set for failover	Ensure that neither controller is configured for failover	SET NOFAILOVER on both controllers, then reset “this” controller for failover
	Failed controller	If the foregoing checks fail to produce a remedy, check for OCP LED codes	Follow repair action
RAIDsets and mirrorsets inoperative			
RAIDsets and mirrorsets failed over to other controller			
All storagesets failed over to other controller			
Unmirrored cache; controller reports failed SIMM	Improperly installed SIMM	Remove cache module and ensure that SIMM is fully seated in its slot. See Figure 1–3 on page 1-7 to determine which cache module contains the failed SIMM.	Reseat SIMM
	Failed SIMM	If the foregoing check fails to produce a remedy	Replace SIMM
Mirrored cache; “this” controller reports SIMM 1 or 2 failed.	Improperly installed SIMM in “this” controller’s cache module (Figure 1–3 on page 1-7)	Remove cache module and ensure that SIMMs are installed properly. See “Adding or Replacing SIMMs,” page 4-12.	Reseat SIMM
	Failed SIMM in “this” controller’s cache module	If the foregoing check fails to produce a remedy	Replace SIMM in “this” controller’s cache module

Table 2–1 Troubleshooting Table (Continued)

Symptom	**Possible Cause**	**Investigation**	**Remedy**
Mirrored cache; “this” controller reports SIMM 3 or 4 failed.	Improperly installed SIMM in “other” controller’s cache module (Figure 1–3 on page 1-7)	Remove cache module and ensure that SIMMs are installed properly. See “Adding or Replacing SIMMs,” page 4-12.	Reseat SIMM
	Failed SIMM in “other” controller’s cache module	If the foregoing check fails to produce a remedy	Replace SIMM in “other” controller’s cache module
Mirrored cache; controller reports battery not present	Cache module was installed before it was connected to an ECB	ECB cable not connected to cache module	Connect ECB cable to cache module, then restart both controllers by pushing their reset buttons simultaneously
Mirrored cache; controller reports cache or mirrored cache has failed	Primary data and its mirrored copy data are not identical.	SHOW THIS_CONTROLLER indicates that the cache or mirrored cache has failed. Spontaneous FMU message indicates: “Primary cache declared failed - data inconsistent with mirror,” or “Mirrored cache declared failed - data inconsistent with primary.”	Enter SHUTDOWN command on controllers that report the problem. (This command flushes the contents of cache to synchronize its primary and mirrored data.) Restart the controllers that you shut down.

Table 2–1 Troubleshooting Table (Continued)

Symptom	Possible Cause	Investigation	Remedy
Invalid cache	Mirrored-cache mode discrepancy. This may occur after you've installed a new controller: its existing cache module is set for mirrored caching, but the new controller is set for unmirrored caching. (It may also occur if the new controller is set for mirrored caching but its existing cache module is not.)	SHOW THIS CONTROLLER indicates "invalid cache." Spontaneous FMU message indicates: "Cache modules inconsistent with mirror mode."	Connect a local terminal to controller reporting the error and clear the error with the following command, all on one line: CLEAR_ERRORS THIS_CONTROLLER NODESTROY INVALID_CACHE
	Cache module may erroneously contain unflushed write-back data. This may occur after you've installed a new controller: its existing cache module may indicate that it contains unflushed write-back data, but the new controller expects to find no data in the existing cache module. (This error may also occur if you install a new cache module for a controller that expects write-back data in the cache.)	SHOW THIS CONTROLLER indicates "invalid cache." No spontaneous FMU message.	Connect a local terminal to controller reporting the error and clear the error with the following command, all on one line: CLEAR_ERRORS THIS_CONTROLLER DESTROY INVALID_CACHE

Table 2–1 Troubleshooting Table (Continued)

Symptom	Possible Cause	Investigation	Remedy
Can't add device	Illegal device	See product-specific release notes that accompanied the software release for the most recent list of supported devices	Replace device
	Device not properly installed in shelf	Check that SBB is fully seated	Firmly press SBB into slot
	Failed device	Check for presence of device LEDs	Follow repair action in the documentation provided with the enclosure or device
	Failed power supplies	Check for presence of power supply LEDs	Follow repair action in the documentation provided with the enclosure or power supply
	Failed bus to device	If the foregoing checks fail to produce a remedy	Replace enclosure or shelf
Can't configure storagesets	Incorrect command syntax	See the *HSZ70 Array Controller HSOF Version 7.0 CLI Reference Manual* for the ADD *storageset* command	Reconfigure storageset with correct command syntax
	Exceeded maximum number of storagesets	Use CFMENU or the SHOW command to count the number of storagesets configured on controller	Delete unused storagesets
	Failed battery on ECB. (An ECB or UPS is required for RAIDsets and mirrorsets.)	Use the SHOW command to check the ECB's battery status	Replace ECB if required

Table 2–1 Troubleshooting Table (Continued)

Symptom	Possible Cause	Investigation	Remedy
Can’t assign unit number to storageset	Incorrect command syntax	See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for correct syntax	Reassign unit number with correct syntax
	Incorrect SCSI target ID numbers set for controller that accesses desired unit. (First number of unit number must be one of the SCSI target ID numbers for the controller.)	Use the SHOW command to check the controller’s SCSI target ID numbers	Reset controller’s SCSI target ID numbers or assign new unit number as desired
Unit is available but not online	This is normal. Units are “available” until the host accesses them, at which point their status is changed to “online.”	None	None
Host cannot access unit	Host files or device drivers not properly installed or configured	Check for the required device special files	Configure device special files as described in the getting started manual that accompanied your software release.

Table 2–1 Troubleshooting Table (Continued)

Symptom	Possible Cause	Investigation	Remedy
Host’s log file indicates that a forced error occurred when the controller was reconstructing a RAIDset or mirrorset	Unrecoverable read errors may have occurred when controller was reconstructing the storageset. Errors occur if another member fails while the controller is reconstructing the storageset.	Conduct a read scan of the storageset using the appropriate utility from the host’s operating system, such as the “dd” utility for a DIGITAL UNIX host.	Rebuild the storageset, then restore its data from a backup source. While the controller is reconstructing the storageset, monitor the activity with FMU for any unrecoverable errors. If unrecoverable errors persist, note the device on which they occurred and replace the device before proceeding.
	Host requested data from a normalizing storageset that didn’t contain the data	SHOW *storageset-name* to see if all of its members are “normal”	Wait for normalizing members to become normal, then resume I/O to it

Checking Failure Entries

The controller's fault-management software reports information about significant events and failures that occur during the controller's operation. This information is derived from the sense data, which the controller sends in response to a Request Sense command as described in the SCSI-2 specifications (Information technology, Small Computer System Interface, X3T9.2, 375R Rev. 10k, 10-Mar-93).

The Fault Management Utility (FMU) provides a limited interface to the controller's fault-management software. Use FMU to:

- Display the last-failure and memory-system-failure entries that the fault-management software stores in the controller's non-volatile memory.
- Translate many of the event messages that are contained in the entries related to the significant events and failures. For example, entries may contain codes that indicate the cause of the event, the software component that reported the event, the repair action, and so on.
- Set the display characteristics of spontaneous events and failures that the fault-management system sends to the local terminal.

Displaying Failure Entries

The controller stores the four most recent last-failure and memory-system failure reports as entries in its non-volatile memory. The occurrence of any failure event will terminate the controller on which it occurred. To display the last-failure and memory-system failure entries:

1. Connect a local terminal to the controller.
2. Start FMU with the following command:

   RUN FMU

3. Show one or more of the entries with the following command:

   SHOW *event_type entry# FULL*

   where:

   - *event-type* is LAST_FAIL or MEMORY_SYSTEM_FAIL

- *entry#* is ALL, MOST_RECENT, or 1 through 4
- *FULL* displays additional information, such as the register contents for the cache, FX, host port, and device ports.

4. Exit FMU with the following command:

EXIT

Example 2–1 Last-Failure Entry

The following example shows a last-failure entry. The Informational Report—the lower half of the entry—contains the instance code, reporting component, and so forth, which you can translate with FMU to learn more about the event.

```
Last Failure Entry: 1. Flags: 000FF301
Template: 1.(01) Description: Last Failure Event
Occurred on 06-DEC-1996 at 09:21:44
Controller Model:
Serial Number: ZG51909900 Hardware Version: 0000(00)
Controller Identifier:
Unique Device Number: 01519090 Model: 40.(28) Class: 1.(01)
Firmware Version: v7.0a
Node Name: "HSZ01"

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
```

Translating Event Codes

To translate the event codes in the fault-management reports for spontaneous events and failures:

1. Connect a local terminal to the controller.
2. Start FMU with the following command:

   RUN FMU

3. Show one or more of the entries with the following command:

   DESCRIBE *code_type code#*

   where *code_type* is one of those listed in Table 2–2 and *code#* is the alpha-numeric value displayed in the entry. The code types marked with an asterisk (*) require multiple code numbers.

Table 2–2 Event-Code Types

Event-Code Type	
instance	event_threshold
repair_action	memory_system_failure
last_failure	restart_type
ASC_ASCQ*	SCSI_command_operation*
controller_unique_ASC_ASCQ*	sense_data_qualifiers*
component	sense_key
device_type	template

Example 2–2 Last_Failure Code

The following example shows the FMU translation of a last-failure code.

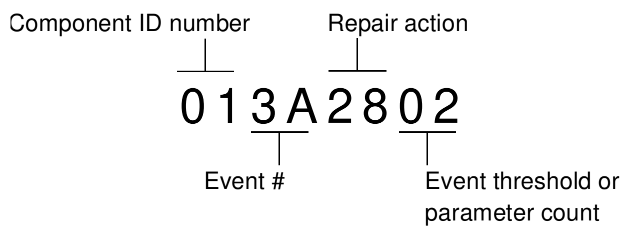
```
Last Failure Code: 206C0020 Description:
 Controller was forced to restart in order for
 new controller code image to take effect.
Reporting Component: 32.(20) Description:
 Command Line Interpreter
Reporting component's event number: 108.(6C)
Restart Type: 2.(02) Description: Automatic hardware restart
```

Instance Codes and Last-Failure Codes

Instance codes identify and accompany significant events that do not cause the controller to terminate operation; last-failure codes identify and accompany failure events that cause the controller to stop operating. Last-failure codes are sent to the host only after the affected controller is restarted successfully.

You can easily translate an instance or last-failure code yourself, rather than using FMU to translate them, if you understand their structure as shown in Figure 2–1.

Figure 2–1 Structure of an Instance or Last-Failure Code



- The component ID number identifies the software component that detected the event. See Component Identifier Codes on page B-74.
- The event number indicates the event that the component detected. When combined with the component ID, this number uniquely identifies the event (two different components may use the same event number to report different events).
- The repair action indicates the action that should be taken when the event threshold is reached. See Repair Action Codes on page B-65.
- The event threshold (reported for instance codes only) indicates the severity of the event and when the repair action should be taken. See Event Threshold Codes on page B-75.
- The parameter count (reported for last-failure codes only) indicates the number of fields in the event template that contain other salient information about the failure.

Controlling the Display of Significant Events and Failures

You can control how the fault-management software displays significant events and failures with FMU’s SET command. Table 2–3 shows and describes the various SET commands that you can enter while you’re running FMU. These commands remain in effect only as long as the current FMU session remains active unless you enter the PERMANENT qualifier—the last entry in Table 2–3.

Table 2–3 FMU SET Commands

Command	Result
SET EVENT_LOGGING SET NOEVENT_LOGGING	These commands enable and disable the spontaneous display of significant device events to the local terminal and host. By default, logging is disabled. If you enable logging, the controller spontaneously displays information about the events on the local terminal. These events are preceded with “%EVL” to identify them. If you disable logging—or choose not to capture the information with a logging mechanism— all information about nonfailure events will be lost. Spontaneous event logging is suspended during the execution of CLI commands and while you’re running utilities on a local terminal. These event logs cannot be recovered because they are spontaneous and not stored anywhere.
SET LAST_FAILURE LOGGING SET NOLAST_FAILURE LOGGING	These commands enable and disable the spontaneous display of failure events. By default, last-failure logging is enabled. If you enable last-failure event logging, the controller spontaneously displays information relevant to the sudden termination of the controller on a local terminal. These last-failure events are preceded with “%LFL” to identify them. In cases of automatic hardware reset, such as a sporadic power failure or pressing the controller’s reset button, the last-failure log display is inhibited—automatic resets don’t allow sufficient time to complete the log display.
SET *log_type* REPAIR_ACTION SET *log_type* NOREPAIR_ACTION	These commands enable and disable the inclusion of repair action information for event logging or last-failure logging. By default, repair actions are not displayed for these log types. If you enable the display of repair actions, the controller displays all of the recommended repair actions—if any—associated with the event.
SET *log_type* VERBOSE SET *log_type* NOVERBOSE	These commands enable and disable the automatic translation of event codes that are contained in event logs or last-failure logs. By default, the additional descriptions are not displayed for these log types. See Translating Event Codes on page 2-13 for instructions to translate these codes manually.

Table 2–3 FMU SET Commands (Continued)

Command	Result
SET PROMPT SET NOPROMPT	These commands enable and disable the display of the CLI prompt string following the log identifier (%EVL or %LFL). This command is useful if you use the CLI prompt string to identify the controllers in a dual-redundant configuration (see the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for instructions to set the CLI command string for a controller). If you enable the CLI prompt, you'll be able to identify which controller sent the log to the local terminal. By default, the CLI prompt is not displayed with event or last-failure logging.
SET TIMESTAMP SET NOTIMESTAMP	These commands enable and disable the display of the current date and time in the first line of an event or last-failure log. By default, the timestamp is not displayed.
SET FMU REPAIR_ACTION SET FMU NOREPAIR_ACTION	These commands enable and disable the inclusion of repair actions when you enter SHOW LAST_FAILURE and SHOW MEMORY_SYSTEM_FAILURE commands. By default, the repair actions are not shown. If you enable the repair actions, the command outputs display all of the recommended repair actions associated with the instance codes or last-failure codes that are used to describe an event.
SET FMU_VERBOSE SET FMU_NOVERBOSE	These commands enable and disable descriptive text when you enter the SHOW LAST_FAILURE and SHOW MEMORY_SYSTEM_FAILURE commands. By default, this descriptive text is not displayed. If you enable the descriptive text it identifies the fields and their numeric content that comprise an event or last-failure entry.
SET CLI_EVENT_REPORTING SET NOCLI_EVENT_REPORTING	These commands enable and disable the asynchronous errors reported at the CLI prompt, such as “swap signals disabled” or “shelf has a bad power supply.” By default, these errors are reported and must be cleared with the CLEAR ERRORS_CLI command. These errors are preceded with “%CER” to identify them.
SHOW PARAMETERS	This command displays the current settings associated with the SET command.
SET command PERMANENT	This qualifier preserves the SET command across controller resets.

Checking for Communication Problems

Use the virtual terminal display (VTDPY) utility to get information about the following communications:

- Communication between the controller and its hosts
- Communication between the controller and the devices in the subsystem
- The state and I/O activity of the logical units, devices, and device ports in the subsystem

To run VTDPY:

1. Connect a local terminal to the controller. The terminal must support ANSI control sequences.
2. Set the terminal to NOWRAP mode to prevent the top line of the display from scrolling off of the screen.
3. Start VTDPY with the following command:

   RUN VTDPY

   Use the following key sequences and commands to control VTDPY:

Table 2–4 VTDPY Key Sequences and Commands

Command	Action
Ctrl/C	Enables command mode; after entering Ctrl/C, enter one of the following commands and press Return: DISPLAY CACHE DISPLAY DEFAULT DISPLAY DEVICE DISPLAY STATUS HELP INTERVAL *seconds* (to change update interval)
Ctrl/G	Updates screen
Ctrl/O	Pauses (and resumes) screen updates
Ctrl/R	Refreshes current screen display
Ctrl/Y	Exits VTDPY

You may abbreviate the commands to the minimum number of characters necessary to identify the command. Enter a question mark (?) after a partial command to see the values that can follow the supplied command. For example, if you enter DISP ?, the utility will list CACHE, DEFAULT, and so forth. (Separate “DISP” and “?” with a space.) Upon successfully executing a command—other than HELP—VTDPY exits command mode. Pressing Return without a command also causes VTDPY to exit command mode.

Checking Controller-to-Host Communications

Use the transfer-rate region of the default display to see how or if the controller is communicating with the host.

Figure 2–2 Xfer Rate Region of the Default Display

```
VTDPY> DISPLAY DEFAULT

                      S/N: ZG64100176 SW: v7.0 HW: CX-02
                    65% I/D Hit  99.8% Idle       0 KB/S       0 Rq/S       Up:   0  5:14.53
Pr   Name  Stk/Max Typ Sta  CPU% Xfer Rate        Target     Unit  ASWC KB/S Rd% Wr% Cm% HT%
 0    NULL   0/  0      Rn  99.8 T W I   Mhz             111111 P0300 o
 1   FCTRL   1/  1 FNC  Bl   0.0 03W 6 10.00   0123456789012345 D0303 o^ b
 2   RECON  10/  1 FNC  Bl   0.0             P1      hH    PDD  D0304 o^ b
 3 HP_MAIN  40/  3 FNC  Bl   0.0             o2      hH    DD D P0400
 4  HP_TIM  10/  1 FNC  Bl   0.0             r3  ????hH         P0401
 7   VTDPY  20/ 12 DUP  Rn   0.0             t4      hH DDD     D0402 x^ b
13 MDATAIO  10/  4 FNC  Bl   0.0              5   P  hH
15 SVANVUP  10/  2 FNC  Bl   0.0              6 DDD  hH
16   MDATA  10/  4 FNC  Bl   0.0
```

Table 2–5 lists the heading and contents for each column of the Xfer Rate region.

Table 2–5 Xfer Rate Columns

Column	Contents
T	SCSI target ID
W	Transfer width: W for 16-bit; blank for 8-bit.
I	Initiator that negotiated synchronous communication.
MHz	Synchronous data rate negotiated by the initiator at the specified SCSI ID number. Async indicates that no communication has been established between the initiator (controller or host) and the SCSI target.

Checking Controller-to-Device Communications

Use the device display to see how or if the controller is communicating with the devices in the subsystem. This display contains three important regions:

- Device map region (upper left)
- Device status region (upper right)
- Device-port status (lower left)

Figure 2–3 Regions on the Device Display

```
VTDPY>DISPLAY DEVICE

                      S/N: ZG64100176 SW: v7.0 HW: CX-02
          67% I/D Hit  99.9% Idle       0 KB/S        0 Rq/S        Up:    0  5:17.54
       Target                        P TL ASWF Rq/S RdKB/S WrKB/S Que Tg CR BR TR
            111111                  P1120 A^      0      0      0   0  0  0  0  0
  0123456789012345                  D1130 A^      0      0      0   0  0  0  0  0
P1      hH    PDD                   D1140 A^      0      0      0   0  0  0  0  0
o2      hH    DD D                  D2120 A^      0      0      0   0  0  0  0  0
r3  ????hH                          D2130 A^      0      0      0   0  0  0  0  0
t4      hH DDD                      D2150 a^      0      0      0   0  0  0  0  0
 5   P  hH                          ?3020   ^ F   0      0      0   0  0  0  0  0
 6 DDD  hH                          ?3030   ^ F   0      0      0   0  0  0  0  0
                                    ?3040   ^ F   0      0      0   0  0  0  0  0
                                    ?3050   ^ F   0      0      0   0  0  0  0  0
                                    D4090 A^      0      0      0   0  0  0  0  0
                                    D4100 A^      0      0      0   0  0  0  0  0
Port Rq/S RdKB/S WrKB/S  CR BR TR   D4110 A^      0      0      0   0  0  0  0  0
 1      0      0      0   0  0  0   P5030 A^      0      0      0   0  0  0  0  0
 2      0      0      0   0  0  0   D6010 A^      0      0      0   0  0  0  0  0
 3      0      0      0   0  0  0   D6020 A^      0      0      0   0  0  0  0  0
 4      0      0      0   0  0  0   D6030 A^      0      0      0   0  0  0  0  0
 5      0      0      0   0  0  0
 6      0      0      0   0  0  0
```

Checking Device Type and Location

The device map region of the device display (upper left) shows all of the devices that the controller recognizes through its device ports. Table 2–6 lists the heading and contents for each column of the device map region.

Table 2–6 Device Map Columns

Column	Contents
Port	SCSI ports 1 through 6.
Target	SCSI targets 0 through 15. Single controllers occupy 7; dual-redundant controllers occupy 6 and 7.

Table 2–6 Device Map Columns (Continued)

Column	Contents
	D = disk drive or CD-ROM drive
	F = foreign device
	H = this controller
	h = other controller in dual-redundant configurations
	P = passthrough device
	? = unknown device type
	= no device at this port/target location

Checking Device Status and I/O Activity

The device status region of the device display (upper right) shows the name and I/O characteristics for all of the devices that the controller recognizes. Table 2–7 lists the heading and contents for each column of the device status region.

Table 2–7 Device Status Columns

Column	Contents
PTL	Kind of device and its port-target-lun (PTL) location:
	D = disk drive
	P = passthrough device
	? = unknown device type
	= no device at this port/target location
A	Availability of the device:
	A = available to this controller
	a = available to other controller
	U = unavailable, but configured on this controller
	u = unavailable, but configured on other controller
	= unknown availability state
S	Spindle state of the device:

Table 2–7 Device Status Columns (Continued)

Column	Contents
	^ = disk is spinning at correct speed; tape is loaded
	> = disk is spinning up
	< = disk is spinning down
	v = disk is not spinning
	= unknown spindle state
W	Write-protection state of the device. For disk drives, a W in this column indicates that the device is hardware write protected. This column is blank for other kinds of devices.
F	Fault state of the device. An F in this column indicates an unrecoverable device fault. If this field is set, the device fault LED should also be lit.
Rq/S	Average request rate for the device during the last update interval. Requests can be up to 32K and generated by host or cache activity.
RdKB/S	Average data transfer rate from the device (reads) during the last update interval.
WrKB/S	Average data transfer rate to the device (writes) during the last update interval.
Que	Maximum number of I/O requests waiting to be transferred to the device during the last update interval.
Tg	Maximum number of requests queued to the device during the last update interval. If the device doesn't support tagged queuing, the maximum value is 1.
CR	Number of SCSI command resets that occurred since VTDPY was started.
BR	Number of SCSI bus resets that occurred since VTDPY was started.
TR	Number of SCSI target resets that occurred since VTDPY was started.

Checking Device-Port Status and I/O Activity

The device-port status region of the device display (lower left) shows the I/O characteristics for the controller's device ports. Table 2–8 lists the heading and contents for each column of the device-port status region.

Table 2–8 Device-Port Status Columns

Column	Contents
Port	SCSI device ports 1 through 6.
Rq/S	Average request rate for the port during the last update interval. Requests can be up to 32K and generated by host or cache activity.
RdKB/S	Average data transfer rate from the devices on the port (reads) during the last update interval.
WrKB/S	Average data transfer rate to the devices on the port (writes) during the last update interval.
CR	Number of SCSI command resets that occurred since VTDPY was started.
BR	Number of SCSI bus resets that occurred since VTDPY was started.
TR	Number of SCSI target resets that occurred since VTDPY was started.

Checking Unit Status and I/O Activity

Use the cache display to see the status and I/O activity for the logical units configured on the controller.

Figure 2–4 Unit Status on the Cache Display

```
VTDPY> DISPLAY CACHE

                       S/N: ZG64100176 SW: v7.0 HW: CX-02
                          66% I/D Hit  99.8% Idle       0 KB/S     0 Rq/S Up:    0  5:16.42
Unit  ASWC  KB/S  Rd% Wr% Cm% HT% PH% MS% Purge BlChd BlHit
P0300 o        0   0   0   0   0   0   0     0     0     0
D0303 o^ b     0   0   0   0   0   0   0     0     0     0
D0304 o^ b     0   0   0   0   0   0   0     0     0     0
P0400          0   0   0   0   0   0   0     0     0     0
P0401          0   0   0   0   0   0   0     0     0     0
D0402 x^ b     0   0   0   0   0   0   0     0     0     0
```

Table 2–7 lists the heading and contents for each column of the device status region.

Table 2–9 Unit Status Columns

Column	Contents
Unit	Kind of unit (and its unit number):
	D = disk drive or CD-ROM drive
	P = passthrough device
	? = unknown device type
A	Availability of the unit:
	a = available to other controller
	d = disabled for servicing. Offline.
	e = mounted for exclusive access by a user
	f = media format error
	i = inoperative
	m = maintenance mode for diagnostic purposes
	o = online. Host may access this unit through “this controller.”
	r = rundown with the SET NORUN command
	v = no volume mounted due to lack of media

Table 2–9 Unit Status Columns (Continued)

Column	Contents
	x = online. Host may access this unit through "other controller."
	= unknown availability
S	Spindle state of the device:
	^ = disk is spinning at correct speed; tape is loaded
	> = disk is spinning up; tape is loading
	< = disk is spinning down; tape is unloading
	v = disk is not spinning; tape is unloaded
	= unknown spindle state
W	Write-protection state. For disk drives, a W in this column indicates that the device is hardware write protected. This column is blank for units that comprise other kinds of devices.
C	Caching state of the device:
	b = read and write-back caching enabled
	r = read caching only
	= caching disabled
KB/S	Average amount of data transferred to and from the unit during the last update interval in 1000-byte increments.
Rd%	Percentage of data transferred between the host and the unit that were read from the unit.
Wr%	Percentage of data transferred between the host and the unit that were written to the unit.
CM%	Percentage of data transferred between the host and the unit were compared. A compare operation can accompany a read or a write operation, so this column is not the sum of columns Rd% and Wr%.
HT%	Cache-hit percentage for data transferred between the host and the unit.
PH%	Partial cache-hit percentage for data transferred between the host and the unit.

Table 2–9 Unit Status Columns (Continued)

Column	Contents
MS%	Cache-miss percentage for data transferred between the host and the unit.
Purge	Number of blocks purged from the cache during the last update interval.
BlChd	Number of blocks added to the cache during the last update interval.
BlHit	Number of blocks hit during the last update interval.

Checking for Disk-Drive Problems

Use the disk inline exerciser (DILX) to check the data-transfer capability of disk drives. DILX generates intense read/write loads to the disk drive while monitoring the drive's performance and status. You may run DILX on as many disk drives as you'd like but, because this utility creates substantial I/O loads on the controller, DIGITAL recommends that you stop host-based I/O during the test. You may also use DILX to exercise the read capability of CD-ROM drives.

Finding a Disk Drive in the Subsystem

Follow these steps to find a disk drive or device in the subsystem:

1. Connect a local terminal to the controller.
2. Show the devices that are configured on the controller with the following command:

   SHOW DEVICES
3. Find the device in the enclosure with the following command:

   LOCATE *device-name*

   This command causes the device's LED to blink continuously. Enter the following command to turn off the LED:

   LOCATE CANCEL

Testing the Read Capability of a Disk Drive

To test the read capability of a disk drive:

1. From a host console, dismount logical unit that contains the disk drive you want to test.
2. Connect a local terminal to the controller that accesses the disk drive you want to test.
3. Run DILX with the following command:

   RUN DILX
4. Decline the Auto-configure option so that you can specify the disk drive to test.
5. Accept the default test settings and run the test in read-only mode.
6. Enter the unit number of the disk drive you want to test. For example, to test D107, enter the number 107.

7. If you want to test more than one disk drive, enter their unit numbers when prompted, otherwise enter “n” to start the test. Use the following control sequences to control DILX during the test.

Table 2–10 DILX Control Sequences

Command	Action
Ctrl/C	Terminates the test
Ctrl/G	Displays the performance summary for the current test and continue testing
Ctrl/Y	Terminates the test and exits DILX

Testing the Read and Write Capabilities of a Disk Drive

Run a DILX Basic Function test to test the read and write capability of a disk drive. During the Basic Function test, DILX runs these four tests. (DILX repeats the last three tests until the time that you set in step 6 on page 2-28 expires.)

- **Write test—**writes specific patterns of data to the disk drive (see Table 2–11 on page 2-29.) DILX does not repeat this test.
- **Random I/O test—**simulates typical I/O activity by issuing read, write, access, and erase commands to randomly chosen logical block numbers (LBNs). You can set the ratio of these commands, as well as the percentage of read and write data that are compared throughout this test. This test takes 6 minutes.
- **Data-transfer test—**tests throughput by starting at an LBN and transferring data to the next LBN that has not been written to. This test takes 2 minutes.
- **Seek test—**stimulates head motion on the disk drive by issuing single-sector erase and access commands. Each I/O uses a different track on each subsequent transfer. You can set the ratio of access and erase commands. This test takes 2 minutes.

To test the read and write capabilities of a specific disk drive:

1. From a host console, dismount the logical unit that contains the disk drive you want to test.
2. Connect a local terminal to the controller that accesses the disk drive you want to test.

3. Run DILX with the following command:

   RUN DILX

4. Decline the auto-configure option so that you can specify the disk drive to test.

Tip Use the auto-configure option if you want to test the read and write capabilities of every disk drive in the subsystem.

---

5. Decline the default settings.
6. Enter the number of minutes you want to run the DILX Basic Function test. (To ensure that DILX accesses the entire diskspace, you should enter 120 or more.)
7. Enter the number of minutes between the display of performance summaries.
8. Choose to include performance statistics in the summary.
9. Choose to display both hard and soft errors.
10. Choose to display the hex dump.
11. Accept the hard-error limit default.
12. Accept the soft-error limit default.
13. Accept the queue depth default.
14. Choose option 1 to run a Basic Function test.
15. Enable phase 1, the write test.
16. Accept the default percentage of requests that DILX issues as read requests during phase 2, the random I/O test. DILX issues the balance as write requests.
17. Choose ALL for the data patterns that DILX issues for write requests.
18. Perform the initial write pass.
19. Allow DILX to compare the read and write data.
20. Accept the default percentage of reads and writes that DILX compares.
21. Enter the unit number of the disk drive you want to test. For example, if you want to test D107, you'd enter the number 107.

22. If you want to test more than one disk drive, enter their unit numbers when prompted, otherwise enter “n” to start the test. Use the command sequences shown in Table 2–10 to control the write test.

