
HSC

HSC Controller Service Manual

Order Number EK-HSCMA-SV-003

Digital Equipment Corporation

Third Edition, July 1991

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

No responsibility is assumed for the use or reliability of software on equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

Restricted Rights: Use, duplication, or disclosure by the U. S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Copyright © Digital Equipment Corporation 1988, 1989, 1991

All Rights Reserved.
Printed in U.S.A.

The postpaid Reader's Comment Card included in this document requests the user's critical evaluation to assist in preparing future documentation.

FCC NOTICE: The equipment described in this manual generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such radio frequency interference when operated in a commercial environment. Operation of this equipment in a residential area may cause interference, in which case the user at his own expense may be required to take measures to correct the interference.

The following are trademarks of Digital Equipment Corporation: CI, DEC, DECdirect, DECnet, DECsystem, DECTAPE, DECwriter, Correspondent, DSDF, HSC, HSC50, LA, MicroVAX, MSCP, PDP, PDP-11, RA, RCTS, RSTS/E, RSX, RT-11, RX33, SA, SDI, SPM, STI, TA, TK, TMSCP, TU, ULTRIX, UNIBUS, VAX, VAXcluster, VAX DOCUMENT, VAXsimPLUS, VAX-11/750, VAX-11/780, VAX 6000, VAX 8200, VAX 8250, VAX 8300, VAX 8350, VAX 8500, VAX 8530, VAX 8550, VAX 8600, VAX 9000, VMS, VT, VT100, VT320, and the DIGITAL logo.

UNIX is a registered trademark of UNIX System Laboratories, Inc.

The HSC50 controller, © 1983 by Digital Equipment Corporation, is covered by one or more of the following U.S. patents: 4,475,212, 4,434,487, 4,413,339, 4,648,035, 4,543,626, 4,592,072, 4,241,399, 4,338,663, 4,349,871, 4,450,572, 4,811,278, 4,811,279, and other patents pending.

The HSC70 controller, © 1985 by Digital Equipment Corporation, is covered by one or more of the following U.S. patents: 4,475,212, 4,434,487, 4,413,339, 4,648,035, 4,543,626, 4,592,072, 4,241,399, 4,338,663, 4,349,871, 4,450,572, 4,811,278, 4,811,279, and other patents pending.

This document was prepared and published by Educational Services Development and Publishing, Digital Equipment Corporation.

Contents

About This Manual xxi

1 General Information

1.1 Introduction 1–1
1.2 Conventions Used In This Manual 1–1
1.3 Host Configuration 1–2
1.4 HSC Controller Model Differences 1–3
1.5 HSC Controller Cabinet 1–6
1.5.1 Front View of Cabinet 1–6
1.5.2 Rear View of Cabinet 1–9
1.6 HSC Controller Module Card Cage 1–11
1.6.1 HSC90 Controller Module Utilization Label 1–11
1.6.2 HSC70 Controller Module Utilization Label 1–12
1.6.3 HSC60 Controller Module Utilization Label 1–13
1.6.4 HSC50 Controller Module Utilization Label 1–14
1.6.5 HSC40 Controller Module Utilization Label 1–15
1.7 External Interfaces 1–15
1.8 Hardware Overview 1–18
1.8.1 I/O Control Processor Module (P.ioj/c) Functions 1–19
1.8.2 Memory Module Functions 1–20
1.8.3 Port Link Module (LINK/LINK2) Functions 1–21
1.8.4 Port Buffer Module (PILA/PILA2) Functions 1–22
1.8.5 Port Processor Module (K.pli/K.pli2) Functions and Interfaces 1–22
1.8.6 Disk Data Channel Module (K.sdi) Functions 1–23
1.8.7 Tape Data Channel Module (K.sti) Functions 1–23
1.8.8 4-Port Data Channel Module (K.si) Functions 1–23
1.8.9 8-Port Data Channel Module (8-port K.si) Functions 1–24
1.8.10 32-Mbyte Cache Option (M.cache) 1–24
1.9 HSC Controller Software Overview 1–25
1.10 Maintenance Strategy 1–26
1.10.1 Maintenance Features 1–27
1.11 Specifications 1–27

2 Controls and Indicators

2.1 Introduction 2–1
2.2 Operator Control Panel (OCP) 2–1
2.3 HSC Controller Inside Front Controls and Indicators 2–5
2.4 HSC50 Controller Inside Front Door Controls and Indicators 2–7
2.5 Logic Module Indicators 2–8
2.6 Module Switches 2–11
2.7 HSC Power Controller 2–15
2.7.1 Operating Instructions 2–16
2.8 HSC50 Power Controller 2–18
2.8.1 Line Phase Indicators 2–18
2.8.2 Fuses 2–19
2.8.3 Remote/Off/Local On Switch 2–20
2.8.4 Circuit Breakers (60 Hz) 2–20
2.8.5 Circuit Breakers (50 Hz) 2–20
2.8.6 Power Controller (60 Hz)—Rear View 2–21
2.8.7 Power Controller (50 Hz)—Rear View 2–22

3 Removal and Replacement Procedures

3.1 Introduction 3–1
3.2 Safety Precautions 3–2
3.3 Taking the HSC50 Controller Offline for Maintenance 3–2
3.3.1 Single HSC50 Controller in a Cluster 3–2
3.3.2 Multiple HSC Controllers in a Cluster 3–2
3.4 Removing and Replacing Field Replaceable Units 3–3
3.4.1 Removing HSC Controller Power 3–3
3.4.2 Removing HSC50 Controller Power 3–6
3.4.3 Removing Field Replaceable Units 3–8
3.4.4 Removing the HSC Cabinet Front Door 3–10
3.4.5 Removing the HSC50 Cabinet Front Door 3–11
3.4.6 Removing the HSC Cabinet Back Door 3–12
3.5 Removing and Replacing Modules 3–13
3.5.1 Removing and Replacing the Port Link Module (LINK and LINK2) 3–14
3.5.1.1 Removing the Port Link Module 3–15
3.5.1.2 Setting the Replacement Port Link Module Switches 3–15
3.5.1.3 Setting the Replacement Port Link Module Jumpers 3–20
3.5.1.4 Replacing the Port Link Module 3–24
3.5.1.5 Testing the Port Link Module 3–24

3.5.2 Removing and Replacing the Port Buffer Module (PILA and PILA2) 3–24
3.5.2.1 Removing the Port Buffer Module 3–25
3.5.2.2 Setting the Replacement Port Buffer Module Switches 3–25
3.5.2.3 Replacing the PILA Module 3–25
3.5.2.4 Testing the PILA Module 3–26
3.5.3 Removing and Replacing the Port Processor Module (K.pli and K.pli2) 3–26
3.5.3.1 Removing the Port Processor Module 3–26
3.5.3.2 Setting the Replacement Port Processor Module Switches 3–27
3.5.3.3 Replacing the Port Processor Module 3–28
3.5.3.4 Testing the Port Processor Module 3–28
3.5.4 Removing and Replacing the I/O Control Processor Module (P.ioj and P.ioc) ... 3–29
3.5.4.1 Removing the P.ioj/c Module 3–29
3.5.4.2 Setting the Replacement P.ioj/c Module Jumpers 3–29
3.5.4.3 Replacing the P.ioj/c Module 3–31
3.5.4.4 Testing the P.ioj/c Module 3–32
3.5.5 Removing and Replacing the Disk Data Channel Module (K.sdi) 3–32
3.5.5.1 Removing the K.sdi Module 3–32
3.5.5.2 Replacing the K.sdi Module 3–33
3.5.5.3 Testing the K.sdi Module 3–33
3.5.6 Removing and Replacing the Tape Data Channel Module (K.sti) 3–34
3.5.6.1 Removing the K.sti Module 3–34
3.5.6.2 Replacing the K.sti Module 3–34
3.5.6.3 Testing the K.sti Module 3–35
3.5.7 Removing and Replacing the Data Channel Module (4-Port K.si and 8-Port K.si) 3–35
3.5.7.1 Removing the K.si Module 3–36
3.5.7.2 Setting the Replacement K.si Module Switches 3–36
3.5.7.3 Configuration of Requestors While Replacing the K.si Module 3–37
3.5.7.4 Replacing the K.si Module 3–38
3.5.7.5 K.si Module External Loop Test 3–38
3.5.7.6 Initializing the K.si Module 3–40
3.5.7.7 Correcting K.si Module Configuration Problems 3–41
3.5.7.8 K.si Module New Boot Microcode 3–42
3.5.7.9 Testing the K.si Module (After Initialization) 3–43
3.5.7.10 Completing the Installation Procedure 3–43
3.5.8 Removing and Replacing the 32-Mbyte Cache Module (M.cache) 3–44
3.5.8.1 Software Version Requirement 3–44
3.5.8.2 Removing the M.cache Module 3–44
3.5.8.3 Replacing the M.cache Module 3–44
3.5.8.4 Testing the M.cache Module 3–45
3.5.9 Removing and Replacing the HSC Memory Module (M.std2 and M.std4) 3–47
3.5.9.1 Removing the Memory Module 3–47
3.5.9.2 Replacing the Memory Module 3–47
3.5.9.3 Testing the Memory Module 3–48

3.5.10 Removing and Replacing the HSC50 Memory Module (M.std) 3–48
3.5.10.1 Removing the M.std Module 3–48
3.5.10.2 Replacing the M.std Module 3–49
3.5.10.3 Testing the M.std Module 3–49
3.6 Removing and Replacing Subunits 3–50
3.6.1 Removing and Replacing the RX33 Disk Drive 3–50
3.6.1.1 Removing the RX33 Disk Drive 3–50
3.6.1.2 Setting the RX33 Disk Drive Jumpers 3–53
3.6.1.3 Replacing the RX33 Disk Drive 3–57
3.6.1.4 Testing the RX33 Disk Drive 3–57
3.6.2 Removing and Replacing the TU58 Tape Drive 3–57
3.6.2.1 Removing the TU58 Tape Drive 3–58
3.6.2.2 Setting the TU58 Tape Drive Jumpers 3–61
3.6.2.3 Replacing the TU58 Tape Drive 3–62
3.6.2.4 Testing the TU58 Tape Drive 3–63
3.6.3 Removing and Replacing the HSC Operator Control Panel (OCP) 3–63
3.6.3.1 Removing the HSC OCP 3–63
3.6.3.2 Replacing the HSC OCP 3–64
3.6.3.3 Testing the HSC OCP 3–65
3.6.4 Removing and Replacing the HSC50 Operator Control Panel (OCP) 3–65
3.6.4.1 Removing the HSC50 OCP 3–65
3.6.4.2 Replacing the HSC50 OCP 3–67
3.6.4.3 Testing the HSC50 OCP 3–67
3.6.5 Removing and Replacing the HSC Airflow Sensor Assembly 3–68
3.6.6 Removing and Replacing the HSC50 Airflow Sensor Assembly 3–70
3.6.7 Removing and Replacing the HSC Blower 3–72
3.6.8 Removing and Replacing the HSC50 Blower 3–74
3.6.9 Removing and Replacing the HSC Power Controller 3–76
3.6.10 Removing and Replacing the HSC50 Power Controller 3–79
3.6.11 Removing and Replacing the HSC Main Power Supply 3–81
3.6.12 Removing and Replacing the HSC50 Main Power Supply 3–85
3.6.13 Removing and Replacing the HSC Auxiliary Power Supply 3–88
3.6.14 Removing and Replacing the HSC50 Auxiliary Power Supply 3–91

4 Initialization Procedures

4.1 Introduction 4–1
4.2 Console/Auxiliary Terminal 4–1
4.2.1 Console Terminal Connection 4–1
4.2.2 HSC50 Auxiliary and Maintenance Terminal Connections 4–3
4.2.3 LA12 Parameters 4–4
4.3 HSC Controller Initialization 4–5
4.3.1 Init P.io Test (INIPIO) 4–6
4.3.2 INIPIO Test System Requirements 4–6
4.3.3 INIPIO Test Prerequisites 4–6
4.3.4 INIPIO Test Operation 4–6

4.4 HSC50 Controller Initialization 4–7
4.4.1 HSC50 Offline Diagnostics Tape 4–7
4.4.2 Init Proc Diagnostic 4–7
4.5 Fault Code Interpretation 4–8

5 Device Integrity Tests

5.1 Introduction 5–1
5.1.1 Generic Prompt Syntax 5–1
5.1.2 Generic Error Message Format 5–2
5.2 ILRX33—RX33 Disk Drive Device Integrity Tests 5–2
5.2.1 System Requirements 5–3
5.2.2 Operating Instructions 5–3
5.2.3 Test Termination 5–3
5.2.4 Parameter Entry 5–3
5.2.5 Progress Reports 5–3
5.2.6 Test Summary 5–4
5.2.7 Error Message Example 5–4
5.2.8 Error Messages 5–4
5.3 ILTU58–TU58 Tape Drive Device Integrity Test 5–5
5.3.1 System Requirements 5–5
5.3.2 Operating Instructions 5–6
5.3.3 Test Termination 5–6
5.3.4 Error Messages 5–6
5.4 ILMEMY—Memory Integrity Tests 5–7
5.4.1 System Requirements 5–7
5.4.2 Operating Instructions 5–8
5.4.3 Test Termination 5–8
5.4.4 Progress Reports 5–8
5.4.5 Test Summary 5–8
5.4.6 Error Message Example 5–8
5.4.7 Error Messages 5–9
5.5 ILCACH—Cache Memory Integrity Tests 5–9
5.5.1 System Requirements 5–10
5.5.2 Operating Instructions 5–10
5.5.3 Test Termination 5–10
5.5.4 Progress Reports 5–10
5.5.5 Test Summaries 5–11
5.5.6 Error Message Example 5–11
5.5.7 Error Messages 5–11
5.6 ILDISK—Disk Drive Integrity Tests 5–12
5.6.1 System Requirements 5–13
5.6.2 Operating Instructions 5–13
5.6.3 Availability 5–13
5.6.4 Test Termination 5–14

5.6.5 Parameter Entry 5–14
5.6.6 Specifying Requestor and Port 5–15
5.6.7 Progress Reports 5–15
5.6.8 Test Summaries 5–15
5.6.9 Error Message Example 5–18
5.6.10 Error Messages 5–18
5.6.11 MSCP Status Codes—ILDISK Error Reports 5–26
5.7 ILTAPE—TAPE Device Integrity Tests 5–27
5.7.1 Operating Instructions 5–27
5.7.2 Test Termination 5–28
5.7.3 User Dialog 5–28
5.7.4 User Sequences 5–31
5.7.5 Progress Reports 5–33
5.7.6 Test Summaries 5–33
5.7.6.1 Interface Test Summary 5–33
5.7.6.2 Formatter Test Summary 5–34
5.7.6.3 User Sequence Test Summary 5–34
5.7.6.4 Canned Sequence Test Summary 5–34
5.7.6.5 Streaming Sequence Test Summary 5–34
5.7.7 Error Message Example 5–34
5.7.8 Error Messages 5–35
5.8 ILTCOM—Tape Compatibility Test 5–37
5.8.1 System Requirements 5–38
5.8.2 Operating Instructions 5–39
5.8.3 Test Termination 5–39
5.8.4 Parameter Entry 5–39
5.8.5 Test Summaries 5–41
5.8.6 Error Message Example 5–41
5.8.7 Error Messages 5–41
5.9 ILEXER—Multidrive Exerciser 5–42
5.9.1 System Requirements 5–42
5.9.2 Operating Instructions 5–43
5.9.3 Test Termination 5–43
5.9.4 Parameter Entry 5–43
5.9.5 Disk Drive Prompts 5–44
5.9.6 Tape Drive Prompts 5–46
5.9.7 Global Prompts 5–47
5.9.8 Data Patterns 5–49
5.9.9 Setting/Clearing Flags 5–50
5.9.10 Progress Reports 5–50
5.9.11 Data Transfer Error Report 5–50
5.9.12 Performance Summary 5–50
5.9.13 Communications Error Report 5–52
5.9.14 Test Summaries 5–52

5.9.15 Error Message Format 5–55
5.9.15.1 Prompt Error Format 5–55
5.9.15.2 Data Compare Error Format 5–55
5.9.15.3 Pattern Word Error Format 5–56
5.9.15.4 Communications Error Format 5–56
5.9.16 Error Messages 5–56
5.9.16.1 Informational Messages 5–56
5.9.16.2 Generic Errors 5–58
5.9.16.3 Disk Errors 5–59
5.9.16.4 Tape Errors 5–60

6 Offline Diagnostics

6.1 Introduction 6–1
6.1.1 Software Requirements 6–1
6.1.2 Offline Diagnostics Load Procedure 6–2
6.2 ROM Bootstrap 6–2
6.2.1 Initialization Instructions 6–3
6.2.2 Failures 6–3
6.2.3 Progress Reports 6–3
6.2.4 Error Information 6–4
6.2.5 Failure Troubleshooting 6–4
6.2.6 Bootstrap Test Summaries 6–4
6.2.7 Generic Error Message Format 6–7
6.3 ODL—Offline Diagnostics Loader 6–8
6.3.1 Loader System Requirements 6–8
6.3.2 Loader Prerequisites 6–8
6.3.3 Loader Operating Instructions 6–8
6.3.4 Loader Commands 6–9
6.3.4.1 HELP Command 6–9
6.3.4.2 SIZE Command 6–9
6.3.4.3 TEST Command 6–9
6.3.4.4 LOAD Command 6–10
6.3.4.5 START Command 6–10
6.3.4.6 EXAMINE and DEPOSIT Commands 6–10
6.3.4.7 EXAMINE and DEPOSIT Symbolic Addresses 6–11
6.3.4.8 Repeating EXAMINE and DEPOSIT Commands 6–12
6.3.4.9 Relocation Register 6–12
6.3.4.10 EXAMINE and DEPOSIT Qualifiers (Switches) 6–13
6.3.4.11 Setting and Showing Defaults 6–13
6.3.5 Unexpected Traps and Interrupts 6–14
6.3.5.1 Trap and Interrupt Vectors 6–15
6.3.5.2 Help File 6–16
6.4 OFLCXT—Offline Pioj Cache Test 6–16
6.4.1 System Requirements 6–17
6.4.2 Operating Instructions 6–17

6.4.3 Test Termination 6–17
6.4.4 Parameter Entry 6–17
6.4.5 Progress Reports 6–18
6.4.6 Test Summaries 6–18
6.4.7 Error Information 6–21
6.4.8 Error Messages 6–21
6.4.9 Test Troubleshooting 6–24

6.5 OBIT—Offline Bus Interaction Test 6–24
6.5.1 System Requirements 6–24
6.5.2 Offline Bus Interaction Test Prerequisites 6–25
6.5.3 Operating Instructions 6–25
6.5.4 Test Termination 6–25
6.5.5 Parameter Entry 6–25
6.5.6 Progress Reports 6–26
6.5.7 Test Summary 6–27
6.5.8 Error Information 6–27
6.5.9 Requestor Error Summary 6–28
6.5.10 Memory Test Configuration 6–28
6.5.11 Error Messages 6–28

6.6 OKTS –Offline K Test Selector 6–31
6.6.1 System Requirements 6–31
6.6.2 Operating Instructions 6–31
6.6.3 Test Termination 6–31
6.6.4 Parameter Entry 6–32
6.6.5 Progress Reports 6–32
6.6.6 Kci Path Status Information 6–33
6.6.7 Test Summaries 6–33
6.6.8 Error Information 6–35
6.6.9 Error Messages 6–35

6.7 OKPM—Offline K/P Memory Test 6–41
6.7.1 System Requirements 6–41
6.7.2 Operating Instructions 6–42
6.7.3 Test Termination 6–42
6.7.4 Parameter Entry 6–42
6.7.5 Progress Reports 6–43
6.7.6 Parity Errors 6–44
6.7.7 Test Summaries 6–44
6.7.8 Error Information 6–45
6.7.9 Requestor Error Summary 6–45
6.7.10 Error Messages 6–46