Table 2–11 Data Patterns for Phase 1: Write Test

Pattern	Pattern in Hexadecimal Numbers
1	0000
2	8B8B
3	3333
4	3091
5	0001, 0003, 0007, 000F, 001F, 003F, 007F, 00FF, 01FF, 03FF, 07FF, 0FFF, 1FFF, 3FFF, 7FFF
6	FIE, FFFC, FFFC, FFFC, FFE0, FFE0, FFE0, FFE0, FE00, FC00, F800, F000, F000, C000, 8000, 0000
7	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	0001, 0002, 0004, 0008, 0010, 0020, 0040, 0080, 0100, 0200, 0400, 0800, 1000, 2000, 4000, 8000
14	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

DILX Error Codes

Table 2–12 explains the error codes that DILX may display during and after testing. Contact your service representitive to interpret the end-message fields.

Table 2–12 DILX Error Codes

Error Code	Explanation
1	Illegal Data Pattern Number found in data pattern header. DILX read data from the disk and discovered that the data did not conform to the pattern in which it was previously written.
2	No write buffers correspond to data pattern. DILX read a legal data pattern from the disk but because no write buffers correspond to the pattern, the data must be considered corrupt.
3	Read data does not match write buffer. DILX compared the read and write data and discovered that they didn’t correspond.

Running a Self Test

During start up, the controller runs a self test—also called the DAEMON tests—that automatically test the device ports, host port, cache module, and value-added functions. If you're experiencing intermittent problems with one of these components, you can manually run the self test in a continuous loop rather than restarting the controller over and over again.

See "DAEMON Tests," page 1-16, for more information about these tests.

To run a self test:

1. Connect a local terminal to the controller.
2. Start the self test with one of the following commands:

```
SELFTEST THIS CONTROLLER
SELFTEST OTHER_CONTROLLER
```

The self test runs until it detects an error or until you press the controller's reset button.

If it detects an error, the self test saves information about the error and produces an OCP LED code for a "daemon hard error." Restart the controller to write the error information to the host's error log, then check the log for a "built-in self-test failure" event report. This report will contain an instance code, located at offset 32 through 35, that you can use to determine the cause of the error. See "Translating Event Codes," page 2-13 for help on translating instance codes.

Shutting Down the Subsystem

Follow these steps to shut down a subsystem:

1. From a host console, dismount the logical units in the subsystem.
2. Connect a maintenance terminal to one of the controllers in your subsystem.
3. Shut down the controllers. In single configurations, you only need to shut down “this controller.” In dual-redundant configurations, shut down the “other controller” first, then shut down “this controller” with the following commands:

   SHUTDOWN OTHER_CONTROLLER
   SHUTDOWN THIS_CONTROLLER

   When the controllers shut down, their reset buttons and their first three LEDs are lit continuously. This may take several minutes, depending on the amount of data that needs to be flushed from the cache modules.
4. Turn off the power to the subsystem.
5. Unplug the subsystem’s power cord.
6. Disable the ECBs by pressing their shut off buttons until their status lights stops blinking—about two seconds.

Restarting the Subsystem

Follow these steps to restart a subsystem:

1. Plug in the subsystem’s power cord.
2. Turn on the subsystem. The controllers automatically restart and the ECB automatically re-enable themselves to provide backup power to the cache modules.

CHAPTER 3

Replacement Procedures

This chapter provides instructions for removing, installing, and replacing the controller, cache module, and external cache battery. See the documentation that accompanies the enclosure for information about replacing its hardware, such as the power supplies, cooling fans, cables, and environmental monitoring unit.

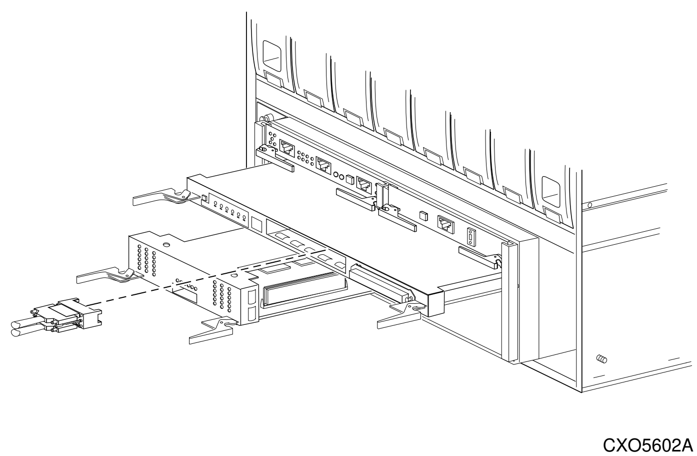
Replacing Modules in a Single Configuration

Follow the instructions in this section to replace modules in a single configuration. If you're replacing modules in a dual-redundant configuration, see "Replacing Modules in a Dual-Redundant Configuration," page 3-8.

Replacing the Controller and Cache Module

Follow these steps to replace a controller and cache module as shown in Figure 3–1.

Figure 3–1 Replacing the Controller and Cache Module



To remove the controller and cache module...

1. From the host console, dismount the logical units in the subsystem.
2. If the controller is operating, connect a local terminal to the controller to obtain the last failure codes if desired. Otherwise, go to step 8.
3. Start the Fault Management Utility (FMU) with the following command:

   RUN FMU
4. Display the instance and last failure codes with the following command:

   SHOW LAST_FAILURE ALL
5. Record the codes in the order they appear.

6. Exit FMU with the following command:

   EXIT

7. Shut down the controller with the following command:

   SHUTDOWN THIS_CONTROLLER

   When the controller shuts down, its reset button and the first three LEDs are lit continuously.

8. Turn off the power to the subsystem.
9. Disconnect the external cache battery (ECB) cable from the cache module.
10. Disable the ECB by pressing its shut off button until the status light stops blinking—about 2 seconds.
11. Remove the ESD cover and program card. Save them for the new controller.
12. Remove the trilink connector but don’t disconnect the bus cables from the trilink connector.
13. Disengage the two retaining levers and remove the controller.
14. Disengage the two retaining levers and remove the cache module.

To install the new controller and cache module...

1. Insert the new cache module into its slot and engage its retaining levers.
2. Connect the ECB cable to the new cache module. Follow the VHDCI Cable Precautions given in the Preface.
3. Insert the new controller into its slot and engage its retaining levers.
4. Connect the trilink connector to the new controller.
5. Insert the program card into the new controller and replace the ESD cover.
6. Restore power to the subsystem. The ECB automatically re-enables itself to provide backup power to the cache module.

   If the subsystem contains a device that was initialized with the SAVE_ CONFIGURATION switch, the controller automatically loads the subsystem’s configuration from that device. Otherwise, you’ll have to reconfigure the controller as described in the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual*.

If the controller you're installing was previously used in another subsystem, it will restart with the configuration that resides in its nonvolatile memory. If this differs from the subsystem's current subsystem's configuration, you can purge the controller's old configuration with the following command:

```
SET THIS_CONTROLLER INITIAL_CONFIGURATION
```

The controller shuts down after returning to its initial configuration. Press its reset button to restart the controller.

7. Install any patches that you had installed on the previous controller.
8. Mount the logical units on the host.

Replacing the Controller

The instructions for this procedure are similar to those for "Replacing the Controller and Cache Module," page 3-2, except that you should disregard the instructions pertaining to the cache module and the external cache battery.

Replacing the Cache Module

The instructions for this procedure are similar to those for "Replacing the Controller and Cache Module," page 3-2, except that you should disregard the instructions pertaining to the controller.

Replacing SIMMs in a Cache Module

The instructions for this procedure are the same as those for "Adding or Replacing SIMMs," page 4-12.

Replacing the External Cache Battery

Follow these instructions to remove and replace a single-battery external cache battery (ECB):

To remove the ECB...

1. If the controller and cache module are not operating, go to step 4. Otherwise, go to the next step.
2. Connect a local terminal to the controller.
3. Shut down the controller with the following command:

```
SHUTDOWN THIS_CONTROLLER
```

When the controller shuts down, its reset button and the first three LEDs are lit continuously.

4. Turn off the power to the subsystem.

To install the new ECB...

1. Insert the new ECB into its slot.
2. Connect the open end of the ECB “y” cable to the new ECB.
3. Restore power to the subsystem. The controller automatically restarts.
4. Wait until the new ECB’s status light is on continuously, then disconnect the ECB cable from the old ECB.

Caution Do not disconnect the old ECB until the batteries in the new ECB are fully charged. The new ECB’s status light will be lit continuously to indicate that its batteries are fully charged. A blinking status light indicates that its batteries are charging.

You may operate the subsystem regardless of the old ECB’s battery status, but do not disconnect the old ECB until the batteries in the new ECB are fully charged.

---

5. Remove the old ECB.

Removing the Controller and Cache Module

The instructions for this procedure are the same as the instructions for removing a controller in “Replacing the Controller and Cache Module,” page 3-2.

Removing the Controller

The instructions for this procedure are similar to the instructions for removing a controller in “Replacing the Controller and Cache Module,” page 3-2, except that you should disregard instructions for removing the cache module and the external cache battery.

Caution Your cache module may contain data if the controller crashed and you weren’t able to shut it down with the SHUTDOWN THIS_CONTROLLER command.

If you won’t be installing a new controller within 24 hours and if the cache module is still holding data, then restore the power to the subsystem after you’ve removed the failed controller. The cache module will hold its data as long as it receives power from the subsystem’s primary or secondary (UPS) power source or an ECB. An ECB only provides power for 24 hours.

Removing the Cache Module

The instructions for this procedure are similar to the instructions for removing a cache module in “Replacing the Controller and Cache Module,” page 3-2, except that you should disregard instructions for removing the controller module.

Installing a Controller and Cache Module

Follow these steps to install a controller and its cache module into an empty subsystem. If you’re upgrading a single-configuration subsystem to a dual-redundant subsystem, follow the instructions for “Upgrading to a Dual-Redundant Configuration,” page 4-10.

1. Turn off the power to the subsystem.
2. Insert the controller into the top slot—controller slot A (see Figure 1–3 on page 1-7). This slot responds to SCSI target ID number 7.
3. Insert the cache module into the bottom left slot—“cache slot A.”
4. Connect the external cache battery (ECB) cable to the cache module.
5. Connect an open end of the ECB “y” cable to the ECB.
6. Connect the trilink connector to the new controller.
7. Insert the program card into the new controller and replace the ESD cover.

8. Restore power to the subsystem. The ECB automatically re-enables itself to provide backup power to the cache module.

   If the subsystem contains a device that was initialized with the SAVE_ CONFIGURATION switch, the controller automatically loads the subsystem's configuration from that device. Otherwise, you'll have to reconfigure the controller as described in the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual*.

   If the controller you're installing was previously used in another subsystem, it will restart with the configuration that resides in its nonvolatile memory. If this differs from the subsystem's current subsystem's configuration, you can purge the controller's old configuration with the following command:

   SET THIS_CONTROLLER INITIAL_CONFIGURATION

   The controller shuts down after returning to its initial configuration. Press its reset button to restart the controller.

9. Install any patches that you had installed on the previous controller.
10. Mount the logical units on the host.

Installing a Controller

The instructions for this procedure are similar to the instructions for installing a controller in "Installing a Controller and Cache Module," page 3-6, except that you should disregard instructions for installing the cache module and the external cache battery.

Installing a Cache Module

The instructions for this procedure are similar to the instructions for installing a cache module in "Installing a Controller and Cache Module," page 3-6, except that you should disregard instructions for installing the controller module.

Replacing Modules in a Dual-Redundant Configuration

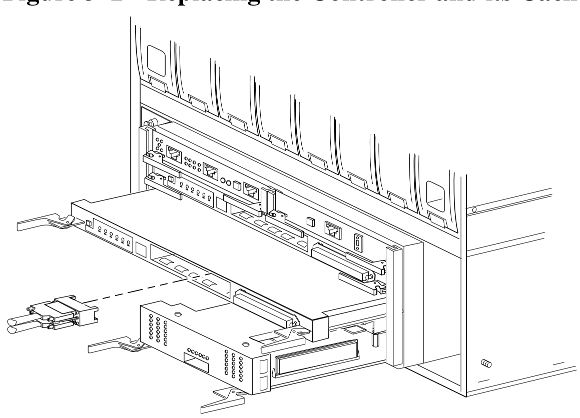
Follow the instructions in this section to replace modules in a dual-redundant configuration. If you're replacing modules in a single configuration, see "Replacing Modules in a Single Configuration," page 3-2.

Replacing a Controller and Cache Module

Follow these steps to replace a controller and its cache module—mirrored or unmirrored—as shown in Figure 3–2.

- The new controller's hardware must be compatible with the functioning controller's hardware. See the product-specific release notes that accompanied the software release for information regarding hardware compatibility.
- The software versions must be the same on both controllers.
- The new cache module must contain the same amount of memory as the module it's replacing.

Figure 3–2 Replacing the Controller and its Cache Module



To remove the controller and its cache module...

1. Connect a local terminal to the operational controller. The controller to which you're connected is "this controller;" the controller that you're removing is the "other controller."
2. Disable failover and take the controllers out of their dual-redundant configuration with the following command:

   SET NOFAILOVER
3. Start FRUTIL with the following command:

   RUN FRUTIL
4. Choose option 1 from the FRUTIL Main Menu to go to the Removal Options menu.
5. Choose option 1 from the Removal Options menu to remove the "other controller" and its cache module.
6. Confirm that you want to remove the "other controller" and its cache module.
7. Wait for FRUTIL to quiesce the ports.
8. Remove the trilink connector from the "other controller" but don't disconnect the bus cables from the trilink connector.
9. Disengage the two retaining levers and remove the "other controller."
10. Disconnect the external cache battery (ECB) cable from the "other controller's" cache module.
11. Disengage the two retaining levers and remove the "other controller's" cache module.

To install the new controller and new cache module...

1. Disable the ECB to which you're connecting the new cache module by pressing its shut off button until the status light stops blinking—about 2 seconds.
2. Connect the ECB cable to the new cache module. Follow the VHDCI Cable Precautions given in the Preface.
3. Indicate to FRUTIL that you're ready to insert the new controller and cache module.
4. Wait for FRUTIL to quiesce the ports.
5. Insert the new cache module into its slot and engage its retaining levers.

6. Ensure that the program card is not in the new controller and insert the new controller into its slot. Engage its retaining levers.
7. Wait for FRUTIL to terminate.
8. Connect the trilink connector to the new controller.
9. Restart the new controller with the following command:

   RESTART OTHER_CONTROLLER
10. Insert the program card into the new controller and replace the ESD cover.
11. Enable failover and re-establish the dual-redundant configuration with the following command:

    SET FAILOVER COPY=THIS_CONTROLLER

    This command copies the subsystem's configuration from "this controller" to the new controller.

Replacing a Controller

The instructions for this procedure are similar to those for "Replacing the Controller and Cache Module," page 3-2, except that you should disregard the instructions pertaining to the cache module and the external cache battery. Also, at step 5 choose option 2 to replace only the "other controller."

Replacing a Cache Module

Follow these steps to replace a cache module. The new cache module must contain the same amount of memory as the module it's replacing.

To remove the cache module...

1. Connect a local terminal to the controller with the operational cache module. The controller to which you're connected is "this controller." You're replacing the "other controller's" cache module in this procedure.
2. Disable failover and take the controllers out of their dual-redundant configuration with the following command:

   SET NOFAILOVER
3. Start FRUTIL with the following command:

   RUN FRUTIL

4. Choose option 1 from the FRUTIL Options menu to go to the Removal Options menu.
5. Choose option 3 from the Removal Options menu to replace the “other controller’s” cache module.
6. Confirm that you want to replace the cache module.
7. Disconnect the ECB cable from the cache module you’re replacing.
8. Disengage the two retaining levers and remove the “other controller’s” cache module.

To install the new cache module...

1. Disable the ECB to which you’re connecting the new cache module by pressing its shut off button until the status light stops blinking—about 2 seconds.
2. Connect the ECB cable to the new cache module. Follow the VHDCI Cable Precautions given in the Preface.
3. Indicate to FRUTIL that you’re ready to insert the new cache module.
4. Wait for FRUTIL to quiesce the ports.
5. Insert the new cache module into its slot and engage its retaining levers.
6. Wait for FRUTIL to terminate.
7. Restart the “other controller” with the following command:

   RESTART OTHER_CONTROLLER

8. Enable failover and re-establish the dual-redundant configuration with the following command:

   SET FAILOVER COPY=THIS_CONTROLLER

   This command copies the subsystem’s configuration from the “this controller” to the new controller. The ECB automatically re-enables itself to provide backup power to the cache module.

Replacing Both Controllers (and Their Cache Modules)

If you’re replacing the controllers only, repeat the instructions for “Replacing a Controller,” page 3-10, for each controller module.

If you’re replacing the controllers and their cache modules, repeat the instructions for “Replacing a Controller and Cache Module,” page 3-8, for each controller and cache module.

Replacing an External Cache Battery

Follow these steps to replace an external cache battery (ECB):

To disconnect the failed ECB...

1. Connect a local terminal to the controller with the operational ECB. The controller to which you're connected is "this controller;" the controller whose ECB you're replacing is the "other controller."
2. Disable failover and take the controllers out of their dual-redundant configuration with the following command:

   SET NOFAILOVER
3. Start FRUTIL with the following command:

   RUN FRUTIL
4. Choose option 3 from the FRUTIL Options menu to begin the replacement procedures.
5. Confirm that you want to replace the ECB.

To install the new ECB...

1. Insert the new ECB into an empty slot.
2. Connect the open end of the ECB "y" cable to the new ECB, then press Return.
3. Restart the "other controller" with the following command:

   RESTART OTHER_CONTROLLER
4. Enable failover and re-establish the dual-redundant configuration with the following command:

   SET FAILOVER COPY=THIS_CONTROLLER

   This command copies the subsystem's configuration from "this controller" to the new controller.
5. Wait until the new ECB's status light is on continuously, then disconnect the ECB cable from the old ECB.

Caution Do not disconnect the old ECB until the batteries in the new ECB are fully charged. The new ECB's status light will be lit continuously to indicate that its batteries are fully charged. A blinking status light indicates that its batteries are charging. You may operate the subsystem regardless of the old ECB's status.

---

6. If you want to backup both cache modules with the new ECB, repeat this procedure for the other controller and its cache module.
7. Remove the old ECB.

Removing a Controller and Cache Module

The instructions for this procedure are the same as the instructions for removing the controller and cache module in “Replacing a Controller and Cache Module,” page 3-8.

Removing a Controller

The instructions for this procedure are the same as the instructions for removing the controller in “Replacing a Controller,” page 3-10.

Removing a Cache Module

The instructions for this procedure are the same as the instructions for removing the cache module in “Replacing a Cache Module,” page 3-10.

Installing a Controller and Cache Module

Follow these steps to install a new controller and cache module into a subsystem that formerly used two controllers in a dual-redundant configuration:

1. Connect a local terminal to the operational controller. The controller to which you’re connected is “this controller;” the controller that you’re installing is the “other controller.”
2. Start FRUTIL with the following command:

   RUN FRUTIL
3. Choose option 2 from the FRUTIL Options menu to go to the Insert Options menu.
4. Choose option 3 from the Insert Options menu to insert the “other controller” and its cache module.
5. Connect the ECB cable to the new cache module. Follow the VHDCI Cable Precautions given in the Preface.
6. Confirm that you want to install the “other controller” and its cache module.
7. Wait for FRUTIL to quiesce the ports.
8. Ensure that the program card is not in the new controller and insert the new controller into its slot. Engage its retaining levers.

9. Insert the new cache module into its slot. Engage its retaining levers.
10. Wait for FRUTIL to terminate.
11. Connect the trilink connector to the new controller.
12. Restart the new controller with the following command:

    RESTART OTHER_CONTROLLER
13. Insert the program card into the new controller and replace its ESD cover.
14. Enable failover and re-establish the dual-redundant configuration with the following command:

    SET FAILOVER COPY=THIS_CONTROLLER

    This command copies the subsystem's configuration from the "this controller" to the new controller.

Installing a Controller

Follow these steps to install a controller into a subsystem that formerly used two controllers in a dual-redundant configuration:

1. Connect a local terminal to the operational controller. The controller to which you're connected is "this controller;" the controller that you're installing is the "other controller."
2. Start FRUTIL with the following command:

   RUN FRUTIL
3. Choose option 2 from the FRUTIL Options menu to go to the Insert Options menu.
4. Choose option 2 from the Insert Options menu to insert the "other controller."
5. Confirm that you want to install the "other controller."
6. Wait for FRUTIL to quiesce the ports.
7. Ensure that the program card is not in the new controller and insert the new controller into its slot. Engage the new controller's retaining levers.
8. Wait for FRUTIL to terminate.
9. Connect the trilink connector to the new controller.
10. Restart the new controller with the following command:

    RESTART OTHER_CONTROLLER

11. Insert the program card into the new controller and replace its ESD cover.
12. Enable failover and re-establish the dual-redundant configuration with the following command:

    SET FAILOVER COPY=THIS_CONTROLLER

    This command copies the subsystem's configuration from the "this controller" to the new controller.

Installing a Cache Module

Follow these steps to install a new cache module into a subsystem that formerly used two controllers in a dual-redundant configuration:

1. Connect a local terminal to the operational controller. The controller to which you're connected is "this controller;" the controller that you're installing is the "other controller."
2. Start FRUTIL with the following command:

   RUN FRUTIL

3. Choose option 2 from the FRUTIL Options menu to go to the Insert Options menu.
4. Choose option 3 from the Insert Options menu to insert the "other controller's" cache module.
5. Connect the ECB cable to the new cache module. Follow the VHDCI Cable Precautions given in the Preface.
6. Confirm that you want to install the cache module.
7. Wait for FRUTIL to quiesce the ports.
8. Insert the new cache module into its slot and engage its retaining levers.
9. Wait for FRUTIL to terminate, then restart the "other controller" with the following command:

   RESTART OTHER_CONTROLLER

10. Enable failover and re-establish the dual-redundant configuration with the following command:

    SET FAILOVER COPY=THIS_CONTROLLER

    This command copies the subsystem's configuration from the "this controller" to the new controller.

Replacing a Failed Storageset Member

If a disk drive fails in a RAIDset or mirrorset, the controller automatically places it into the failedset. If the spareset contains a replacement drive that satisfies the storageset's replacement policy, the controller automatically replaces the failed member with the replacement drive. If the spareset is empty or doesn't contain a satisfactory drive, the controller simply "reduces" the storageset so that it can operate without one of its members.

The storageset remains in this reduced state until the spareset contains a satisfactory drive. When the controller senses a satisfactory drive in the spareset, it automatically places the drive into the storageset and restores the storageset to normal. Therefore, replacing a failed storageset member means putting a satisfactory drive into the spareset.

To remove a failed RAIDset or mirrorset member...

1. Connect a local terminal to a controller that accesses the reduced RAIDset or mirrorset.
2. Enable AUTOSPARE with the following command:

   ```
   SET FAILEDSET AUTOSPARE
   ```

   With AUTOSPARE enabled, any new disk drive that you insert into the PTL location of a failed disk drive is automatically initialized and placed into the spareset.
3. Remove the failed disk drive.

To install the new member...

1. Insert a new disk drive that satisfies the replacement policy of the reduced storageset into the PTL location of the failed disk drive.

Note The controller automatically initializes the new disk drive and places it into the spareset. As soon as it becomes a member of the spareset, the controller automatically uses the new disk drive to restore the reduced RAIDset or mirrorset. If initialization fails, the new disk drive is placed into the failedset. Insert another disk drive.

CHAPTER 4

Upgrading the Subsystem

This chapter provides instructions for upgrading subsystems that use the controller, cache module, and external cache battery.

Upgrading Controller Software

You can upgrade the controller's software two ways:

- Install a new program card that contains the new software.
- Download a new software image and use the menu-driven Code Load/Code Patch utility (CLCP) to write it onto the existing program card. (You may also use this utility to list, install, and delete patches to the controller software.)

Installing a New Program Card

Follow these steps to install a program card that contains the new coftware. If you're only upgrading the software in a single-configuration controller, disregard references to the "other controller" and read the plural "controllers" as the singular "controller."

To upgrade the software by installing a new program card:

1. From the host console, dismount the storage units in the subsystem.
2. Connect a local terminal to one of the controllers.
3. Shut down the controllers with the following commands:

   ```
   SHUTDOWN OTHER_CONTROLLER
   SHUTDOWN THIS_CONTROLLER
   ```

   When the controllers shut down, their reset buttons and their first three LEDs are lit continuously.

Caution Do not change the subsystem's configuration or replace any of its modules until you've completed this procedure to upgrade the controller software.

---

4. Remove the program card ESD covers.
5. Press and hold the reset button while ejecting the program card on each controller. Release the reset buttons after you've removed the program cards.
6. Press and hold the reset button while inserting the new program cards. The controllers automatically restart. Their reset buttons will flash about once per second to indicate that they're ready to handle I/O.
7. Replace the ESD covers and push their pins to lock them into place.
8. Mount the storage units on the host.

Downloading New Software

Use option 1 from the CLCP Main Menu to download new software to the program card while it's installed in the controller.

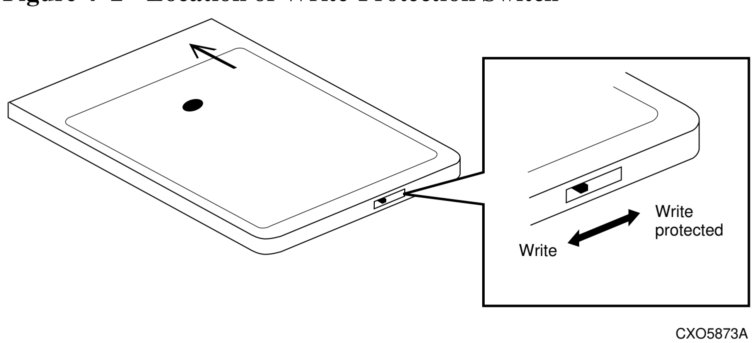
Figure 4–1 CLCP Main Menu

```
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] ?
```

To upgrade the software with CLCP:

1. Obtain the new binary software image file from a customer service representative.
2. Load the image onto a PC using the file- or network-transfer capabilities of your PC.
3. Disable any screen saver or terminate-and-stay-resident programs on your PC that may activate during the CLCP process.
4. From a host console, dismount the storage units in the subsystem.
5. Connect the PC to the controller's local connection port (you'll need the PC-serial port adapter shown in Figure 1–2 on page 1-4).
6. Configure the KERMIT transfer protocol on the PC to 19200 baud, eight bits, no parity, and one stop bit.
7. Remove the ESD cover. If your program card is equipped with a write-protection switch, disable write-protection by sliding the switch to the left as shown in Figure 4–2.

Figure 4–2 Location of Write-Protection Switch



8. From a terminal emulator, start CLCP with the following command.

   RUN CLCP

9. Choose option 1 from the CLCP Main Menu to start the Code LOAD local program.
10. Use KERMIT to transfer the binary image from the PC to the controller.

    When the download is complete, CLCP automatically writes the new image to the program card and restarts the controller.

11. Verify that the controller is running the new software version with the following command:

    SHOW THIS CONTROLLER

12. Slide the program card's write-protection switch to the right to re-enable write protection.
13. Replace the ESD cover.
14. Repeat the procedure to upgrade the other controller in dual-redundant subsystems.
15. Mount the storage units in the subsystem.

Using CLCP to List, Install, and Delete Software Patches

Use option 2 from the CLCP Main Menu to manage software patches. These small programming changes are placed into the controller's NVMEM and become active as soon you restart the controller. The controller reserves enough NVMEM memory for about ten patches, depending upon the size of the patches you're installing.

Keep the following points in mind while installing or deleting patches:

- Patches are associated with specific software versions. CLCP verifies the patch against the currently installed version.
- Patches are sequential: patch one (1) must be entered before patch two (2) and so on.
- Deleting one patch also deletes all higher-numbered patches. For example, if you delete patch two (2), you'll automatically delete patches three, four, and so on.
- Controllers in a dual-redundant configuration must have the same patches applied. You must install patches into each controller separately.

To install, delete, or list software patches:

1. If you're installing a software patch, obtain the patch file from a customer service representative.
2. Load the patch file onto a PC using the file- or network-transfer capabilities of your PC.
3. Connect the PC to the controller's local connection port (you'll need the PC-serial port adapter shown in Figure 1–2 on page 1-4).
4. Configure the KERMIT transfer protocol on the PC to 19200 baud, eight bits, no parity, and one stop bit.
5. Start CLCP with the following command.

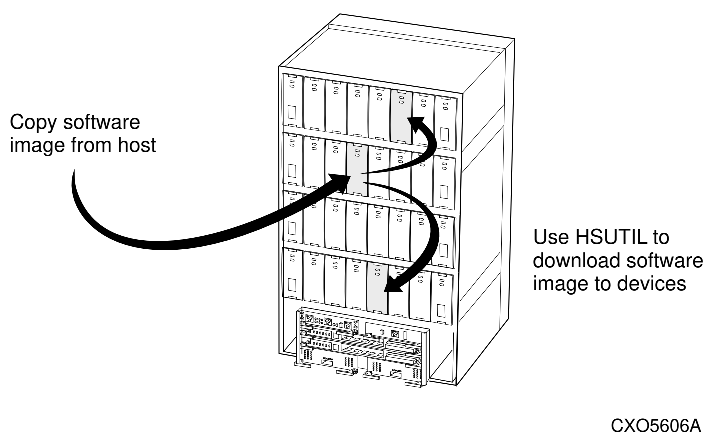
   RUN CLCP

6. Choose option 2 from the CLCP Main Menu to start the Code PATCH local program.
7. Choose option 1, 2, or 3 to install, delete, or list patches, respectively.
8. If you installed or deleted patches, press the controller's reset button to restart the controller.

Upgrading Firmware on a Device

Use HSUTIL to upgrade a device with firmware located in contiguous blocks at a specific LBN on a source disk drive configured as a unit on the same controller. Upgrading firmware on a disk or tape drive is a two-step process as shown in Figure 4–3: first, copy the new firmware from your host to a disk drive configured as a unit in your subsystem; then use HSUTIL to load the firmware onto the devices in the subsystem.

Figure 4–3 Upgrading Device Firmware



Keep the following points in mind while using HSUTIL to upgrade firmware on a device:

- HSUTIL has been tested with the qualified devices listed in the product-specific release notes that accompanied the software release. You may attempt to install firmware on unsupported devices—HSUTIL won't prevent this—but, if the upgrade fails, the device may be rendered unusable and therefore 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 I/O to the bus that services the device you're upgrading.