6.8 OMEM—Offline Memory Test 6–52
6.8.1 System Requirements 6–52
6.8.2 Operating Instructions 6–52
6.8.3 Test Termination 6–52
6.8.4 Parameter Entry 6–53

6.8.5 Progress Reports 6–54
6.8.6 Parity Errors 6–54
6.8.7 Test Summaries 6–55
6.8.8 Error Information 6–56
6.8.9 Error Messages 6–57
6.9 OMCA—Offline Memory Cache Test 6–65
6.9.1 System Requirements 6–65
6.9.2 Operating Instructions 6–66
6.9.3 Test Termination 6–66
6.9.4 Parameter Entry 6–66
6.9.5 Progress Reports 6–67
6.9.6 Test Summaries 6–67
6.9.7 Error Information 6–68
6.9.8 Error Messages 6–68
6.10 OFLRXE—RX33 Offline Exerciser 6–69
6.10.1 System Requirements 6–69
6.10.2 Operating Instructions 6–69
6.10.3 Test Termination 6–69
6.10.4 Parameter Entry 6–70
6.10.5 Progress Reports 6–70
6.10.6 Test Summaries 6–71
6.10.7 Data Patterns 6–72
6.10.8 Error Information 6–72
6.10.9 Error Messages 6–73
6.11 ORFT—Offline Refresh Test 6–75
6.11.1 System Requirements 6–76
6.11.2 Operating Instructions 6–76
6.11.3 Test Termination 6–76
6.11.4 Parameter Entry 6–76
6.11.5 Progress Reports 6–77
6.11.6 Test Summaries 6–77
6.11.7 Error Information 6–77
6.11.8 Error Messages 6–78
6.12 OOCP—Offline Operator Control Panel (OCP) Test 6–76
6.12.1 System Requirements 6–79
6.12.2 Operating Instructions 6–79
6.12.3 Test Termination 6–79
6.12.4 Parameter Entry 6–79
6.12.5 Test Summaries 6–81
6.12.6 Error Information 6–83
6.12.7 Error Messages 6–83

6.12.8 Troubleshooting Registers and Displays through ODT 6–84
6.12.8.1 Switch Check through ODT 6–84
6.12.8.2 Lamp Bit Check 6–85
6.12.8.3 Secure/Enable Switch Check 6–86
6.12.8.4 State LED Check 6–87
6.13 OCSL—Offline Control Store Loader 6–88
6.13.1 System Requirements 6–88
6.13.2 Operating Instructions 6–88
6.13.3 Test Termination 6–89
6.13.4 Parameter Entry 6–89
6.13.5 Test Summaries 6–89
6.13.6 Error Information 6–90
6.13.7 Error Messages 6–90

7 Utilities

7.1 Introduction 7–1
7.2 DKUTIL — Offline Disk Utility 7–1
7.2.1 Starting DKUTIL 7–1
7.2.2 Command Syntax 7–2
7.2.3 Command Modifiers 7–2
7.2.4 Command Descriptions 7–3
7.2.4.1 Command Summary 7–3
7.2.4.2 DEFAULT Command 7–4
7.2.4.3 DISPLAY Command 7–5
7.2.4.4 DUMP Command 7–6
7.2.4.5 EXIT Command 7–8
7.2.4.6 GET Command 7–8
7.2.4.7 POP Command 7–9
7.2.4.8 PUSH Command 7–9
7.2.4.9 SET Command 7–9
7.2.5 Sample Session 7–10
7.2.6 Error and Information Messages 7–12
7.2.6.1 Error Message Variables 7–12
7.2.6.2 Error Message Severity Levels 7–13
7.2.6.3 Fatal Error Messages 7–13
7.2.6.4 Error Messages 7–13
7.2.6.5 Information Messages 7–15
7.3 VERIFY — Offline Disk Verifier Utility 7–15
7.3.1 Running VERIFY 7–16
7.3.2 Sample Session 7–17

7.3.3 Error and information Messages 7–18
7.3.3.1 Variable Output Error Fields 7–18
7.3.3.2 Error Message Severity Levels 7–18
7.3.3.3 Fatal Error Messages 7–19
7.3.3.4 Warning Messages 7–19
7.3.3.5 Information Messages 7–21
7.4 FORMAT — Offline Disk Formatter Utility 7–23
7.4.1 Running FORMAT 7–23
7.4.2 Sample Session 7–25
7.4.3 Error and Information Messages 7–26
7.4.3.1 Error Message Variables 7–26
7.4.3.2 Message Severity Levels 7–26
7.4.3.3 Fatal Error Messages 7–26
7.4.3.4 Warning Message 7–28
7.4.3.5 Information Messages 7–28
7.4.3.6 Error Messages 7–29
7.4.3.7 Success Messages 7–29
7.5 PATCH — Offline Load Media Modification Utility 7–29
7.5.1 PATCH Commands 7–29
7.5.2 Running PATCH 7–30
7.5.3 Sample Session 7–32
7.5.4 Error and Information Messages 7–33
7.5.4.1 Fatal Error Messages 7–33
7.5.4.2 PATCH Error Messages 7–33
7.5.4.3 Warning Messages 7–34
7.5.4.4 Informational Messages 7–34
7.5.4.5 Success Messages 7–34

8 Troubleshooting Techniques

8.1 Introduction 8–1
8.2 How To Use This Chapter 8–1
8.3 Initialization Error Indications 8–2
8.3.1 OCP Fault Code Displays 8–2
8.3.1.1 Fault Code Interpretation 8–3
8.3.2 Module LEDs 8–13
8.3.2.1 I/O Control Processor LEDs 8–13
8.3.2.2 Power-up Sequence of I/O Control Processor LEDs 8–13
8.3.2.3 Memory Module LEDs 8–14
8.3.2.4 Data Channel Module LEDs 8–14
8.3.2.5 M.cache Module LEDs 8–15
8.3.2.6 Host Interface LEDs 8–16
8.3.3 Communication Errors 8–16
8.3.4 Requestor Status Codes 8–17
8.3.5 HSC Boot Flow and Troubleshooting Chart 8–17

8.3.6 HSC50 controller Flow and Troubleshooting Chart 8–23
8.3.7 Boot Diagnostic Indications 8–28
8.4 Software Error Messages 8–28
8.4.1 MSCP/TMSCP Error Format, Description, and Flags 8–28
8.4.1.1 Error Format 8–28
8.4.1.2 Error Message Fields 8–29
8.4.1.3 Format Type Codes 8–29
8.4.1.4 Error Flags 8–30
8.4.2 MSCP Errors 8–31
8.4.2.1 MSCP/TMSCP Controller Errors 8–31
8.4.2.2 MSCP SDI Errors 8–32
8.4.2.3 MSCP Disk Transfer Errors 8–36
8.4.2.4 Bad Block Replacement Errors (BBR) 8–39
8.4.3 TMSCP Errors 8–40
8.4.3.1 STI Communication or Command Errors 8–41
8.4.3.2 STI Formatter Error Log 8–41
8.4.3.3 STI Drive Error Log 8–42
8.4.3.4 Breakdown of GEDS Text Field 8–45
8.4.3.5 Breakdown of GSS Text Field 8–46
8.4.3.6 GSS Text Field Bit Interpretation 8–46
8.4.3.7 Tape Transfer Error Log 8–49
8.4.4 Out-of-Band Errors 8–50
8.4.4.1 RX33 Errors 8–50
8.4.4.2 Disk Functional Errors 8–53
8.4.4.3 Tape Functional Errors 8–53
8.4.4.4 Miscellaneous Errors 8–53
8.4.5 Traps 8–53
8.4.5.1 NXM (Trap through 4) 8–53
8.4.5.2 Reserved Instruction (Trap through 10) 8–54
8.4.5.3 Parity Error (Trap through 114) 8–54
8.4.5.4 Level 7 K Interrupt (Trap through 134) 8–54
8.4.5.5 Control Bus Error Conditions (Hardware-Detected) 8–54
8.4.5.6 Level 7 K Interrupt Example 8–55
8.4.5.7 MMU (Trap through 250) 8–57
8.5 Alphabetical Listing of Software Error Messages 8–59

A Internal Cabling Diagrams

A.1 Introduction A–1
A.2 HSC Internal Cabling A–1
A.3 HSC50 Internal Cabling A–7
A.4 HSC50 (Modified) Internal Cabling A–14

B Exception Codes and Messages

B.1 Crash Dump Printout B–1
B.2 SINI-E Error Printout B–2
B.3 Submitting a Software Performance Report B–3
B.4 Exception Messages B–4

C Generic Error Log Fields

C.1 Introduction C–1
C.2 Error flags C–2
C.3 MSCP/TMSCP Status or Event Codes C–2

D Interpretation of Status Code Bytes

D.1 Introduction D–1
D.2 K-Detected Error Example Examination D–3
D.3 Normal Operation Status Codes for K-Requestors D–3
D.4 K-Detected Failure Code Analysis D–4

Examples

6–1 Example HELP file display 6–16
7–1 Example Patch of a File 7–32
8–1 MSCP/TMSCP Error Message Format 8–28
8–2 Controller Error Message Example 8–31
8–3 MSCP SDI Error Example 8–32
8–4 Disk Transfer Error Example 8–36
8–5 Bad Block Replacement Error Example 8–39
8–6 STI Communication or Command Error Example 8–41
8–7 STI Formatter Error Log Example 8–41
8–8 STI Drive Error Log Example 8–42
8–9 Tape Drive Related Error Message 8–45
8–10 Additional Tape Drive-Related Error Message 8–46
8–11 Tape Transfer Error Log Example 8–49
B–1 Crash Dump Example B–1
B–2 SINI-E Exception Code B–2
C–1 Error Log Fields Example C–1
D–1 K-detected Error Example D–1

Figures

1–1 Cluster Configuration ... 1–3
1–2 HSC Controller Cabinet Front View ... 1–6
1–3 HSC Cabinet Inside Front View ... 1–7
1–4 HSC50 Cabinet Inside Front View ... 1–8
1–5 HSC Cabinet Inside Rear View ... 1–9
1–6 HSC50 Cabinet Inside Rear View ... 1–10
1–7 HSC90 Controller Module Utilization Label Example ... 1–11
1–8 HSC70 Controller Module Utilization Label Example ... 1–12
1–9 HSC60 Controller Module Utilization Label Example ... 1–13
1–10 HSC50 Controller Module Utilization Label Example ... 1–14
1–11 HSC40 Controller Module Utilization Label Example ... 1–15
1–12 HSC Controller External Interfaces ... 1–16
1–13 HSC50 Controller External Interfaces ... 1–16
1–14 HSC Controller Block Diagram ... 1–19
1–15 HSC Controller Internal Software ... 1–25
1–16 Specifications for HSC Controllers Using Single-Phase AC Power ... 1–28
1–17 Specifications for HSC Controllers Using Three-Phase AC Power ... 1–29
2–1 Operator Control Panel ... 2–2
2–2 Operator Control Panel Fault Codes ... 2–4
2–3 HSC Controller Inside Front Door Controls/Indicators ... 2–5
2–4 HSC50 Controller Inside Front Door Controls and Indicators ... 2–7
2–5 Logic Module LED Indicators ... 2–9
2–6 LINK2 (L0118) Module Switches ... 2–12
2–7 K.si Module (L0119-YA/YB) Switches ... 2–13
2–8 HSC Power Controller—Front Panel Controls ... 2–16
2–9 HSC Power Controller Rear Panel ... 2–17
2–10 HSC50 Power Controller (60 Hz)—Front View ... 2–18
2–11 HSC50 Power Controller (50 Hz)—Front View ... 2–19
2–12 HSC50 Power Controller (60 Hz)—Rear View ... 2–21
2–13 HSC50 Power Controller (50 Hz)—Rear View ... 2–22
3–1 HSC DC Power Switch ... 3–4
3–2 HSC Power Controller Circuit Breaker ... 3–5
3–3 HSC50 DC Power Switch ... 3–6
3–4 HSC50 Line Power Circuit Breakers ... 3–7
3–5 HSC Controller FRU Removal Sequence ... 3–8
3–6 HSC50 Controller FRU Removal Sequence ... 3–9
3–7 HSC OCP Signal/Power Line Connector ... 3–10
3–8 HSC50 Maintenance Access Panel Connectors ... 3–12
3–9 HSC Card Cage Cover Removal ... 3–13
3–10 HSC50 Card Cage Cover Removal ... 3–14
3–11 LINK Module (L0100) Node Address Switches ... 3–16
3–12 LINK Module (L0100-E2/L0118) Node Address Switches ... 3–17
3–13 LINK Module (L0100) Jumper Configuration ... 3–21
3–14 LINK Module (L0118-B1) Jumper Configuration ... 3–22
3–15 LINK Module (L0118-00 Rev 2/L0118-YA) Jumper Configuration ... 3–23

3–16 L0109 Hardware Revision Level Switch 3–25
3–17 K.pli (L0107-YA) Hardware Revision Level Switch 3–27
3–18 K.pli2 (L0124-AA) Module Switchpack 3–28
3–19 Location of HSC Controller Type Jumpers on LO111 Rev F Modules 3–30
3–20 P.ioc (L0105) Baud Rate Jumper 3–31
3–21 K.si Switchpack 3–37
3–22 Location of M.cache Module Jumper J1 3–45
3–23 HSC DC Power Switch 3–51
3–24 Removing the RX33 Cover Plate 3–52
3–25 RX33 Disk Drive Removal 3–53
3–26 Revision A1 Jumper Configurations 3–55
3–27 Revision A3 Jumper Configurations 3–56
3–28 HSC50 DC Power Switch 3–58
3–29 Removing the TU58 Bezel Assembly 3–59
3–30 Disconnecting the HSC50 OCP Cables 3–60
3–31 Disconnecting the HSC50 TU58 Controller Cables 3–61
3–32 TU58 Baud Rate Jumpers 3–62
3–33 Removing the HSC OCP 3–64
3–34 Removing the HSC50 OCP 3–66
3–35 HSC Power Controller Circuit Breaker 3–68
3–36 Removing and Replacing the HSC Airflow Sensor Assembly 3–69
3–37 HSC50 Power Controller Circuit Breaker 3–70
3–38 Removing and Replacing the HSC50 Airflow Sensor Assembly 3–71
3–39 HSC Power Controller Circuit Breaker 3–72
3–40 Removing and Replacing the HSC Main Cooling Blower Duct 3–73
3–41 HSC50 Power Controller Circuit Breaker 3–74
3–42 Removing and Replacing the HSC50 Blower Duct 3–75
3–43 HSC Power Controller Circuit Breaker 3–76
3–44 Removing and Replacing the HSC Power Controller 3–77
3–45 HSC Total Off Connector 3–78
3–46 HSC50 Power Controller Circuit Breaker 3–79
3–47 Removing and Replacing the HSC50 Power Controller 3–80
3–48 HSC Power Controller Circuit Breaker 3–81
3–49 HSC Main Power Supply Cables and Test Points 3–83
3–50 Removing and Replacing the HSC70 Main Power Supply 3–84
3–51 HSC50 Power Controller Circuit Breaker 3–85
3–52 HSC50 Main Power Supply Cables and Voltage Test Points 3–87
3–53 Removing and Replacing the HSC50 Main Power Supply 3–88
3–54 HSC Power Controller Circuit Breaker 3–89
3–55 HSC Auxiliary Power Supply Cable and Test Points 3–90
3–56 Removing and Replacing the HSC Auxiliary Power Supply 3–91
3–57 HSC50 Power Controller Circuit Breaker 3–92
3–58 HSC50 Auxiliary Power Supply Cable and Voltage Test Points 3–94
3–59 Removing and Replacing the HSC50 Auxiliary Power Supply 3–95
4–1 Console Terminal Connection 4–2
4–2 Auxiliary or Maintenance Terminal Connection 4–3

6–1 P.ioj Switch Display Register Layout 6–85
6–2 P.ioj Control and Status Register Layout 6–87
8–1 Operator Control Panel Fault Codes 8–3
8–2 OCP Fault Code 1 8–4
8–3 OCP Fault Code 2 8–4
8–4 OCP Fault Code 3 8–5
8–5 OCP Fault Code 10 8–5
8–6 OCP Fault Code 11 8–5
8–7 OCP Fault Code 12 8–6
8–8 OCP Fault Code 21 8–6
8–9 OCP Fault Code 22 8–6
8–10 OCP Fault Code 23 8–7
8–11 OCP Fault Code 25 8–8
8–12 OCP Fault Code 26 8–8
8–13 OCP Fault Code 30 8–9
8–14 OCP Fault Code 31 8–9
8–15 OCP Fault Code 32 8–11
8–16 OCP Fault Code 33 8–12
8–17 HSC Boot Flow and Troubleshooting Chart 8–18
8–18 HSC50 Boot Flow and Troubleshooting Chart 8–24
8–19 Request Byte Field 8–34
8–20 Mode Byte Field 8–34
8–21 Error Byte Field 8–35
8–22 Controller Byte Field 8–35
8–23 GSS Text Field Bits Summary Breakdown 8–46
8–24 RX33 Floppy Controller CSR Breakdown 8–51
8–25 RX33 Error Message Last Line Breakdown 8–52
8–26 MMSR0 Bit Breakdown 8–58
A–1 HSC Internal Cabling A–2
A–2 HSC50 Internal Cabling A–8
A–3 HSC50 (Modified) Internal Cabling A–15

Tables

1–1 Configuration of HSC Controller Models 1–4
1–2 Memory modules 1–21
2–1 OCP Indicators And Switches 2–2
2–2 Inside Front Door Indicators and Switches (HSC) 2–6
2–3 Inside Front Door Indicators and Switches (HSC50) 2–8
2–4 Logic Module LEDs 2–10
2–5 Logic Module Switches 2–14
2–6 Line Cord Part Numbers for Various Countries 2–15
3–1 L0118 LINK Module and CI Adapter Module Switch and Jumper Settings 3–19
3–2 L0118 LINK Module S3 Switch Slot Count Timing Settings 3–20
3–3 Kpli2 (L0124-AA) Module Switchpack Functions 3–27
3–4 Ksi Switchpack Functions 3–36
3–5 Relative Speeds of Various Requestors 3–37

3–6 K.si Module New Microcode Load Conditions 3–43
3–7 M.cache Module Indicator Functions 3–46
3–8 RX33 Jumper Description 3–54
5–1 ILTAPE Test Levels 5–34
5–2 ILTCOM Header Record 5–37
5–3 ILTCOM Data Patterns 5–38
6–1 RX33 Error Table 6–6
6–2 RX33 Error Code Table 6–6
6–3 Trap and Interrupt Vectors 6–15
7–1 PATCH Commands 7–29
8–1 UPAR Register Addresses 8–10
8–2 Control Program Bits 8–10
8–3 Status of Requestors for Level 7 Interrupt 8–11
8–4 Required Configuration Checks for HSC Controllers 8–12
8–5 I/O Control Processor LEDs 8–13
8–6 Memory Module LEDs 8–14
8–7 Data Channel Module LEDs 8–14
8–8 M.cache Module LEDs 8–15
8–9 Host Interface Module Set LEDs 8–16
8–10 MSCP/TMSCP Error Message Field Descriptions 8–29
8–11 MSCP/TMSCP Error Message Format Type Code Numbers 8–29
8–12 MSCP/TMSCP Error Flags 8–30
8–13 MSCP/TMSCP Controller Error Message Field Descriptions 8–31
8–14 MSCP SDI Error Field Descriptions 8–32
8–15 Request Byte Field Descriptions 8–34
8–16 Mode Byte Field Descriptions 8–34
8–17 Error Byte Field Descriptions 8–35
8–18 Controller Byte Field Descriptions 8–36
8–19 Disk Transfer Error Field Descriptions 8–37
8–20 Original Error Flags Field Descriptions 8–38
8–21 Recovery Flags Field Definitions 8–38
8–22 Bad Block Replacement Error Field Definitions 8–39
8–23 Replace Flags Field Bit Descriptions 8–40
8–24 STI Communication or Command Error Printout Field Descriptions 8–41
8–25 STI Formatter Error Log Field Descriptions 8–42
8–26 STI Formatter E Log 8–42
8–27 STI Drive Error Log Field Descriptions 8–42
8–28 GEDS Text 8–43
8–29 STI Drive Error Log (TA78 Drive Product Specific) 8–43
8–30 Tape Transfer Error Log Field Descriptions 8–49
8–31 Status Register Summary 8–52
B–1 Obtaining Data Structure Information B–3
C–1 Generic Error Log Fields C–1
C–2 Error Flags C–2
C–3 MSCP/TMSCP Status or Event Codes C–3
D–1 Normal Operation Status Codes for K-requestors D–3

D–2 K.ci Status Code Bytes For HSC40, HSC50, and HSC70 Controllers During Initialization D–5
D–3 K.ci Status Code Bytes For HSC60 and HSC90 Controllers During Initialization D–8
D–4 K.sdi Status Code Bytes D–12
D–5 K.sti Status Code Bytes D–14
D–6 K.si Disk Status Code Bytes D–16
D–7 K.si Tape Status Code Bytes D–18
D–8 Status Codes for K.si Requestors With Microcode Load Failure D–20

About This Manual

Introduction

This manual contains information and servicing procedures for the HSC90, HSC70, HSC60, HSC50, HSC50 (modified), and HSC40 controllers. In this manual, the term "HSC controller" refers to all models. When a specific model of the HSC controller is being addressed, it is referred to by its model name. The term "HSC50 controller" includes the HSC50 and HSC50 (modified) controllers, unless specifically stated.

This manual describes controls and indicators, error reporting, field replaceable units (FRUs), troubleshooting, and diagnostic procedures. All information in this manual is informational/instructional and is designed to assist service personnel with maintenance information. Operational theory is included wherever such background is helpful to service personnel.

Installation procedures, most HSC controller utilities, and detailed technical descriptions are not included in this manual. For source material on these and other subjects not within the scope of this manual, refer to the list of related documentation in this section.

Audience

This manual is intended for use by Level 1 Digital Customer Service engineers and other personnel who maintain the components of the HSC controller.

Scope

This manual is divided into the following sections:

- Chapters:
  1. General Information
  2. Controls and Indicators
  3. Removal and Replacement Procedures
  4. Initialization Procedures
  5. Device Integrity Tests
  6. Offline Diagnostics
  7. Utilities
  8. Troubleshooting Techniques
- Appendixes:
  A. Internal Cabling Diagrams

B. Exception Codes and Messages

C. Generic Error Log Fields

D. Interpretation of Status Code Bytes

Related Documentation

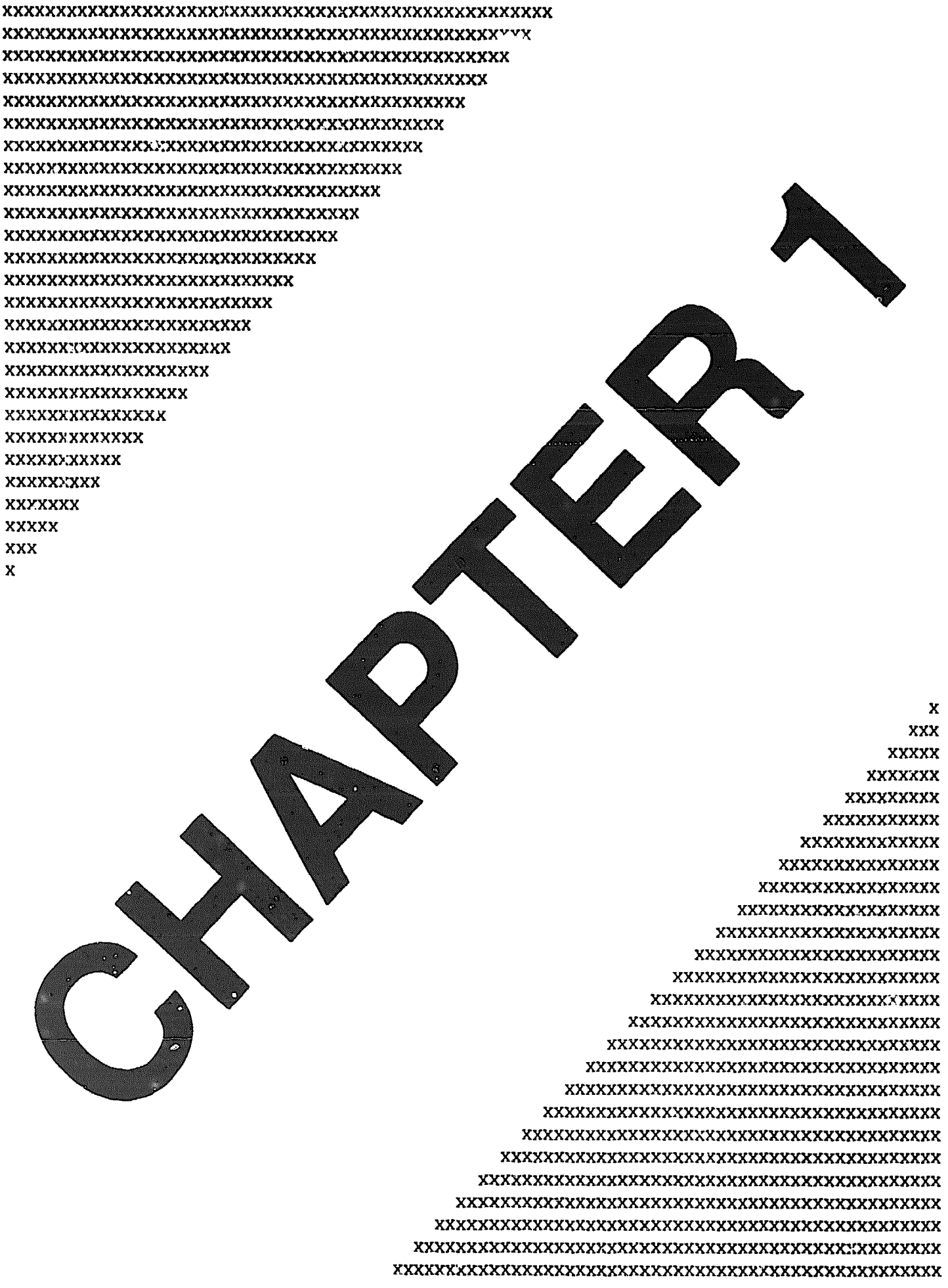
Documents related to the HSC controller are available under the following titles and part numbers:

- *HSC Controller User Guide* (HSC50 only: AA–GMEAA–TK)
- *HSC Controller User Guide* (All other models: AA–GMFAK–TK)
- *HSC Controller Installation Manual* (EK–HSCMN–IN–002)
- *HSC70 Controller Illustrated Parts Breakdown* (EK–HSC70–IP)
- *HSC50 Controller Illustrated Parts Breakdown* (EK–HSC50–IP)
- *HSC50 Controller Device Integrity Tests User Documentation* (EK–IHSC5–UG)
- *HSC50 Controller Offline Diagnostics User Documentation* (EK–OHS–UG)
- *HSC50 Controller Utilities User Documentation* (EK–UHSC5–UG)
- *VT320 Owner's Manual* (EK–VT320–UG)
- *VT320 Programmer Pocket Guide* (EK–VT320–HR)
- *VT320 Installation Guide* (EK–VT320–IN)
- *VT220 Owner's Manual* (EK–VT220–UG)
- *VT220 Programmer Pocket Guide* (EK–VT220–HR)
- *VT220 Installation Guide* (EK–VT220–IN)
- *Installing and Using the LA50 Printer* (EK–0LA50–UG)
- *LA50 Printer Programmer Reference Manual* (EK–0LA50–RM)
- *Installing and Using the LA75 Printer* (EK–0LA75–UG)
- *LA75 Printer Programmer Reference Manual* (EK–0LA75–RM)
- *Star Coupler User Guide* (EK–SC008–UG)
- *CI780 User Guide* (EK–CI780–UG)
- *DECwriter Correspondent Technical Manual* (EK–CPL12–TM)
- *TU58 DECTAPE II User Guide* (EK–0TU58–UG)

These documents (except for the *HSC Controller User Guide*) can be ordered from Publication and Circulation Services, 10 Forbes Road, Northboro, Massachusetts 01532 (RCS code: NR12; mail code: NR03/W3).

The *HSC Controller User Guide* can be ordered from the Software Distribution Center, Digital Equipment Corporation, Northboro, Massachusetts 01532.

NOTE
Please consult the *HSC Controller Software Release Notes* for the latest hardware revision levels.


CHAPTER 1

1 General Information

1.1 Introduction

This chapter includes general information about the Hierarchical Storage Controller (HSC) mass storage server, including:

- Host configuration
- Model differences
- Cabinet layout
- External interfaces
- Hardware overview
- Module descriptions
- Software overview
- Maintenance strategy
- Specifications

1.2 Conventions Used In This Manual

In this manual, the term "HSC controller" refers to all models, including:

- HSC90
- HSC70
- HSC60
- HSC50
- HSC50 (modified)
- HSC40

Any models not included in this term are specifically addressed in an accompanying section.

When a specific model of the HSC controller is being addressed, it is referred to by its model name. The term "HSC50 controller" includes the HSC50 or HSC50 (modified) controller, unless specifically stated. The HSC50 (modified) controller uses the 30-24374-XX 881 power controller, while the HSC50 controller uses the 70-19122-XX power controller.

1.3 Host Configuration

The HSC controller acts as a mass storage server for a host computer or a cluster of multiple host computers. It connects with the host(s) over a CI (computer interconnect) bus. The CI use two redundant paths (path A and path B) for reliability. It connects with the mass storage devices over an SDI (standard disk interconnect) or STI (standard tape interconnect). These are called collectively standard interconnect (SI) busses.

Figure 1–1 illustrates a five-node cluster configuration with two HSC controllers and three host computers. Through dual porting, both HSC controllers can access the tape formatters and the disk drives.

The HSC controller connects to a load device for software loading and to an operator through a terminal and operator control panel (OCP).

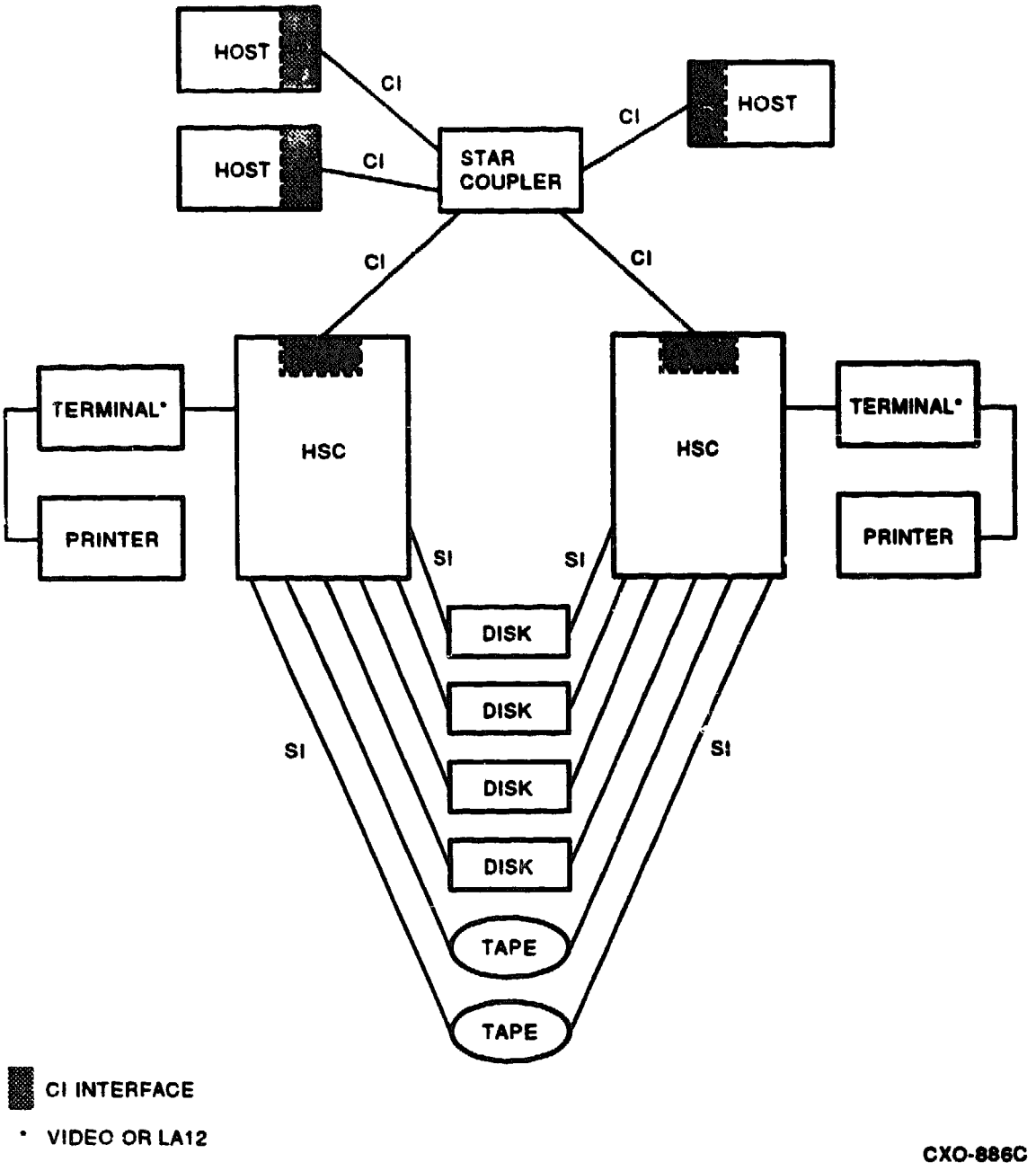


Figure 1–1 Cluster Configuration

1.4 HSC Controller Model Differences

The HSC controller module set includes a processor module, a memory module, a three-module host interface set, and a number of disk/tape data channel modules. The data cache module is an option on some HSC controller models. Module configuration for the various models of HSC controllers is shown in Table 1–1. This table also relates the module name to the engineering designation and to the part order (L number) designation.

Table 1–1 Configuration of HSC Controller Models

Item Name	Engineering Designation	Module Designation	HSC90	HSC70	HSC60	HSC50	HSC40
Port processor	K.pli	L0107–YA	No	Yes	No	Yes	Yes
Port processor	K.pli2	L0124–AA	Yes	No	Yes	No	No
Port link	LINK	L0100 E2 L0118–00	No	Yes	No	Yes	Yes
Port link	LINK2	L0118–YA	Yes	No	Yes	No	No
Port buffer	PILA	L0109	No	Yes	No	Yes	Yes
Port buffer	PILA2	L0125–AA	Yes	No	Yes	No	No
I/O control processor	P.ioc	L0105–00	No	No	No	Yes	No
I/O control processor	P.ioj	L0111–00	No	Yes	No	No	No
I/O control processor	P.ioj	L0111–YA	No	No	No	No	Yes
I/O control processor	P.ioj-18	L0111–YC	Yes	No	No	No	No
I/O control processor	P.ioj-18	L0111–YD	No	No	Yes	No	No
Memory	M.std	L0106–AA	No	No	No	Yes	No
Memory	M.std2	L0117–AA	No	Yes	No	No	Yes
Memory	M.std4	L0123–AA	Yes	No	Yes	No	No
32-Mbyte cache	M.cache	L0121–AA	Option	No	Option	No	No
Disk data channel	K.sdi	L0108–YA	Option	Option	Option	Option	Option
Tape data channel	K.sti	L0108–YB	Option	Option	Option	Option	Option
Disk/tape data channel	K.si 4-port	L0119–YA	Option	Option	Option	Option	Option
Disk data channel	K.si 8-port	L0119–YB	Option	No	Option	No	No
Maximum data channels	-	-	8	8	3	6	3
Maximum ports	-	-	48	32	20	24	12
Load devices	-	-	RX33	RX33	RX33	TU58	RX33
Aux power supply	-	-	Yes	Yes	[1]	[2]	No

[1]The HSC60–AA without the cache option does not have an auxiliary power supply. The HSC60–AA with the cache option does have an auxiliary power supply. The HSC60–BA does have an auxiliary power supply.

[2]If the HSC50 has four or more requestors, it requires an auxiliary power supply.

Kits to upgrade HSC40, HSC60, and HSC70 controllers to larger capability products are shown in the following list:

- Kit number HSC6X–AA is available to upgrade the HSC40 controller to an HSC60 controller.
- Kit number HSC7X–AA/AB is available to upgrade the HSC40 controller to an HSC70 controller.
- Kit number HSC9X–CA/CB is available to upgrade the HSC60 controller to an HSC90 controller.
- Kit number HSC9X–AA is available to upgrade the HSC70 controller to an HSC90 controller.

1.5 HSC Controller Cabinet

HSC controller logic and power systems are housed in a modified H9642 cross-products cabinet with both front and rear access. The front cabinet door is secured with a lock that requires a key. The door key is part of the door-lock mechanism (part number 12–25411–01).

1.5.1 Front View of Cabinet

The front of the cabinet contains the OCP switches and indicators. Switch operation and indicator functions are described in Chapter 2.

Figure 1–2 shows a typical front view of the cabinet.

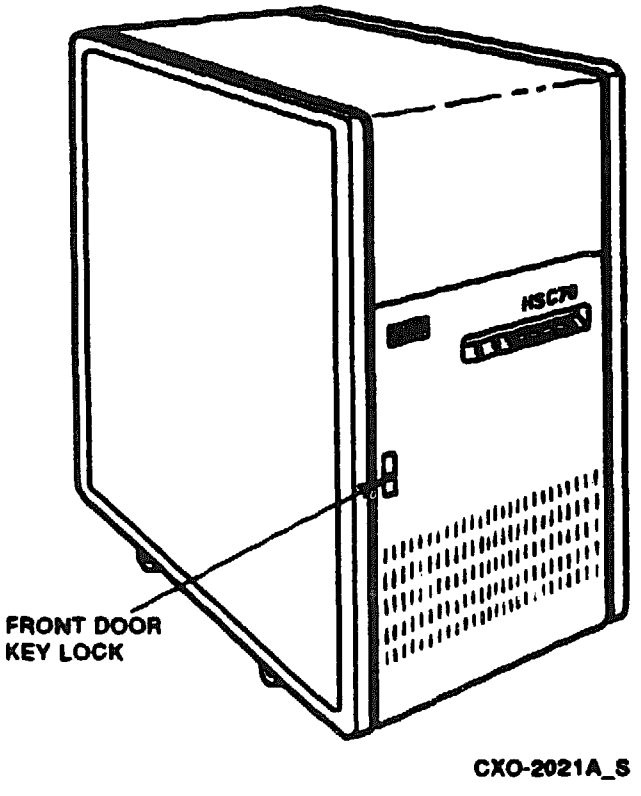


Figure 1–2 HSC Controller Cabinet Front View

Figure 1–3 shows a typical HSC controller cabinet with the front door open.