- 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 has previously been configured as such, you'll have to delete the unit number and storageset name associated with it.
- During the installation, the source disk drive is not available for other subsystem operations.
- Some devices may not reflect the new firmware version number when viewed from the "other" controller in a dual-redundant configuration. If you experience this, enter the following CLI command: CLEAR_ERRORS *device-name* UKNOWN.

To upgrade firmware with HSUTIL:

1. Connect a local terminal to the controller that accesses the device you want to upgrade.
2. Configure a single-disk unit. (In the next steps, you'll copy the firmware image to this unit, then use HSUTIL to distribute it to the devices you're upgrading. This unit must be a raw disk with no label or file structure to ensure that the firmware image resides in contiguous blocks starting from LBN 0 or another known LBN.)

   See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for instructions on configuring a single-disk unit.
3. Copy the firmware image to the single-disk unit that you configured in step 2. The firmware image must begin at a known LBN—usually 0—and must be contiguous. See the documentation that accompanied your host's operating system for instructions on copying firmware images to a disk drive.
4. Start HSUTIL with the following command.

   RUN HSUTIL
5. Choose option 2 or 3 from the HSUTIL menu.
6. Choose the single-disk unit as the source disk for the download.
7. Enter the starting LBN of the firmware image—usually LBN 0.
8. Enter the product ID of the device you want to upgrade. This ID corresponds to the product information that's reported in the "Type" column when you issue the SHOW DISK FULL command, such as RZ28 or RZ29.

HSUTIL lists all devices that correspond to the product ID you entered.

9. Enter the disk or tape name of the device you want to upgrade.
10. Confirm or enter the byte count of the firmware image.
11. Confirm the download.
12. Some disk firmware releases require that you reformat the disk after upgrading its firmware. See the documentation that accompanied the firmware to determine if you need to reformat the device.
13. When HSUTIL finishes downloading the firmware, it displays the new firmware revision for the disk drive.

HSUTIL Messages

HSUTIL may produce one or more of the following messages while you are formatting disk drives or installing new firmware. Many of the self-explanatory messages have been omitted from Table 4–1.

Table 4–1 HSUTIL Messages and Inquiries

Message	Description
Insufficient resources	HSUTIL cannot find or perform the operation because internal controller resources are not available.
Unable to change operation mode to maintenance for unit	HSUTIL was unable to put the source single disk drive unit into maintenance mode to enable formatting or code load.
Unit successfully allocated	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.
Unable to allocate unit	HSUTIL could not allocate the single disk drive unit. An accompanying message explains the reason.
Unit is owned by another sysop	Device cannot be allocated because it is being used by another subsystem function or local program.
Unit is in maintenance mode	Device cannot be formatted or code loaded because it is being used by another subsystem function or local program.
Exclusive access is declared for unit	Another subsystem function has reserved the unit shown.
The other controller has exclusive access declared for unit	The companion controller has locked out this controller from accessing the unit shown.

Table 4–1 HSUTIL Messages and Inquiries (Continued)

Message	Description
The RUNSTOP_SWITCH is set to RUN_DISABLED for unit	The RUN\NORUN unit indicator for the unit shown is set to NORUN; the disk cannot spin up.
What BUFFER SIZE, (in BYTES), does the drive require (2048, 4096, 8192) [8192]?	HSUTIL detects that an unsupported device has been selected as the target device and the firmware image requires multiple SCSI Write Buffer commands.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.
What is the TOTAL SIZE of the code image in BYTES [*device default*]?	HSUTIL detects that an unsupported device has been selected as the target device. You must enter the total number of bytes of data to be sent in the code load operation.
Does the target device support only the download microcode and save?	HSUTIL detects that an unsupported device has been selected as the target device. You must specify whether the device supports the SCSI Write Buffer command’s download and save function.
Should the code be downloaded with a single write buffer command?	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.

Upgrading to a Dual-Redundant Configuration

Follow these steps to upgrade a single-configuration subsystem to a dual-redundant configuration subsystem. You'll need the following items before you begin this procedure:

- Controller with the same software version that's installed on the subsystem's current single controller.
- Cache module with the same amount of memory that's installed in the current cache module.
- External cache battery (ECB) for a dual-redundant configuration.
- ECB cable.
- Dual-controller cable and trilink connector shown in Figure 1–12 on page 1-32.

To prepare the single-controller subsystem...

1. From a host console, dismount the storage units in the subsystem.
2. Connect a local terminal to the controller.
3. Shut down the controller with the following command:

   SHUTDOWN THIS_CONTROLLER

   When the controller shuts down, its reset button and the first three LEDs shine continuously.
4. Turn off the power to the subsystem.
5. Disconnect the ECB cable from the cache module.
6. Disable the ECB by pressing its shut off button until the status light stops blinking—about 2 seconds.
7. Disconnect the ECB cable from the ECB.
8. Remove the single-battery ECB.
9. Remove the trilink connector from the controller but do not disconnect the host cables from the trilink connector.

To install the new controller, cache module, and ECB...

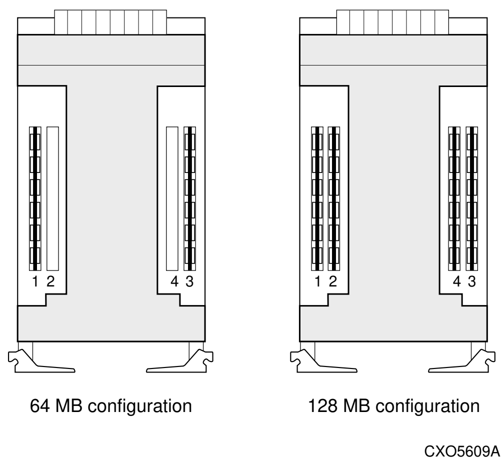
1. Ensure that the program card is not in the new controller, then insert the new controller into the bottom slot—controller slot “B.” This slot responds to SCSI target ID number 6. (See Figure 1–3 on page 1-7.) Engage its retaining levers.
2. Insert the new cache module into the bottom right slot—cache slot “B”—and engage its retaining levers.
3. Insert the new, two-battery ECB into the empty slot at the top of the cabinet.
4. Connect an ECB cable to each cache module.
5. Connect an open “y” end of each ECB cable to the new ECB.
6. Connect the controllers to the host as shown in Figure 1–12 on page 1-32.
7. Restore power to the subsystem.
8. Press and hold the reset button while inserting the program card into the new controller. The new controller initializes automatically and the ECB enables itself to provide backup power to the cache modules.

   The reset button flashes about once per second when initialization is complete.
9. Replace the ESD cover on the new controller.
10. See the *HSZ70 Array Controller HSOF Version 7.0 Configuration Manual* for instructions on configuring the controller and connecting it to the host.

Adding or Replacing SIMMs

The cache module may contain 64MB (2 x 32MB) or 128MB (4 x 32MB) of memory installed in the configurations shown in Figure 4–4.

Figure 4–4 Cache-Module Memory Configurations



Follow these steps to add or replace SIMMs in dual-redundant configurations. For single configurations, disregard references to the “other controller” and read the plural “controllers,” “cache modules,” and so on, as the singular “controller,” “cache module,” and so on.

1. From a host console, dismount the storage units in the subsystem.
2. Connect a local terminal to one of the controllers in the subsystem. The controller to which you’re connected is “this controller.”
3. Shut down both controllers in the following order with these commands:

   ```
   SHUTDOWN OTHER_CONTROLLER
   SHUTDOWN THIS_CONTROLLER
   ```

   When the controllers shut down, their reset buttons and their first three LEDs are lit continuously.
4. Turn off the power to the subsystem.
5. Disconnect the external cache battery (ECB) cables from both cache modules.
6. Disable both ECBs by pressing their shut off buttons until their status lights stop blinking—about 2 seconds.

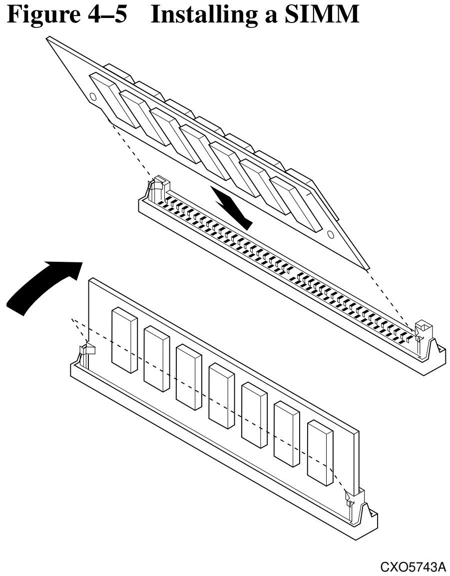
7. Disengage the two retaining levers on each cache module and remove both cache modules.

To install the SIMMs...

1. Insert the SIMM at a 45 degree angle as shown in Figure 4–5.
2. Rock the SIMM gently until it’s seated in the socket.
3. Tip the SIMM upright until both retaining clips engage the SIMM.

Caution Both cache modules must contain the same amount of memory. Populate sockets 1 and 3 for 64MB of memory, or all of the sockets for 128MB of memory, as shown in Figure 4–4.

Figure 4–5 Installing a SIMM



To re-install the cache modules...

1. Insert each cache module into its slot and engage its retaining levers.
2. Connect the ECB cables to the cache modules.
3. Restore power to the subsystem. The controllers automatically restart and the ECBs automatically re-enable themselves to provide backup power to the cache modules.
4. Mount the storage units on the host.

APPENDIX A

LED Codes

This appendix shows and describes the LED codes that you may encounter while servicing the controller, cache module, and external cache battery.

Operator Control Panel LED Codes

Use Table A–1 to interpret solid OCP patterns and Table A–2 to interpret flashing OCP patterns. Use this legend for both of these tables:

■ = reset button on
□ = reset button off
● = LED on
❍ = LED off

Note If the reset button is flashing and an LED is lit continuously, either the devices on that LED's bus don't match the controller's configuration, or an error has occurred in one of the devices on that bus.

Solid OCP Patterns

Table A–1 Solid OCP Patterns

Pattern	Error	Repair Action
■●●●●●●	DAEMON hard error	Verify that cache module is present and operating. If the error persists, replace controller.
■●●●●●❍	Repeated firmware bugcheck	Replace controller
■●●●●❍●	NVMEM version mismatch	Replace program card with latest software version
■●●●●❍❍	NVMEM write error	Replace controller
■●●●❍●●	NVMEM read error	Replace controller
■●●●❍●❍	NMI error within firmware bugcheck	Reset controller
■●●●❍❍●	Inconsistent NVMEM structures repaired	Reset controller
■●●●❍❍❍	Bugcheck with no restart	Reset controller
■●●❍●●●	Firmware induced restart following bugcheck failed to occur	Replace controller
■●●❍●●❍	Hardware induced restart following bugcheck failed to occur	Replace controller
■●●❍●❍●	Bugcheck within bugcheck controller	Reset controller
■●●❍❍●●	NVMEM version is too low	Verify that the program card contains the latest software version. If the error persists, replace controller.
■●●❍❍●❍	Program card write fail	Replace card
■●●❍❍❍●	ILF, INIT unable to allocate memory	Reset controller
■●●❍❍❍❍	Bugcheck before subsystem initialization completed	Reset controller
■●❍●●●●	Illegal SIMM configuration or mirrored cache with less than 64MB each or different amounts of memory.	Verify that SIMMs are installed as shown in Figure 1–3 on page 1-7. If cache is mirrored, ensure that both cache modules contain the same amount of memory: either 64MB or 128MB.

Table A–1 Solid OCP Patterns (Continued)

Pattern	Error	Repair Action
■●❍●●●❍	Two or more cabinets are using the same PVA ID in an extended subsystem	Reconfigure PVA ID to uniquely identify each cabinet in the subsystem. The cabinet with the controllers must be set to PVA ID 0. The additional cabinets must use PVA ID 2 and 3.
■●❍●●❍●	The cabinet with the controllers is not configured to PVA ID 0	Set PVA ID to 0 for the cabinet with the controllers. If problem persists, replace PVA module. If problem persists, replace EMU. If problem persists, replace the cabinet.
■●❍●●❍❍	Termination power for one or more of the cabinet's device SCSI buses is absent or unacceptable	Ensure that all of the cabinet's device SCSI buses have an I/O module. If problem persists, replace the failed I/O module.
■●❍●❍●●	One or more of the cabinet's buses are jumpered instead of terminated	Ensure that cabinet's buses are terminated. If problem persists, replace the failed terminator.
■●❍●❍●❍	Illegal I/O module configuration in an extended subsystem	All I/O modules in an extended subsystem must be of the same kind: either single-ended or differential.
■●❍●❍❍●	EMU microcode is incompatible with controller's software version	Upgrade either the EMU microcode or the software so that they're compatible. See the release notes that accompanied the controller's software release.
■❍❍❍❍❍❍	No program card detected	Ensure that program card is properly seated then reset controller. If the error persists, try the card in another controller; if the error persists, replace the card, otherwise, replace the controller that reported the error.

Flashing OCP Patterns

Table A–2 Flashing OCP Patterns

Pattern	Error	Repair Action
■❍❍❍❍❍●	Program card EDC error	Replace program card
■❍❍❍●❍❍	Timer zero in the timer chip will run when disabled	Replace controller
■❍❍❍●❍●	Timer zero in the timer chip decrements incorrectly	Replace controller
■❍❍❍●●❍	Timer zero in the timer chip did not interrupt the processor when requested	Replace controller
■❍❍❍●●●	Timer one in the timer chip decrements incorrectly	Replace controller
■❍❍•❍❍❍	Timer one in the timer chip did not interrupt the processor when requested	Replace controller
■❍❍●❍❍●	Timer two in the timer chip decrements incorrectly	Replace controller
■❍❍●❍●❍	Timer two in the timer chip did not interrupt the processor when requested	Replace controller
■❍❍●❍●●	Memory failure in the I/D cache	Replace controller
■❍❍●●❍❍	No hit or miss to the I/D cache when expected	Replace controller
■❍❍●●❍●	One or more bits in the diagnostic registers did not match the expected reset value	Replace controller
■❍❍●●●❍	Memory error in the nonvolatile journal SRAM	Replace controller
■❍❍●●●●	Wrong image seen on program card	Replace program card
■❍●❍❍❍❍	At least one register in the controller DRAB does not read as written	Replace controller
■❍●❍❍❍●	Main memory is fragmented into too many sections for the number of entries in the good memory list	Replace controller
■❍●❍❍●❍	The controller DRAB chip does not arbitrate correctly	Replace controller

Table A–2 Flashing OCP Patterns (Continued)

Pattern	Error	Repair Action
■○●○○●●	The controller DRAB chip failed to detect forced parity, or detected parity when not forced	Replace controller
■○●○●○○	The controller DRAB chip failed to verify the EDC correctly	Replace controller
■○●○●○●	The controller DRAB chip failed to report forced ECC	Replace controller
■○●○●●○	The controller DRAB chip failed some operation in the reporting, validating, and testing of the multibit ECC memory error	Replace controller
■○●○●●●	The controller DRAB chip failed some operation in the reporting, validating, and testing of the multiple single-bit ECC memory error	Replace controller
■○●●○○○	The controller main memory did not write correctly in one or more sized memory transfers	Replace controller
■○●●○○●	The controller did not cause an I-to-N bus timeout when accessing a “reset” host port chip	Replace controller
■○●●○●○	The controller DRAB chip did not report an I-to-N bus timeout when accessing a “reset” host port chip.	Replace controller
■○●●○●●	The controller DRAB chip did not interrupt the controller processor when expected	Replace controller
■○●●●○○	The controller DRAB chip did not report an NXM error when nonexistent memory was accessed	Replace controller
■○●●●○●	The controller DRAB chip did not report an address parity error when one was forced	Replace controller
■○●●●●○	There was an unexpected nonmaskable interrupt from the controller DRAB chip during the DRAB memory test.	Replace controller
■○●●●●●	Diagnostic register indicates there is no cache module, but an interrupt exists from the non-existent cache module	Replace controller

Table A–2 Flashing OCP Patterns (Continued)

Pattern	Error	Repair Action
■●❍❍❍❍❍	The required amount of memory available for the code image to be loaded from the program card is insufficient	Replace controller
■●❍❍❍❍●	The required amount of memory available in the pool area is insufficient for the controller to run	Replace controller
■●❍❍❍●❍	The required amount of memory in the buffer area is insufficient for the internal debugger to run	Replace controller
■●❍❍❍●●	The required amount of memory available in the buffer area is insufficient for the controller to run	Replace controller
■●❍❍●❍❍	The code image was not the same as the image on the card after the contents were copied to memory	Replace controller
■●❍❍●❍●	Diagnostic register indicates that the cache module does not exist, but access to that cache module caused an error	Replace backplane of controller shelf
■●❍❍●●❍	Diagnostic register indicates that the cache module does not exist, but access to that cache module did not cause an error	Replace backplane of controller shelf
■●❍●❍❍●	Non-existent memory regions were not trapped as required	Replace controller
■●●❍❍❍❍	The journal SRAM battery is bad	Replace controller
■●●●❍●❍	There was an unexpected interrupt from a read cache or the present and lock bits are not working correctly	Replace controller
■●●●❍●●	There is an interrupt pending on the controller's policy processor when there should be none	Replace controller
■●●●●❍❍	There was an unexpected fault during initialization	Replace controller

Table A–2 Flashing OCP Patterns (Continued)

Pattern	Error	Repair Action
■●●●●❍●	There was an unexpected maskable interrupt received during initialization	Replace controller
■●●●●●❍	There was an unexpected nonmaskable interrupt received during initialization	Replace controller
■●●●●●●	An illegal process was activated during initialization	Replace controller

APPENDIX B

Event Codes

This appendix describes the event codes that the fault-management software generates for spontaneous events and last-failure events.

Instance Codes

This table contains the instance codes that can be issued by the controller's fault-management software.

Table B–1 Instance Codes

Instance Code	Description	Template
01010302	An unrecoverable hardware fault occurred.	01
0102030A	An unrecoverable firmware inconsistency was detected or an intentional restart or shutdown of controller operation was requested.	01
01032002	Nonvolatile parameter memory component EDC check failed; content of the component reset to default settings.	11
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.	14
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.	14
01292602	The Master DRAB detected a Cache Timeout condition during an access attempt to a CACHEA0, CACHEA1, CACHEB0, or CACHEB1 DRAB registers region or memory region, the addressed region failed to respond.	14
012A3702	The CACHEA0 DRAB unexpectedly reported a Cache Timeout condition.	14
012B3702	The CACHEA1 DRAB unexpectedly reported a Cache Timeout condition.	14
012C3702	The CACHEB0 DRAB unexpectedly reported a Cache Timeout condition.	14
012D3702	The CACHEB1 DRAB unexpectedly reported a Cache Timeout condition.	14
012E2702	The Master DRAB detected an Nbus Transfer Error Acknowledge (TEA) condition – the TEA signal was asserted by an Nbus device during an i960 to Nbus device transaction.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
012F3702	The Master DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	14
01303702	The CACHEA0 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	14
01313702	The CACHEA1 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	14
01323702	The CACHEB0 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	14
01333702	The CACHEB1 DRAB unexpectedly reported an Nbus Transfer Error Acknowledge condition.	14
01342802	A Multiple Bit ECC error was detected during a memory refresh attempt by the Master DRAB.	14
01352902	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEA0 DRAB.	14
01362902	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEA1 DRAB.	14
01372A02	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEB0 DRAB.	14
01382A02	A Multiple Bit ECC error was detected during a memory refresh attempt by the CACHEB1 DRAB.	14
01392802	The Master DRAB detected a Multiple Bit ECC error during an FX attempt to read buffer memory.	14
013A2802	The Master DRAB detected a Multiple Bit ECC error during a Host Port attempt to read buffer memory.	14
013B2802	The Master DRAB detected a Multiple Bit ECC error during a Device Port attempt to read buffer memory.	14
013C2802	The Master DRAB detected a Multiple Bit ECC error during an i960 attempt to read buffer memory.	14
013D2902	The CACHEA0 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEA0 memory.	14
013E2902	The CACHEA0 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEA0 memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
013F2902	The CACHEA0 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEA0 memory.	14
01402902	The CACHEA0 DRAB detected a Multiple Bit ECC error during an i960 attempt to read CACHEA0 memory.	14
01412902	The CACHEA1 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEA1 memory.	14
01422902	The CACHEA1 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEA1 memory.	14
01432902	The CACHEA1 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEA1 memory.	14
01442902	The CACHEA1 DRAB detected a Multiple Bit ECC error during an i960 attempt to read CACHEA1 memory.	14
01452A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEB0 memory.	14
01462A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEB0 memory.	14
01472A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEB0 memory.	14
01482A02	The CACHEB0 DRAB detected a Multiple Bit ECC error during an i960 attempt to read CACHEB0 memory.	14
01492A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during an FX attempt to read CACHEB1 memory.	14
014A2A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during a Host Port attempt to read CACHEB1 memory.	14
014B2A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during a Device Port attempt to read CACHEB1 memory.	14
014C2A02	The CACHEB1 DRAB detected a Multiple Bit ECC error during an i960 attempt to read CACHEB1 memory.	14
014D3702	The Master DRAB unexpectedly reported a Multiple Bit ECC error.	14
014E3702	The CACHEA0 DRAB unexpectedly reported a Multiple Bit ECC error.	14
014F3702	The CACHEA1 DRAB unexpectedly reported a Multiple Bit ECC error.	14
01503702	The CACHEB0 DRAB unexpectedly reported a Multiple Bit ECC error.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01513702	The CACHEB1 DRAB unexpectedly reported a Multiple Bit ECC error.	14
01522B02	The Master DRAB detected an Ibus to Nbus Timeout condition during an i960 to Nbus device transaction, the Nbus device failed to respond.	14
01533702	The CACHEA0 DRAB unexpectedly reported an Ibus to Nbus Timeout condition.	14
01543702	The CACHEA1 DRAB unexpectedly reported an Ibus to Nbus Timeout condition.	14
01553702	The CACHEB0 DRAB unexpectedly reported an Ibus to Nbus Timeout condition.	14
01563702	The CACHEB1 DRAB unexpectedly reported an Ibus to Nbus Timeout condition.	14
01572C02	The Master DRAB detected a Nonexistent Memory Error condition during an FX attempt to write buffer memory.	14
01582C02	The Master DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to buffer memory.	14
01592C02	The Master DRAB detected a Nonexistent Memory Error condition during an FX attempt to read buffer memory.	14
015A2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write buffer memory.	14
015B2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to buffer memory.	14
015C2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read buffer memory.	14
015D2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write buffer memory.	14
015E2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to buffer memory.	14
015F2C02	The Master DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read buffer memory.	14
01602C02	The Master DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write buffer memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01612C02	The Master DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write a byte to buffer memory.	14
01622C02	The Master DRAB detected a Nonexistent Memory Error condition during an i960 attempt to read buffer memory.	14
01632D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEA0 memory.	14
01642D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEA0 memory.	14
01652D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEA0 memory.	14
01662D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEA0 memory.	14
01672D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEA0 memory.	14
01682D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEA0 memory.	14
01692D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEA0 memory.	14
016A2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEA0 memory.	14
016B2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEA0 memory.	14
016C2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write CACHEA0 memory.	14
016D2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write a byte to CACHEA0 memory.	14
016E2D02	The CACHEA0 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to read CACHEA0 memory.	14
016F2D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEA1 memory.	14
01702D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEA1 memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01712D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEA1 memory.	14
01722D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEA1 memory.	14
01732D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEA1 memory.	14
01742D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEA1 memory.	14
01752D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEA1 memory.	14
01762D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEA1 memory.	14
01772D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEA1 memory.	14
01782D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write CACHEA1 memory.	14
01792D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write a byte to CACHEA1 memory.	14
017A2D02	The CACHEA1 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to read CACHEA1 memory.	14
017B2E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEB0 memory.	14
017C2E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEB0 memory.	14
017D2E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEB0 memory.	14
017E2E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEB0 memory.	14
017F2E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEB0 memory.	14
01802E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEB0 memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01812E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEB0 memory.	14
01822E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEB0 memory.	14
01832E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEB0 memory.	14
01842E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write CACHEB0 memory.	14
01852E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write a byte to CACHEB0 memory.	14
01862E02	The CACHEB0 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to read CACHEB0 memory.	14
01872E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write CACHEB1 memory.	14
01882E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to write a byte to CACHEB1 memory.	14
01892E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an FX attempt to read CACHEB1 memory.	14
018A2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write CACHEB1 memory.	14
018B2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to write a byte to CACHEB1 memory.	14
018C2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Host Port attempt to read CACHEB1 memory.	14
018D2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write CACHEB1 memory.	14
018E2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to write a byte to CACHEB1 memory.	14
018F2E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during a Device Port attempt to read CACHEB1 memory.	14
01902E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write CACHEB1 memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01912E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to write a byte to CACHEB1 memory.	14
01922E02	The CACHEB1 DRAB detected a Nonexistent Memory Error condition during an i960 attempt to read CACHEB1 memory.	14
01933702	The Master DRAB unexpectedly reported a Nonexistent Memory Error condition.	14
01943702	The CACHEA0 DRAB unexpectedly reported a Nonexistent Memory Error condition.	14
01953702	The CACHEA1 DRAB unexpectedly reported a Nonexistent Memory Error condition.	14
01963702	The CACHEB0 DRAB unexpectedly reported a Nonexistent Memory Error condition.	14
01973702	The CACHEB1 DRAB unexpectedly reported a Nonexistent Memory Error condition.	14
01982F02	An Address Parity error was detected during a memory refresh attempt by the Master DRAB.	14
01993002	An Address Parity error was detected during a memory refresh attempt by the CACHEA0 DRAB.	14
019A3002	An Address Parity error was detected during a memory refresh attempt by the CACHEA1 DRAB.	14
019B3102	An Address Parity error was detected during a memory refresh attempt by the CACHEB0 DRAB.	14
019C3102	An Address Parity error was detected during a memory refresh attempt by the CACHEB1 DRAB.	14
019D2F02	The Master DRAB detected an Address Parity error during an FX attempt to read buffer memory.	14
019E2F02	The Master DRAB detected an Address Parity error during a Host Port attempt to read buffer memory.	14
019F2F02	The Master DRAB detected an Address Parity error during a Device Port attempt to read buffer memory.	14
01A02F02	The Master DRAB detected an Address Parity error during an i960 attempt to read buffer memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01A13002	The CACHEA0 DRAB detected an Address Parity error during an FX attempt to read CACHEA0 memory.	14
01A23002	The CACHEA0 DRAB detected an Address Parity error during a Host Port attempt to read CACHEA0 memory.	14
01A33002	The CACHEA0 DRAB detected an Address Parity error during a Device Port attempt to read CACHEA0 memory.	14
01A43002	The CACHEA0 DRAB detected an Address Parity error during an i960 attempt to read CACHEA0 memory.	14
01A53002	The CACHEA1 DRAB detected an Address Parity error during an FX attempt to read CACHEA1 memory.	14
01A63002	The CACHEA1 DRAB detected an Address Parity error during a Host Port attempt to read CACHEA1 memory.	14
01A73002	The CACHEA1 DRAB detected an Address Parity error during a Device Port attempt to read CACHEA1 memory.	14
01A83002	The CACHEA1 DRAB detected an Address Parity error during an i960 attempt to read CACHEA1 memory.	14
01A93102	The CACHEB0 DRAB detected an Address Parity error during an FX attempt to read CACHEB0 memory.	14
01AA3102	The CACHEB0 DRAB detected an Address Parity error during a Host Port attempt to read CACHEB0 memory.	14
01AB3102	The CACHEB0 DRAB detected an Address Parity error during a Device Port attempt to read CACHEB0 memory.	14
01AC3102	The CACHEB0 DRAB detected an Address Parity error during an i960 attempt to read CACHEB0 memory.	14
01AD3102	The CACHEB1 DRAB detected an Address Parity error during an FX attempt to read CACHEB1 memory.	14
01AE3102	The CACHEB1 DRAB detected an Address Parity error during a Host Port attempt to read CACHEB1 memory.	14
01AF3102	The CACHEB1 DRAB detected an Address Parity error during a Device Port attempt to read CACHEB1 memory.	14
01B03102	The CACHEB1 DRAB detected an Address Parity error during an i960 attempt to read CACHEB1 memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01B13702	The Master DRAB unexpectedly reported an Address Parity error.	14
01B23702	The CACHEA0 DRAB unexpectedly reported an Address Parity error.	14
01B33702	The CACHEA1 DRAB unexpectedly reported an Address Parity error.	14
01B43702	The CACHEB0 DRAB unexpectedly reported an Address Parity error.	14
01B53702	The CACHEB1 DRAB unexpectedly reported an Address Parity error.	14
01B63202	The Master DRAB detected an Ibus Parity Error during an i960 ID/ Cache access attempt.	14
01B73202	The Master DRAB detected an Ibus Parity Error during an i960 buffer memory access attempt.	14
01B83202	The Master DRAB detected an Ibus Parity Error during an i960 buffer memory access attempt with a simultaneous but unrelated CACHExn memory access.	14
01B93202	The Master DRAB detected an Ibus Parity Error during an i960 CACHEA memory access with a simultaneous but unrelated buffer memory access.	14
01BA3202	The Master DRAB detected an Ibus Parity Error during an i960 CACHEB memory access with a simultaneous but unrelated buffer memory access.	14
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.	14
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.	14
01BD3702	The Master DRAB unexpectedly reported an Ibus Parity error.	14
01BE3702	The CACHEA0 DRAB unexpectedly reported an Ibus Parity error.	14
01BF3702	The CACHEA1 DRAB unexpectedly reported an Ibus Parity error.	14
01C03702	The CACHEB0 DRAB unexpectedly reported an Ibus Parity error.	14
01C13702	The CACHEB1 DRAB unexpectedly reported an Ibus Parity error.	14
01C22F02	The Master DRAB detected a Write Data Parity error during an FX attempt to write buffer memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01C32F02	The Master DRAB detected a Write Data Parity error during an FX attempt to write a byte to buffer memory.	14
01C42F02	The Master DRAB detected a Write Data Parity error during a Host Port attempt to write buffer memory.	14
01C52F02	The Master DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to buffer memory.	14
01C62F02	The Master DRAB detected a Write Data Parity error during a Device Port attempt to write buffer memory.	14
01C72F02	The Master DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to buffer memory.	14
01C82F02	The Master DRAB detected a Write Data Parity error during an i960 attempt to write buffer memory.	14
01C92F02	The Master DRAB detected a Write Data Parity error during an i960 attempt to write a byte to buffer memory.	14
01CA3002	The CACHEA0 DRAB detected a Write Data Parity error during an FX attempt to write CACHEA0 memory.	14
01CB3002	The CACHEA0 DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEA0 memory.	14
01CC3002	The CACHEA0 DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEA0 memory.	14
01CD3002	The CACHEA0 DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEA0 memory.	14
01CE3002	The CACHEA0 DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEA0 memory.	14
01CF3002	The CACHEA0 DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEA0 memory.	14
01D03002	The CACHEA0 DRAB detected a Write Data Parity error during an i960 attempt to write CACHEA0 memory.	14
01D13002	The CACHEA0 DRAB detected a Write Data Parity error during an i960 attempt to write a byte to CACHEA0 memory.	14
01D23002	The CACHEA1 DRAB detected a Write Data Parity error during an FX attempt to write CACHEA1 memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01D33002	The CACHEA1 DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEA1 memory.	14
01D43002	The CACHEA1 DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEA1 memory.	14
01D53002	The CACHEA1 DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEA1 memory.	14
01D63002	The CACHEA1 DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEA1 memory.	14
01D73002	The CACHEA1 DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEA1 memory.	14
01D83002	The CACHEA1 DRAB detected a Write Data Parity error during an i960 attempt to write CACHEA1 memory.	14
01D93002	The CACHEA1 DRAB detected a Write Data Parity error during an i960 attempt to write a byte to CACHEA1 memory.	14
01DA3102	The CACHEB0 DRAB detected a Write Data Parity error during an FX attempt to write CACHEB0 memory.	14
01DB3102	The CACHEB0 DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEB0 memory.	14
01DC3102	The CACHEB0 DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEB0 memory.	14
01DD3102	The CACHEB0 DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEB0 memory.	14
01DE3102	The CACHEB0 DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEB0 memory.	14
01DF3102	The CACHEB0 DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEB0 memory.	14
01E03102	The CACHEB0 DRAB detected a Write Data Parity error during an i960 attempt to write CACHEB0 memory.	14
01E13102	The CACHEB0 DRAB detected a Write Data Parity error during an i960 attempt to write a byte to CACHEB0 memory.	14
01E23102	The CACHEB1 DRAB detected a Write Data Parity error during an FX attempt to write CACHEB1 memory.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
01E33102	The CACHEB1 DRAB detected a Write Data Parity error during an FX attempt to write a byte to CACHEB1 memory.	14
01E43102	The CACHEB1 DRAB detected a Write Data Parity error during a Host Port attempt to write CACHEB1 memory.	14
01E53102	The CACHEB1 DRAB detected a Write Data Parity error during a Host Port attempt to write a byte to CACHEB1 memory.	14
01E63102	The CACHEB1 DRAB detected a Write Data Parity error during a Device Port attempt to write CACHEB1 memory.	14
01E73102	The CACHEB1 DRAB detected a Write Data Parity error during a Device Port attempt to write a byte to CACHEB1 memory.	14
01E83102	The CACHEB1 DRAB detected a Write Data Parity error during an i960 attempt to write CACHEB1 memory.	14
01E93102	The CACHEB1 DRAB detected a Write Data Parity error during an i960 attempt to write a byte to CACHEB1 memory.	14
01EA3702	The Master DRAB unexpectedly reported a Write Data Parity error.	14
01EB3702	The CACHEA0 DRAB unexpectedly reported a Write Data Parity error.	14
01EC3702	The CACHEA1 DRAB unexpectedly reported a Write Data Parity error.	14
01ED3702	The CACHEB0 DRAB unexpectedly reported a Write Data Parity error.	14
01EE3702	The CACHEB1 DRAB unexpectedly reported a Write Data Parity error.	14
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.	51
02032001	Journal SRAM backup battery failure; detected during system restart. The Memory Address field contains the starting physical address of the Journal SRAM.	12
02042001	Journal SRAM backup battery failure; detected during periodic check. The Memory Address field contains the starting physical address of the Journal SRAM.	12