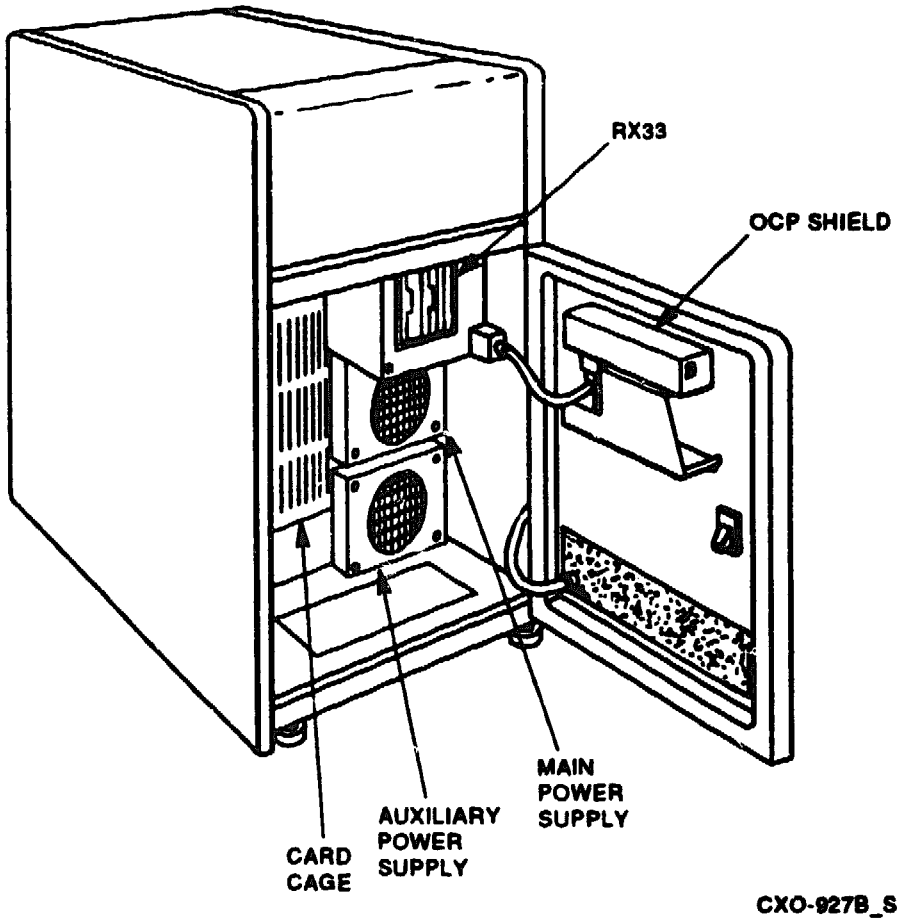


Figure 1–3 HSC Cabinet Inside Front View

The upper right side of the cabinet houses two RX33 disk drives and connectors for the OCP. The card cage and backplane occupy the left side of the cabinet.

The HSC controller power supplies are housed under the RX33 disk drives. Each power supply has a fan drawing air from the front of the cabinet across the power unit and exhausting it through a rear duct.

Figure 1–4 shows a typical front view of the HSC50 controller cabinet with the front door open.

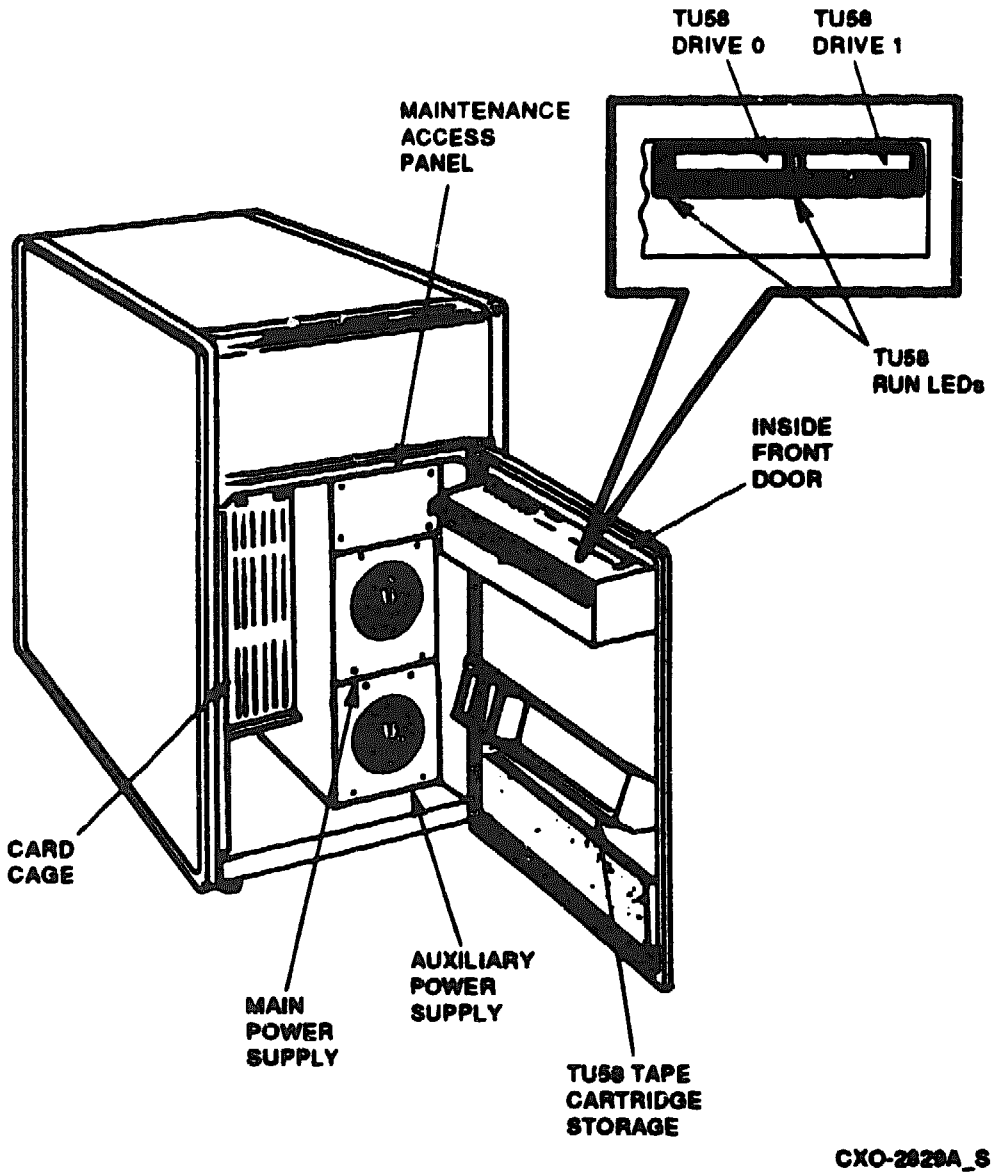


Figure 1–4 HSC50 Cabinet Inside Front View

The inside of the front door contains two TU58 tape drives and slots for tape storage. The HSC50 controller power supplies are housed under the maintenance access panel on the right side of the cabinet. A dc power on/off switch and connectors for the TU58 tape drive, the operator control panel (OCP), and the maintenance terminal port are located on this panel.

Power supply units are housed under the maintenance panel. A basic HSC50-AA/AB contains one power supply capable of providing power for three data channels. If more than three data channels are used, an auxiliary power supply is required. Each power supply has a fan drawing air from the front of the cabinet across the power unit and exhausting it through a rear duct. The card cage and backplane occupy the left side of the cabinet.

1.5.2 Rear View of Cabinet

The rear cabinet door is secured with a lock that requires a 5/32-inch hex key. The logic modules are cooled by a blower mounted behind the card cage. Air is drawn in through the front door louvers, up through the modules, and exhausted through the larger duct at the rear.

Two levels of cable connections are found in the HSC controller: backplane to bulkhead and bulkhead to outside the cabinet. All connections to the logic modules are made through the backplane. All cables attach to the backplane with press-on connectors.

The power controller is located in the lower left side the cabinet. The power control bus, delayed output line, and noise isolation filters are housed in the power controller.

Exterior CI, SDI, and STI buses are shielded up to the I/O cabling bulkhead at the rear of the HSC controller. These cables are attached to bulkhead connectors located at the bottom rear of the cabinet. The I/O cables are routed to the backplane from the I/O bulkhead connectors.

A rear view of the HSC controller cabinet with the back door open is shown in Figure 1–5.

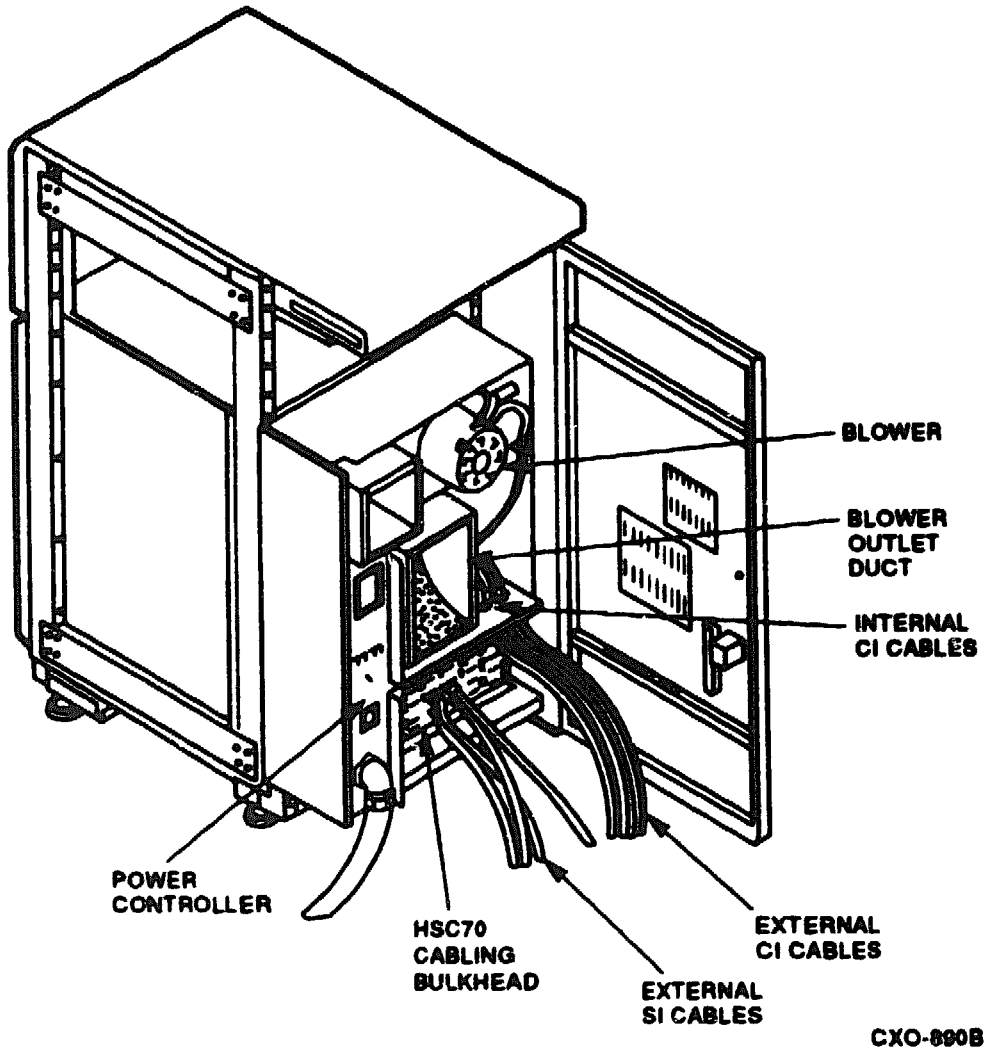


Figure 1–5 HSC Cabinet Inside Rear View

NOTE
Figure 1–5 shows the blower motor outlet duct for late production models. Earlier models have a smaller blower motor outlet duct.

Figure 1–6 shows the inside rear view of the HSC50 controller cabinet.

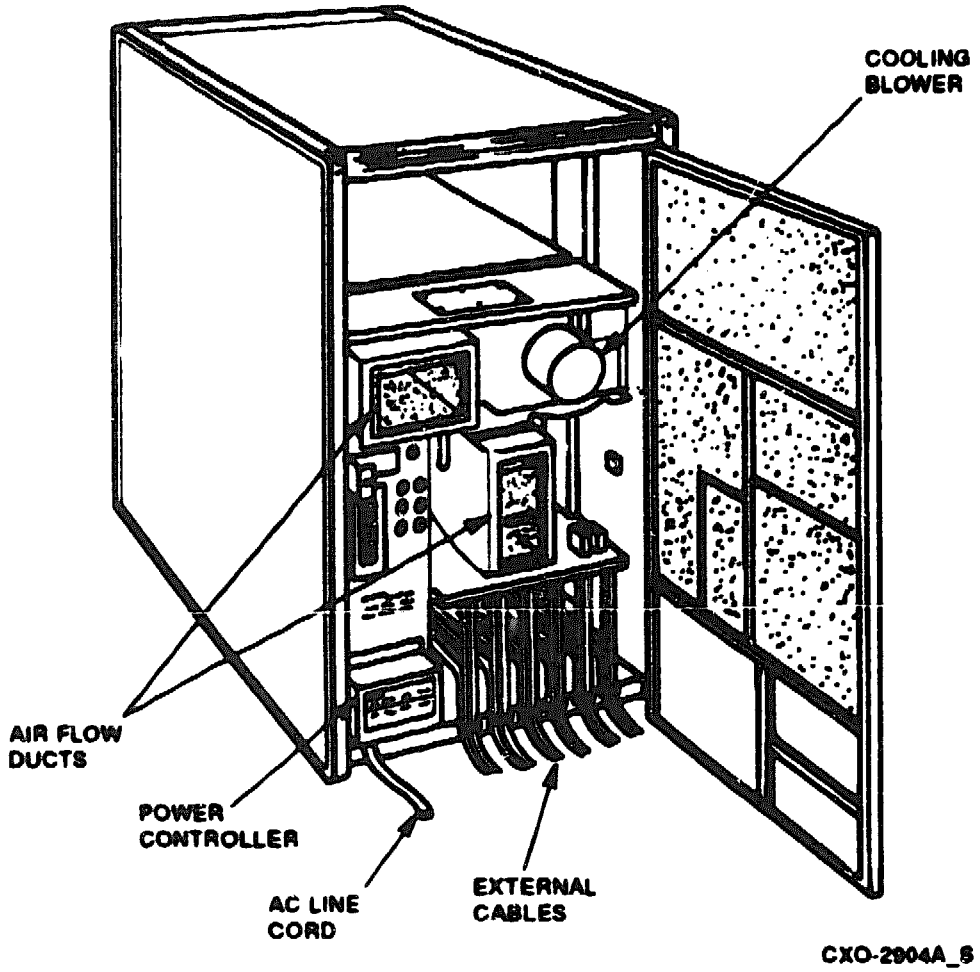


Figure 1–6 HSC50 Cabinet Inside Rear View

1.6 HSC Controller Module Card Cage

A 14-slot card cage with a corresponding backplane contains the set of L-series extended hex logic modules. The card cage occupies the left side of the cabinet. Above the card cage is a module utilization label indicating the slot location of each module.

1.6.1 HSC90 Controller Module Utilization Label

Figure 1–7 shows a typical HSC90 controller utilization label.

Slots 10, 9, 8, 7, 6, 5, 4, and 3 can be used for 4-port disk or tape data channels. Slots 9, 8, 7, and 6 can be used for 8-port disk data channels. Slot 11 can be used for the cache option. Appropriate labels are provided with each data channel option ordered.

Unused slots must contain an airflow baffle.

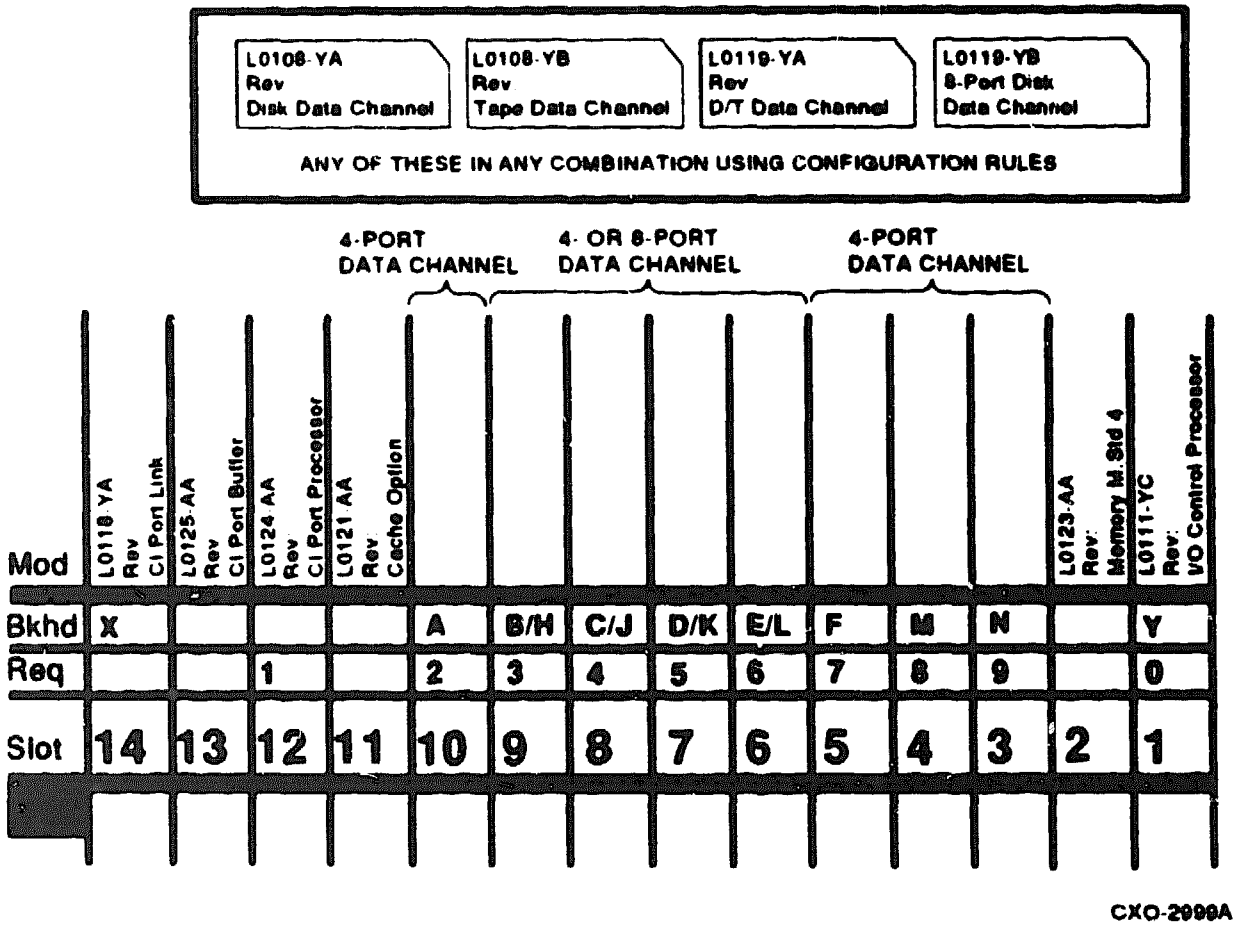


Figure 1–7 HSC90 Controller Module Utilization Label Example

1.6.2 HSC70 Controller Module Utilization Label

Figure 1–8 shows a typical HSC70 controller module utilization label.

Slots 10, 9, 8, 7, 6, 5, 4, and 3 can be used for 4-port disk or tape data channels. Slot 11 is unassigned and cannot be used. Appropriate labels are provided with each data channel option ordered.

Unassigned and unused slots must contain an airflow baffle.

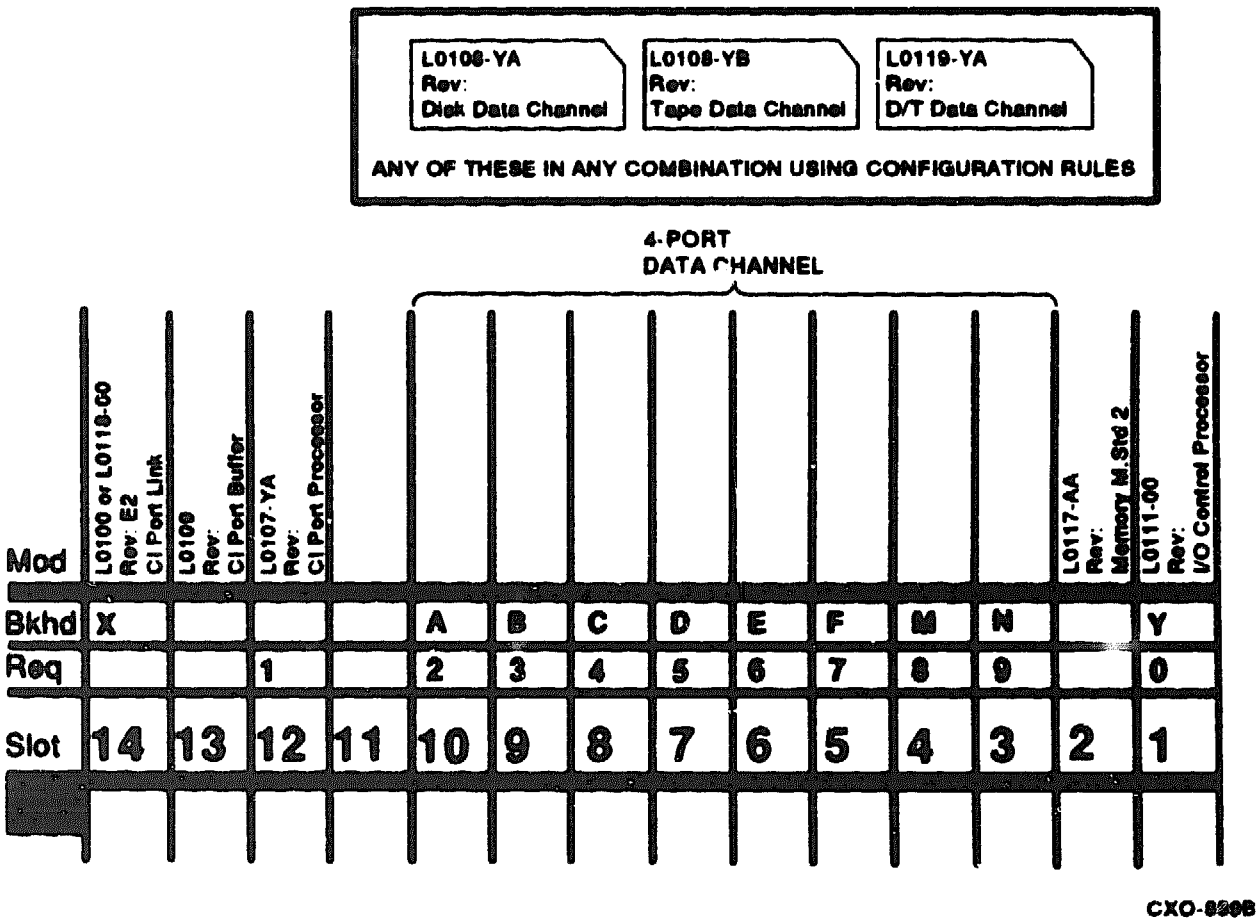


Figure 1–8 HSC70 Controller Module Utilization Label Example

1.6.3 HSC60 Controller Module Utilization Label

Figure 1–9 shows a typical HSC60 controller module utilization label.

Slots 10, 9, and 8 can be used for 4-port disk or tape data channels. Slots 9 and 8 can be used for 8-port disk data channels. Slots 11, 7, 6, 5, 4, and 3 are unassigned and cannot be used. Appropriate labels are provided with each data channel option ordered.

Unassigned and unused slots must contain an airflow baffle.

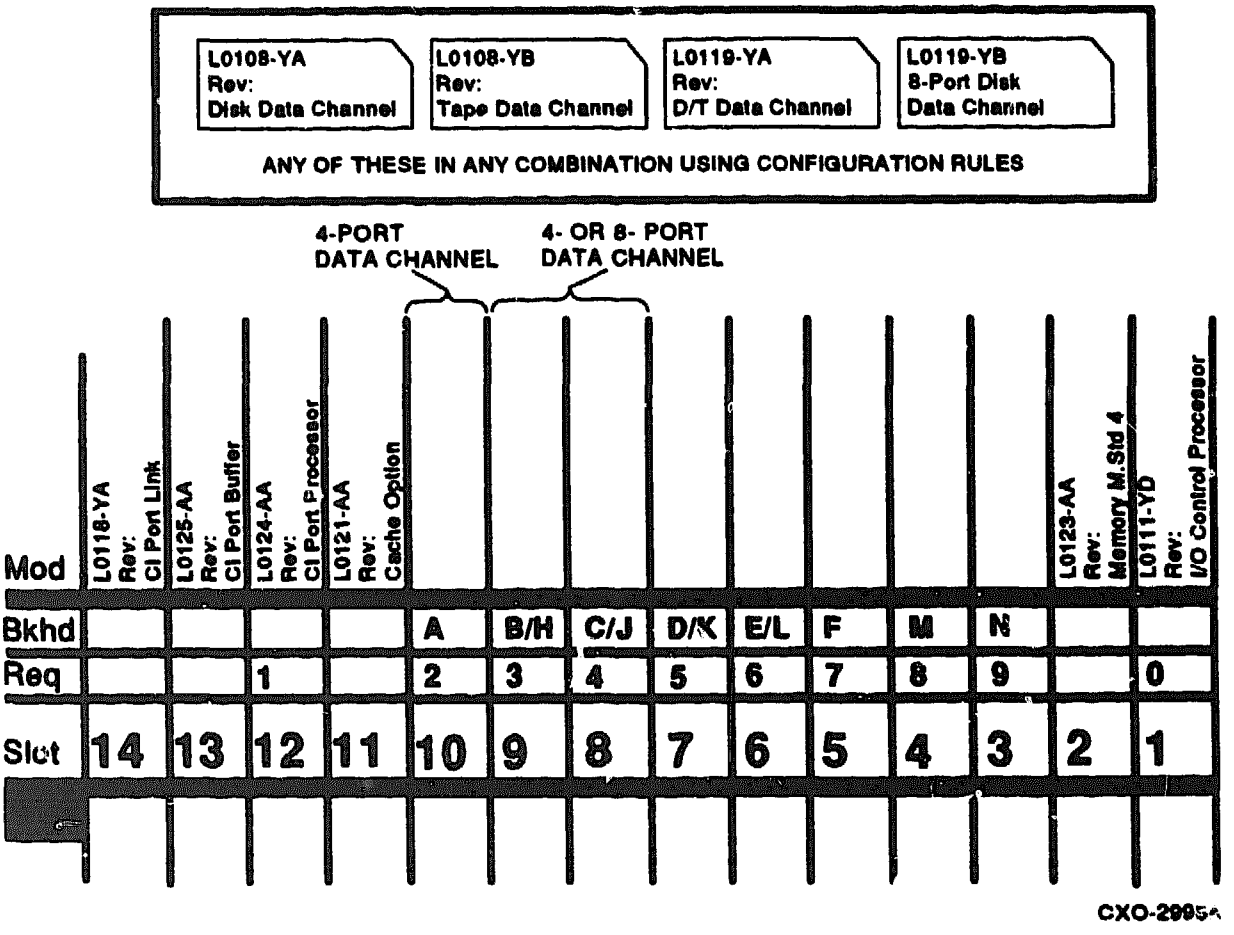


Figure 1–9 HSC60 Controller Module Utilization Label Example

1.6.4 HSC50 Controller Module Utilization Label

Figure 1–10 shows a typical HSC50 controller module utilization label.

Slots 10, 9, 8, 6, and 4 can be used for 4-port disk or tape data channels. Slots 11, 7, 5, and 3 are unassigned and cannot be used. Appropriate labels are provided with each data channel option ordered.

Unassigned and unused slots must contain an airflow baffle.

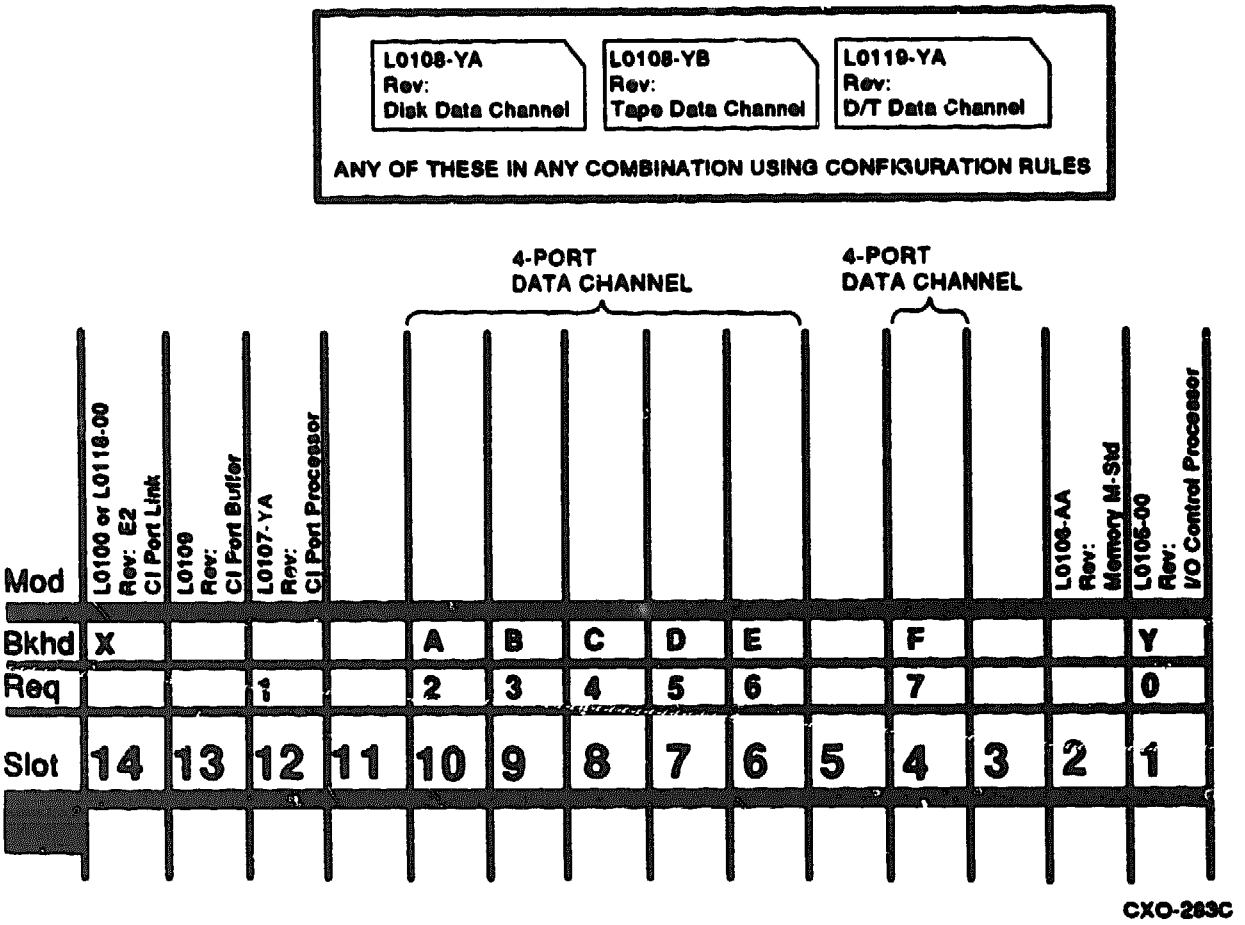


Figure 1–10 HSC50 Controller Module Utilization Label Example

1.6.5 HSC40 Controller Module Utilization Label

Figure 1–11 shows a typical HSC40 controller module utilization label.

Slots 10, 9, and 8 can be used for 4-port disk or tape data channels. Slots 11, 7, 6, 5, 4, and 3 are unassigned and cannot be used. Appropriate labels are provided with each data channel option ordered.

Unassigned and unused slots must contain an airflow baffle.

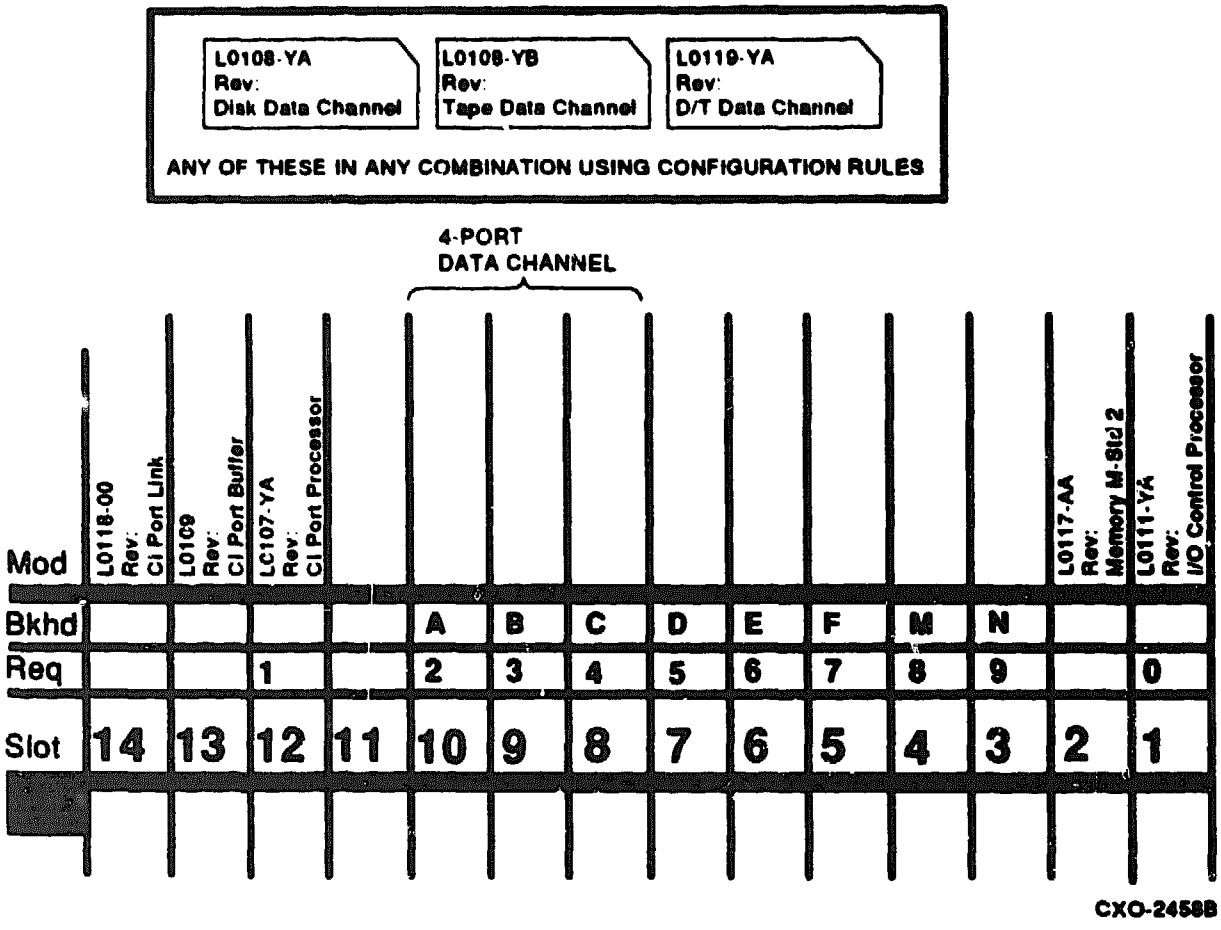


Figure 1–11 HSC40 Controller Module Utilization Label Example

1.7 External Interfaces

Figure 1–12 shows the external hardware interface lines used by the HSC controller. Figure 1–13 shows the external hardware interface lines used by the HSC50 controller.

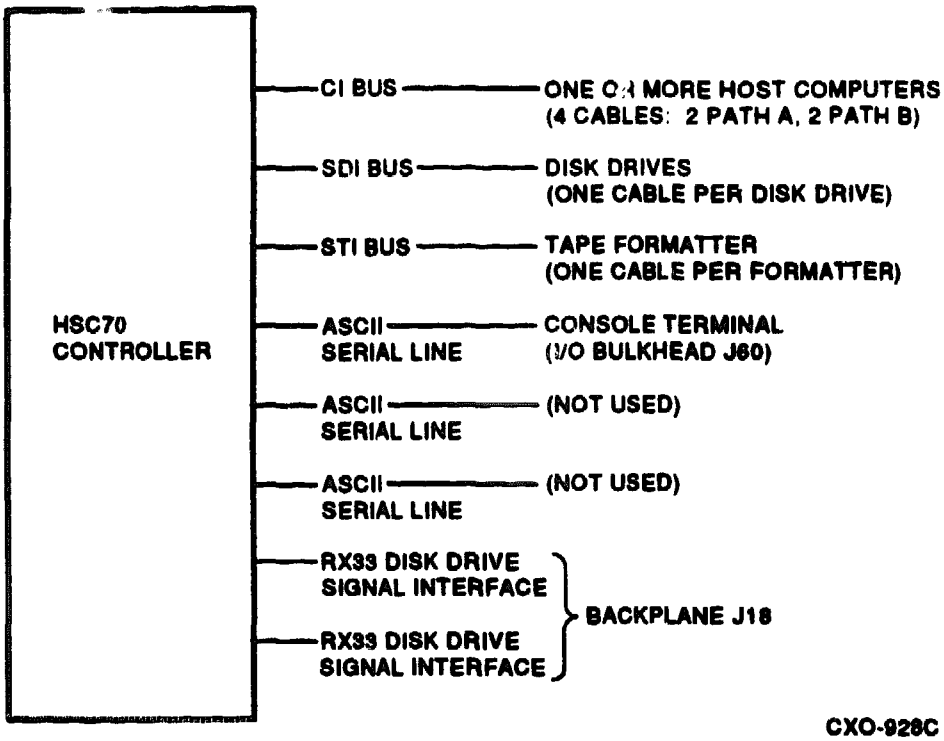


Figure 1–12 HSC Controller External Interfaces

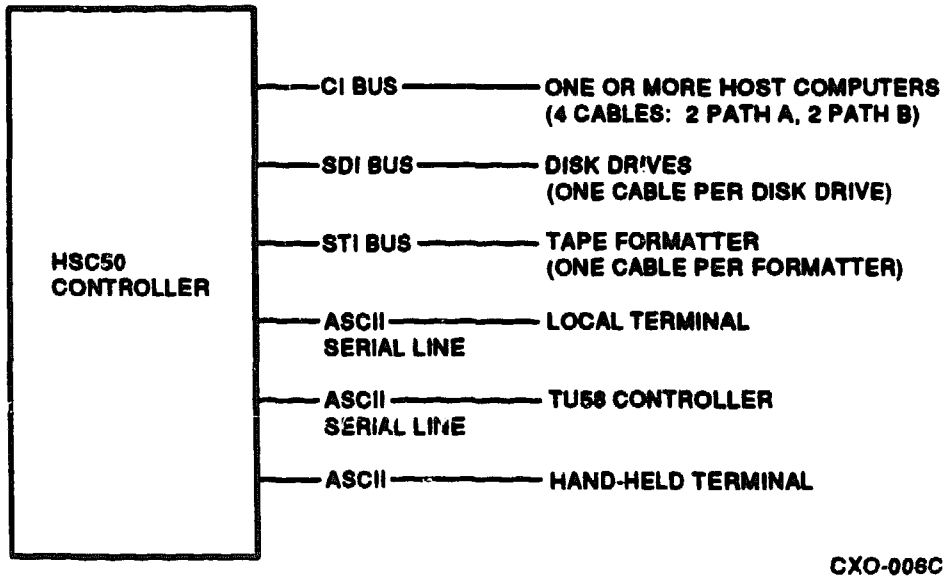


Figure 1–13 HSC50 Controller External Interfaces

The external hardware interface lines perform the following functions:

Line	Function
CI bus	Four coaxial cables (BNCIA-xx): two-path (path A and path B) serial bus with a transmit and receive cable in each path. This is the communication path between system host(s) and the HSC controller.
SDI bus	Four shielded wires for serial communication between the HSC controller and the disk drives (one SDI cable per drive per controller) (BC26V-xx).
STI bus	Four shielded wires for serial communication between the HSC controller and the tape formatter (one STI cable per formatter) (BC26V-xx).
ASCII serial line	RS-232-C cable for local console terminal communication with the I/O control processor module.
ASCII serial line	RS-232-C cable in the HSC50 controller to link the TU58 tape drive to the cabinet.
RX33 disk drive signal interface	Cable linking RX33 disk drives with the RX33 disk drive controller on the M.std2/M.std4 module of the HSC controller.