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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 CACHEA0 memory.	12
02062301	The CACHE backup battery has been declared bad. Either it failed testing performed by the Cache Diagnostics during system startup or it was low (insufficiently charged) for longer than the expected duration. The Memory Address field contains the starting physical address of the CACHEA0 memory.	12
02072201	The CACHE Dynamic Ram controller and ArBitration engine 0 (DRAB0) failed testing performed by the Cache Diagnostics. The Memory Address field contains the starting physical address of the CACHEA0 memory.	14
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.	14
02090064	A data compare error was detected during the execution of a compare modified READ or WRITE command.	51
020B2201	Failed read test of a write-back metadata page residing in cache. 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 CACHEA0 memory.	14
020C2201	Cache Diagnostics have declared the cache bad during testing. The Memory Address field contains the starting physical address of the CACHEA0 memory.	14
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.	14
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.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	14
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.	14
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.	51
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) 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.	14
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.	41
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.	41
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.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	51
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 Copying state.	51
022C0064	The device specified in the Device Locator has transitioned from Copying or Normalizing state to Normal state.	51
022E0064	The device specified in the Device Locator field has been converted to a Mirrorset associated with the logical unit.	51
022F0064	The mirrored device specified in the Device Locator field has been converted to a single device associated with the logical unit.	51
02382201	The Cache Dynamic Ram Controller and Arbitration Engine 1 (DRAB1) which resides on the other cache module failed testing performed by the cache diagnostics. This is the mirrored cache DRAB. The Memory Address field contains the starting physical address of the CACHEB0 menory.	14
02392201	Both the Cache Dynamic Ram Controller and Arbitration Engine 0 (DRAB0) and 1 (DRAB1), which resides on the other cache module, failed testing performed by the cache diagnostics. Data cannot be accessed in the primary cache or the mirror cache. The Memory Address field contains the starting physical address of the CACHEA0 memory.	14
023E2401	Metadata residing on the two cache modules disagree as to the mirror mode. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	14
023F2301	The CACHE B backup battery covering the mirror cache is insufficiently charged. The Memory Address field contains the starting physical address of the CACHEB1 memory	12
02402301	The CACHE B backup battery covering the mirror cache has been declared bad. Either it failed testing performed by the Cache Diagnostics during system startup or it was low (insufficiently charged) for longer than the expected duration. The Memory Address field contains the starting physical address of the CACHEB1 memory.	12

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
02412401	Mirrored cache writes have been disabled. Either the primary or the mirror cache has been declared bad or invalid and will not be used. Note that in this instance the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	14
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.	14
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.	14
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.	14
02452201	The Cache Dynamic Ram controller and Arbitration Engine 0 and 1(DRAB0 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 CACHEB0 memory.	14
02492401	The write cache module which is the mirror for the primary cache is not present (missing). A cache is expected to be configured and it may contain dirty write cached data. Note that in this instance, the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	14
024A2401	Mirroring is enabled and the primary write cache module is not present (missing). A cache is expected to be configured and it may contain dirty write cached data. Note that in this instance, the Memory Address, Byte Count, DRAB register, and Diagnostic register fields are undefined.	14
024B2401	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.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	14
0251000A	This 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.	51
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.	51
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.	51
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	51
0255000A	The controller was unable to successfully transfer data to target unit. The Information field of the Device Sense Data contains the block number of the first block in error	51
0256000A	The write operation failed because the unit is Data Safety Write Protected. The Information field of the Device Sense Data contains the block number of the first block in error	51
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	51
0258000A	This command was aborted prior to completion. The Information field of the Device Sense Data contains the block number of the first block in error	51
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	51

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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	51
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	51
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	51
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	51
025F2201	Memory diagnostics performed during controller initialization detected an excessive number (512 pages or more) of memory errors detected on the primary cache memory. Diagnostics have not declared the cache failed, due to the isolated bad memory regions, but this is a warning to replace the cache as soon as possible in case of further degradation. The firmware performed the necessary error recovery as appropriate. Note that in this instance the Memory Address and Byte Count fields are undefined.	14
02602201	Memory diagnostics performed during controller initialization detected an excessive number (512 pages or more) of memory errors detected on mirrored cache memory. Diagnostics has not declared the cache failed, due to the isolated bad memory regions, but this is a warning to replace the cache as soon as possible in case of further degradation. The firmware performed the necessary error recovery as appropriate. Note that in this instance the Memory Address, Byte Count fields are undefined.	14
02613801	Memory diagnostics performed during controller initialization detected that the SIMM in location 1 failed on the cache module. Note that in this instance the Byte Count field in undefined.	14
02623801	Memory diagnostics performed during controller initialization detected that the SIMM in location 2 failed on the cache module. Note that in this instance the Byte Count field in undefined.	14
02633801	Memory diagnostics performed during controller initialization detected that the SIMM in location 3 failed on the cache module. Note that in this instance the Byte Count field in undefined.	14

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
02643801	Memory diagnostics performed during controller initialization detected that the SIMM in location 4 failed on the cache module. Note that in this instance the Byte Count field in undefined.	14
02653801	Memory diagnostics performed during controller initialization detected that the SIMM in location 3 on the other controller’s cache module (on mirrored cache) failed. Mirroring has been disabled. Note that in this instance the Byte Count field in undefined.	14
02663801	Memory diagnostics performed during controller initialization detected that the SIMM in location 4 on the other controller’s cache module (on mirrored cache) failed. Mirroring has been disabled. Note that in this instance the Byte Count field in undefined.	14
02675201	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.	51
0268530A	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.	51
02695401	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.	51
026A5001	The RAIDset associated with the logical unit has gone inoperative.	51
026B0064	The RAIDset associated with the logical unit has transitioned from Normal state to Reconstructing state.	51
026C0064	The RAIDset associated with the logical unit has transitioned from Reconstructing state to Normal state.	51
026D5201	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.	51
026E0001	The device specified in the Device Locator field has been reduced from the Mirrorset associated with the logical unit. The nominal number of members in the mirrorset has been decreased by one. The reduced device is now available for use.	51
026F530A	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.	51

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
02705401	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.	51
02710064	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 Device Sense Data Information field.	51
02725101	The Mirrorset associated with the logical unit has gone inoperative.	51
02730001	The device specified in the Device Locator field had a read error which has been repaired with data from another mirrorset member.	51
02745A0A	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.	51
02755601	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.	51
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.	41
03022002	SCSI interface chip command timeout during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	41
03034002	Byte transfer timeout during disk operation. Note that in this instance the Associated Additional Sense Code and Associated Additional Sense Code Qualifier fields are undefined.	41
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.	41
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.	41
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.	41

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	41
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.	41
03094002	An unrecoverable disk drive error was encountered while performing work related to disk unit operations.	51
030C4002	A Drive failed because a Test Unit Ready command or a Read Capacity command failed.	51
030D000A	Drive was failed by a Mode Select command received from the host.	51
030E4002	Drive failed due to a deferred error reported by drive.	51
030F4002	Unrecovered Read or Write error.	51
03104002	No response from one or more drives.	51
0311430A	Nonvolatile memory and drive metadata indicate conflicting drive configurations.	51
0312430A	The Synchronous Transfer Value differs between drives in the same storageset.	51
03134002	Maximum number of errors for this data transfer operation exceeded.	51
03144002	Drive reported recovered error without transferring all data.	51
03154002	Data returned from drive is invalid.	51
03164002	Request Sense command to drive failed.	51
03170064	Illegal command for pass through mode.	51
03180064	Data transfer request error.	51
03194002	Premature completion of a drive command.	51
031A4002	Command timeout.	51
031B0101	Watchdog timer timeout.	51
031C4002	Disconnect timeout.	51
031D4002	Unexpected bus phase.	51

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
031E4002	Disconnect expected.	51
031F4002	ID Message not sent by drive.	51
03204002	Synchronous negotiation error.	51
03214002	The drive unexpectedly disconnected from the SCSI bus.	51
03224002	Unexpected message.	51
03234002	Unexpected Tag message.	51
03244002	Channel busy.	51
03254002	Message Reject received on a valid message.	51
0326450A	The disk device reported Vendor Unique SCSI Sense Data.	51
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.	41
0328450A	The disk device reported standard SCSI Sense Data.	51
03324002	SCSI bus selection timeout	
03330002	Device power on reset	
03344002	Target assertion of REQ after WAIT DISCONNECT	
03354002	During device intialization a Test Unit Ready command or a Read Capacity comand to the device failed.	
03364002	During device initialization the device reported a deferred error.	
03374002	During device initialization the maximum number of errors for a data transfer operation was exceeded.	
03384002	Request Sense command to the device failed	
03394002	Command timeout.	
033A4002	Disconnect timeout.	
033B4002	Unexpected bus phase.	
033C4002	The device unexpectedly disconnected from the SCSI bus.	
033D4002	Unexpected message.	

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
033E4002	Message Reject received on a valid message.	
033F0101	No command control structures available for passthrough device operation.	
03402002	Device port SCSI chip reported gross error.	
03410101	Miscellaneous SCSI Port Driver coding error.	
03420101	A passthrough device related internal error code was reported which is not recognized by the Fault Management firmware.	
03434002	During device initialization the device reported unexpected standard SCSI Sense Data.	
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.	41
03C92002	SCSI interface chip command timeout 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.	41
03CA4002	Byte transfer timeout 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.	41
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.	41
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.	41
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.	41

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	41
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.	41
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.	41
03D14002	The identification of a device does not match the organization information. The actual device type is unknown to the controller. Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	41
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.	41
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.	41
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.	41
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.	41

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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).	41
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.	41
03D8450A	During device initialization, the device reported the SCSI Sense Key ILLEGAL REQUEST. 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 shall 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.	41
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.	41
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.	41
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.	41
03DC450A	During device initialization, the device reported a SCSI Vendor Specific Sense Key. This sense key is available for reporting vendor specific conditions.	41

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	41
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.	41
03DF450A	During device initialization, the device reported the SCSI Sense Key EQUAL. This indicates a SEARCH DATA command has satisfied an equal comparison.	41
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.	41
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.	41
03E2450A	During device initialization, the device reported a reserved SCSI Sense Key.	41
03EE0064	The EMU for the cabinet indicated by the Associated Port field has become available. Note that the Associated Target, Associated Additional Sense Code, and the Associated Additional Sense Code Qualifier fields are undefined.	41
03EF8301	The EMU for the cabinet indicated by the Associated Port field has become unavailable. Note that the Associated Target, Associated Additional Sense Code, and the Associated Additional Sense Code Qualifier fields are undefined.	41
03F10502	The SWAP interrupt from the device port indicated by the Associated 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, both controller front panel button presses and removal/ insertion of devices are not 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.	41

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
03F20064	The SWAP interrupts have been cleared and re-enabled for all device ports. Note that in this instance the Associated Port, Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	41
03F30064	An asynchronous SWAP interrupt was detected by the controller for the device port indicated by the Associated Port field. Possible reasons for this occurrence include: ■ device insertion or removal ■ shelf power failure ■ SWAP interrupts reenabled Note that in this instance the Associated Target, Associated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	41
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.	41
03F60402	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 supply has failed. ■ One of the shelf cooling fans has failed. Note that in this instance the Associated Target, Assoicated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	41
03F70401	The shelf indicated by the Associated 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 hte Associated Target, Assoicated Additional Sense Code, and Associated Additional Sense Code Qualifier fields are undefined.	41
03F80701	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.	41

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
03F90601	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.	41
03FA0D01	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.	41
03FB0E01	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.	41
03FC0F01	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.	41
03FD0F01	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.	41
03FE0F01	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.	41
03FF0F01	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.	41
03FF0F01	The EMU-detected external air sense fault is now fixed. Note that the Associated Target, Associated Additional Sense Code, and the Associated Additional Sense Code Qualifier fields are undefined.	41
03EF8301	The EMU for the cabinet indicated by the Associated Port field has become available. Note that the Associated Target, Associated Additional Sense Code, and the Associated Additional Sense Code Qualifier fields are undefined.	41
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.	05
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.	05

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	05
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.	05
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.	05
07080B0A	Failover Control was unable to send keepalive 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.	05
43010064	Host Port Protocol component has detected that the other controller has failed and that this controller has taken over the units specified in the extended sense data.	04
43020064	Host Port Protocol component has detected that this controller has taken over (failed back) the units specified in the extended sense data.	04
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.	13
82042002	A spurious interrupt was detected during the execution of a Subsystem Built-In Self Test.	13
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.	13

Table B–1 Instance Codes (Continued)

Instance Code	Description	Template
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.	13
82072002	An unrecoverable error was detected during execution of the FX Subsystem Test.	13
82082002	An unrecoverable error was detected during execution of the Nbus init test.	13

Last Failure Codes

This table contains the last failure codes can be issued by the controller's fault-management software.

Table B–2 Last Failure Codes

Code	Description
01000100	Memory allocation failure during executive initialization.
01010100	An interrupt without any handler was triggered.
01020100	Entry on timer queue was not of type AQ or BQ.
01030100	Memory allocation for a facility lock failed.
01040100	Memory initialization called with invalid memory type.
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.
01070100	Timer chip setup failed.
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.
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

Table B–2 Last Failure Codes (Continued)

Code	Description
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.
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).
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).
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 a reference to a memory region that is not implemented. 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.
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 occurence for the first boot following manufacture of the controller module and during the transition from one firmware version to another if and only 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.
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 manufactruing configuration activities. If this event is reported at any other time, follow the recommended repair action associated with this Last Failure code.
01100100	Non-maskable interrupt entered but no Non-maskable interrupt pending. This is typically caused by an indirect call to address 0.

Table B–2 Last Failure Codes (Continued)

Code	Description
01110106	A bugcheck occurred during EXEC$BUGCHECK processing. ■ Last Failure Parameter [0] contains the executive flags value. ■ Last Failure Parameter [1] contains the RIP from the bugcheck call stack. ■ Last Failure Parameter [2] contains the first SIP last failure parameter value. ■ Last Failure Parameter [3] contains the second SIP last failure. ■ Last Failure Parameter [4] contains the SIP last failure code value. ■ Last Failure Parameter [5] contains the EXEC$BUGCHECK call last failure code value.
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 ■ Last Failure Parameter [4] contains the SIP last failure code value. ■ Last Failure Parameter [5] contains the EXEC$BUGCHECK call last failure code value.
018000A0	A powerfail interrupt occurred.
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.
018700A0	A processor interrupt was generated with an indication that the (//) RESET button on the controller module was depressed.
018800A0	A processor interrupt was generated with an indication that the program card was removed.
018900A0	A processor interrupt was generated with an indication that the controller inactivity watch dog timer expired.
018C2580	A DRAB_INT interrupt was generated with an indication that a memory system problem occurred.
018D2580	The memory address range for which buffer SYSCOM was linked is not available

Table B–2 Last Failure Codes (Continued)

Code	Description
018E2582	A NMI interrupt was generated with an indication that a memory system problem occurred. ■ Last Failure Parameter [0] contains the memory controller register address which encounterd the error. ■ Last Failure Parameter [1] contains the memory controller's Command Status Register value.
02000100	Initialization code was unable to allocate enough memory to setup the receive data descriptors.
02010100	Initialization code was unable to allocate enough memory to setup the send data descriptors.
02040100	Unable to allocate memory necessary for data buffers.
02050100	Unable to allocate memory for the Free Buffer Array.
02080100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the disk read DWD stack.
02090100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the disk write DWD stack.
020A0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the tape read DWD stack.
020B0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the tape write DWD stack.
020C0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the miscellaneous DWD stack.
02100100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when creating the device services state table.
02170100	Unable to allocate memory for the Free Node Array.
021D0100	Unable to allocate memory for the Free Buffer Array.
021F0100	Unable to allocate memory for WARPs and RMDs.
02210100	Invalid parameters in CACHE$OFFER_META call.
02220100	No buffer found for CACHE$MARK_META_DIRTY call.

Table B–2 Last Failure Codes (Continued)

Code	Description
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.
022C0100	A READ_LONG operation was requested for a Local Buffer Transfer. READ_LONG is not supported for Local Buffer Transfers.
022D0100	A WRITE_LONG operation was requested for a Local Buffer Transfer. WRTE_LONG is not supported for Local Buffer Transfers.
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.
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).
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).
02440100	The logical unit mapping type was detected invalid in va_set_disk_geometry()

Table B–2 Last Failure Codes (Continued)

Code	Description
02530102	An invalid status was returned from CACHE$LOOKUP_LOCK(). ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
02560102	An invalid status was returned from CACHE$LOOKUP_LOCK(). ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
02570102	An invalid status was returned from VA$XFER() during a operation. ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
025A0102	An invalid status was returned from CACHE$LOOKUP_LOCK(). ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
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.
02620102	An invalid status was returned from CACHE$LOOKUP_LOCK(). ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
02690102	An invalid status was returned from CACHE$OFFER_WRITE_DATA(). ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
02790102	An invalid status was returned from VA$XFER() in a complex read operation. ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
027B0102	An invalid status was returned from VA$XFER() in a complex ACCESS operation. ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.

Table B–2 Last Failure Codes (Continued)

Code	Description
027D0100	Unable to allocate memory for a Failover Control Block.
027E0100	Unable to allocate memory for a Failover Control Block.
027F0100	Unable to allocate memory for a Failover Control Block.
02800100	Unable to allocate memory for a Failover Control Block.
02840100	Unable to allocate memory for the XNode Array.
02860100	Unable to allocate memory for the Fault Management Event Information Packet used by the Cache Manager in generating error logs to the host.
02880100	Invalid FOC Message in cmfoc_snd_cmd.
02890100	Invalid FOC Message in cmfoc_rcv_cmd.
028A0100	Invalid return status from DIAG$CACHE_MEMORY_TEST.
028B0100	Invalid return status from DIAG$CACHE_MEMORY_TEST.
028C0100	Invalid error status given to cache_fail.
028E0100	Invalid DCA state detected in init_crashover.
02910100	Invalid metadata combination detected in build_raid_node.
02920100	Unable to handle that many bad dirty pages (exceeded MAX_BAD_DIRTY). Cache memory is bad.
02930100	There was no free or freeable buffer to convert bad metadata or to borrow a buffer during failover of bad dirty.
02940100	A free Device Correlation Array entry could not be found during write-back cache failover.
02950100	Invalid DCA state detected in start_crashover.
02960100	Invalid DCA state detected in start_failover.
02970100	Invalid DCA state detected in init_failover.
02990100	A free RAID Correlation Array entry could not be found during write-back cache failover.
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.
029D0100	Invalid metadata combination detected in build_bad_raid_node.

Table B–2 Last Failure Codes (Continued)

Code	Description
029F0100	The Cache Manager software has insufficient resources to handle a buffer request pending.
02A00100	VA change state is trying to change device affinity and the cache has data for this device.
02A10100	Pubs not one when transportable
02A20100	Pubs not one when transportable
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.
02A40100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating VAXDs.
02A50100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating DILPs.
02A60100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating Change State Work Items.
02A70100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when allocating VA Request Items.
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.
02AA0100	An invalid call was made to CACHE$DEALLOCATE_CLD. Either that device had dirty data or it was bound to a RAIDset.
02AB0100	An invalid call was made to CACHE$DEALLOCATE_SLD. A RAIDset member either had dirty data or write-back already turned on.
02AC0100	An invalid call was made to CACHE$DEALLOCATE_SLD. The RAIDset still has data (strip nodes).
02AD0180	The FX detected a compare error for data that was identical. This error has always previously occurred due to a hardware problem.
02AE0100	The mirrorset member count and individual member states are inconsistent. Discovered during a mirrorset write or erase.

Table B–2 Last Failure Codes (Continued)

Code	Description
02AF0102	An invalid status was returned from VA$XFER() in a write operation. ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
02B10100	A mirrorset read operation was received and the round robin selection algorithm found no normal members in the mirrorset. Internal inconsistency.
02B20102	An invalid status was returned from CACHE$LOCK_READ during a mirror copy operation. ■ Last Failure Parameter[0] contains the DD address. ■ Last Failure Parameter[1] contains the invalid status.
02B30100	CACHE$CHANGE_MIRROR_MODE invoked illegally (cache bad, dirty data still resident in the cache.)
02B52200	Cache A was declared bad during memory diagnostic testing of the metadata while in mirrored mode. A reboot is necessary to recover any dirty data from the mirror.
02B72200	Cache B which contains the mirror for Cache A was declared bad during memory diagnostic testing of the metada while in mirrored mode. A reboot is necessary to recover any dirty data from the primary cache.
02B90100	Invalid code loop count attempting to find the Cache ID Blocks.
02BC0100	A mirrorset read operation was received and the preferred member selection algorithm found no normal members in the mirrorset. Internal inconsistency.
02BD0100	A mirrorset metadata online operation found no normal members in the mirrorset. Internal inconsistency.
02BE0100	No free pages in the other cache. In performing mirror cache failover, a bad page was found and an attempt was made to recover the data from the good copy (primary/mirror), but no free good page was found on the other cache to copy the data to.
02BF0100	Report_error routine encountered an unexpected failure status returned from DIAG$LOCK_AND_TEST_CACHE_B.
02C00100	Copy_buff_on_this routine expected the given page to be marked bad and it wasn't.
02C10100	Copy_buff_on_other routine expected the given page to be marked bad and it wasn't.
02C30100	CACHE$CREATE_MIRROR was invoked by C_SWAP under unexpected conditions (other controller not dead, bad lock state).

Table B–2 Last Failure Codes (Continued)

Code	Description
02C42200	Cache A was declared bad during memory diagnostic testing of the metadata while in mirrored mode. A reboot is necessary to recover any dirty data from the mirror.
02C52200	Cache B which contains the mirror for Cache A was declared bad during memory diagnostic testing of the metadata while in mirrored mode. A reboot is necessary to recover any dirty data from the primary cache.
02C60100	Mirroring transfer found CLD with writeback state OFF.
02C70100	Bad BBR offsets for active shadowset, detected on write.
02C80100	Bad BBR offsets for active shadowset, detected on read.
02C90100	Illegal call made to CACHE$PURGE_META when the storageset wasn't quiesced.
02CA0100	Illegal call made to VA$RAID5_META_READ when another read (of metadata) is already in progress on the same strip.
02CB0000	A restore of the configuration has been done. This cleans up and restarts with the new configuration.
02CC0100	On an attempt, which is not allowed to fail, to allocate a cache node, no freeable cache node was found.
02CE1010	Serial number mismatch was detected during an attempt to restore saved configuration information.
02CF0100	An unsupported message type or terminal request was received by the VA_SAVE_CONFIG virtual terminal code from the CLI.
02D00100	Not all alter_device requests from VA_SAVE_CONFIG completed within the timeout interval.
02D30100	The controller has insufficient memory to allocate enough data structures used to manage metadata operations.
02D50100	No resources are available to handle a new metadata work request.
02D60100	An invalid storage set type was specified for metadata initialization.
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.
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.
02D90100	Bad CLD pointer passed setwb routine.

Table B–2 Last Failure Codes (Continued)

Code	Description
02DA0100	A fatal logic error occurred while trying to restart a stalled data transfer stream.
02DB0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the disk read PCX DWD stack.
02DC0100	A call to EXEC$ALLOCATE_MEM_ZEROED failed to return memory when populating the disk write PCX DWD stack.
02DD0100	The VA state change deadman timer expired, and at least one VSI was still interlocked. ■ Last Failure Parameter [0] contains the nv_index.
02DE0100	An attempt to allocate memory for a null pub failed to get the memory.
02DF0100	License identified in Last Failure Parameter [0] was not forced valid.
02E00180	Mirror functionality is broken.
02E11016	While attempting to restore saved configuration, information for two, unrelated controllers was encountered. The restore code is unable to determine which disk contains the correct information. The PTL information for the two disks is contained in the parameter list. (The Last Failure Parameters 0, 1, and 2 contain the first disk's P, T, and L respectively. Parameters 3, 4, and 5 contain the second disk's P, T, and L respectively.) Remove the disk that contains the incorrect configuration, restart the controller, then enter the SET THIS_CONTROLLER INITIAL_CONFIGURATION command. When the controller restarts, it will load the correct configuration from the disk.
02E20100	An attempt to allocate a va_cs_work item from the S_va_free_cs_work_queue failed.
02E30100	An attempt to allocate a free VAR failed.
02E40100	An attempt to allocate a free VAR failed.
O2E50100	An attempt to allocate a free VAR failed.
02E60100	An attempt to allocate a free VAR failed.
02E70100	An attempt to allocate a free VAR failed.
02E80100	An attempt to allocate a free VAR failed.
02E90100	An attempt to allocate a free VAR failed.
02EA0100	An attempt to allocate a free VAR failed.

Table B–2 Last Failure Codes (Continued)

Code	Description
02EE0102	A CLD is already allocated when it should be free. The Last Failure Parameter 0 contains the requesting entity; parameter 1 contains the CLD index.
02EF0102	A CLD is free when it should be allocated. The Last Failure Parameter 0 contains the requesting entity; parameter 1 contains the CLD index.
02F60103	An invalid modification to the no_interlock VSI flag was attempted. The Last Failure Parameter 0 contains the nv_index of the configuration on which the problem was found. Parameter 1 contains the modification flag. (If the modification flag is 1, then an attempt was made to set the no_interlock flag, which was not clear at the time. If the modification flag is 0, then an attempt was made to clear the no_interlock flag, which was clear (==1) at the time.) Parameter 2 contains the current value of the no_interlock flag.
02F70100	Initialization diagnostics found one or more failed device ports. (The diagnositcs may occasionally fail a good port. Restart the controller to ensure that the device ports were not falsely declared to be failed. If the port is actually failed, the diagnostics contain logic that will halt the controller during restart.)
03010100	Failed request for port-specific scripts memory allocation.
03020101	Invalid SCSI direct-access device opcode in misc command DWD. ■ Last Failure Parameter[0] contains the SCSI command opcode.
03040101	Invalid SCSI CDROM device opcode in misc command DWD. ■ Last Failure Parameter[0] contains the SCSI command opcode.
03060101	Invalid SCSI device type in PUB.
03070101	Invalid CDB Group Code detected during create of misc cmd DWD ■ Last Failure Parameter[0] contains the SCSI device type. ■ Last Failure Parameter[0] contains the SCSI command opcode.
03080101	Invalid SCSI OPTICAL MEMORY device opcode in misc command DWD. ■ Last Failure Parameter[0] contains the SCSI command opcode.
030A0100	Error DWD not found in port in_proc_q.