1.8 Hardware Overview

The HSC controller has an internal I/O processor module to control the I/O operations requested by the host(s) through the K.ci host interface. The I/O processor fetches its software instructions from a program memory (located on the memory module) through a program bus on the backplane.

A number of requestor modules in the HSC backplane function as disk or tape data channels. The maximum number of requestors in a given HSC installation depends on the HSC controller model.

There are two shared memories located on the memory module. One of these is the control memory. The controllers, as well as the I/O processor, access control memory through the control bus on the backplane and use it to exchange control information. The various software processes (in the controllers, as well as the I/O processor) communicate through software structures located in control memory.

The other shared memory is the data memory. The controllers, as well as the I/O processor, access data memory through the data bus on the backplane and use it primarily for buffering data between the data channel controllers and the host interface controller.

The HSC90 and HSC60 controllers can also have the 32-Mbyte cache M.cache module option. Figure 1–14 shows a block diagram of the HSC controller. Each major block is a module unless otherwise specified.

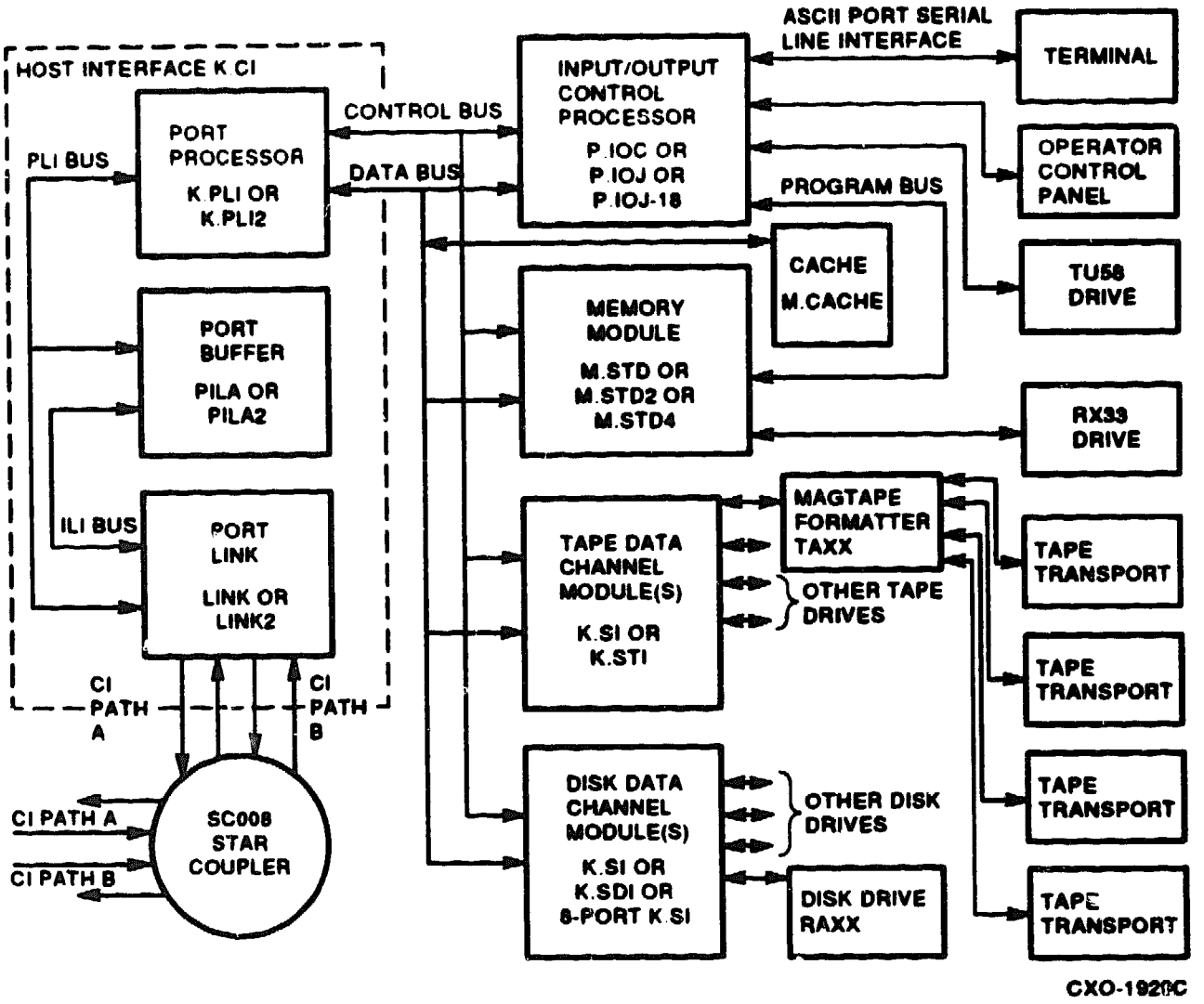


Figure 1–14 HSC Controller Block Diagram

1.8.1 I/O Control Processor Module (P.ioj/c) Functions

The I/O control processor provides the platform for an MSCP (Mass Storage Control Protocol) disk server, a TMSCP (Tape MSCP) tape server, a DUP (diagnostic utility protocol) server, and various utilities and diagnostics. The software is loaded from a local load media and stored in program memory. The software sets up many software structures in control memory that are used to communicate with the various K.xxx controllers.

The HSC50 controller uses the F–11 (PDP–11) chip set on the P.ioc (L0105) processor module, while the other HSC models use the a P.ioj module with a J–11 chip set. The following HSC controller models use various versions of the P.ioj module:

- The HSC90 controller uses the P.ioj–18 (L0111–YC)
- The HSC70 controller uses the P.ioj (L0111–00).
- The HSC60 controller uses the P.ioj–18 (L0111–YD).
- The HSC40 controller uses the P.ioj (L0111–YA).

All processor modules contain memory management and memory interfacing logic. These processors execute their respective internal software. The I/O control processor modules also contain the following functional blocks:

- Modified I/O page plus special registers for initialization and OCP communications
- Special control window logic similar to a memory management unit (MMU) to allow special access to control memory.
- Bootstrap read-only memory (ROM)
- Arbitration and control logic for the control and data buses
- Processes for all parity checking and generation for access to memory
- Program memory instruction and data cache, 8-Kbytes of direct map high-speed memory (except HSC50 controller)

The I/O control processor modules use the following hardware interfaces:

- Program memory through the backplane program memory bus
- Data memory through the backplane data bus
- Control memory through the backplane control bus
- Interrupt structure through the backplane control bus
- M.cache module memory through the backplane data bus
- Console terminal RS-423 compatible signal levels (except HSC50 controller)
- TU58 tape drives (HSC50 only)
- Auxiliary terminal through an RS-232-C interface (HSC50 only)

The I/O control processor uses software structures in control memory to communicate with processes in the K.xxx controllers.

1.8.2 Memory Module Functions

Three types of memory modules (M.std, M.std2, M.std4) are used in the different HSC models. The three memory modules differ primarily in memory size. The M.std4 module can be substituted for a M.std2 module. See Table 1–2 for a comparison.

The M.std2 and M.std4 modules provide physical board space for the RX33 controller, even though that controller is logically an I/O peripheral device, accessed as part of the I/O processor's I/O page. The RX33 controller was placed on the memory module for practical reasons and it is not logically part of memory.

When the M.cache module is installed, the data memory on the M.std4 module is not used and the data memory function is carried on the M.cache module.

Table 1–2 Memory modules

Engineering Designation	Module Designation	HSC Model	RX33 Controller	M.prog size	M.dat size	M.ctl size
M.std	L0106–AA	HSC50	No	256-KByte	128-Kbyte	128-Kbyte
M.std2	L0117–AA	HSC70, 40	Yes	1-Mbyte	512-Kbyte	256-Kbyte[1]
M.std4	L0123–AA	HSC90, 60	Yes	3-Mbyte	512-Kbyte	256-Kbyte[1]

[1]There are two redundant banks of control memory. During initialization, these are tested and one is selected for use. The other bank is unused.

CAUTION
The switch pack on the M.std2 and M.std4 modules controls timing parameters of the RX33 disk drive controller. Do not change the setting of this switch pack; this is a factory adjustment.

Each memory module contains three separate and independent memories, each accessed by separate and independent backplane buses. Onboard memory characteristics are as follows:

- **M.prog** (program memory) is a dynamic RAM accessed through the program bus by the I/O processor and the RX33 controller (for DMA data transfers) and is used for storage of software for the I/O control processor. Program memory cannot be accessed by the host interface or the data channels.
- **M.data** (data memory) is a static RAM accessed through the data bus by the host interface and data channels for storage of data being transferred between the host and the disk/tape units. Data memory can be accessed by the I/O processor, if needed by the software for error correction or storage of large messages.
- **M.ctl** (control memory) is a dynamic RAM accessed through the control bus by the host interface, data channels, and the I/O processor for exchange of control information and interprocess communication.

1.8.3 Port Link Module (LINK/LINK2) Functions

The port link module (L0100, L0118 or L0118–YA) is a part of the host interface module set (K.ci/K.ci2) and provides reception and transmission of communication packets from/to the CI bus. These separate functions are explained in the following paragraphs:

- As a receiver, the port link module monitors the signals on the CI. This module decouples the coax cable, detects carrier presence, decodes the Manchester-encoded signal, checks the serial bit stream for header and sync patterns, and monitors the packet header information. If the node address in the header matches the node address set in the switches on the port link module, the module accepts the packet as incoming information. If there is no match, the port link module ignores the packet.

  The incoming information (header and message body) is deserialized and passed to the port buffer module as 8-bit bytes. The cyclic redundancy check (CRC) frame is checked. If the CRC is correct and the port buffer module accepts the packet, the port link module returns an acknowledge (ACK) packet to the sender. If the CRC was correct, but the port buffer module is unable to accept the packet, the port link module returns a negative acknowledge (NAK) packet to the sender and requests a retry. The lack of either an ACK or a NAK tells the sender that either the CRC check failed or some other cause for unsuccessful transmission occurred. A retry is also requested for the packet.

- As a transmitter, the port link module monitors the signals on the CI, if waiting to transmit a packet. When there is a break in the communication, the port link module arbitrates for use of the CI. When the port link module wins the arbitration, it transmits the leader, sync, and header (including destination and source node addresses). The port link module then takes the 8-bit bytes from the port buffer module and converts them to serial, encodes them into Manchester encoding, and transmits them, forming the body of the packet. The port link module then generates and transmits the CRC as well as the trailer and awaits an ACK or a NAK from the receiver. It retries packet transmission if necessary.

The port link module communicates with the port buffer module and the port processor module over backplane internal link interconnect (ILI) and port/link interface (PLI) buses.

With all configuration switches and jumpers in default positions, the L0118 and L0118–YA modules are functionally identical with the L0100 module. The location and default positions are described in Chapter 3. The L0118-YA module is only supported in the HSC60 and HSC90 controllers.

1.8.4 Port Buffer Module (PILA/PILA2) Functions

The port buffer module (L0109 or L0125–AA) is a part of the host interface module set (K.ci/K.ci2). The port buffer module provides a limited number of high-speed buffers to accommodate the difference between the burst data rate of the CI bus and internal memory buses. It generates and checks byte parity for the buffer. The port buffer module communicates with the port link module through the ILI signals and the port processor module through PLI signals.

1.8.5 Port Processor Module (K.pli/K.pli2) Functions and Interfaces

The port processor module (L0107–YA or L0124–AA) is a part of the host interface module set and controls the flow of message and data packets being exchanged between the HSC controller and the host processor(s). It contains a microprocessor operating on microcode instructions. The port processor module performs the following functions:

- Communicates with the I/O control processor through shared software structures located in control memory and through an interrupt mechanism on the control bus
- Communicates with the host processor through messages over the CI and performs some low level functions for the host
- Executes and validates low-level CI protocol
- Moves command/message packets to/from the control memory and notifies the correct server process of incoming messages
- Moves data packets to/from the data memory
- Checks the byte parity of data taken out of the port buffer and ensures correct byte parity of data being stored in data memory for data being transferred from the CI to data memory
- Checks the byte parity of data taken out of the data memory and ensures correct byte parity of data being stored in port buffer for data being transferred from the data memory to the CI
- Generates the 16-bit error detection code (EDC) attached to each 512-byte data buffer for data being transferred from the CI to data memory
- Checks the 16-bit EDC attached to each 512-byte data buffer for data being transferred from the data memory to the CI

The port processor module connects to three buses:

- PLI bus—interfaces the port buffer and port link modules
- Control memory bus—interfaces the control memory
- Data memory bus—interfaces the data memory and M.cache memory modules

1.8.6 Disk Data Channel Module (K.sdi) Functions

The disk data channel module (L0108–YA) operation is controlled by an onboard microprocessor using microcode instructions stored in an onboard ROM. The basic functions of this controller are to analyze software structures set up in the control memory by the I/O processor and perform the function requested. These functions involve communication with the disk drives and transferring data between the disk drives and the data memory.

The data channel module performs the following functions:

- Transmits control and status information to the disk drives.
- Monitors real-time status information from the disk drives.
- Monitors in real-time the rotational position of all the disk drives attached to it.
- Transmits data between data memory and the disk drives.
- Checks the EDC and generates the error correction code (ECC) for data being transferred to the disk. The ECC is appended to the data and the EDC.
- Checks and strips the ECC and verifies the EDC for data being transferred from the disk.

Commands and responses pass between the disk data channel microprocessor, the I/O processor, and the K.ci through software structures located in control memory. The disk data channel module also connects to the data memory and to the four disk drives with four individual SDI buses. Table 1–1 shows the maximum disk or tape drive combinations of the various HSC controller models. Configuration guidelines can also be found in the *HSC Controller Installation Manual*.

The K.sdi module does not support the enhanced performance ESE20 storage element; these units require either a 4-port or 8-port K.si module. For support of the TA90 and TA91 tape drives, you must have a 4-port K.si module configured as a tape data channel.

1.8.7 Tape Data Channel Module (K.sti) Functions

The tape data channel module (L0108–YB) operation is essentially the same as the disk data channel except that it communicates with a tape formatter over an STI bus (slightly different) and sends/checks a 16-bit EDC at every 512-byte boundary (plus last portion thereof) of the data stream. The K.sti does not perform ECC.

1.8.8 4-Port Data Channel Module (K.si) Functions

The 4-port data channel module (L0119–YA) is similar in function to the K.sdi or K.sti. It is capable of handling either disk or tape (not both) and requires loading of appropriate disk or tape microcode from the HSC software load media.

1.8.9 8-Port Data Channel Module (8-port K.si) Functions

The 8-port data channel module (L0119–YB) is a disk data channel similar in function to a K.sdi or K.si, except it handles eight SDI ports, and cannot be configured for a tape data channel.

1.8.10 32-Mbyte Cache Option (M.cache)

The optional HSC60/HSC90 controller **cache memory** module (L0121–AA, M.cache) contains 32 MB of dynamic error correction code (ECC) memory used as a disk cache for any disks attached to the HSC controller. The M.cache module also contains 512 KB of dual-ported data memory. Other features of the M.cache module include:

- Single-bit error correction and double-bit error detection for cache memory.
- High-speed state machine logic to move data between cache data memory and cache memory.
- High-speed self-test of all cache data memory and cache memory upon power-up.

The M.cache module must be used with the M.std4 memory module.

When the M.cache option is installed, the data memory on the M.std4 module is disabled and the data memory residing on the M.cache module is enabled. The M.cache module occupies card cage slot 11.

1.9 HSC Controller Software Overview

The HSC controller uses internal software to perform various tasks and to communicate with an operator through a dedicated terminal. The *HSC Software Release Notes* for your version of software describes the unique features of the software. These software release notes are shipped with each HSC controller, and with updates of the software. The major HSC controller software modules are shown at a block level in Figure 1–15.

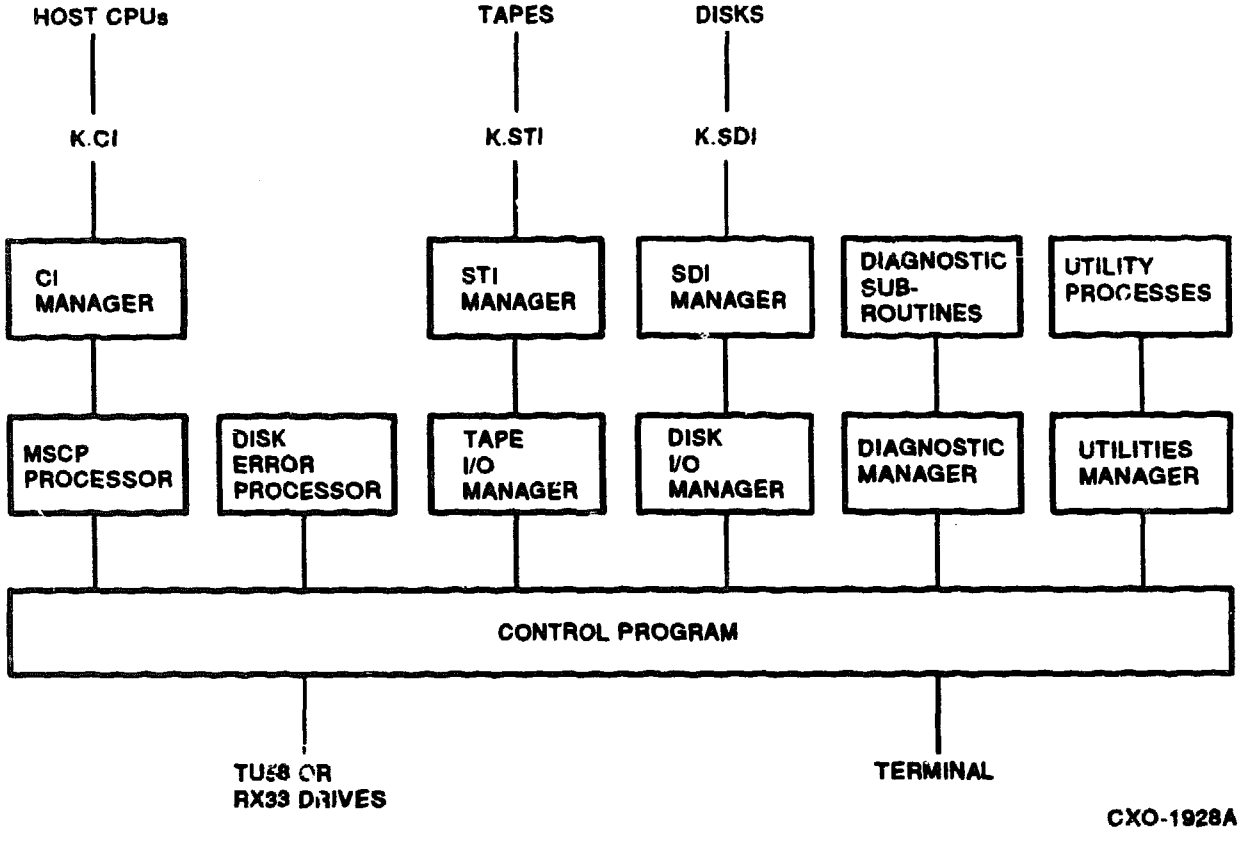


Figure 1–15 HSC Controller Internal Software

The HSC control program is found on the system diskette for the HSC controller and the system tape for the HSC50 controller. This software module is the lowest level manager and provides a set of subroutines and services shared by all processes. The control program performs the following functions:

- Interprets incoming utility requests
- Sets up the appropriate environment for operation of the requested utility
- Invokes the utility process
- Returns to its normal environment upon completion of the utility execution
- Initializes and reinitializes
- Executes all auxiliary terminal I/O

- Schedules processes (both functional and diagnostic) for execution by the I/O control processor module
- Provides a set of system services and system subroutines to processes
- Manages the RX33 disk drive local storage media (HSC only)
- Manages the TU58 tape drive local storage media (HSC50 only)

Functional processes within the HSC controller communicate with each other and the control program through shared data structures and send/receive messages.

The MSCP class server validates, interprets, and routes incoming MSCP commands and dispatches MSCP completion acknowledgments. The following are part of the MSCP class server:

- **SDI manager**—handles the SDI protocol, responds to attention conditions, and manages the online/offline status of the disk drives.
- **Disk I/O manager**—translates logical disk addresses into drive-specific physical addresses, organizes the data-transfer structures for disk operations, and manages the physical positioning of the disk heads.

The CI manager handles virtual circuit and server connection activities.

The disk error processor responds to all detected error conditions. It reports errors to the diagnostic manager and attempts to recover from errors, such as ECC, bad block replacement, and retries. When recovery is not possible, a diagnostic is run to determine if the HSC controller can function without the failing resource. Then, appropriate action is taken to remove the failing resource or to terminate operation.

The TMSCP class server sets up the data transfer structures for tape operations and manages the physical positioning of the tape. The STI manager is the part of the TMSCP class server that handles the STI protocol, responds to attention conditions, and manages the online/offline status of the tape drives.

The diagnostic manager handles all diagnostic requests, error reporting, and error logging. It also provides decision-making and diagnostic-sequencing functions, and can access a large set of resource-specific diagnostic subroutines.

The diagnostic subroutines run under the control of the diagnostic manager and are classified as device integrity tests.

The utility processes perform volume-management functions such as formatting, disk-to-disk copy, disk-to-tape copy, tape-to-disk restore. These processes also handle miscellaneous operations required for modifying controller parameters, such as COPY, PATCH, and error dump, and are used in analyzing controller problems.

1.10 Maintenance Strategy

Maintenance of the HSC controller is accomplished with field replaceable units (FRUs). Procedures for removal and replacement are described in Chapter 3. Do not attempt to replace or repair component parts within FRUs.

Solid failures can be efficiently isolated due to the logical partitioning of the modules and extensive internal diagnostics. In addition to the device-resident diagnostics, the HSC controller-resident offline diagnostics are available to support and verify corrective maintenance decisions.

1.10.1 Maintenance Features

The following features assist in troubleshooting the HSC controller:

- **Self-contained and self-initiated diagnostics**—On initialization, various levels of diagnostics execute in the HSC controller. Read-only memory (ROM) diagnostics test each microprocessor in the disk and tape data channels, port processor, and I/O processor modules. Pressing the Init button starts all internal ROM diagnostics.
- **OCP fault code display**—The OCP or the console terminal displays any failures. If further diagnostics are needed, use the terminal to initiate diagnostics stored on the system boot media or the offline diagnostic media.
- **Console terminal**—The console terminal is used for housekeeping functions such as changing requestor configurations, using the SET/SHOW commands to examine or set configuration parameters, and running online device integrity tests or offline diagnostic tests. The console terminal also displays error and crash messages.
- **Module LED indicators**—All logic modules have at least one LED to indicate board status. See Chapter 2 for the location of these LEDs.

The HSC controller allows logical assignment of a disk drive or tape formatter to the diagnostics. Device integrity tests allow drive diagnosis, even though other active drives are connected to the HSC controller.

Background (periodic) diagnostics test HSC controller logic not currently in use by the HSC controller. Failures cause a reboot and the initialization diagnostics will execute.

Requestor-detected data memory errors initiate the in-line memory diagnostics to test the buffer causing the error. Failures found in any data buffer cause removal of that buffer from service. If no failure is found, the tested buffer is returned to service. If the same buffer is sent to test twice, it is retired from service, even though no failure is found.

1.11 Specifications

Figure 1–16 lists the HSC controller physical and environmental specifications for models using single-phase ac power.

Figure 1–17 lists the HSC controller physical and environmental specifications for models using three-phase ac power (881 power controller).

Refer to Section 2.7 for a description of these power controllers. Section 2.7 also contains a listing of line cord options for the HSCxx-BB power controller (using 50 Hz 220/240 Vac input power).

DESCRIPTION	OPTION DESIGNATION
HSC MASS STORAGE SERVER WITH HSC POWER CONTROLLER	HSCXX-BA = 60 HZ, 100/120 V
	HSCXX-BB = 50 HZ, 220/240 V

MECHANICAL

MOUNTING CODE	WEIGHT		HEIGHT		WIDTH		DEPTH		CAB TYPE (IF USED)
	LBS	KG	IN	CM	IN	CM	IN	CM	
FS	450	240.0	41.1	105.9	21.3	54.0	35.0	91.4	MODIFIED H9642

POWER (AC)

AC VOLTAGE NOMINAL	AC VOLTAGE TOLERANCE	FREQUENCY AND TOLERANCE	PHASE	STEADY-STATE CURRENT (RMS)	POWER CONSUMPTION (MAX)
100/120	90 - 132	60 HZ ± 3	1	22.5A	1846 WATTS
220/240	174 - 264	50 HZ ± 3	1	12.2A	1846 WATTS

POWER (AC)

PLUG TYPE	POWER CORD LENGTH	INTERRUPT TOLERANCE	APPARENT POWER (KVA)
NEMA - L5 - 30P	15 FT (4.5 M)	4 MS (MIN)	1.5 (KVA)
IEC 320 - C20*	15 FT (4.5 M)	4 MS (MIN)	1.7 (KVA)

POWER (AC)

HSC OPTION	INRUSH CURRENT	SURGE DURATION
HSCXX - BA	140 AMPS	16 MS
HSCXX - BB	140 AMPS	20 MS

DEVICE ENVIRONMENT

TEMPERATURE		RELATIVE HUMIDITY		RATE OF CHANGE		HEAT DISSIPATION	
OPERATING**	STORAGE	OPERATING	STORAGE	TEMP	HUMIDITY	60 HZ	50 HZ
59 - 90° F	40 - 151° F	20 - 80%	5 - 95%	20° F/HR	20%/HR	1588 BTU/HR	1656 KJ/HR
15 - 32° C	40 - 66° C			11° C/HR			

DEVICE ENVIRONMENT

ALTITUDE (MAX) **		AIR VOLUME (AT INLET)		AIR QUALITY
OPERATING	STORAGE	FT^3/MIN	M^3/MIN	PARTICLE COUNT (MAX)
8000 FT	30,000 FT	210	5.92	N/A
2.4 KM	9.1 KM			

* HSCXX-BB HAS INLET FOR REMOVABLE LINE CORD OPTIONS.

**ALTITUDE CHANGES: DERATE THE MAXIMUM TEMPERATURE 1.8° C PER THOUSAND METERS (1.0° F PER THOUSAND FEET).

CXO-3135A

Figure 1–16 Specifications for HSC Controllers Using Single-Phase AC Power

DESCRIPTION	OPTION DESIGNATION
HSC MASS STORAGE SERVER WITH 881 POWER CONTROLLER	HSCXX-AA = 60 HZ, 120/180 V
	HSCXX-AB = 50 HZ, 380/415 V

MECHANICAL

MOUNTING CODE	WEIGHT		HEIGHT		WIDTH		DEPTH		CAB TYPE (IF USED)
	LBS	KG	IN	CM	IN	CM	IN	CM	
FS	450	240.0	41.1	105.9	21.3	54.0	35.0	91.4	MODIFIED H9642

POWER (AC) (881 POWER CONTROLLER)

AC VOLTAGE NOMINAL	AC VOLTAGE TOLERANCE	FREQUENCY AND TOLERANCE	PHASE	STEADY-STATE CURRENT (RMS)	POWER CONSUMPTION (MAX)
120/208	90-132/155-228	60 HZ ± 3	3	N/A	2250 WATTS
220-240/330-415	174-264/301-457	50 HZ ± 3	3	N/A	2245 WATTS

POWER (AC) (881 POWER CONTROLLER)

AMP (MAX) BY PHASE			
120 V	PHASE A = 1	380 V	PHASE A = 1
	PHASE B = 12		PHASE B = 7
	PHASE C = 12		PHASE C = 7
	NEUTRAL = 17		NEUTRAL = 9

POWER (AC)

PLUG TYPE	POWER CORD LENGTH	INTERRUPT TOLERANCE	APPARENT POWER (KVA)
NEMA - L21 - 30P	15 FT (4.5 M)	4 MS (MIN)	3.4 (KVA)
HUBBELL - 520 P6	15 FT (4.5 M)	4 MS (MIN)	3.4 (KVA)

POWER (AC)

HSC OPTION	INRUSH CURRENT	SURGE DURATION
HSCXX - AA	70 AMPS/PHASE	16 MS
HSCXX - AB	70 AMPS/PHASE	20 MS

DEVICE ENVIRONMENT

TEMPERATURE		RELATIVE HUMIDITY		RATE OF CHANGE		HEAT DISSIPATION	
OPERATING*	STORAGE	OPERATING	STORAGE	TEMP	HUMIDITY	60 HZ	50 HZ
59 - 90° F	.40 - 151° F	20 - 80%	5 - 95%	20° F/HR	20%/HR	7676 BTU/HR	8078 KJ/HR
15 - 32° C	.40 - 66° C			11° C/HR			

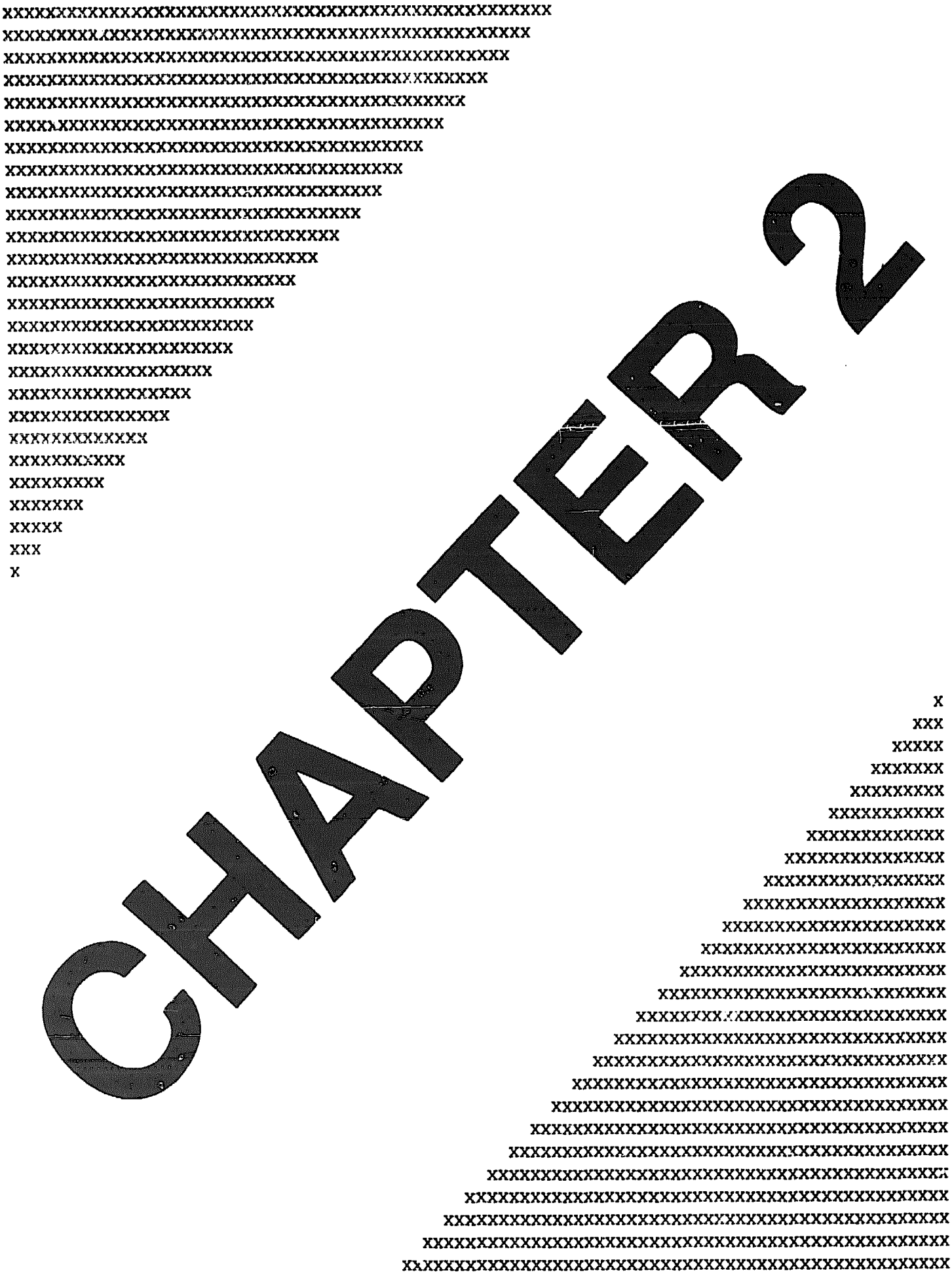
DEVICE ENVIRONMENT

ALTITUDE (MAX) *		AIR VOLUME (AT INLET)		AIR QUALITY
OPERATING	STORAGE	FT^3/MIN	M^3/MIN	PARTICLE COUNT (MAX)
8000 FT	30,000 FT	210	5.92	N/A
2.4 KM	9.1 KM			

*ALTITUDE CHANGES: DERATE THE MAXIMUM TEMPERATURE 1.8° C PER THOUSAND METERS (1.0° F PER THOUSAND FEET).

CXO-3136A

Figure 1–17 Specifications for HSC Controllers Using Three-Phase AC Power


CHAPTER 2

2
Controls and Indicators

2.1 Introduction

This chapter describes the following controls and indicators located in the various areas of the HSC controller:

- Operator control panel (OCP)
- Inside front door
- RX33 disk drives
- TU58 tape drives (HSC50)
- Maintenance access panel (HSC50)
- Logic modules
- Power controllers (60 Hz and 50 Hz)

2.2 Operator Control Panel (OCP)

Figure 2–1 shows the indicators and switches on the OCP. Table 2–1 explains their functions. Figure 2–2 lists the OCP fault code display indications. Refer to Chapter 8 for detailed information on interpreting these fault codes.

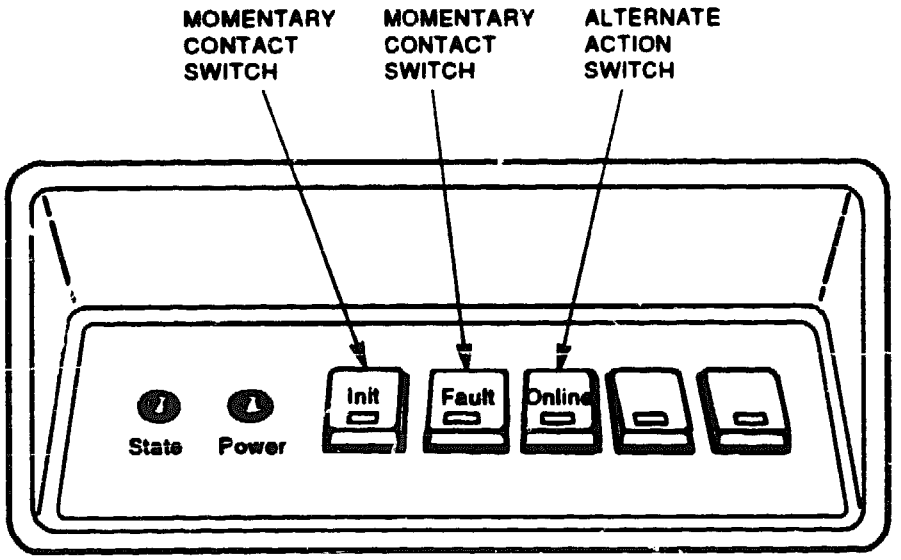


Figure 2–1 Operator Control Panel

Table 2–1 OCP Indicators And Switches

Name	Item	Function
STATE	Indicator	HSC software blinks this indicator during normal operation.
POWER	Indicator	Lit to indicate that dc voltages are present, as determined by a circuit on the P.ioc/j module. This does not mean the voltages are within specs. This indicator also monitors the Power Fail signal from the power supplies and goes out for power fail.
INIT	Indicator	Indicates initialization is in progress.
INIT	Switch	Pushing and releasing this momentary-contact switch clears the HSC controller and starts the initialization process, including rebooting. Holding this switch in provides a loopback for the terminal.
FAULT	Indicator	Indicates a fault. If it is a hard (fatal) fault, the state indicator will not flash, but will be on or off depending on the fault. Depressing and releasing the switch causes a fault code to be displayed in the OCP indicators. If it is a soft (non-fatal) fault, the indicator will be on and the state indicator will continue to flash. Depressing and releasing the switch causes a fault code to be displayed. If there is more than one soft error, continued depressing and releasing of the switch causes the queued fault codes to be displayed.

Table 2–1 (Cont.) OCP Indicators And Switches

Name	Item	Function
FAULT	Switch	Depressing and releasing this momentary-contact switch causes the fault code to be displayed. (See explanation in description of FAULT indicator above.) Holding this switch in provides a lamp test of the OCP indicators, without affecting operation of the HSC controller.
ONLINE	Indicator	Indicates there is at least one virtual circuit (software relationship) established between the HSC controller and a host processor.
ONLINE	Switch	When this alternate-action switch is in, the HSC controller will allow a host to open a virtual circuit with the HSC. When it is out, the HSC controller will not allow any more virtual circuits to be opened, but will not close any that are already established.
BLANK	Indicators (2)	Unused, except as part of fault code display.
BLANK	Switches (2)	Unused.

DESCRIPTION	HEX	OCT	BINARY	OCP INDICATORS				
				INIT	FAULT	ONLINE		
K PLI/K PLI2 ERROR	01	01	00001	OFF	OFF	OFF	OFF	ON
K.SDI/K SI INCORRECT VERSION OF MICROCODE	02	02	00010	OFF	OFF	OFF	ON	OFF
K.STI/K SI INCORRECT VERSION OF MICROCODE	03	03	00011	OFF	OFF	OFF	ON	ON
P IOJ CACHE FAILURE[1]	08	10	01000	OFF	ON	OFF	OFF	OFF
K CI FAILURE[1]	09	11	01001	OFF	ON	OFF	OFF	ON
DATA CHANNEL MODULE ERROR[1]	0A	12	01010	OFF	ON	OFF	ON	OFF
P IOJ/C MODULE FAILURE	11	21	10001	ON	OFF	OFF	OFF	ON
M.STD2/M STD4 MODULE FAILURE[4]	12	22	10010	ON	OFF	OFF	ON	OFF
BOOT DEVICE FAILURE[2]	13	23	10011	ON	OFF	OFF	ON	ON
PORT LINK NODE ADDRESS SWITCHES OUT OF RANGE	15	25	10101	ON	OFF	ON	OFF	ON
MISSING FILES REQUIRED[3]	16	26	10110	ON	OFF	ON	ON	OFF
NO WORKING K.CI, K.SDI, K.STI, OR K SI IN SUBSYSTEM	18	30	11000	ON	ON	OFF	OFF	OFF
INITIALIZATION FAILURE	19	31	11001	ON	ON	OFF	OFF	ON
SOFTWARE INCONSISTENCY	1A	32	11010	ON	ON	OFF	ON	OFF
ILLEGAL CONFIGURATION[5]	1B	33	11011	ON	ON	OFF	ON	ON

1. THESE ARE TERMED SOFT OR NONFATAL ERRORS.
2. POSSIBLE MEMORY MODULE/CONTROLLER (EXCEPT ON THE HSC50 CONTROLLER).
3. THIS FAULT CODE WILL ALSO BE DISPLAYED IF THE P.IOC MODULE IS NOT AT THE MINIMUM REVISION LEVEL.
4. SWAP MEMORY MODULE FIRST. IF PROBLEM PERSISTS, TRY REPLACING THE P.IOJ/C MODULE.
5. REFER TO TABLE 1-1 AND CHECK PROPER MODULE CONFIGURATION.