Table B–2 Last Failure Codes (Continued)

Code	Description
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.
03150100	More DBDs than allowed for in mask.
031E0100	Can’t find in_error dwd on in-process queue.
031F0100	Either DWD_ptr is null or bad value in dsps.
03280100	SCSI CDB contains an invalid group code for a transfer command.
03290100	The required Event Information Packet (EIP) or device work descriptor (DWD) were not supplied to the Device Services error logging code.
032B0100	A Device Work Descriptor (DWD) was supplied with a NULL Physical Unit Block (PUB) pointer.
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.

Table B–2 Last Failure Codes (Continued)

Code	Description
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 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.
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 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.

Table B–2 Last Failure Codes (Continued)

Code	Description
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.
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.

Table B–2 Last Failure Codes (Continued)

Code	Description
03380188	A device port's DSTAT register contains multiple asserted bits, or an invalidly 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.
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 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.
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.

Table B–2 Last Failure Codes (Continued)

Code	Description
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.
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.
03410101	Invalid SCSI device type in PUB. ■ Last Failure Parameter[0] contains the PUB SCSI device type.

Table B–2 Last Failure Codes (Continued)

Code	Description
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.
03440188	A Host Parity Error was detected by a 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 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.
03470100	Insufficient memory available for target block allocation.
03480100	Insufficient memory available for device port info block allocation.
03490100	Insufficient memory available for autoconfig buffer allocation.
034A0100	Insufficient memory available for PUB allocation.

Table B–2 Last Failure Codes (Continued)

Code	Description
034B0100	Insufficient memory available for DS init buffer allocation.
034C0100	Insufficient memory available for static structure allocation.
034D0100	DS init DWDs exhausted.
034E2080	Diagnostics report all device ports are broken.
03500100	Insufficient memory available for command disk allocation.
03520100	A failure resulted when an attempt was made to allocate a DWD for use by DS CDI.
035A0100	Invalid SCSI message byte passed to DS.
035B0100	Insufficient DWD resources available for SCSI message passthrough.
03640100	Processing run_switch disabled for LOGDISK associated with the other controller.
03650100	Processing pub unblock for LOGDISK associated with the other controller.
03660100	No memory available to allocate pub to tell the other controller of reset to one if its LUNs
03670100	No memory available to allocate pub to tell the other controller of a BDR to one if its LUNs
04010101	The requester id component of the instance code passed to FM$REPORT_EVENT is larger than the maximum allowed for this environment. ■ Last Failure Parameter[0] contains the instance code value.
04020102	The requester's error table index passed to FM$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.
04030102	The USB index supplied in the Event Information Packet (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.

Table B–2 Last Failure Codes (Continued)

Code	Description
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 Event Information Packet (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.
04050100	The Fault Manager could not allocate memory for its Event Information Packet (EIP) buffers.
040A0100	The caller of FM$CANCEL_SCSI_DE_NOTIFICATION passed an address of a deferred error notification routine which doesn't match the address of any routines for which deferred error notification is enabled.
040E0100	FM$ENABLE_DE_NOTIFICATION was called to enable deferred error notification but the specified routine was already enabled to receive deferred error notification.
040F0102	The Event Information Packet (EIP)->generic.mscp1.flgs field of the EIP passed to FM$REPORT_EVENT contains an invalid flag. ■ Last Failure Parameter[0] contains the instance code value. ■ Last Failure Parameter[1] contains the value supplied in the Event Information Packet (EIP)->generic.mscp1.flgs field.
04100101	Unexpected template type found during fmu_display_errlog processing. ■ Last Failure Parameter[0] contains the unexpected template value.
04110101	Unexpected instance code found during fmu_memerr_report processing. ■ Last Failure Parameter[0] contains the unexpected instance code value.
04120101	CLIB$SDD_FAO call failed. ■ Last Failure Parameter[0] contains the failure status code value.
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 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.

Table B–2 Last Failure Codes (Continued)

Code	Description
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 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.
05010100	In recursive_nonconflict could not get enough memory for scanning the keyword tables for configuration name conflicts.
06010100	The DUART was unable to allocate enough memory to establish a connection to the CLI.
06020100	A port other than terminal port A was referred to by a set terminal characteristics command. This is illegal.
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.
06040100	Attempted to detach unattached maintenance terminal.
06050100	Attempted output to unattached maintenance terminal.
06060100	Attempted input from output only maintenance terminal service.
06070100	The DUART was unable to allocate enough memory for its input buffers
06080000	Controller was forced to restart due to entry of a CNTRL-K character on the maintenance terminal.
07010100	All available slots in the FOC notify table are filled.
07020100	FOC$CANCEL_NOTIFY() was called to disable notification for a rtn that did not have notification enabled.
07030100	Unable to start the Failover Control Timer before main loop.
07040100	Unable to restart the Failover Control Timer.
07050100	Unable to allocate flush buffer.
07060100	Unable to allocate active receive fcb.
07070100	The other controller killed this, but could not assert the kill line because nindy on or in debug. So it killed this now.
07080000	The other controller crashed, so this one must crash too.

Table B–2 Last Failure Codes (Continued)

Code	Description
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.
08020100	No memory could be allocated for a NVFOC information packet.
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.
08040101	Unknown work value received by the S_nvfoc_bque. ■ Last Failure Parameter[0] contains the unknown work value.
08060100	A write command was received when the NV memory was not locked.
08070100	A write to NV memory was received while not locked.
08080000	The other controller requested this controller to restart.
08090010	The other controller requested this controller to shutdown.
080A0000	The other controller requested this controller to selftest.
080B0100	Could not get enough memory to build a FCB to send to the remote routines on the other controller.
080C0100	Could not get enough memory for FCBs to receive information from the other controller.
080D0100	Could not get enough memory to build a FCB to reply to a request from the other controller.
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.
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.
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.
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.
08140100	Could not allocate memory to build a workblock to queue to the NVFOC thread.

Table B–2 Last Failure Codes (Continued)

Code	Description
08160100	A request to clear the remote configuration was received but the memory was not locked.
08170100	A request to read the next configuration was received but the memory was not locked.
08180100	Could not get enough memory for FLS FCBs to receive information from the other controller.
08190100	An unlock command was received when the NV memory was not locked.
081A0100	Unable to allocate memory for remote work.
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.
081C0101	Bad member management work received. ■ Last Failure Parameter[0] contains the bad member management value that was detected.
081D0000	In order to go into mirrored cache mode, the controllers must be restarted.
081E0000	In order to go into nonmirrored cache mode, the controllers must be restarted.
081F0000	An FLM$INSUFFICIENT_RESOURCES error was returned from a FLM lock or unlock call.
08200000	Expected restart so the write_instance may recover from a configuration mismatch.
08210100	Unable to allocate memory to setup NVFOC lock/unlock notification routines.
09010100	Unable to acquire memory to initialize the FLM structures.
09640101	Work that was not FLM work was found on the FLM queue. Bad format detected or the formatted string overflows the output buffer. Last Failure Parameter [0] contains the work found.
09650101	Work that was not FLM work was found on the FLM queue. Last Failure Parameter [0] contains the structure found.
09670101	Local FLM detected an invalid facility to act upon. Last Failure Parameter [0] contains the faciltiy found.
09680101	Remote FLM detected an error and requested the local controller to restart. Last Failure Parameter [0] contains the reason for the request.

Table B–2 Last Failure Codes (Continued)

Code	Description
09C80101	Remote FLM detected an error and requested an invalid facility to act upon. Last Failure Parameter [0] contains the facility found.
09C90101	Remote FLM detected an invalid work type. Last Failure Parameter [0] contains the work type found.
09CA0101	Remote FLM detected an invalid work type. Last Failure Parameter [0] contains the work type found.
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 the controller's FLM revision. Last Failure Parameter [1] contains the other controller's FLM revision.
0A010100	CACHE$FIND_LOG_BUFFERS returned continuation handle>0.
0A020100	ILF$CACHE_READY unable to allocate necessary DWDs.
0A030100	ILF$CACHE_READY buffers_obtained > non-zero stack entry count.
0A040100	ILF$CACHE_READY DWD overrun.
0A050100	ILF$CACHE_READY DWD underrun.
0A080100	Not processing a bugcheck.
0A090100	No active DWD.
0A0A0100	Current entry pointer is not properly aligned.
0A0B0100	Next entry pointer is not properly aligned.
0A0C0100	Next entry was partially loaded.
0A0D0100	Another free DWD is not queued as expected.
0A0E0100	Active DWD is not a DISK WRITE DWD as expected.
0A0F0100	New active DWD is not a DISK WRITE DWD as expected.
0A100100	Data buffer pointer is not properly aligned.
0A110100	DWD count was wrong and a free DWD actually exists.
0A120100	Data buffer pointer is not properly aligned.
0A130100	Data buffer pointer is not properly aligned.
0A140100	New entry pointer is not properly aligned.

Table B–2 Last Failure Codes (Continued)

Code	Description
0A150100	New entry record type is out of range.
0A160102	ilf_issue_log_write marker entry page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A170102	ilf_get_new_dwd first page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A180102	ilf_distribute_cache_DWDs first page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A190102	ilf_depopulate_DWD_to_cache first page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A1A0102	ilf_io_success page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A1B0102	ilf_io_success page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A1C0102	ILF$LOG_ENTRY page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A1D0102	ILF$LOG_ENTRY page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A1E0102	ILF$LOG_ENTRY page guard check failed. Last Failure Parameter 0 contains the DWD address value; parameter 1 contains the buffer address.
0A1F0100	ilf_rebind_cache_buffs_to_DWDs found duplicate buffer for current DWD.
0A200101	Unknown bugcheck code passed to ilf_cache_interface_crash. Last Failure Parameter 0 contains the unknown bugcheck code value.
0A210100	ilf_rebind_cache_buffs_to_DWDs found buffer type not IDX_ILF.
0A220100	ilf_rebind_cache_buffs_to_DWDs found buffer DBD index too big.
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.
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.
20030100	The type of work received on the CLI work queue wasn't of type CLI.

Table B–2 Last Failure Codes (Continued)

Code	Description
20060100	A work item of an unknown type was placed on the CLI’s SCSI Virtual Terminal thread’s work queue by the CLI.
20080000	This controller requested this controller to restart.
20090010	This controller requested this controller to shutdown.
200A0000	This controller requested this controller to selftest.
200B0100	Could not get enough memory for FCBs to receive information from the other controller.
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.
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.
200F0101	A config_info node was discovered with an unrecognized structure type. ■ Last Failure Parameter[0] contains the structure type number that was unrecognized.
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.
20110100	An attempt to allocate memory so the CLI prompt messages could be deleted failed.
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.
20130101	While traversing the structure of a unit, the device was of an unrecognized type. ■ Last Failure Parameter[0] contains the SCSI device type that was unrecognized.
20150100	On failover, both controllers must be restarted for failover to take effect. This is how this controller is restarted in COPY=OTHER.

Table B–2 Last Failure Codes (Continued)

Code	Description
20160000	In order to go into mirrored cache mode, the controllers must be restarted.
20160100	Unable to allocate resources needed for the CLI local program.
20170000	In order to go into unmirrored cache mode, the controllers must be restarted.
20180010	User requested this controller's parameters to be set to initial configuration state.
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.
201A0100	An attempt to allocate memory so a CLI prompt message could be reformatted failed.
201B0100	Insufficient resources to get memory to lock CLI.
201C0100	Insufficient resources to get memory to unlock CLI.
20640000	Nindy was turned on.
20650000	Nindy was turned off.
20692010	To enter dual-redundant mode, both controllers must be of the same type.
206A0000	Controller restart forced by DEBUG CRASH REBOOT command.
206B0100	Controller restart forced by DEBUG CRASH NOREBOOT command.
206C0020	Controller was forced to restrart in order for new controller code image to take effect.
206D0000	Controller code load was not completed because the controller could not rundown all units.
43000100	Encountered an unexpected structure type on S_shis_ctl.scsi_q.
43030100	Unable to allocate the necessary number of large Sense Data buckets in HPP_init().
43100100	Encountered a NULL completion routine pointer in a DD.
43130100	Could not allocate a large sense bucket.
43160100	A sense data bucket of unknown type (neither LARGE or SMALL) was passed to deallocate_SDB().
43170100	Call to VA$ENABLE_NOTIFICATION() failed due to INSUFFICIENT_RESOURCES.
43190100	Unable to allocate necessary memory in HPP_int().
431A0100	Unable to allocate necessary timer memory in HPP_int().

Table B–2 Last Failure Codes (Continued)

Code	Description
43210101	HPP detected unknown error indicated by HPT. Last Failure Parameter [0] contains the error value.
44000104	Interrupt from SCSI host port chip indicated condition that is not handled (unexpected). ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSTAT Register. ■ Last Failure Parameter [2] contains SIEN/SIST Registers. ■ Last Failure Parameter [3] contains Chip Register Base.
44010104	Interrupt from SCSI host port chip indicated ATN condition at unexpected script location. ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSTAT Register. ■ Last Failure Parameter [2] contains Script PC (DSP). ■ Last Failure Parameter [3] contains Chip Register Base.
44020104	Interrupt from SCSI host port chip indicated interrupt with an unexpected reason (pass value) ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSTAT Register. ■ Last Failure Parameter [2] contains Pass Value. ■ Last Failure Parameter [3] contains Chip Register Base.
44030104	Interrupt from SCSI host port chip indicated interrupt with an unexpected reason but invalid conditions ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSP Register. ■ Last Failure Parameter [2] contains Code (Condition). ■ Last Failure Parameter [3] contains Chip Register Base.

Table B–2 Last Failure Codes (Continued)

Code	Description
44040104	Interrupt from SCSI host port chip indicated interrupt with an unexpected reason but invalid conditions ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSTAT Register. ■ Last Failure Parameter [2] contains Script PC (DSP). ■ Last Failure Parameter [3] contains Chip Register Base.
44050104	Interrupt from SCSI host port chip indicated STO condition at unexpected script location. ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSTAT Register. ■ Last Failure Parameter [2] contains Script PC (DSP). ■ Last Failure Parameter [3] contains Chip Register Base.
44060104	Interrupt from SCSI host port chip indicated HTH condition at unexpected script location. ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSTAT Register. ■ Last Failure Parameter [2] contains Script PC (DSP). ■ Last Failure Parameter [3] contains Chip Register Base.
44070100	Unable to locate the IDENTIFY msg in HTB.
44090100	Encountered an unknown MESSAGE OUT message.
440A0104	Interrupt from SCSI host port chip indicated parity error at unexpected script location. ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSTAT Register. ■ Last Failure Parameter [2] contains Script PC (DSP). ■ Last Failure Parameter [3] contains Chip Register Base.
440B0100	Encountered unknown structure on port queue in HPT$ABORT_HTB.
440C0100	No available Abort Records to process abort request.

Table B–2 Last Failure Codes (Continued)

Code	Description
440D0100	No available FOR Records to process Failover request.
440E0100	Unable to allocate the necessary number of HTBS in hpt_init().
440F0104	Interrupt from SCSI host port chip indicated interrupt with an unexpected reason but invalid conditions. ■ Last Failure Parameter [0] contains ISTAT Register. ■ Last Failure Parameter [1] contains DSP Register. ■ Last Failure Parameter [2] contains Code (Condition). ■ Last Failure Parameter [3] contains Chip Register Base.
44100100	Unable to allocate the necessary memory for scripts in hpt_init().
44110100	Unable to allocate the necessary memory for abort records in hpt_init().
44120100	Unable to allocate the necessary memory for tables in hpt_init().
64000100	Insufficient buffer memory to allocate data structures needed to propagate SCSI Mode Select changes to other controller.
64010100	During an initialization of LUN specific mode pages, an unexpected device type was encountered.
80010100	An HTB was not available to issue an I/O when it should have been.
80030100	DILX tried to release a facility that wasn't reserved by DILX.
80040100	DILX tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources.
80050100	DILX tried to change the usb unit state from MAINTENANCE_MODE to NORMAL but DILX never received notification of a successful state change.
80060100	DILX tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was not successful.
80070100	DILX aborted all cmds via va$d_abort() but the HTBS haven't been returned.
80090100	DILX received an end msg which corresponds to an op code not supported by DILX.
800A0100	DILX was not able to restart his timer.
800B0100	DILX tried to issue an I/O for an opcode not supported.
800C0100	DILX tried to issue a oneshot I/O for an opcode not supported.

Table B–2 Last Failure Codes (Continued)

Code	Description
800D0100	A DILX device control block contains an unsupported unit_state.
800F0100	A DILX cmd completed with a sense key that DILX does not support.
80100100	DILX could not compare buffers because no memory was available from EXEC$ALLOCATE_MEM_ZEROED.
80110100	While DILX was deallocating his deferred error buffers, at least one could not be found.
80120100	DILX expected an Event Information Packet (EIP) to be on the receive EIP queue but no EIPs were there.
80130100	DILX was asked to fill a data buffer with an unsupported data pattern.
80140100	DILX could not process an unsupported answer in dx$reuse_params().
80150100	A deferred error was received with an unsupported template.
83020100	An unsupported message type or terminal request was received by the CONFIG virtual terminal code from the CLI.
83030100	Not all alter_device requests from the CONFIG utility completed within the timeout interval.
83050100	An unsupported message type or terminal request was received by the CFMENU utility code from the CLI.
83060100	Not all alter_device requests from the CFMENU utility completed within the timeout interval.
84010100	An unsupported message type or terminal request was received by the CLONE virtual terminal code from the CLI.
85010100	HSUTIL tried to release a facility that wasn't reserved by HSUTIL.
85020100	HSUTIL tried to change the unit state from MAINTENANCE_MODE to NORMAL but was rejected because of insufficient resources.
85030100	HSUTIL tried to change the usb unit state from MAINTENANCE_MODE to NORMAL but HSUTIL never received notification of a successfull state change.
85040100	HSUTIL tried to switch the unit state from MAINTENANCE_MODE to NORMAL but was not successful.
86000020	Controller was forced to restart in order for new code load or patch to take effect.

Table B–2 Last Failure Codes (Continued)

Code	Description
86000020	Controller was forced to restart due to execution of the CRASH utility.
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.
8A020080	A memory error was encountered on the new cache module. The controller has been automatically restarted to clear the error.

Repair Action Codes

This table contains the repair action codes assigned to each significant event in the system.

Table B–3 Repair Action Codes

Code	Description
00	No action necessary.
01	An unrecoverable hardware detected fault occurred or an unrecoverable firmware inconsistency was detected. Proceed with controller support avenues. Contact Digital Services.
03	Follow the recommended repair action contained as indicated in the Last Failure Code.
04	Two possible problem sources are indicated: ■ 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. ■ One of the shelf blowers has failed. Follow repair action 06.
05	Four possible problem sources are indicated: ■ Total power supply failure on a shelf. Follow repair action 09. ■ A device inserted into a shelf that has a broken internal SBB connector. Follow repair action 0A. ■ A standalone device is connected to the controller with an incorrect cable. Follow repair action 08. ■ A controller hardware failure. Follow repair action 20.
06	Determine which blower has failed and replace it.
07	Replace power supply.
08	Replace the cable. Refer to the specific device documentation.
09	Determine power failure cause.
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.

Table B–3 Repair Action Codes (Continued)

Code	Description
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 that 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: ■ A controller hardware failure. ■ A controller backplane failure. First, follow repair action 20 for the “Killed” controller. If the problem persists follow repair action 20 for the “Surviving” controller. If the problem still persists replace the controller backplane.
0D	The Environmental Monitor Unit has detected an elevated temperature condition. Check the shelf and its components for the cause of the fault.
0E	The Environmental Monitor Unit 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 Environmental Monitor Unit is now fixed. This event report is notification that the repair was successful.
10	Restore on-disk configuration information to original state.
20	Replace the controller module.
22	Replace the indicated cache module or the appropriate memory SIMMs on the indicated cache module.
23	Replace the indicated write cache battery. CAUTION: BATTERY REPLACEMENT MAY CAUSE INJURY.

Table B–3 Repair Action Codes (Continued)

Code	Description
24	Check for the following invalid write cache configurations: ■ If the wrong write cache module is installed, replace with the matching module or clear the invalid cache error via the CLI. ■ If the write cache module is missing, reseat cache if it is actually present, or add the missing cache module, or clear the invalid cache error via the CLI. ■ If in a dual-redundant configuration and one of the write cache modules is missing, match write cache boards with both controllers. ■ If in a dual-redundant configuration and both caches are not of the same type (both write cache), replace a cache module to assure both are compatible. ■ If in 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 action(s) contained therein.
26	The Master DRAB detected a Cache Timeout condition. The cache regions in effect are identified in the Master DRAB RSR register: 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, and 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. 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.

Table B–3 Repair Action Codes (Continued)

Code	Description
29	A Multiple Bit ECC error was detected by the CACHEA0 or CACHEA1 DRAB. 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. 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.
2B	The Master DRAB detected an Ibus to Nbus Timeout 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 Master DRAB CSR register bits 10 through 12 contains the value 1 and WDR1 register bit 26 is clear or Master DRAB CSR register bits 10 through 12 contains the value 2 and WDR1 register bit 27 is clear or Master DRAB CSR register bits 10 through 12 contains the value 3 and WDR1 register bit 28 is clear or Master DRAB CSR register bits 10 through 12 contains the value 4 and WDR1 register bit 29 is clear or Master DRAB CSR register bits 10 through 12 contains the value 5 and WDR1 register bit 30 is clear or Master DRAB CSR register bits 10 through 12 contains the value 6 and WDR1 register bit 31 is clear, a firmware fault is indicated; follow repair action 01. Otherwise, follow repair action 36.
2C	The Master DRAB detected a Nonexistent Memory Error condition. 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.

Table B–3 Repair Action Codes (Continued)

Code	Description
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. 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. 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.

Table B–3 Repair Action Codes (Continued)

Code	Description
30	The CACHEA0 or CACHEA1 DRAB detected an Address Parity Error or a Write Data Parity Error condition. 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 set, 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. 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.
32	The Master DRAB detected an Ibus Parity Error condition. 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 nonzero value, a firmware fault is indicated; follow repair action 01. Otherwise, follow repair action 36.

Table B–3 Repair Action Codes (Continued)

Code	Description
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, a firmware fault is indicated; follow repair action 01. Otherwise, follow repair action 36.
35	If bits 20 through 23 of the WDR1 register contain a nonzero value, a firmware fault is indicated; follow repair action 01. Otherwise, follow repair action 36.
36	Unfortunately, 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 DRAB 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.
38	Replace the indicated cache memory SIMM.
40	If the Sense Data FRU field is non-zero, follow repair action 41. Otherwise, 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.
50	The RAIDset is inoperative for one or more of the following reasons: ■ More than one member malfunctioned. Perform repair action 55. ■ More than one member is missing. Perform repair action 58. ■ Before reconstruction of a previously replaced member completes another member becomes missing or malfunctions. Perform repair action 59. ■ The members have been moved around and the consistency checks show mismatched members. Perform repair action 58.

Table B–3 Repair Action Codes (Continued)

Code	Description
51	The mirrorset is inoperative for one or more of the following reasons: ■ The last NORMAL member has malfunctioned. Perform repair actions 55 and 59. ■ The last NORMAL member is missing. Perform repair action 58. ■ The members have been moved around and the consistency checks show mismatched members. Perform repair action 58.
52	The indicated Storageset member was removed for one of the following reasons: ■ The member malfunctioned. Perform repair action 56. ■ By operator command. Perform repair action 57.
53	The storageset may be in a state that prevents the adding of a replacement member, check the state of the storageset and its associated unit and resolve the problems found before adding the replacement member.
54	The device may be in a state that prevents adding it as a replacement member or may not be large enough for the storageset. Use another device for the ADD action and perform repair action 57 for the device that failed to be added.
55	Perform the repair actions indicated in any and all event reports found for the devices that are members of the storageset.
56	Perform the repair actions indicated in any and all event reports found for the member device that was removed from the storageset. Then perform repair action 57.
57	Delete the device from the failedset and redeploy, perhaps by adding it to the spareset so it will be available to be used to replace another failing device.
58	Install the physical devices that are members of the storageset in the proper port, target, and LUN locations.
59	Delete the storageset, recreate it with the appropriate ADD, INITIALIZE, and ADD UNIT commands and reload its contents from backup storage.
5A	Restore the mirrorset data from backup storage.
69	An unrecoverable fualt occurred at the host port. There may be more than one entity attempting to use the same SCSI ID number, or some other bus-configuration error may have occurred, such as improper termination. If you don’t find any SCSI host bus configuration problems, follow repair action 01.

Table B–3 Repair Action Codes (Continued)

Code	Description
80	An EMU fault has occurred.
81	The EMU reported terminator power out of range. Replace the indicated I/O modules.
83	An EMU has become unavailable. (If the EMU and its enclosure have been removed from the subsystem, no action is required. If the enclosure has lost power, restore power to the enclosure. If the EMU-to-EMU cable has been disconnected or is broken, reconnect or replace the cable. If the EMU has failed, replace the EMU.)

Component Identifier Codes

This table lists the component identifier codes.

Table B–4 Component Identifier Codes

Code	Description
01	Executive Services
02	Value Added Services
03	Device Services
04	Fault Manager
05	Common Library Routines
06	Dual Universal Asynchronous Receiver/Transmitter Services
07	Failover Control
08	Nonvolatile Parameter Memory Failover Control
09	Facility Lock Manager
0A	Integrated Logging Facility
20	Command Line Interpreter
43	Host Port Protocol Layer
44	Host Port Transport Layer
64	SCSI Host Value Added Services
80	Disk Inline Exercise (DILX)
82	Subsystem Built-In Self Tests (BIST)
83	Device Configuration Utilities (CONFIG/CFMENU)
84	Clone Unit Utility (CLONE)
85	Format and Device Code Load Utility (HSUTIL)
86	Code Load/Code Patch Utility (CLCP)
8A	Field Replacement Utility (FRUTIL)

Event Threshold Codes

This table lists the classifications for event notification and recovery threshold values.

Table B–5 Event Notification/Recovery Threshold Classifications

Threshold Value	Classification	Description
01	IMMEDIATE	Failure or potential failure of a component critical to proper controller operation is indicated; immediate attention is required.
02	HARD	Failure of a component that affects controller performance or precludes access to a device connected to the controller is indicated.
0A	SOFT	An unexpected condition detected by a controller firmware component (e.g., protocol violations, host buffer access errors, internal inconsistencies, uninterpreted device errors, etc.) or an intentional restart or shutdown of controller operation is indicated.
64	INFORMATIO NAL	An event having little or no effect on proper controller or device operation is indicated.

ASC/ASCQ Codes

This table lists SCSI ASC and ASCQ codes.

Table B–6 ASC and ASCQ Codes

ASC Code	ASCQ Code	Description
3F	85	Test Unit Ready or Read Capacity Command failed
3F	87	Drive failed by a Host Mode Select command.
3F	88	Drive failed due to a deferred error reported by drive.
3F	90	Unrecovered Read/Write error.
3F	C0	No response from one or more drives.
3F	C2	NV memory and drive metadata indicate conflicting drive configurations.
3F	D2	Synchronous Transfer Value differences between drives.
80	00	Forced error on Read
82	01	No Command control structures available.
84	04	Command failed - SCSI ID verification failed.
85	05	Data returned from drive is invalid.
89	00	Request Sense command to drive failed.
8A	00	Illegal command for pass through mode.
8C	04	Data transfer request error.
8F	00	Premature completion of a drive command.
93	00	Drive returned vendor unique sense data.
A0	00	Last failure event report.
A0	01	Nonvolatile parameter memory component event report.
A0	02	Backup battery failure event report.
A0	03	Subsystem built-in self test failure event report.
A0	04	Memory system failure event report.
A0	05	Failover event report.
A0	07	RAID membership event report.

Table B–6 ASC and ASCQ Codes (Continued)

ASC Code	ASCQ Code	Description
A0	08	Multibus failover event
A0	09	Multibus failover event
A1	00	Shelf OK is not properly asserted.
A1	01	Unable to clear SWAP interrupt. Interrupt disabled.
A1	02	Swap interrupt re-enabled.
A1	03	Asynchronous SWAP detected.
A1	04	Controller shelf OK is not properly asserted.
A1	0A	EMU fault: Power Supplies not OK.
A1	0B	EMU fault: Fans not OK.
A1	0C	EMU fault: Temperature not OK.
A1	0D	EMU fault: External Air Sense not OK.
A1	10	Power supply fault is now fixed.
A1	11	Fans fault is now fixed.
A1	12	Temperature fault is now fixed.
A1	13	External Air Sense fault is now fixed.
A1	14	Controller vendor specific
A1	15	Controller vendor specific
B0	00	Command timeout.
B0	01	Watchdog timer timeout.
D0	01	Disconnect timeout.
D0	02	Chip command timeout.
D0	03	Byte transfer timeout.
D1	00	Bus errors.
D1	02	Unexpected bus phase.
D1	03	Disconnect expected.
D1	04	ID Message not sent.

Table B–6 ASC and ASCQ Codes (Continued)

ASC Code	ASCQ Code	Description
D1	05	Synchronous negotiation error.
D1	07	Unexpected disconnect.
D1	08	Unexpected message.
D1	09	Unexpected tag message.
D1	0A	Channel busy.
D1	0B	Device initialization failure. Device sense data available.
D2	00	Miscellaneous SCSI driver error.
D2	03	Device services had to reset the bus.
D3	00	Drive SCSI chip reported gross error.
D4	00	Non-SCSI bus parity error.
D5	02	Message Reject received on a valid message.
D7	00	Source driver programming error.
E0	03	Fault Manager detected an unknown error code.
E0	06	Maximum number of errors for this I/O exceeded.
E0	07	Drive reported recovered error without transferring all data.

Templates

Figure B–1 Passthrough Device Reset Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Valid	Error Code						
1	Segment							
2	FM	EOM	ILI	Rsvd	Sense Key			
3-6	Information							
7	Additional Sense Length							
8-11	Instance Code							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Field Replaceable Unit Code							
15	SKSV	Sense Key Specific						
16	Sense Key Specific							
17	Sense Key Specific							

CXO-5093A-MC

Figure B–2 Controller Level Sense Data Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32-35	Instance Code							
36	Template							
37	Rsvd	Rsvd	Rsvd	Rsvd	Rsvd	Rsvd	Rsvd	HCE
38–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74-75	Reserved							
76	LUN Status							
77–159	Template Dependent Information							

CXO-4656B-MC

Figure B–3 Device Level Sense Data Format

off \ bit	7	6	5	4	3	2	1	0
0	Valid	Error Code						
1	Segment							
2	FM	EOM	ILI	Rsvd	Sense Key			
3-6	Information							
7	Additional Sense Length							
8-11	Command Specific Information							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Field Replaceable Unit Code							
15	SKSV							
16	Sense Key Specific							
17								
18–19	Reserved							
20	Total Number of Errors							
21	Total Retry Count							
22	Most Recent ASC							
23	Most Recent ASCQ							
24	Least Recent ASC							
25	Least Recent ASCQ							
26	Port							
27	Target							
28	Logical Unit Number							
29–31	Reserved							
32–35	Instance Code							
36	Template							
37	Rsvd	Rsvd	Rsvd	Rsvd	Rsvd	Rsvd	Rsvd	HCE
38	Reserved							
39	Command Opcode							
40	DSSD	IDSD	FBW	MSBD	UWEUO	BUFMODE		
41	Operation Code							

off \ bit	7	6	5	4	3	2	1	0
42	LUN			Reserved				
43–46	Logical Block Address							
47	Reserved							
48–49	Transfer, Parameter, or Allocation Length							
50	Control							
51	Host ID							
52–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74–75	Reserved							
76	LUN Status							
77-78	Reserved							
79-82	Device Firmware Revision Level							
83–98	Device Product ID							
99–100	Reserved							
101	Device Type							
102–103	Reserved							
104	Valid	Error Code						
105	Segment							
106	FM	EOM	ILI	Rsvd	Sense Key			
107–110	Information							
111	Additional Sense Length							
112–115	Command Specific Information							
116	Additional Sense Code (ASC)							
117	Additional Sense Code Qualifier (ASCQ)							
118	Field Replaceable Unit Code							
119	SKSV							
120	Sense Key Specific							
121								
132–159	Reserved							

CXO-4657B-MC

Figure B–4 Template 01 - Last Failure Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32-35	Instance Code							
36	Template							
37	Template Flags							
38–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74–75	Reserved							
76	LUN Status							
77–103	Reserved							
104-107	Last Failure Code							
108–111	Last Failure Parameter(0)							
112–115	Last Failure Parameter(1)							
116–119	Last Failure Parameter(2)							
120–123	Last Failure Parameter(3)							
124–127	Last Failure Parameter(4)							
128–131	Last Failure Parameter(5)							
132–135	Last Failure Parameter(6)							
136–139	Last Failure Parameter(7)							
140-159	Reserved							

CXO-4660B-MC

Figure B–5 Template 04 - Multibus -Failover Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–26	Reserved							
27	Failed Controller Target Number							
28–31	Affected LUNs							
32–35	Instance Code							
36	Template							
37	Template Flags							
38–53	Other Controller Board Serial Number							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74-75	Reserved							
76	LUN Status							
77–159	Reserved							

CXO-5314A-MC

Figure B–6 Template 05 - Failover Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3–6	Unused							
7	Additional Sense Length							
8–11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32–35	Instance Code							
36	Template							
37	Template Flags							
38–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74–75	Reserved							
76	LUN Status							
77-103	Reserved							
104–107	Last Failure Code							
108–111	Last Failure Parameter(0)							
112–115	Last Failure Parameter(1)							
116–119	Last Failure Parameter(2)							
120–123	Last Failure Parameter(3)							
124–127	Last Failure Parameter(4)							
128–131	Last Failure Parameter(5)							
132–135	Last Failure Parameter(6)							
136–139	Last Failure Parameter(7)							
140–159	Reserved							

CXO-4661B-MC

Figure B–7 Template 11 - Nonvolatile Parameter Memory Component Event Sense Data Response

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32-35	Instance Code							
36	Template							
37	Template Flags							
38–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74–75	Reserved							
76	LUN Status							
77-103	Reserved							
104–107	Memory Address							
108–111	Byte Count							
112–114	Number of Times Written							
115	Undefined							
116–159	Reserved							

CXO-4663B-MC

Figure B–8 Template 12 - Backup Battery Failure Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32-35	Instance Code							
36	Template							
37	Template Flags							
38–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74-75	Reserved							
76	LUN Status							
77–103	Reserved							
104–107	Memory Address							
108–159	Reserved							

CXO-4664B-MC

Figure B–9 Template 13 - Subsystem Built-In Self Test Failure Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32-35	Instance Code							
36	Template							
37	Template Flags							
38–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74–75	Reserved							
76	LUN Status							
77-103	Reserved							
104–105	Undefined							
106	Header Type							
107	Header Flags							
108	TE							
109	Test Number							
110	Test Command							
111	Test Flags							
112–113	Error Code							
114–115	Return Code							
116–119	Address of Error							
120–123	Expected Error Data							
124–127	Actual Error Data							
128–131	Extra Status 1							
132–135	Extra Status 2							
136–139	Extra Status 3							
140-159	Reserved							

CXO-4665B-MC

Figure B–10 Template 14 - Memory System Failure Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32-35	Instance Code							
36	Template							
37	Template Flags							
38–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74–75	Reserved							
76	LUN Status							
77-103	Reserved							
104–107	Memory Address							
108–111	Byte Count							
112–115	DSR							
116–119	CSR							
120–123	DCSR							
124–127	DER							
128–131	EAR							
132–135	EDR							
136–139	ERR							
140-143	RSR							
144–147	RDR0							
148–151	RDR1							
152–155	WDR0							
156–159	WDR1							

CXO-4666B-MC

Figure B–11 Template 41 - Device Services Non-Transfer Error Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0	Unusd	Error Code						
1	Unused							
2	Unused				Sense Key			
3-6	Unused							
7	Additional Sense Length							
8-11	Unused							
12	Additional Sense Code (ASC)							
13	Additional Sense Code Qualifier (ASCQ)							
14	Unused							
15–17	Unused							
18–31	Reserved							
32-35	Instance Code							
36	Template							
37	Template Flags							
38–53	Reserved							
54–69	Controller Board Serial Number							
70-73	Controller Firmware Revision Level							
74-75	Reserved							
76	LUN Status							
77–103	Reserved							
104	Associated Port							
105	Associated Target							
106	Associated Additional Sense Code							
107	Associated Additional Sense Code Qualifier							
108–159	Reserved							

CXO-4667B-MC

Figure B–12 Template 51 - Disk Transfer Error Event Sense Data Response Format

off \ bit	7	6	5	4	3	2	1	0
0–17	Standard Sense Data							
18–19	Reserved							
20	Total Number of Errors							
21	Total Retry Count							
22–25	ASC/ASCQ Stack							
26–28	Device Locator							
29–31	Reserved							
32–35	Instance Code							
36	Template							
37	Template Flags							
38	Reserved							
39	Command Opcode							
40	Sense Data Qualifier							
41–50	Original CDB							
51	Host ID							
52–53	Reserved							
54–69	Controller Board Serial Number							
70–73	Controller Firmware Revision Level							
74–75	Reserved							
76	LUN Status							
77–78	Reserved							
79-82	Device Firmware Revision Level							
83–98	Device Product ID							
99–100	Reserved							
101	Device Type							
102–103	Reserved							
104–121	Device Sense Data							
122–159	Reserved							

CXO-4668B-MC

APPENDIX C

Warranty Terms and Conditions

This appendix contains the warranty terms and conditions for storage products.

DIGITAL EQUIPMENT CORPORATION
WARRANTY TERMS AND CONDITIONS SUMMARY

WARRANTED PRODUCTS This appendix contains warranty terms and conditions for the Products specified in the Warranty Attributes section of each warranty statement.

"DIGITAL" The term "DIGITAL" in each of the language versions refers to either Digital Equipment Corporation or the applicable Digital Equipment Corporation subsidiary which initially sold or licensed the Product(s).

LANGUAGE VERSIONS & APPLICABLE COUNTRIES Purchases made in the countries or regions designated below are subject to the designated language version. Purchases made in other countries or regions are subject to the English language version. Versions indicated by a * are not included in this warranty appendix, but are available on the Internet at http://www.digital.com or by calling the number listed in the warranty statements for service in that country. These versions are planned to be included in the next printing.

Chinese*Peoples Republic of China
(simplified)

Chinese*Taiwan
(standard)

EnglishAustralia, Bahamas, Barbados Bermuda, Canada (except Quebec), Cayman Islands, Croatia, Czech Republic, Finland, Hong Kong, Hungary, Indonesia, Jamaica, India, Ireland, Malaysia, Netherlands, New Zealand, Philippines, Poland, Russia, Singapore, Slovak Repub, Slovenia, UK, USA

FrenchBelgium, France, Haiti, Quebec, Suisse Romande

GermanAustria, Deutschweiz, Germany, Liechtenstein

ItalianItaly, Ticino

Japanese*Japan

Korean*South Korea

PortugueseBrazil, Portugal

SpanishBolivia, Costa Rica, Colombia, Dominican Repub, Ecuador, Guatemala, Mexico, Panama, Paraguay, Spain, Uruguay.

SwedishDenmark, Norway, Sweden

Thai*Thailand

DIGITAL Warranty Terms and Conditions

DIGITAL Products are warranted to the end user customer ("Customer") and not to DIGITAL Business Partners through which the Products may be remarketed. This English language version applies to purchases in the countries or regions listed below under Purchase Countries. Copies of referenced documents are available from DIGITAL or its Business Partners.

Equipment

DIGITAL warrants that DIGITAL Equipment will be free of defects in workmanship and material for defects reported during the warranty period specified in Warranty Attributes below. Equipment may be manufactured using refurbished components or may have been used internally for reliability or performance testing. Spare parts may be refurbished.

Software

DIGITAL Software designated as warranted in Warranty Attributes will substantially conform to the applicable Software Product Description or user documentation accompanying the Software for the warranty period specified in Warranty Attributes. All Software not expressly designated as warranted is provided "AS IS". Documentation is not warranted. Media is warranted against defects preventing Software execution.

Third Party Products

DIGITAL does not warrant Third Party Products, which DIGITAL distributes "AS IS" unless otherwise specified in Warranty Attributes. Third Party Products may be warranted by the third party as specified in the documentation provided with the Third Party Products.

Warranty Commencement

Warranty will commence upon delivery to Customer for Products sold without installation, and upon installation for Products sold with installation. In the case of the purchase of Product from a DIGITAL Business Partner, warranty commences upon delivery to the Customer.

Exclusions

The above warranties do not apply to conditions resulting from improper use, unsupported configurations, external causes, modifications, service or installation not performed by DIGITAL or its authorized service providers, operation outside the environmental parameters specified for the Product, or to Products from which the serial numbers have been removed. DIGITAL does not warrant that the operation of any Product will be uninterrupted or error free. Warranty service may not be performed if DIGITAL reasonably believes conditions at the Customer's site represent a safety or health risk. Customer shall be responsible to pay DIGITAL's Per Call Rates for Customer requested service not covered by these warranty terms.

NO OTHER WARRANTY OR CONDITION EXPRESS OR IMPLIED, SHALL APPLY. DIGITAL SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NO REPRESENTATION OR WARRANTY INCLUDING BUT NOT LIMITED TO STATEMENTS OF CAPACITY, SUITABILITY FOR USE OR PERFORMANCE WHETHER MADE BY DIGITAL EMPLOYEES OR BY A DIGITAL BUSINESS PARTNER'S PERSONNEL SHALL BE CONSIDERED TO BE A WARRANTY BY DIGITAL, FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF DIGITAL WHATSOEVER. NOTHING IN THESE WARRANTY TERMS AND CONDITIONS IS INTENDED TO LESSEN OR DETRACT FROM ANY RIGHTS OR REMEDIES OF CUSTOMER WHICH ARE MANDATED BY APPLICABLE LAW, AND TO THE EXTENT THAT SUCH TERMS OR CONDITIONS DO SO LESSEN OR DETRACT, THEY ARE OF NO EFFECT.

Warranty Remedies

DIGITAL will provide the following exclusive warranty remedies provided Customer promptly notifies DIGITAL during the specified warranty period of any non-conformance to the above warranties:

- DIGITAL will repair or replace defective DIGITAL Equipment in the manner specified in Warranty Attributes.
- DIGITAL will remedy warranted DIGITAL Software in the manner specified in Warranty Attributes.
- If in DIGITAL's opinion, DIGITAL is unable to remedy the warranty non-conformance, DIGITAL may accept return of the Equipment or Software and refund the purchase price, or if mandated by statute, DIGITAL may elect to pay the cost of replacing the Products or acquiring equivalent Products.

DIGITAL will honor Warranty Attributes worldwide, where DIGITAL maintains a direct service presence, without regard to the country of origin. In countries where DIGITAL does not have a direct service presence, warranty is not available except with the express written consent of the country distributor or other local partner. See below for countries with direct service presence, and contact DIGITAL or its authorized service provider for further information.

For on-site warranty, Customer will assist in fault diagnosis. For Return-to-DIGITAL warranty, Customer will diagnose fault to the Field Replaceable Unit level, call DIGITAL for instructions, package per instructions, pre-pay transportation, and assume risk of loss for the return to the nearest DIGITAL return center. DIGITAL is responsible for such costs and risks for returns to Customer.

DIGITAL'S LIABILITY TO CUSTOMER FOR ANY CAUSE WHATSOEVER SHALL BE FOR DIRECT DAMAGES ONLY AND WILL BE LIMITED TO ONE (1) MILLION DOLLARS (US). THIS LIMITATION WILL APPLY REGARDLESS OF THE FORM OF ACTION. THE LIMITATION DOES NOT APPLY TO PERSONAL INJURY CAUSED BY DIGITAL'S NEGLIGENCE. IN NO EVENT WILL DIGITAL BE LIABLE FOR ANY DAMAGES RESULTING FROM THE LOSS OF USE, LOSS OF DATA, LOST PROFITS OR ANY INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES.

Purchase Countries (Purchases in the following countries or regions covered by this English language version):

Americas: Bahamas; Barbados; Bermuda; Canada (except Quebec); Cayman Islands; Jamaica; Trinidad; USA
Asia Pacific: Australia; India; Malaysia; New Zealand; Philippines, Singapore
Europe: Croatia, Czech Republic, Hungary, the Netherlands, Poland, Slovak Republic, Slovenia, UK,

Current Direct Presence Countries* (Warranty Attributes honored in these countries):
Americas: Brazil; Canada; Mexico; Puerto Rico; USA; Venezuela
Asia Pacific: Australia; Fiji; Hong Kong; Japan; S. Korea; Malaysia; New Zealand; Philippines; Singapore; Taiwan; Thailand
Europe/Mid East: Algeria; Austria; Belgium; Cote D'Ivoire; Cyprus; Czech Republic; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Ireland; Israel; Italy; Morocco; Luxembourg; Netherlands; Norway; Poland; Portugal; Romania; Russia; Saudi Arabia; Slovak Rep; Spain; Sweden; Switzerland; Turkey; Ukraine; United Kingdom

* Subject to change without notice

Warranty Attributes

StorageWorks(tm) and Storage Products Limited Warranty

Hardware Warranty Attributes	Warranty Duration
SCSI Winchester Disk's, disk SBB's	5 Years
Controllers(1), adapters, cabinets	3 Years
Solid state disks, solid state disk SBB's	3 Years
AC/DC power supplies, CD-ROM in SBB'S	3 Years
DLT Tapes, DLT tape SBB's	2 Years
Other tapes, other tape SBB's, Loaders	1 Year
Optical drives and optical jukeboxes	1 Year
Batteries (All)	1 Year

Software Warranty Attributes

Software (all Storage products): Conformance to SPD	1 Year
Advisory telephone support	90 Days

Notes:

- SBB'S = StorageWorks(tm) building blocks
- First year of hardware warranty is onsite. The balance of warranty term, if any, is Return-To-DIGITAL.
- Configured systems with differing warranties by component will receive warranty at the component level.
- All battery power supplies and batteries, including batteries integrated into other products, carry a 1 year warranty.
- Cables receive the greater of a 1 year Return-to-DIGITAL warranty or the level of warranty on the Storage Subsystem packaging.
- All warranties exclude consumables.
- Tape Media, disk packs, disk cartridges — One year return to DIGITAL
- Documentation — 90 days return to DIGITAL
- Accessories and supplies — 90 days return to DIGITAL

DIGITAL Phone Support

The following service numbers are provided for your use during the product warranty period.

United States	1-800-354-9000	Australia	61-1-800-252-277	Austria	0222-86630-2000
Belgium	02-7297-744	Brazil	0800-218499	Canada (Engl)	1-800-267-5251
Canada (French)	1-800-267-2603	Czech Repub	42-2-61108158	Denmark	80301005
Fiji Islands	679-315-699	Finland	9800 2878	France	33--+1-6987-4123
Germany	0180-330-5353	Greece (Ath)	01-682-1980	Greece (Thes)	031-427-261
Hong Kong	852-2805-3333	Hungary	11-65-2655	India	91-80-344077
Indonesia	6221-572-1171	Israel	09-59-3300	Italy	2-1678 20062
Japan	0120-11-3035	Korea	822-3771-2955	Luxembourg	49-81771
Malaysia	603-800-3435	Mexico	91-800-00210	Netherlands	030-2832888
New Zealand	0800-801-727	N.Ireland	01232 381245	Norway	22-76-86-00
PRC Beijing	8610-68492266	PRC Guangz	8620-6665666	PRC Shanghai	86-21-6545-7460
Philippines	623-840-6383	Poland	22-640-00-00	Portugal	351-1-388-9107
Puerto Rico	800-981-4764	Rep of Ireland	01-838-1216	Russia	+7-095-974-76-38
Singapore	65-3366129	Spain (Barc)	93-401-2222	Spain(Madrid)	91-583-4257
Sweden	08-98-8835	Switzerland	155-21-61	Taiwan	8862-5797555
Thailand	662-312-0500	Turkey	0-800-261-1914	Ukraine	380-44-293-6249
UnitedKingdom	01-256-57122	Venezuela	58-2-263-95-11		

DIGITAL Gewährleistungsbedingungen Für Deutschland

DIGITAL erbringt gegenüber seinen Vertragspartnern die vertragliche Gewährleistung für DIGITAL-Produkte zu den nachfolgenden Bedingungen. Soweit der Vertragspartner von DIGITAL ein Wiederverkäufer ist und dieser seine vertraglichen Gewährleistungsansprüche mit Zustimmung von DIGITAL an seinen Endkunden abgetreten hat, erbringt DIGITAL die Gewährleistung auch gegenüber dem Endkunden (Vertragspartner und Endkunde nachfolgend „Kunde“ genannt).

Die nachfolgenden Gewährleistungsbedingungen gelten für den Erwerb von DIGITAL-Produkten in den unten aufgeführten „Ländern des Erwerbs“. Auf Wunsch sind DIGITAL oder seine Vertriebspartner gerne bereit, die in diesen Gewährleistungsbedingungen angesprochenen Dokumente zur Verfügung zu stellen.

1. Hardware

1.1 DIGITAL leistet Gewähr, daß gelieferte Hardwareprodukte im Zeitpunkt des Gefahrübergangs frei von Material- und Herstellungsmängeln sind, die den Wert oder die Tauglichkeit der Ware erheblich mindern, und die von DIGITAL ausdrücklich zugesicherten Eigenschaften besitzen. Eine Gewähr für die Weiterverkäuflichkeit der Produkte oder deren Eignung zu einem bestimmten Verwendungszweck übernimmt DIGITAL nicht. Von DIGITAL herausgegebene technische Daten, Spezifikationen oder Qualitätsbeschreibungen stellen keine Zusicherungen dar, es sei denn, sie sind ausdrücklich als solche von DIGITAL schriftlich bestätigt worden.

1.2 Im Gewährleistungsfall erfolgt nach Wahl von DIGITAL kostenlose Nachbesserung oder Ersatzlieferung. Schlägt die Mängelbeseitigung auch innerhalb einer vom Kunden schriftlich gesetzten angemessenen Nachfrist endgültig fehl, ist der Kunde berechtigt, entweder Rückgängigmachung des Vertrages oder eine angemessene Herabsetzung des Kaufpreises zu verlangen.

1.3 DIGITAL bietet für seine Produkte einen jeweils definierten Gewährleistungsumfang und unterschiedliche Gewährleistungsfristen an. Einzelheiten hierzu sind dem Absatz Gewährleistungsumfang“ zu entnehmen. Die Gewährleistungsfrist beginnt ab Installation, sofern diese von DIGITAL übernommen ist, sonst ab Lieferung. Für Ersatzteile gilt eine Gewährleistungsfrist von sechs (6) Monaten.

1.4 Die Gewährleistungsarbeiten werden nach Wahl und auf Kosten von DIGITAL entweder beim Kunden oder in einem DIGITAL Servicestandort durchgeführt.

1.5 Eine Abtretung der Gewährleistungsansprüche durch den Kunden bedarf der vorherigen Zustimmung von DIGITAL.

1.6 Die Gewährleistung entfällt, wenn das Produkt durch den Kunden oder Dritte verändert, unsachgemäß installiert, gewartet, repariert, benutzt oder Umgebungsbedingungen ausgesetzt wird, die nicht den Installationsanforderungen von DIGITAL entsprechen, es sei denn, der Kunde weist nach, daß diese Umstände nicht ursächlich für den gerügten Mangel sind. Die Gewährleistung entfällt ferner, wenn technische Originalkennzeichen geändert oder beseitigt werden.

1.7 Ergibt die Überprüfung einer Mängelanzeige, daß ein Gewährleistungsfall nicht vorliegt, werden die Kosten der Überprüfung und Reparatur zu den jeweils gültigen Verrechnungssätzen für Einzelaufträge von DIGITAL berechnet.

2. Software

2.1 DIGITAL gewährleistet, dass lizenzierte Softwareprodukte von DIGITAL die Funktionen und Leistungsmerkmale erfüllen, die in der jeweiligen, im Zeitpunkt der Lizenzerteilung gültigen „Software Product

Description“ (Softwareproduktbeschreibung) enthalten sind. Sofern eine „Software Product Description“ in englischer Sprache verfasst ist, erhält der Kunde auf Wunsch deutschsprachige Erläuterungen. Die technischen Daten, Spezifikationen und Leistungsbeschreibungen in der „Software Product Description“ stellen keine Zusicherungen dar, es sei denn, sie sind schriftlich als solche von DIGITAL bestätigt worden.

2.2 Für den Fall, daß bestimmte Funktionen oder Leistungsmerkmale der „Software Product Description“ nicht erfüllt werden, erfolgt nach Wahl von DIGITAL Nachbesserung, ggf. in Form der Lieferung einer neuen Version der Software, oder Rücknahme der Software gegen Erstattung bereits geleisteter Lizenzvergütungen.

2.3 Kein Gewährleistungsanspruch besteht (i) für nicht von DIGITAL gelieferte bzw. nicht in Einklang mit den DIGITAL Softwarelizenbedingungen erstellte Softwarekopien oder (ii) für Software, die auf einem Computersystem betrieben wird, das nicht die Mindesthardware-Konfiguration und Softwareausstattung gemäss „Software Product Description“ aufweist.

2.4 Im übrigen gelten die Bestimmungen der Ziffer 1.3 bis 1.7 entsprechend.

3. Erfüllung Der Gewährleistungsverpflichtung

DIGITAL wird die ihr obliegende Gewährleistungsverpflichtung in jedem Land der Erde, in dem ein DIGITAL Servicestandort existiert, erfüllen. In Ländern, in denen kein DIGITAL Servicestandort existiert, wird die Gewährleistung nur nach ausdrücklicher schriftlicher Zustimmung des lokalen Distributors oder des lokalen DIGITAL Partners erbracht. Eine Liste der Länder mit aktuellen DIGITAL Servicestandorten finden Sie nachfolgend. Weitere Informationen erteilt Ihnen auf Wunsch DIGITAL oder jeder autorisierte Servicepartner.

4. Haftungsbeschränkung

4.1 DIGITAL haftet für Schäden, gleich aus welchem Rechtsgrund, unbegrenzt, soweit

- diese durch grobe Fahrlässigkeit oder Vorsatz verursacht wurden,
- diese auf das Fehlen einer zugesicherten Eigenschaft zurückzuführen sind oder
- das Produktehaftungsgesetz eine zwingende Haftung vorsieht.

4.2 DIGITAL haftet darüber hinaus, soweit sich aus Ziffer 4.1 nichts anderes ergibt, nur in folgendem Umfang:

- Für die schuldhafte Verletzung wesentlicher Vertragspflichten insgesamt höchstens bis DM 2.000.000 (i.W.: zwei Millionen Deutsche Mark) für Personen- und Sachschäden und bis DM 200.000 (i.W.: zweihunderttausend Deutsche Mark) für sonstige Schäden.
- Im Falle eines von DIGITAL zu vertretenden Verlustes von Daten oder Programmen für den Wiederherstellungsaufwand nur in Höhe des Aufwandes, der entsteht, wenn der Vertragspartner regelmäßige Datensicherungen durchgeführt und dadurch sichergestellt hat, daß verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

4.3 Die Haftung von DIGITAL ist, soweit sich aus Ziffer 4.1 nichts anderes ergibt,

- für entgangenen Gewinn, Mangelfolgeschäden und sonstige mittelbare Schäden,
- für leichte Fahrlässigkeit und
- für Schäden, deren Entstehung bei Vertragsschluß typischerweise nicht vorhersehbar war, ausgeschlossen.

4.4 Soweit sich aus den vorstehenden Absätzen dieser Ziffer 4 nichts anderes ergibt, ist jede Haftung von DIGITAL, gleich aus welchem Rechtsgrund, ausgeschlossen.

DIGITAL Gewährleistungsbedingungen
Für Die Schweiz, österreich Und Das Fürstentum Liechtenstein

DIGITAL leistet für ihre Produkte nicht dem Business Partner, sondern dessen Endkunden (“Kunde”) zu den nachfolgenden Bedingungen Gewähr. Die vorliegenden Gewährleistungsbedingungen finden Anwendung für Bezüge in den obgenannten Ländern. Auf Wunsch sind DIGITAL oder ihre Vertriebspartner gerne bereit, die in diesen Gewährleistungsbedingungen angesprochenen Dokumente zur Verfügung zu stellen.

Hardware

DIGITAL leistet dafür Gewähr, dass gelieferte DIGITAL Hardware zum Zeitpunkt der Lieferung an den Endkunden frei von durch DIGITAL zu vertretenden Material- und Herstellungsmängeln ist. Der Gewährleistungsumfang richtet sich nach den nachfolgenden Beschreibungen. DIGITAL kann für ihre Produkte Komponenten oder Ersatzteile einsetzen, die bereits einmal Verwendung gefunden haben (z.B. für Performance Testing).

Software

DIGITAL leistet dafür Gewähr, dass die in den Gewährleistungsbeschreibungen aufgeführten Softwareprodukte die Funktionen und Leistungsmerkmale erfüllen, die in der jeweiligen, im Zeitpunkt der Lizenzerteilung gültigen Softwareproduktebeschreibung enthalten sind. Software, welche nicht explizit in einer der nachstehenden Gewährleistungsumfang-Beschreibung aufgeführt ist, sowie Dokumentation werden ohne Gewährleistung ausgeliefert. Die Gewährleistung für Media betrifft einzig die Möglichkeit, die Software abzuspielen.

Drittherstellerprodukte

Eine Gewähr für Produkte von Drittherstellern besteht nicht, es sei denn eine solche Gewähr sei explizit in einer der nachstehenden Gewährleistungsumfang-Beschreibungen aufgeführt. Drittherstellerprodukte können vom jeweiligen Hersteller mit einer eigenen Garantie versehen sein.

Garantiebeginn

Die Garantie beginnt bei Produkten, welche ohne Installationsleistungen verkauft wurden, mit deren Auslieferung an den Kunden, ansonsten mit deren Installation. Bei Erwerb der Produkte über einen DIGITAL Business Partner beginnt die Garantie in jedem Fall mit Auslieferung an den Kunden.

Garantiebeschränkung

Die Gewährleistung entfällt, wenn das Produkt durch den Kunden oder Dritte verändert, unsachgemäss installiert, gewartet, repariert, benutzt oder Umgebungsbedingungen ausgesetzt wird, die nicht den Installationsanforderungen von DIGITAL entsprechen oder wenn technische Originalkennzeichen geändert oder beseitigt werden. DIGITAL garantiert nicht, dass der Vertrieb von Produkten ununterbrochen oder fehlerfrei vorgenommen werden kann. DIGITAL kann die Erfüllung von Garantieleistungen aussetzen, soweit deren Vorname am Kundenstandort ein Sicherheits- oder Gesundheitsrisiko darstellen kann. Ergibt die Überprüfung einer Mängelanzeige, dass ein Gewährleistungsfall nicht vorliegt, werden die Kosten der Überprüfung und Reparatur zu den jeweils gültigen Ansätzen von DIGITAL berechnet.

DIE AUFGEFÜHRTE GARANTIE IST ABSCHLIESSEND. DIGITAL LEISTET INSBESONDERE KEINE GEWÄHR FÜR DIE WEITERVERKÄUFLICHKEIT VON DIGITAL-PRODUKTEN, FÜR DEREN EIGNUNG ZU EINEM BESTIMMTEN VERWENDUNGSZWECK, FÜR KAPAZITÄTS-, LEISTUNGS- O.Ä. ZUSAGEN, SEIEN SOLCHE DURCH DIGITAL ODER EINEN BUSINESS PARTNER ABGEGEBEN WORDEN. VORBEHALTEN BLEIBEN WEITERGEHENDE ANSPRÜCHE AUFGRUND ZWINGENDEN RECHTS.

Garantieleistungen

DIGITAL wird abschliessend unter Ausschluss von weitergehenden gesetzlichen Gewährleistungsmöglichkeiten die nachstehenden Leistungen erbringen, sofern der Kunde DIGITAL während der Gewährleistungsdauer bei Auftreten eines Mangels sofort benachrichtigt:

- DIGITAL wird nach ihrer Wahl kostenlose Nachbesserungen oder Ersatzlieferung von DIGITAL-Hardware im Rahmen des nachstehend beschriebenen Gewährleistungsumfangs vornehmen.
- Die Garantie für Software richtet sich ebenfalls nach der entsprechenden Gewährleistungsumfang-Beschreibung.
- Ist nach Ansicht von DIGITAL eine Nachbesserung oder Ersatzlieferung nicht möglich, kann sie die Produkte zurücknehmen und den Kaufpreis zurückerstatten.

DIGITAL wird die ihr obliegenden Gewährleistungsverpflichtungen weltweit in jedem Land, in dem ein DIGITAL Servicestandort existiert, erfüllen. In Ländern, in denen kein DIGITAL Servicestandort existiert, wird die Gewährleistung nur nach ausdrücklicher schriftlicher Zustimmung des lokalen Distributors oder des lokalen DIGITAL Business Partner erbracht. Eine Liste der Länder mit aktuellen DIGITAL Servicestandorten folgt nachstehend. Weitere Information erteilt Ihnen auf Wunsch DIGITAL oder jeder autorisierte Service Partner.

Bei Garantiearbeiten am Standort des Kunden (on-site), wird dieser DIGITAL in der Fehlerdiagnose unterstützen. Für Rücksendung an DIGITAL (return-to-depot) Gewährleistung, wird der Kunde den Fehler auf Austauschkomponentenebene diagnostizieren, bei DIGITAL die entsprechenden Instruktionen einholen und darauf die Komponente auf seine Kosten und Risiko an die nächste DIGITAL Servicestelle senden. Die Kosten und das Risiko für die Rücksendung an den Kunden trägt DIGITAL.

DIE HAFTUNG VON DIGITAL FÜR SCHULDHAFT VERURSACHTE PERSONENSCHÄDEN IST UNBEGRÄNZT. DIE HAFTUNG FÜR SACHSCHÄDEN IST AUF DEN BETRAG VON CHF 1 MIO. FÜR KUNDEN IN DER SCHWEIZ UND IM FÜRSTENTUM LIECHTENSTEIN, BZW. öS 10 MIO. FÜR KUNDEN IN öSTERREICH BESCHRÄNKT. JEDE HAFTUNG VON DIGITAL ODER IHREN ERFÜLLUNGSGEFHILFEN FÜR ANDERE ODER WEITERGEHENDE ANSPRÜCHE UND SCHÄDEN, INSBESONDERE ANSPRÜCHE AUF ERSATZ VON MITTELBAREN, INDIREKTEN ODER FOLGESCHÄDEN, MANGELFOLGESCHÄDEN, ENTGANGENEM GEWINN ODER VERDIENSTAUSFALL SOWIE DATENVERLUST - GLEICH AUS WELCHEM RECHTSGRUND - IST AUSDRÜCKLICH AUSGESCHLOSSEN.

Länder Des Erwerbs (Für den Produkterwerb in folgenden Ländern oder Regionen gelten die nachstehenden Gewährleistungsbedingungen in deutscher Sprache):

- Deutschland: DIGITAL Gewährleistungsbedingungen für Deutschland
- Deutschschweiz; österreich; Fürstentum Liechtenstein: DIGITAL Gewährleistungsbedingungen für die Schweiz, österreich und das Fürstentum Liechtenstein

Länder Mit DIGITAL-Service-Standorten* (die Gewährleistung wird in diesen Ländern erbracht):

Amerika: Brasilien; Kanada; Mexiko; Puerto Rico; USA; Venezuela
Asien/Pazifik: Australien; Fiji; Hong Kong; Japan; Malaysia; Neuseeland; Philippinen; Singapur; Südkorea; Taiwan; Thailand
Europa/Mittlerer Osten: Algerien; Belgien; Zypern; Elfenbeinküste; Dänemark; Deutschland; Estland; Finnland; Frankreich; Griechenland; Irland; Israel; Italien; Luxemburg; Marokko; Niederlande; Norwegen, österreich; Polen; Portugal; Rumänien; Russland; Saudi Arabien; Schweden; Schweiz; Slowakische Republik; Spanien; Tschechische Republik; Türkei; Ukraine; Ungarn; Vereinigtes Königreich
*Änderungen vorbehalten

Beschränkte Gewährleistung für StorageWorks(tm) und Speicherprodukte

Hardware-Gewährleistungsumfang	Gewährleistungsdauer
SCSI Winchester Disks, Disk SBB’s	5 Jahre
Controllers(1), Adapters, Cabinets	3 Jahre
Solid State Disks, Solid State Disk SBB’s	3 Jahre
AC/DC Power Supplies, CD-ROM in SBB’s	3 Jahre
DLT Tapes, DLT Tape SBB’s	2 Jahre
Sonstige Tapes, sonstige Tape SBB’s, Loaders	1 Jahr
Optical Drives und Optical Jukeboxes	1 Jahr
Batterien (alle)	1 Jahr

Software-Gewährleistungsumfang

Software (alle Speicherprodukte)	1 Jahr
Telephonische Unterstützung	90 Tage

Anmerkungen:

- SBB’s = StorageWorks(tm) Building Blocks
- Das erste Jahr der Hardwaregewährleistung ist vor Ortgewährleistung (on-site). Für eine eventuell verbleibende Gewährleistungsfrist gilt eine „Rücksendung an DIGITAL“-Gewährleistung (return to depot).
- Für konfigurierte Systeme mit unterschiedlicher Gewährleistung für die einzelnen
- Komponenten gilt die Gewährleistung für die jeweiligen Komponenten.
- Für alle Batterie Power Supplies und Batterien einschließlich von Batterien, die in andere Produkte eingebaut sind, beträgt die Gewährleistung 1 Jahr.
- Für Kabel gilt nach Wunsch des Kunden entweder eine einjährige "Rücksendung an DIGITAL"-Gewährleistung (return to depot) oder die Gewährleistung für das Storage Subsystem Packaging.
- Verbrauchsteile sind von der Gewährleistung ausgeschlossen.
- Tape Media, Disk Packs, — 1 Jahr "Rücksendung an
- Disk Cartridges — DIGITAL"-Gewährleistung
- Dokumentation — 90 Tage "Rücksendung an DIGITAL"-Gewährleistung
- Accessoires und Supplies — 90 Tage "Rücksendung an DIGITAL"-Gewährleistung

Telephonische Unterstützung Durch DIGITAL

Während der Garantiezeit für das Produkt stehen Ihnen folgende Servicetelephone zur Verfügung:

Australien	61-1-800-252-277	Norwegen	22-76-86-00
Belgien	02-7297-744	österreich	0222-86630-2000
Brasilien	0800-218499	Philippinen	623-840-6383
Dänemark	80301005	Polen	22-640-00-00
Deutschland	0180-5252 526	Portugal	351-1-388-9107
Fiji Inseln	679-315-699	Puerto Rico	800-981-4764
Finnland	9800 2878	Republik Irland	01-838-1216
Frankreich	33+1-6987-4123	Russland	+7-095-974-76-38
Griechenland (Ath)	01-682-1980	Singapur	65-3366129
Griechenland (Thes)	031-427-261	Spanien (Bac.)	93-401-2222
Hong Kong	852-2805-3333	Spanien (Madrid)	91-583-4257
Indien	91-80-344077	Schweden	08-98-8835

Indonesien	6221-572-1171
Israel	09-59-3300
Italien	2-1678 20062
Japan	0120-11-3035
Kanada (engl.)	1-800-267-5251
Kanada (franz.)	1-800-267-2603
Korea	822-3771-2955
Luxemburg	49-81771
Malaysia	603-800-3435
Mexiko	91-800-00210
Niederlande	030-2832888
Neuseeland	0800-801-727
Nordirland	01232 381245
Schweiz und FL	155-21-61
Taiwan	8862-5797555
Thailand	662-312-0500
Tschechische Rep.	42-2-61108158
Türkei	0-800-261-1914
Ukraine	380-44-293-6249
Ungarn	11-65-2655
Venezuela	58-2-263-95-11
Vereinigtes Königreich	01-256-57122
Vereinigte Staaten	1-800-354-9000
Volksrepublik China:	
Beijing	8610-68492266
Guangzhou	8620-6665666
Shanghai	86-21-6545-7460

Termini E Condizioni Delle Garanzie DIGITAL

I prodotti DIGITAL sono garantiti ai clienti consumatori finali ("Clienti") e non ai Soggetti Autorizzati per il cui tramite i Prodotti possono essere commercializzati. La presente versione in lingua italiana si applica agli acquisti fatti nei paesi o nelle regioni elencati di seguito, sotto il titolo di "Paesi di Acquisto".

Apparecchiature

DIGITAL garantisce che le Apparecchiature DIGITAL saranno immuni da difetti di fabbricazione o dei materiali, purchè i difetti siano segnalati durante il periodo di garanzia specificato in seguito, sotto il titolo "Estremi della garanzia". Le Apparecchiature possono essere costruite usando componenti rigenerati o possono essere state usate presso la DIGITAL per prove di affidabilità o di resa. Le parti di ricambio possono essere riattate.

Software

Il Software DIGITAL indicato come garantito negli Estremi della Garanzia sarà sostanzialmente conforme alla Descrizione del Prodotto Software o alla documentazione per l'utente annessa al Software, per il periodo di garanzia specificato negli Estremi di Garanzia. Tutto il Software che non è espressamente indicato come garantito viene fornito nello stato in cui si trova. La documentazione non è garantita. I Media sono garantiti contro difetti che impediscano l'esecuzione del Software.

Prodotti Di Terzi

DIGITAL non garantisce i Prodotti di Terzi che DIGITAL distribuisce nello stato in cui si trovano, salvo che sia diversamente specificato negli Estremi di Garanzia. I Prodotti di Terzi possono essere garantiti dagli stessi, come specificato nella documentazione fornita assieme ai Prodotti di Terzi.

Decorrenza Della Garanzia

La garanzia avrà inizio all'atto della consegna al Cliente per i Prodotti venduti senza installazione e all'atto dell'installazione per i Prodotti venduti con installazione compresa. Nel caso di acquisto di Prodotti da un Soggetto Autorizzato da DIGITAL la Garanzia ha inzio all'atto della consegna al Cliente.

Esclusioni

Le garanzie di cui sopra non si applicano a vizi derivanti da uso non corretto, configurazioni non autorizzate, cause esterne, modifiche, servizi o installazioni non eseguiti da DIGITAL o dai suoi prestatori di servizi autorizzati, operazioni al di fuori dei parametri ambientali specificati per il prodotto, o a Prodotti dai quali siano stati rimossi i numeri di serie. DIGITAL non garantisce che l'operatività dei Prodotti sia continua o esente da errori.

I servizi in garanzia potranno non essere prestati se DIGITAL ragionevolmente riterrà che le condizioni locali del Cliente presentino rischi alla sicurezza o alla salute. Il Cliente dovrà pagare a DIGITAL secondo le Tariffe di Chiamata per il Cliente il corrispettivo dei servizi richiesti dal Cliente che non siano coperti dai presenti termini di garanzia.

NON SI APPLICHERA' ALCUNA ALTRA GARANZIA ESPRESSA O IMPLICITA. DIGITAL SPECIFICAMENTE DECLINA LA GARANZIA IMPLICITA DI COMMERCIABILITA' O DI IDONEITA' AD UNO SCOPO PARTICOLARE. NESSUNA DICHIARAZIONE O GARANZIA, COME AD ESEMPIO AFFERMAZIONI DI CAPACITA', IDONEITA' ALL'USO OD A PRESTAZIONI, SIANO ESSE FATTE DA PERSONALE DELLA DIGITAL O PERSONALE DI SOGGETTI AUTORIZZATI DA DIGITAL, POTRA' ESSERE CONSIDERATA COME UNA GARANZIA DATA DA DIGITAL, PER QUALSIASI SCOPO, NE' DARA' LUOGO AD ALCUNA RESPONSABILITA' DI DIGITAL, DI QUALSIASI GENERE.

PRESTAZIONI OFFERTE IN GARANZIA

DIGITAL fornirà soltanto le seguenti prestazioni garantite, purchè il Cliente notifichi prontamente a DIGITAL durante il periodo di garanzia specificato l'eventuale difformità rispetto alle garanzie di cui sopra.

- DIGITAL riparerà o sostituirà le Attrezzature DIGITAL difettose, nel modo specificato negli Estremi della Garanzia.
- DIGITAL porrà rimedio ai difetti del Software DIGITAL garantito, nel modo specificato negli Estremi della Garanzia.
- Se, a giudizio di DIGITAL, DIGITAL non sarà in grado di por rimedio in altro modo alla difformità rispetto alla Garanzia, DIGITAL potrà accettare la restituzione dell'Attrezzatura o del Software e restituire il prezzo di acquisto.

DIGITAL farà fronte agli Estremi della Garanzia in tutto il mondo, dove DIGITAL direttamente dispone di un servizio di assistenza, senza tenere conto del paese di origine. Nei paesi in cui DIGITAL non dispone di un servizio di assistenza diretta, la garanzia non è applicabile salvo che vi sia l'espresso consenso scritto del distributore in detto paese o di altro collaboratore locale. Vedasi sotto per i paesi con servizio di assistenza diretto e si contatti DIGITAL od il suo fornitore di servizi autorizzato per ulteriori informazioni.

Per i servizi in garanzia prestati presso il Cliente, il Cliente parteciperà all'identificazione dei difetti. Per i servizi in garanzia che prevedono la Restituzione a DIGITAL, il Cliente diagnosticherà i difetti della parte da sostituire, dovrà chiamare DIGITAL per ricevere istruzioni, confezionare il prodotto secondo le istruzioni ricevute, anticipare il costo del trasporto ed assumere il rischio di perdite per la restituzione al più vicino centro di restituzioni DIGITAL. DIGITAL sarà responsabile del pagamento di tali costi e rischi per le restituzioni ai Clienti.

LA RESPONSABILITÀ DI DIGITAL VERSO IL CLIENTE, QUALSIASI NE SIA LA CAUSA, RIGUARDERÀ SOLTANTO I DANNI DIRETTI E SARÀ LIMITATA AD UN MILIONE DI DOLLARI USA. QUESTA LIMITAZIONE SI APPLICHERÀ A QUALSIASI TIPO DI AZIONE INTRAPRESA. ESSA NON SI APPLICHERÀ ALLE LESIONI PERSONALI CAUSATE DA NEGLIGENZA DELLA DIGITAL. IN NESSUN CASO DIGITAL SARÀ RESPONSABILE PER DANNI DERIVANTI DALLA PERDITA DELL'USO, PERDITA DI DATI, PERDITA DI PROFITTI O QUALSIASI ALTRO DANNO CONNESSO, CONSEGUENTE O INDIRETTO.

Per I Prodotti Acquistati Nei Seguenti Paesi Sono Vigenti Condizioni Di Garanzia In Lingua Inglese:

Americhe: Bahamas, Barbados, Bermuda, Canada (eccetto Quebec), Isole Caymane, Jamaica, Trinità, Stati Uniti d'America
Asia Pacifico: Australia, India, Malesia, Nuova Zelanda, Filippine
Europa: Cecoslovacchia, Croazia, Ungheria, Polonia, Singapore, Repubblica Slovacca, Slovenia, Regno Unito

Per I Prodotti Acquistati Nei Seguenti Paesi Sono Vigenti Condizioni Di Garanzia In Lingua Locale: *

Americhe: Brasile, Canada, Messico, Porto Rico, Stati Uniti d'America, Venezuela
Asia Pacifico: Australia, Fiji, Hong Kong, Giappone, Corea del Sud, Malesia, Nuova Zelanda, Filippine, Singapore, Taiwan, Tailandia
Europa/Medio Oriente: Algeria, Austria, Belgio, Costa d'Avorio, Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Irlanda, Israele, Italia, Marocco, Lussemburgo, Paesi Bassi, Norvegia, Polonia, Portogallo, Romania, Russia, Arabia Saudita, Repubblica Slovacca, Spagna, Svezia, Svizzera, Turchia, Ucraina, Regno Unito.

* Soggetti a cambiamenti senza preavviso.

Garanzia limitata per StorageWorks (marchio) e Storage Products

Estremi della Garanzia Hardware	Durata della Garanzia
SCSI Winchester Disk's, disk SBB's	5 anni
Controllers (1), adapters, cabinets	3 anni
Solid state disks, solid state disk SBB's	3 anni
AC/DC power supplies, CD-ROM in SBB's	3 anni
DLT Tapes, DLT tape SBB's	2 anni
Altri tapes, altro tape SBB, Loaders	1 anno
Optical drives e optical jukeboxes	1 anno
Batterie (tutte)	1 anno

Estremi della Garanzia del Software

Software (tutti i prodotti storage): conformità SPD	1 anno
90 giorni di supporto telefonico di consulenza.	

Note:

- SBB = StorageWorks (marchio) building blocks.
- Il primo anno di garanzia hardware è presso il Cliente. Per gli anni eventualmente restanti, Restituzione a DIGITAL.
- I sistemi configurati con garanzie differenti a livello di componenti, riceveranno garanzia al livello dei singoli componenti.
- Tutti i carica batteria e le batterie, incluse le batterie integrate in altri prodotti, avranno una garanzia di 1 anno.
- I cavi avranno il massimo fra la Garanzia di Restituzione a DIGITAL di 1 anno ed il livello di garanzia previsto dal pacchetto Storage Subsystem.
- Tutte le garanzie escludono materiali di consumo.
- Tape, Media,
  disk packs,
  disk cartridgesGaranzia di un anno previa restituzione a DIGITAL
- Documentazione — Garanzia di 90 giorni previa restituzione a DIGITAL
- Accessori e simili — Garanzia di 90 giorni previa restituzione a DIGITAL

Approvazione Specifica

A' sensi e per gli effetti degli articoli 1341 e 1342 c.c. dichiariamo di aver letto e di approvare specificamente le clausole limitative di garanzia sopra contenute nel capitolo "Termini e condizioni delle Garanzie DIGITAL", paragrafo "Esclusioni".

Supporto Telefonico DIGITAL

I seguenti numeri di servizio sono forniti per l'utilizzo da parte vostra durante il periodo di garanzia dei Prodotti.

Stati Uniti	1-800-354-9000	Australia	61-1-800-252-277	Austria	0222-86630-2000
Belgio	02-7297-744	Brasile	0800-218499	Canada (ingl)	1-800-267-5251
Canada (fr)	1-800-267-2603	Rep.Ceca	42-2-61108158	Danimarca	80301005
Isole Fiji	679-315-699	Finlandia	9800 2878	Francia	33-1-6987-4123
Germania	0180-330-5353	Grecia(Ath)	01-682-1980	Grecia(Thes)	031-427-261
Hong Kong	852-2805-3333	Ungheria	11-65-2655	India	91-80-344077
Indonesia	6221-572-1171	Israele	09-59-3300	Italia	1678-20062
Giappone	0120-11-3035	Corea	822-3771-2955	Lussemburgo	49-81771
Malesia	603-800-3435	Messico	91-800-00210	Paesi Bassi	030-2832888
Nuova Zelanda	0800-801-727	N.Irlanda	01232 381245	Norvegia	22-76-86-00
PRC Beijing	8610-68492266	PRC Guangz	8620-6665666	PRC Shanghai	86-21-6545-7460
Philippines	623-840-6383	Polonia	22-640-00-00	Portogallo	351-1-388-9107
Porto Rico	800-981-4764	Rep. Irlanda	01-838-1216	Russia	+7-095-974-76-38
Singapore	65-3366129	Spagna(Barc)	93-401-2222	Spagna(Madrid)	91-583-4257
Svezia	08-98-8835	Svizzera	155-21-61	Taiwan	8862-5797555
Tailandia	662-312-0500	Turchia	0-800-261-1914	Ucraina	380-44-293-6249
Regno Unito	01-256-57122	Venezuela	58-2-263-95-11		

DIGITALs Garantivillkor

DIGITALs garanti avseende/vedrørende Produkter riktar/retter sig endast/alene till slutanvändare (kunden) och inte till DIGITALs Business Partners som marknadsför Produkterna. Denna Skandinaviska version gäller i de länder som anges nedan under rubriken **"**Inköpsland**".**

Maskinvara

DIGITALS Maskinvara omfattas av en garanti mot material- och fabrikationsfel under den garantiperiod som anges under Garanti Attribut (Garanti Specifikation) nedan. Maskinvara kan innefatta återanvända (brugte eller renovertde) delar liksom ha nyttjats internt för tillgänglighets- och prestandatester. Reservdelar kan vara återanvända.

Programvara

DIGITALs Programvara som enligt Garanti Attribut omfattas av garanti uppfyller vad som sägs i motsvarande "Software Product Description"("SPD") i allt väsentligt eller i den användardokumentation som medföljer Programvaran under den garantiperiod som anges för Programvaran under Garanti Attribut.

Tredjepartsprodukter

DIGITAL ansvarar inte för fel eller brist avseende/vedrørende Tredjepartsprodukter, om ej annat särskilt anges under Garanti Attribut. Tredjepartsprodukter kan omfattas av en garanti från tredje part om så framgår av den dokumentation som tillhandahålls/udleveres tillsammans med Tredjepartsprodukten.

Garantistart

Garanti träder ikraft vid leverans till Kunden för Produkter där installation inte ingår. Har installation beställts tillsammans med produkten gäller garantin från installation. Har Produkten inköpts från/af en DIGITAL Business Partner gäller garantin från leverans till dess kund.

Begränsningar

Ovanstående garantier gäller inte händelser förorsakade av felaktigt handhavande/anvendelse, ej understödda konfigurationer, yttre orsaker/årsager, modifieringar, reparation eller installation utförd av annan än DIGITAL eller dess auktoriserade serviceleverantör, nyttjande utanför de miljöbetingelser som angivits för Produkten, eller för Produkter där serienumret avlägsnats eller gjorts oläsligt. DIGITAL garanterar inte att någon Produkt är felfri eller att nyttjande kan ske utan avbrott DIGITAL förbehåller sig rätten att avbryta garantiarbete om förhållandena på platsen enligt DIGITALs bedömning påverkar hälsa och säkerhet. Kunden skall erlägga betalning till DIGITAL för beställd service som ej omfattas av denna garanti, enligt avgift för "Per Call".

DIGITAL ansvar för fel eller brist är begränsat till det ovan sagda och inga andra garantier, direkta eller indirekta, är giltiga. digital svarar inte i något fall för produktens lämplighet för ett visst ändamål eller för fel eller brist till följd av dess användande eller som utgör resultatet av sådant användande. inga uttalanden eller uppgifter avseende produkterna, t.ex. angående kapacitet, prestanda. lämplighet etc, är att se som en garanti från digital , oavsett om de lämnats av digitals personal eller av digitals business partner.

Avhjälpande

DIGITAL avhjälper fel eller brist på något av följande exklusiva sätt förutsatt att Kunden snarast under garantiperioden meddelar DIGITAL om avvikelse mot garantin:

- DIGITAL reparerar eller byter ut felaktig Maskinvara på det sätt som anges i Garanti Attribut.
- DIGITAL åtgärdar Programvara som omfattas av garanti på det sätt som sägs i Garanti Attribut.
- Om det enligt DIGITALs bedömning inte är möjligt att avhjälpa felet eller bristen äger DIGITAL återta Maskinvaran eller Programvaran mot återbetalning av vad som erlagts för densamma.

Garanti Attribut äger giltighet i samtliga de länder i världen där DIGITAL har direkt serviceorganisation, oavsett var Produkten anskaffats. I de länder där DIGITAL inte har direkt serviceorganisation, förutsätter garantin för sin giltighet att särskild skriftlig överenskommelse träffats med lokal representant. Nedan anges de länder där direkt serviceorganisation finns. Kontakta DIGITAL eller dess auktoriserade serviceleverantör för ytterligare information.

Vid på-platsen service skall Kunden assistera vid feldiagnosticering. Vid ”Retur-till-DIGITAL” garanti skall Kunden diagnosticera felet till utbytbar enhetsnivå (”Field Replaceble Unit”), kontakta DIGITAL för instruktion, förbetala transport samt stå risken för transport till närmaste DIGITAL inlämningsställe (”return center”). DIGITAL står motsvarande kostnad och risk vid returtransport till Kunden.

DIGITALS ANSVAR GENTEMOT KUNDEN OMFATTAR ENDAST DIREKT SKADA ORSAKAD AV FöRSUMMELSE AV DIGITAL ELLER DESS PERSONAL OCH ÄR BEGRÄNSAT TILL MOTVÄRDET AV EN (1) MILJON USD. DENNA BEGRÄNSNING GÄLLER OAVSETT TYP AV SKADA, DOCK EJ PERSONSKADA. DIGITAL ANSVARAR INTE I NÅGOT FALL FöR FöRLUST AV DATA, UTEBLIVEN VINST, SKADA TILL FöLJD AV ANVÄNDNING, INDIREKT SKADA ELLER FöLJDSKADA.

Inköpsländer (Denna Skandinaviska version omfattar inköp i följande länder):

Europa: Danmark, Finland *, Norge, Sverige

* För Finland äger även motsvarande engelskspråkiga version (”English version”) tillämpning.

***Länder Där Garanti Attribut Gäller** :*

Amerika: Brasilien; Kanada; Mexico; Puerto Rico; USA; Venezuela

Asien/Australien: Australia; Fidji; Hong Kong; Japan; Sydkorea; Malaysia; Nya Zeeland; Filippinerna; Singapore; Taiwan; Thailand

Europa/Afrika: Algeriet; Belgien; Elfenbenskusten; Cypern; Tjeckien; Danmark; Estland; Finland; Frankrike; Tyskland; Grekland; Ungern; Irland; Israel; Italien; Marocko; Luxemburg; Nederländerna; Norge; Polen; Portugal; Rumänien; Russland; Saudi Arabien; Slovakien; Spanien; Sverige; Schweiz; Turkiet; Ukraina; Storbritannien, österrike

* Dessa kan ändras utan föregående meddelande.

Begränsad Garanti för StorageWorks(tm) och Storage Produkter

Maskinvara - Garanti Attribut	Garantitid (år)
SCSI Winchester Disk's, disk SBB's	5
Controllers(1), adapters, cabinets	3
Solid state disks, solid state disk SBB's	3
AC/DC power supplies, CD-ROM in SBB's	3
DLT Tapes, DLT tape SBB's	2
Other tapes, other tape SBB's, Loaders	1
Optical drives and optical jukeboxes	1
Batteries (All)	1

Programvara - Garanti Attribut

Programvara (alla Storage produkter):	1 års överensstämmelse med SPD.
90 dagars telefonsupport	

Note:

- SBB'S = StorageWorks(tm) building blocks
- På-platsen gäller för maskinvaran år 1. För eventuell ytterligare garantitid gäller retur till DIGITAL.
- Konfigurerade system med komponenter med olika garantitid gäller garanti på komponentnivå.
- Alla laddningsaggregat för batterier och batterier, inklusive batterier som är integrerade i andra produkter, omfattas av 1 års garanti.
- För kablar gäller 1 års retur till DIGITAL eller, om längre, garantinivån för respektive "Storage Subsystem packaging".
- Förbrukningsmateriel ingår ej i någon garanti.
- Tape Media, disk packs, disk cartridges: 1 års retur till DIGITAL
- Dokumentation: 90 dagars retur till DIGITAL
- Tillbehör: 90 dagars retur till DIGITAL

DIGITAL Telefonnummer

Följande telefonnummer är till för er hjälp under garantiperioden.

U.S.A.	1-800-354-9000	Australien	61-1-800-252-277	österrike	0222-86630-2000
Belgien	02-7297-744	Brasilien	0800-218499	Kanada (Engl)	1-800-267-5251
Kanada (Fr)	1-800-267-2603	Tjeckien	42-2-61108158	Danmark	80301005
Fidjiöarna	679-315-699	Finland	9800 2878	Frankrike	33--+1-6987-4123
Tyskland	0180-330-5353	Grekland (Ath)	01-682-1980	Grekland (Thes)	031-427-261
Hong Kong	852-2805-3333	Ungern	11-65-2655	Indien	91-80-344077
Indonesien	6221-572-1171	Israel	09-59-3300	Italien	2-1678 20062
Japan	0120-11-3035	Korea	822-3771-2955	Luxemburg	49-81771
Malaysia	603-800-3435	Mexico	91-800-00210	Nederländerna	030-2832888
Nya Zeeland	0800-801-727	Nord-Irland	01232 381245	Norge	22-76-86-00
Kina, Beijing	8610-68492266	Kina Guangz	8620-6665666	Kina Shanghai	86-21-6545-7460
Filippinerna	623-840-6383	Polen	22-640-00-00	Portugal	351-1-388-9107
Puerto Rico	800-981-4764	Irland	01-838-1216	Ryssland	+7-095-974-76-38
Singapore	65-3366129	Spanien (Bar)	93-401-2222	Spanien(Madrid)	91-583-4257
Sverige	08-98-8835	Schweiz	155-21-61	Taiwan	8862-5797555
Thailand	662-312-0500	Turkiet	0-800-261-1914	Ukraina	380-44-293-6249
Storbrittanien	01-256-57122	Venezuela	58-2-263-95-11	Tjeckien	42-2-61108158
Slovakien	42-7-213586				

GARANTÍA DIGITAL TÉRMINOS Y CONDICIONES

DIGITAL proporciona garantía a los Productos comprados por los clientes finales (“Cliente”) y no a los Distribuidores Autorizados que comercializan dichos Productos. Esta versión en lengua española es aplicable a las compras que se realizan en los países y regiones que se indican posteriormente bajo el encabezamiento Países de Compra.

Equipo

DIGITAL garantiza que los Productos DIGITAL quedarán libres de defectos de mano de obra y materiales durante el período especificado en el apartado Características de la Garantía. Los equipos pueden ser fabricados utilizando componentes reciclados o pueden haber sido utilizados internamente para pruebas de fiabilidad y rendimiento. Las piezas de repuestos pueden ser recicladas.

Software

El Software de DIGITAL que se designa como garantizado en las Características de la Garantía será conforme de manera sustancial a la Descripción del Producto Software (SPD) correspondiente, aplicable durante el período de garantía especificado en las Características de la Garantía o en la documentación de usuario adjunta al Software. Todo Software que no se haya designado como garantizado se entrega en su estado actual. La documentación no queda cubierta por la garantía. La Media está garantizada contra defectos que impidan la ejecución del Software.

Productos De Terceros

DIGITAL no garantiza los productos de Terceros que DIGITAL distribuye a menos que se especifique de otra forma en el apartado de Características de la Garantía. Los productos de Terceros pueden estar garantizados por el Tercero tal como se indica en la documentación suministrada con dichos productos.

Comienzo De La Garantía

La garantía entra en vigor desde la fecha en la que se concluye la instalación de los equipos o bien en la fecha de entrega, si no es DIGITAL quien instala los equipos. En el supuesto que el equipo haya sido comprado a través de un Distribuidor Autorizado, la garantía comienza en la fecha de entrega del equipo al cliente.

Exclusiones

Las garantías anteriores no serán aplicables a productos cuyos números de serie hayan sido retirados o a defectos que provengan del mal uso, modificaciones no autorizadas, funcionamiento o almacenamiento en condiciones que se aparten de las especificaciones ambientales del producto, daños por causa ajenas, instalación y mantenimiento no realizados por DIGITAL o por un servicio técnico autorizado.. El servicio de garantía puede no realizarse cuando DIGITAL crea razonablemente que las instalaciones del cliente representa un riego de higiene y seguridad. El cliente será el responsable de pagar a DIGITAL las tarifas Per Call cuando el cliente requiera un servicio no cubierto por los términos y condiciones de esta garantía.

SALVO POR IMPERATIVO LEGAL, NINGUNA OTRA GARANTÍA O CONDICIóN EXPRESA O IMPLÍCITA RESULTARA APLICABLE. DIGITAL EXCLUYE ESPECÍFICAMENTE LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD Y ADECUACIóN PARA UN FIN PARTICULAR CONCRETO. NINGUNA REPRESENTACIóN O GARANTÍA INCLUSO MANIFESTACIONES SOBRE CAPACIDAD, DISPONIBILIDAD PARA SU UTILIZACIóN O CRITERIOS DE EJECUCIóN, YA SEAN REALIZADAS POR EMPLEADOS DE DIGITAL O POR EMPRESAS MIEMBROS DE SUS CANALES DE DISTRIBUCIóN PODRÁ CONSIDERARSE COMO UNA GARANTÍA OTORGADA POR DIGITAL O DAN LUGAR RESPONSABILIDADES ALGUNA DE DIGITAL.

Contenido De La Garantía

DIGITAL proporcionará exclusivamente los siguientes servicios en el ámbito de la garantía tan pronto como el Cliente notifique cualquier disconformidad del producto en relación con las garantías arriba mencionadas a DIGITAL durante el periodo de garantía aplicable:

- DIGITAL reparará o reemplazará cualquier equipo DIGITAL defectuoso en la manera especificada en las Características de la Garantía.
- DIGITAL corregirá el Software de DIGITAL garantizado en la manera especificada en las Características de la Garantía.
- Si en opinión de DIGITAL, DIGITAL no pudiera remediar la disconformidad garantizada, DIGITAL podrá aceptar la devolución del Equipo/Software y reembolsar el precio de compra de los mismos o si fuera obligatorio por mandato legal, DIGITAL podrá elegir entre pagar el coste de sustitución de los Productos o la adquisición de Productos equivalentes.

DIGITAL garantizará a nivel mundial en conformidad con las Características de la Garantía en aquellos países donde mantiene un servicio directo de asistencia técnica independientemente del país de origen. En aquellos países donde DIGITAL no mantiene un servicio directo de asistencia técnica, la garantía no está disponible excepto con el consentimiento escrito de Distribuidor autorizado. Más abajo quedan reseñados los países con servicio directo de asistencia técnica, y se ruega que se contacte con DIGITAL o su servicio de asistencia autorizado para más información.

Para servicios de Garantía en las instalaciones del Cliente, El cliente colaborará en el diagnostico del fallo. Para Garantía con Retorno, el cliente diagnosticará los fallos, y llamará a DIGITAL, que le proporcionará instrucciones para la devolución del material, embalaje. El cliente pagará los gastos de transporte y asumirá el riesgo de pérdida correspondiente a la devolución del producto en garantía al centro de reparación DIGITAL más cercano. DIGITAL pagará los gastos de transporte y riesgos correspondientes del reenvío del producto al cliente

LA RESPONSABILIDAD MÁXIMA DE DIGITAL PARA CON EL CLIENTE POR CUALQUIER CAUSA SERÁ SOLO POR DAÑOS DIRECTOS Y QUEDARA LIMITADA A 1 MILLóN DE DóLARES DE ESTADOS UNIDOS. DICHA LIMITACIóN SE APLICARA SIN TENER EN CUENTA LA FORMA DE LA ACCIóN. LA LIMITACIóN NO SE APLICARA A DAÑOS PERSONALES CAUSADOS POR LA NEGLIGENCIA DE DIGITAL. DIGITAL NO SERÁN DE FORMA ALGUNA RESPONSABLE POR DAÑOS QUE PUDIERAN SURGIR DE PERDIDA DE DATOS, LUCRO CESANTE O DE USO O POR DAÑOS ESPECIALES, INDIRECTOS, ACCIDENTALES O CONSECUENTES.

Países De Compra_(Las compras en los siguientes países o regiones están cubiertas por la versión de lengua española.) **América:** Bolivia, Costa Rica, Colombia, Chile , Ecuador, Guatemala, México, Panamá, Paraguay, Puerto Rico, República Dominicana, Venezuela, Uruguay. **Europa**: España.

Países De Asistencia Técnica Directa Actualmente * (A ellos se refieren las Características de la Garantía). **América:** Brasil; Canadá; México; Puerto Rico; USA; Venezuela. **Asia Pacifico:** Australia; Fiji; Hong Kong; Japón; Corea del Sur; Malasia; Nueva Zelanda; Filipinas; Singapur; Taiwan; Tailandia. **Europa/Oriente Medio:** Alemania; Arabia Saudi; Argelia; Austria; Bélgica; Costa de Marfil; Chipre; República Checa; Dinamarca; Estonia; España; Finlandia; Francia; Grecia; Hungría; Irlanda; Israel; Italia; Marruecos; Luxemburgo; Noruega; Países Bajos; Polonia; Portugal; Rumania; Rusia; Reino Unido; República Checa ; República Eslovaca; Suecia; Suiza; Turquía; Ucrania;

* Sujeto a cambio sin previo aviso

Garantía Limitada de StorageWorks(tm) y Productos de Almacenamiento

Características de la Garantía Hardware	Duración Garantía
Discos SCSI Winchester , Disco SBB	5 Años
Controladores(1), Cabinas , Adaptadores	3 Años
Discos estado sólido, discos estado sólido SBB	3 Años
Fuente Alimentación AC/DC, CD-ROM en SBB	3 Años
Cintas DLT , Cintas DLT SBB	2 Años
Otras cintas, otras cintas SBB, Cargadores	1 Año
Dispositivos ópticos y jukeboxes ópticos	1 Año
Baterías (TODAS)	1 Año

Características de la Garantía Software

El Software (de todos los productos de Almacenamiento): 1 año de Conformidad al SPD.
90 días de asistencia telefónica

Notas:

- SBB'= StorageWorks(tm) modulares.
- 1er año de garantía hardware en las instalaciones del cliente. El resto de la garantía es de Retorno a DIGITAL.
- Los sistemas configurados por componentes de diferentes garantías recibirán una garantía a nivel de componente.
- Todas las baterías, incluso sus cargadores y aquellas que están integradas en otros productos disfrutan 1 año de garantía.
- Los cables reciben la garantía mayor entre 1 año de Retorno a DIGITAL o el nivel de garantía del empaquetado del Subsistema de Almacenamiento.
- Todas las garantías excluyen los consumibles.
- Cintas , paquetes de discos, cartuchos de discos : 1 año de Retorno a DIGITAL.
- Documentación: 90 días Retorno a DIGITAL
- Accesorios y materiales: 90 días Retorno a DIGITAL

ASISTENCIA TELEFóNICA DIGITAL

A continuación se indica los número de teléfonos de los Servicios DIGITAL para su utilización durante el período de garantías:

Estados Unidos	1-800-354-9000	Australia	61-1-800-252-277	Austria	0222-86630-2000
Bélgica	02-7297-744	Brasil	0800-218499	Canadá (Engl)	1-800-267-5251
Canadá (Fr)	1-800-267-2603	Rep. Checa	42-2-61108158	Dinamarca	80301005
Islas Fiji	679-315-699	Finlandia	9800 2878	Francia	33--+1-6987-4123
Alemania	0180-330-5353	Grecia (Ath)	01-682-1980	Grecia(Thes)	031-427-261
Hong Kong	852-2805-3333	Hungría	11-65-2655	India	91-80-344077
Indonesia	6221-572-1171	Israel	09-59-3300	Italia	2-1678 20062
Japón	0120-11-3035	Corea	822-3771-2955	Luxemburgo	49-81771
Malasia	603-800-3435	México	91-800-00210	Países Bajos	030-2832888
Nueva Zelanda	0800-801-727	Norte Irlanda	01232 381245	Noruega	22-76-86-00
China Beijing	8610-68492266	ChinaGuangz	8620-6665666	China Shanghai	86-21-6545-7460
Filipinas	623-840-6383	Polonia	22-640-00-00	Portugal	351-1-388-9107
Puerto Rico	800-981-4764	Irlanda	01-838-1216	Rusia	+7-095-974-76-38
Singapur	65-3366129	España	901 27 27 27		
Suecia	08-98-8835	Suiza	155-21-61	Taiwan	8862-5797555
Tailandia	662-312-0500	Turquía	0-800-261-1914	Ucrania	380-44-293-6249
Reino Unido	01-256-57122	Venezuela	58-2-263-95-11		

Conditions De Garantie DIGITAL

La garantie DIGITAL est fournie au Client Utilisateur Final (le "Client") et non aux partenaires commerciaux DIGITAL par l'intermédiaire desquels les produits peuvent être revendus. La version en langue anglaise s'applique aux produits commandés dans les pays indiqués ci-dessous à l'alinéa "Pays d'Achat".

Matériel

DIGITAL garantit que le matériel DIGITAL sera exempt de défauts de fabrication et de matière première pendant le délai de garantie indiqué dans les Modalités de Garantie ci-dessous. Le matériel peut être fabriqué avec des composants reconditionnés en usine ou avoir déjà été utilisé chez DIGITAL à des fins d'essai de fiabilité ou de performance. Les pièces détachées peuvent avoir été reconditionnées.

Logiciels

Les logiciels DIGITAL, indiqués comme étant garantis dans les Modalités de Garantie, sont conformes pour l'essentiel à la description de produit logiciel ou documentation d'utilisateur applicable jointe au logiciel pendant le délai de garantie indiqué aux Modalités de Garantie. Tous les logiciels qui ne sont pas expressément garantis sont fournis "en l'état". La documentation n'est pas garantie. Les supports sont garantis contre les défauts empêchant l'exécution des logiciels.

Produits Tiers

DIGITAL ne garantit pas les produits tiers, qu'elle distribue "en l'état", sauf indication contraire dans les Modalités de Garantie. Les produits tiers peuvent être garantis par les tiers fournisseurs selon les indications de la documentation fournie avec ces produits.

Début de la garantie

La garantie commence à la date de livraison au Client pour les produits vendus sans installation et à la date de l'installation pour les produits vendus avec installation. Dans le cas de l'achat d'un produit à un Partenaire Commercial DIGITAL, la garantie commence à la date de livraison au Client.

Exclusions

Les garanties ci-dessus ne sont pas applicables en cas de défaillance due à une mauvaise utilisation, configurations non maintenues, causes externes, modifications, entretien ou installation non réalisés par DIGITAL ou ses prestataires agréés de services d'entretien, ou fonctionnement hors des paramètres d'environnement indiqués pour le produit, ou aux produits dont les numéros de série ont été enlevés. DIGITAL ne garantit pas que le fonctionnement des produits sera ininterrompu ou exempt d'erreurs. DIGITAL pourra décider de ne pas intervenir sur le site Client si ce dernier présente des risques pour la santé et la sécurité de ses employés.

DIGITAL facturera au Client les coûts d'intervention pour tout service demandé par le Client et non couvert au titre de la présente garantie.

Prestations

Dans la mesure où le Client aura averti rapidement DIGITAL de toute non conformité aux garanties décrites survenue pendant la période de garantie, DIGITAL:

- réparera ou remplacera le matériel DIGITAL défectueux de la manière indiquée aux Modalités de Garantie,
- corrigera les logiciels DIGITAL garantis de la manière indiquée aux Modalités de Garantie,
- si DIGITAL juge qu'elle n'est pas capable d'assurer la garantie, DIGITAL acceptera le retour des matériels ou logiciels concernés et remboursera le prix d'achat de ces derniers.

DIGITAL honorera la garantie dans le monde entier, quel que soit le pays d'origine dans tous les pays où DIGITAL a une représentation de service après-vente directe. Dans les pays où DIGITAL ne dispose pas d'une représentation directe, la garantie n'est assurée qu'avec le consentement exprès donné par écrit du distributeur DIGITAL du pays concerné ou de toute autre partenaire DIGITAL local, à condition que DIGITAL fournisse les pièces et assure la formation. Voir ci-dessous les pays où il y a des Centres de Services DIGITAL, et contacter DIGITAL ou son prestataire de services agréé pour plus de précisions.

Pour les garanties sur site, le Client devra assister DIGITAL dans le diagnostic. Pour les garanties "retour", le Client diagnostique les défauts dans la mesure du possible, appelle DIGITAL pour demander des instructions, emballe le produit conformément aux instructions et le retourne au Centre de Support DIGITAL à ses frais et à ses risques. DIGITAL prendra en charge les frais de retour au Client.

La responsabilité de DIGITAL vis-à-vis du Client pour quelque raison que ce soit sera limitée à un million de dollars US (1.000.000 US$).

En aucun cas DIGITAL ne sera responsable pour tout dommage résultant de pertes de données, pertes de profits, perte d'exploitation ou pour tout autre dommage indirect.

Certains systèmes de droit ne reconnaissant pas la validité des exclusions ou limitations de garantie, dans ce cas la limitation de garantie figurant ci-dessus n'est pas applicable.

Pays D'achat Où S'applique La Version Anglaise De La Garantie:

Amérique: Canada (Québec), Haiti
Afrique: Côte d'Ivoire
Europe: France, Belgique, Suisse Romande

Pays Disposant Actuellement D'un Centre De Support DIGITAL (*)

Amérique : Brésil, Canada, Mexique, Porto Rico, Etats-Unis, Venezuela
Asie-Pacifique : Australie, Fidji, Hongkong, Japon, Corée S, Malaisie, Nouvelle Zélande, Philippines, Singapour, Taiwan, Thaïlande.
Europe - Proche Orient : Algérie, Autriche, Belgique, Côte d'Ivoire, Chypre, République Tchèque, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Irlande, Israël, Italie, Maroc, Luxembourg, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Russie, Arabie Saoudite, République Slovaque, Espagne, Suède, Suisse, Turquie, Ukraine, Royaume-Uni.

* Liste modifiable sans préavis.

Garantie limitée des produits de stockage StorageWorks©

Matériel sous garantie	Durée de la garantie
Disques Winchester SCSI, blocs SBB de disques	5 ans
Contrôleurs (1), cartes, boîtiers	3 ans
Disques à semi-conducteurs, blocs SBB de disques à semi-conducteurs	3 ans
Alimentations ca/cc, CD-ROM en blocs SBB	3 ans
Lecteurs de bande DLT, blocs SBB de lecteurs de bande DLT	2 ans
Autres lecteurs de bande, autres blocs SBB de lecteurs de bande, chargeurs	1 an
Disques optiques et chargeurs de disques optiques	1 an
Batteries (tous types)	1 an

Logiciels sous garantie

Logiciels (pour tous les produits de stockage) : conformément au descriptif du produit 1 an.
Bénéficie d'une assistance téléphonique de 90 jours.

Notes

- SBB (StorageWorks Building Blocks) = ensembles fonctionnels modulaires.
- Garantie sur site la première année pour le matériel, sinon retour atelier, le cas échéant.
- Les systèmes configurés dont les modules sont couverts par des garanties différentes bénéficient de la garantie applicable aux modules.
- Toutes les alimentations secourues par batterie et toutes les batteries, y compris les batteries intégrées à d'autres produits, sont couvertes par une garantie d'un an.
- Les câbles bénéficient au maximum d'une garantie d'un an avec retour atelier ou de la garantie couvrant le sous-système de stockage.
- Aucune garantie ne couvre les consommables.
- Bandes, disques amovibles, chargeurs
  Un an avec retour atelier
- Documentation
  90 jours avec retour atelier
- Accessoires et fournitures
  90 jours avec retour atelier

Assistance Téléphonique DIGITAL:

Les numéros d'assistance suivants sont à votre service pendant la période de garantie des produits.

Etats-Unis	1-800-354-9000	Australie	008-252-277	Autriche	0222-86630-555
Belgique	02-7297744	Brésil	0800-218499	Canada (An.)	1-800-267-5251
Canada (Fr.)	1-800-267-2603	Danemark	80301005	Finlande	9800 2870
France	1-69.87.41.23	Allemagne	01307702	Grece (Ath)	01-682-1980
Grece (Thes)	031-427-261	Hongkong	852-8053333	Inde	91-80-3444077
Indonésie	6221-5721077	Israël	052-592-300	Italie	2-167820062
Malaisie	603-800-3435	Mexique	91-800-00210	Phillipines	623-840-6383
Pologne	22-640-00-00	Portugal	351-1-388-9107	Porto Rico	800-981-4764
Irlande	01-838-1216	Russie	+7-095-974-76-38	Singapour	65-3366129
Espagne (Barc)	93-401-2222	Espagne (Madrid)	91-583-4257	Suede	08-98-8835
Suisse	155-21-61	Taiwan	8862-579755	Thailande	662-312-0500
Turquie	0800-261-1914	Ukraine	380-44-293-6249	Venezuela	58-2-263-9511
Czech Repub	42-2-61108158	Fiji Islands	679-315-699	Pays-Bas	030-2832888
N.Ireland	01232 381245	PRC Beijing	8610-68492266	PRC Guangz	8620-6665666
PRC Shanghai	86-21-6545-7460	United Kingdom	01-256-57122		

Termos E Condições De Garantias

A garantia dos Produtos DIGITAL é concedida ao Cliente Final (adiante designado por Cliente), e não aos Parceiros Comerciais da DIGITAL, através dos quais os Produtos poderão ser revendidos. Estas condições são aplicáveis aos Produtos DIGITAL adquiridos nos países ou nas regiões abaixo indicados como Países de Compra.

Produtos

Durante o Período de Garantia, indicado nas Condições da Garantia, os Produtos DIGITAL estão garantidos contra defeitos de fabrico, incluindo-se nestes os de mão-de-obra e os de materiais. Os Produtos DIGITAL poderão incluir componentes recondicionados ou terem sido utilizados internamente em testes de fiabilidade ou de performance. Os sobressalentes podem ser recondicionados.

Software

O Software DIGITAL que seja designado como garantido nas Condições da Garantia deverá estar em conformidade com o Software Product Description (SPD) aplicável, ou com a documentação do utilizador que acompanha o Software, durante o período de garantia especificado nas Condições da Garantia. Todo o Software que não esteja expressamente indicado como garantido é fornecido no no estado em que se encontra. A documentação não está abrangida pela garantia. Os suportes magnéticos estão garantidos contra defeitos de fabrico e de materiais.

Produtos De Terceiros

A DIGITAL não garante os Produtos de Terceiros que a DIGITAL distribui, a menos que de outro modo se encontre especificado nas Condições da Garantia. Os Produtos fornecidos por Terceiros podem por eles ser garantidos, de acordo com o especificado na documentação fornecida juntamente com os Produtos.

Início Da Garantia

A Garantia entrará em vigor após a entrega ao Cliente dos Produtos vendidos sem instalação e após a instalação de Produtos vendidos com instalação. Se a compra de um Produto for efectuada a um Parceiro Comercial da DIGITAL, a garantia entrará em vigor após a data de entrega ao Cliente.

Exclusões

As garantias acima mencionadas não serão aplicáveis se o defeito alegado resultar de utilização inadequada, configurações não suportadas, causas externas, alterações, serviço ou instalação que não seja realizada pela DIGITAL ou pelos seus fornecedores de serviços de assistência autorizados, funcionamento fora dos parâmetros ambientais que estão especificados para o Produto, ou a Produtos de onde tenham sido retirados os números de série.

A garantia não inclui a reparação de dados ou o aumento do tempo de serviço devidos a acidente estranho à DIGITAL e seu pessoal, desastre (incluindo designadamente incêncio, inundação, água, vento e faíscas), transporte, negligência ou uso indevido, anomalias no fornecimento de energia eléctrica, falta ou falha do sistemas de fornecimento de ar condicionado ou do controlo de temperatura ou de humidade, deterioração de suportes magnéticos de informação.

A DIGITAL não garante que o funcionamento de qualquer Produto seja ininterrupto ou isento de erros.

Para que os produtos beneficiem dos serviços de garantia é necessário que as instalações do Cliente satisfaçam as condições de segurança e de saúde necessárias. O Cliente é responsável pelo pagamento à DIGITAL de Taxas de Chamada relativas a serviços pedidos pelo Cliente, os quais não se encontram incluídos nas condições da presente garantia.

AS GARANTIAS CONCEDIDAS NAS CONDIÇõES E COM AS LIMITAÇõES AQUI PREVISTAS, SÃO AS

ÚNICAS CONCEDIDAS PELA DIGITAL, EXCLUINDO-SE TODAS E QUAISQUER GARANTIAS CUJA CONCESSÃO POSSA CONSIDERAR-SE IMPLÍCITA. DIGITAL EXCLUI ESPECIFICAMENTE AS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO OU ADEQUAÇÃO DO PRODUTO A UM DETERMINADO FIM.

Reparação Durante A Garantia

A DIGITAL fornecerá exclusivamente os seguintes serviços de garantia desde que o Cliente notifique imediatamente a DIGITAL, durante o período de garantia especificado, de qualquer não conformidade com as garantias acima mencionadas:

- A DIGITAL reparará ou substituirá o Equipamento DIGITAL que tenha deficiências, conforme especificado nas Condições da Garantia.
- A DIGITAL reparará o Software DIGITAL garantido, conforme especificado nas Condições da Garantia.
- No caso de a DIGITAL não se considerar com capacidade para reparar o defeito alegado, poderá aceitar a devolução do Equipamento ou do Software, e efectuar o reembolso do respectivo preço de aquisição, ou se a lei assim estipular, a DIGITAL pode decidir pagar o custo de substituição do Produto ou adquirir Produtos similares.

A DIGITAL respeitará as Condições da Garantia em todos os países onde a DIGITAL mantém um serviço de assistência directo, independentemente dos países de origem onde os Produtos tenham sido adquiridos. Nos países onde a DIGITAL não possui um serviço de assistência directo, a garantia não está disponível, salvo em caso de consentimento expresso, por escrito, do país distribuidor ou de outro parceiro local. Para mais informações, consulte abaixo os países que possuem serviços de assistência directos e contacte a DIGITAL ou o seu fornecedor autorizado de assistência técnica.

No que concerne à garantia prestada nas instalações do Cliente, este dará assistência à DIGITAL durante o diagnóstico da falha. Relativamente à garantia de reparação nos centros de reparação DIGITAL, o Cliente efectuará o diagnóstico da falha ao nível da Unidade Substituível, contactará a DIGITAL para obter instruções, efectuará a embalagem do produto de acordo com as instruções, pagará antecipadamente os transportes, e assumirá todos os riscos referentes ao transporte para o Centro de Reparações da DIGITAL mais próximo.

A RESPONSABILIDADE DA DIGITAL PERANTE O CLIENTE, POR QUALQUER CAUSA, SEJA ELA QUAL FOR, SERÁ APENAS POR DANOS DIRECTOS E A MESMA LIMITAR-SE-Á A ESC. 150.000.000$00. ESTA LIMITAÇÃO SERÁ APLICÁVEL, SEJA QUAL FOR A FORMA DE ACÇÃO. A LIMITAÇÃO NÃO SE APLICA A DANOS PESSOAIS CAUSADOS POR NEGLIGÊNCIA DA DIGITAL. EM CASO ALGUM A DIGITAL SERÁ RESPONSÁVEL POR QUAISQUER DANOS RESULTANTES DE PERDA DE UTILIZAÇÃO, PERDA DE DADOS, PERDA DE LUCROS OU QUAISQUER OUTROS DANOS ACIDENTAIS, CONSEQUENCIAIS OU INDIRECTOS.

PAÍSES DE COMPRA: (Compras nos seguintes países ou regiões cobertos pela versão em língua Portuguesa):
América: Brasil
Pacífico/Ásia: Macau
Europa: Portugal

Países Com Assistência Directa* (Condições da Garantia respeitadas nestes países):
América: Brasil; Canadá; México; Porto Rico; EUA; Venezuela
Pacífico/Ásia: Austrália; Ilhas Fiji; Hong Kong; Japão; Coreia do Sul; Malásia; Nova Zelândia; Filipinas; Singapura; Taiwan; Tailândia
Europa/Médio Oriente: Algéria; Áustria; Bélgica; Costa do Marfim; Chipre; República Checa; Dinamarca; Estónia; Finlândia; França; Alemanha; Grécia; Hungria; Irlanda; Israel; Itália; Marrocos; Luxemburgo; Países Baixos; Noruega; Polónia; Portugal; Roménia; Rússia; Arábia Saudita; República Eslovaca; Espanha; Suécia; Suiça;

Turquia; Ucrânia; Reino Unido

*Sujeitos a alteração sem aviso prévio

Garantia Limitada ao Tempo de Vida de StorageWorks(tm) e Produtos de Armazenamento

Condições da Garantia do Hardware	Duração da Garantia
Discos SCSI Winchester, Disco SBB	5 Anos
Unidade de Controlo(1), adaptadores, armários	3 Anos
Solid State Disks, Solid State Disk SBB's	3 Anos
Fonte Alimentação AC/DC, CD-ROM em SBB	3 Anos
Bandas DLT, Banda DLT SBB	2 Anos
Outras bandas, outras bandas SBB, alimentadores	1 Ano
Unidades ópticas e jukeboxes ópticas	1 Ano
Baterias (todas)	1 Ano

Condições da Garantia do Software

Software (todos os produtos Storage): Conformidade com a SPD durante 1 Ano
Apoio de aconselhamento telefónico durante 90 dias.

Notas:

- SBB's = StorageWorks(tm) de construção de blocos
- A reparação do Hardware, durante o primeiro ano de garantia, é efectuada no local da instalação do hardware. Durante o restante prazo da garantia, se o houver, a reparação será efectuada nas instalações da DIGITAL (Return-to-DIGITAL).
- Os sistemas configurados por componentes com garantias diferentes, terão uma garantia ao nível do componente.
- Todas as fontes de alimentação de baterias e baterias, incluindo as baterias integradas noutros produtos, terão uma garantia de 1 ano.
- Os cabos terão uma garantia superior a 1 ano ao prazo de Garantia de Devolução à DIGITAL (Return-to-DIGITAL) ou ao nível da garantia de programas de Storage System.
- Todas as garantias excluem os consumíveis.
- Media Tape, Disk Embalagens, cartuchos de disco: 1 ano com devolução à DIGITAL
- Documentação: 90 dias com devolução à DIGITAL
- Acessórios e alimentadores: 90 dias com devolução à DIGITAL

(1) Os modelos da unidade de controlo StorageWorks(tm) abaixo discriminados beneficiam de suporte ao hardware e ao software durante um ano.
Modelos: HSJ30, HSJ40/42/44, HSD30 und HSZ40, SWXRC-04/05 und HS1CP.
O suporte ao Software inclui apoio telefónico através de aconselhamento e apresentação de soluções a eventuais problemas, o direito a novas versões e a serviços de distribuição Media-return-required (PCMCIA).

Apoio Telefónico Da DIGITAL

Para sua utilização, fornecem-se os seguintes números de telefone dos serviços de assistência durante o período de vigência de garantia do produto:

Alemanha	0180-330-5353	Austrália	61-1-800-252-277	Áustria	0222-86630-2000
Bélgica	02-7297-744	Brasil	0800-216499	Canada (Inglês)	1-800-267-5261
Canadá (Francês)	1-800-267-2603	Coreia	822-3771-2955	Dinamarca	80301008
Espanha (Barcelona)	93-401-2222	Espanha (Madrid)	91-583-4257	Estados Unidos	1-800-354-9000
Filipinas	623-840-6383	Finlândia	9800-2878	França	33-1-6987-4123
Grécia (Atenas)	01-682-1980	Grécia (Tesalon.)	031-427-261	Hong Kong	852-2805-3333
Hungria	11-665-2656	Ilhas Fiji	679-315-699	Índia	99-80-344077
Indonésia	6221-572-1171	Irlanda do Norte	01232-381-845	Israel	09-59-3300
Itália	2-167820062	Japão	0120-11-8035	Luxemburgo	44-81771
Malásia	603-800-9438	México	91-800-00210	Noruega	22-76-86-00
Nova Zelândia	0800-88492266	Países Baixos	030-2532888	Polónia	22-640-00-00
Porto Rico	800-981-4764	Portugal	351-1-388-9107	Reino Unido	01-256-57122
República Checa	42-2-61108158	República da Irlanda	01-838-1216	RPC - Beijing	8610-88492266
RPC - Guangz.	8620-6665666	RPC - Xangai	86-21-6545-7460	Rússia	+7-095-974-76-38
Singapura	65-3366129	Suécia	08-98-8835	Suiça	155-21-61
Tailândia	662-312-0500	Taiwan	8862-5797555	Turquia	0-800-261-1914
Ucrânia	380-44-293-6240	Venezuela	58-2-263-95-11		

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.
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.
CLI	Command line interpreter. Operator command line interface for the HS family controller firmware.
Controller	A hardware/software device that facilitates communications between a host and one or more devices organized in an array. The HSZ70 controller is an example of an array controller.
Controller shelf	A StorageWorks shelf designed to contain controller and cache modules.
Data center cabinet	A generic reference to the large cabinets, such as the SW800-series, in which StorageWorks components can be mounted.
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.

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.

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 Any EIA-423 compatible terminal plugged into the controller's local connection port. This terminal is used to identify the controller, enable host paths, define the initial configuration, and check controller status. It is not required for normal operations. It is sometimes referred to as 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.

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.

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.

Partitioning Device partitioning is the process of dividing up a single large container into a number of smaller containers.

Port 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 (0-5), 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.
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 15 devices. The StorageWorks device interface is implemented according to SCSI-2 standard, allowing the synchronous transfer of 16-bit data at rates of up to 40 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 15. Also referred to as a target ID.

SCSI-A cable A 50-conductor (25 twisted pair cable used for single-ended, SCSI bus connector.

SCSI-P cable A 68-conductor (34 twisted pair cable used for differential bus connector.

Small Computer System Interface See SCSI.

Spareset A pool of disk drives used by the controller to replace failed members of a RAIDset or mirrorset.

SPD Software product description. A document that contains the legal description of a product.

Storageset Any collection of containers, such as partitions, 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.

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

D

T

U

V

W