CXO-3133A

Figure 2–2 Operator Control Panel Fault Codes

2.3 HSC Controller Inside Front Controls and Indicators

The controls and indicators located inside the front door of the HSC controller, other than HSC50 controller, are shown in Figure 2–3 and explained in Table 2–2.

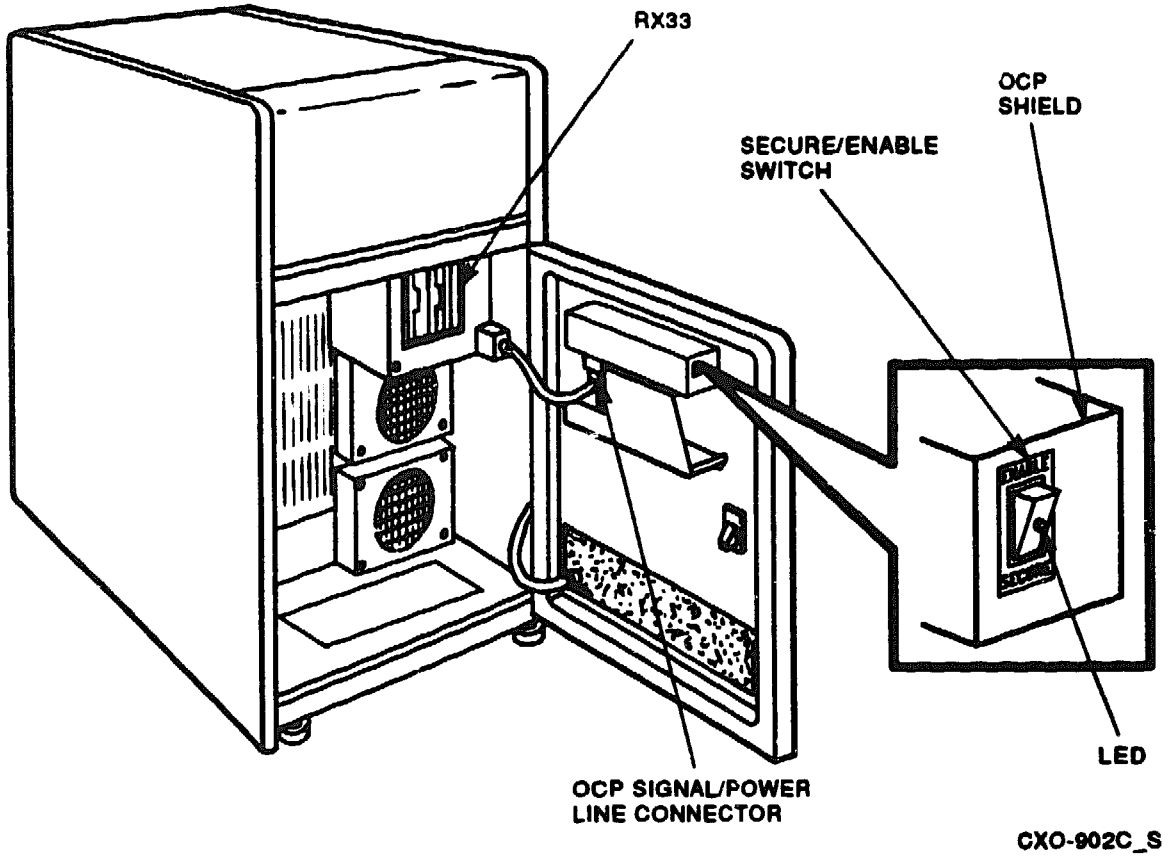


Figure 2–3 HSC Controller Inside Front Door Controls/Indicators

Table 2–2 Inside Front Door Indicators and Switches (HSC)

Name	Item	Function
Secure/ Enable	Switch	When in the SECURE position, this switch disables the Init switch on the OCP and the SETSHO utility SET commands. Otherwise, these functions are permitted.
Enable	Indicator	Indicates position of the Secure/Enable switch.
RX33	Indicators	Indicates drive in use.
DC power	Switch	When in the 0 position, it removes dc power from the HSC logic so modules can be replaced.

2.4 HSC50 Controller Inside Front Door Controls and Indicators

The controls and indicators located inside the front door of the HSC50 controller are shown in Figure 2–4 and explained in Table 2–3.

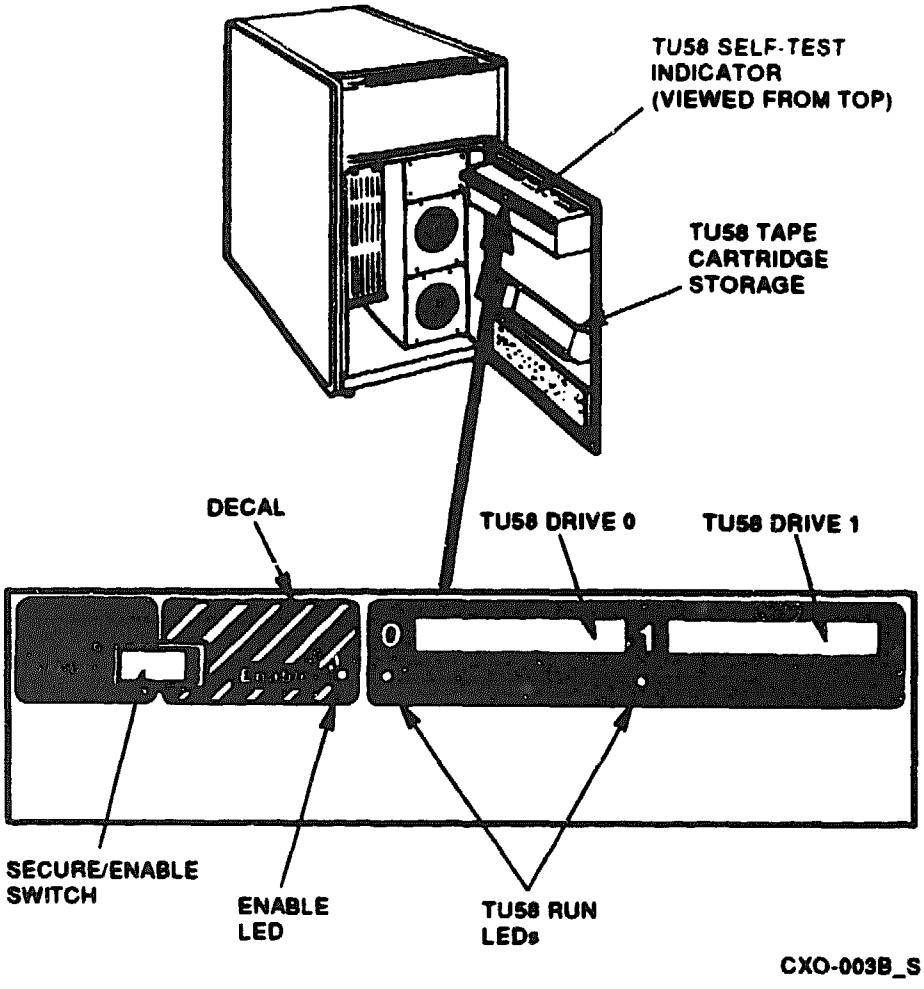


Figure 2–4 HSC50 Controller Inside Front Door Controls and Indicators

Table 2–3 Inside Front Door Indicators and Switches (HSC50)

Name	Item	Function
Secure/ Enable	Switch	When in the secure position, this switch disables the Init switch on the OCP and the SETSHO utility SET commands. Otherwise, these functions are permitted.
Enable	Indicator	Indicates position of the Secure/Enable switch.
TU58 Run	Indicators	Indicates tape in motion.
TU58 self-test	Indicator	Indicates TU58 controller has passed self-test.
DC power	Switch	When in the 0 position, it removes dc power from the HSC logic so modules can be replaced.

2.5 Logic Module Indicators

All logic modules have at least one indicator to show board status. Additionally, three of these logic modules contain specific switches. Figure 2–5 shows the location of the LEDs and Table 2–4 explains the functions of these LEDs. Refer to Chapter 8 for information on troubleshooting the HSC controller using the module LEDs.

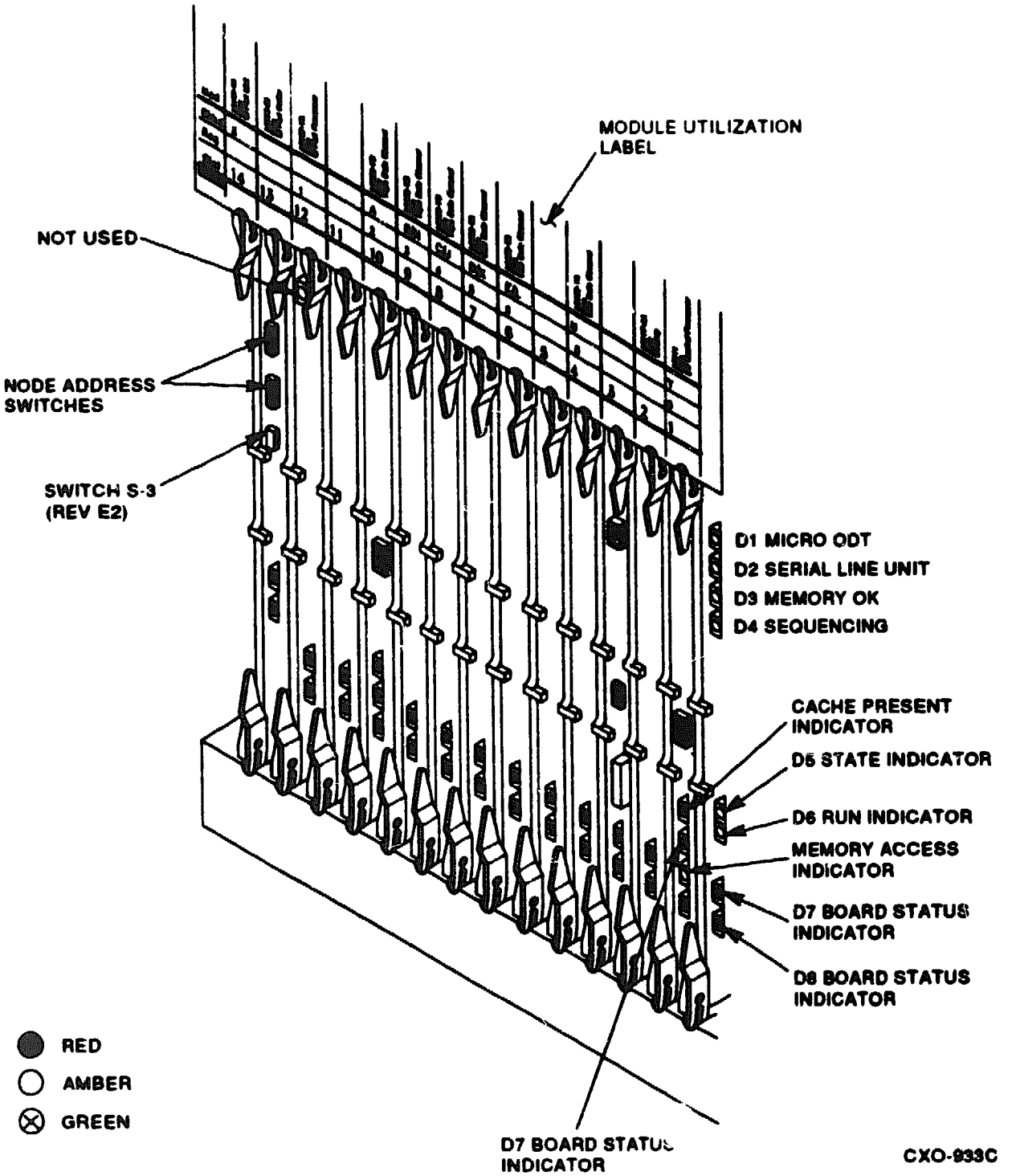


Figure 2–5 Logic Module LED Indicators

Table 2–4 Logic Module LEDs

Module	Color	Function
LINK (L0100) LINK (L0118–00) LINK2 (L0118–YA)	Green Red	Local CI activity Internal maintenance mode
PILA (L0109) PILA2 (L0125)	Green Red Amber	Passed initialization tests Failed initialization tests Always lit (test LED for Engineering)
K.pli (L0107–YA) K.pli2 (L0124–AA)	Green Red	Passed initialization tests Failed initialization tests
K.pli2 only	Amber (upper) Amber Amber Amber Amber Amber Amber Amber	 Parity LED 6 Parity LED 5 Parity LED 4 Parity LED 3 Parity LED 2 Parity LED 1 Parity LED 0
K.sdi (L0108–YA) K.sti (L0108–YB) K.si 4-port (L0119–YA) K.si 8-port (L0119–YB)	Green Red	Passed initialization tests Failed initialization tests
K.si only	Amber (upper) Amber Amber Amber Amber Amber Amber Amber	D1—Off for PROM load, on for RAM load. D2—Parity LED 6 D3—Parity LED 5 D4—Parity LED 4 D5—Parity LED 3 D6—Parity LED 2 D7—Parity LED 1 D8—Parity LED 0
M.std (L0106–AA)	Green	Memory activity
M.std2 (L0117–AA) M.std4 (L0123–AA)	Amber Red Green Amber	Memory activity Failed initialization tests Passed initialization tests M.cache module present (M.std4 only)
M.std4 only	Amber (upper) Amber Amber Amber Amber Amber Amber Amber	D1—Single bit error D2—Multiple bit error D3—High-byte parity error D4—Low-byte parity error D5—NIB3 error D6—NIB2 error D7—NIB1 error D8—NIB0 error

Table 2–4 (Cont.) Logic Module LEDs

Module	Color	Function
P.ioc (L0106–00)	Amber (upper)	State indicator
	Amber	Processor clock
	Red	Failed initialization tests
	Green	Passed initialization tests
P.ioj (L0111–00)	Amber (upper)	D1—J–11 power-up test or micro ODT mode
P.ioj (L0111–YA)	Amber	D2—J–11 power-up test
P.ioj (L0111–YC)	Amber	D3—J–11 power-up test
P.ioj (L0111–YD)	Amber	D4—J–11 power-up test
	Amber	D5—State indicator
	Amber	D6—Processor clock
	Red	D7—Failed initialization tests
	Green	D8—Passed initialization tests
M.cache (L0121–AA)	Green	Passed initialization tests
	Amber	Initialization tests in progress
	Red	Failed initialization tests
	Amber (upper)	D1—Single bit ECC error
	Amber	D2—Multiple bit ECC error
	Amber	D3—Hi-byte data memory parity error
	Amber	D4—Lo-byte data memory parity error
	Amber	D5—Functional state machine activity
	Amber	D6—Diagnostics state machine activity
	Amber	D7—M.cache waiting to be enabled
	Amber	D8—Pattern compare failure

2.6 Module Switches

The functions of the module switches are explained in Table 2–5. The locations of the switches are shown in Figures 2–6 and 2–7. Do not attempt to change the settings of any switches or jumpers designated "Mfg. only."

Refer to Chapter 3 for detailed information on setting these switches.

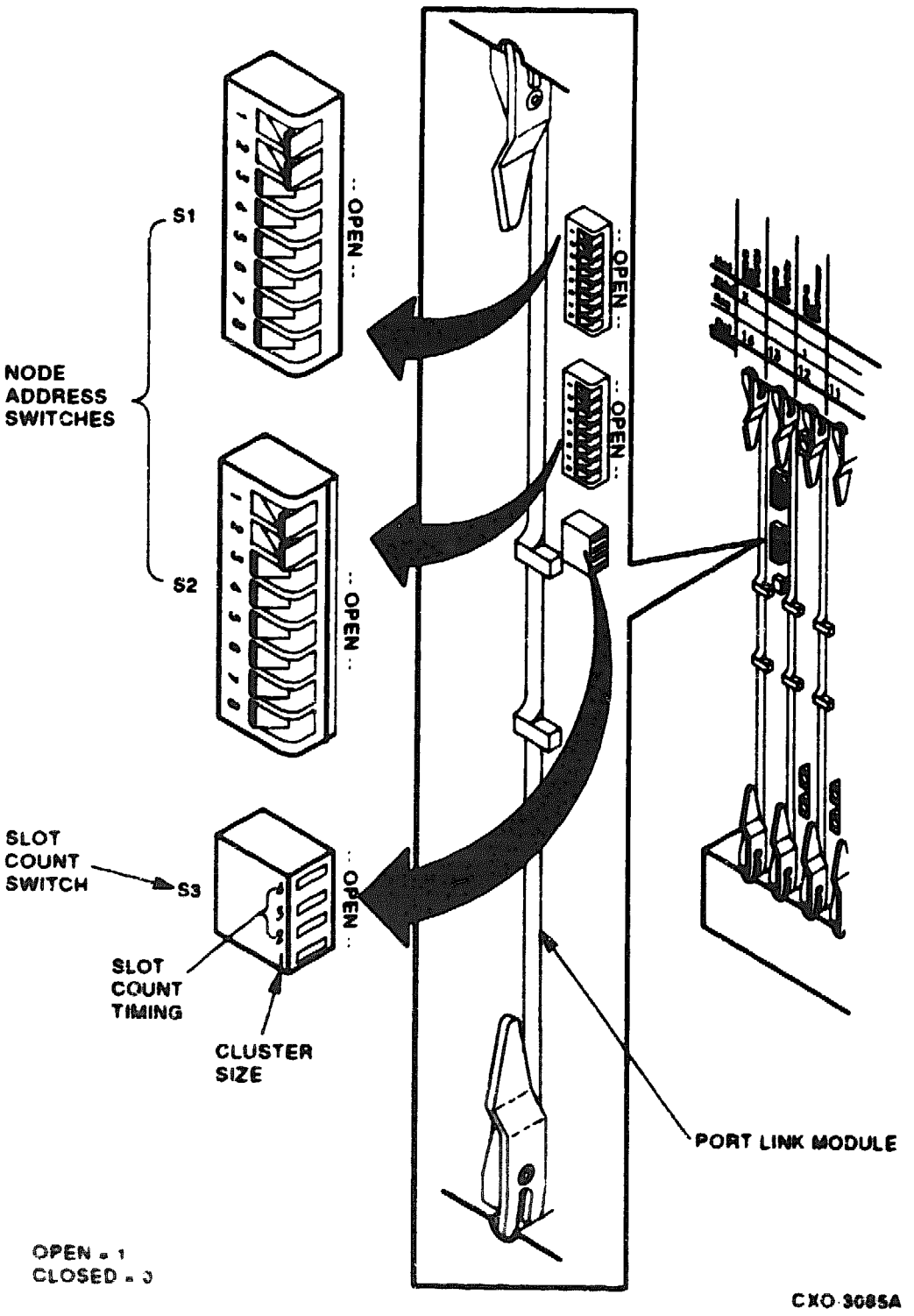


Figure 2–6 LINK2 (L0115) Module Switches

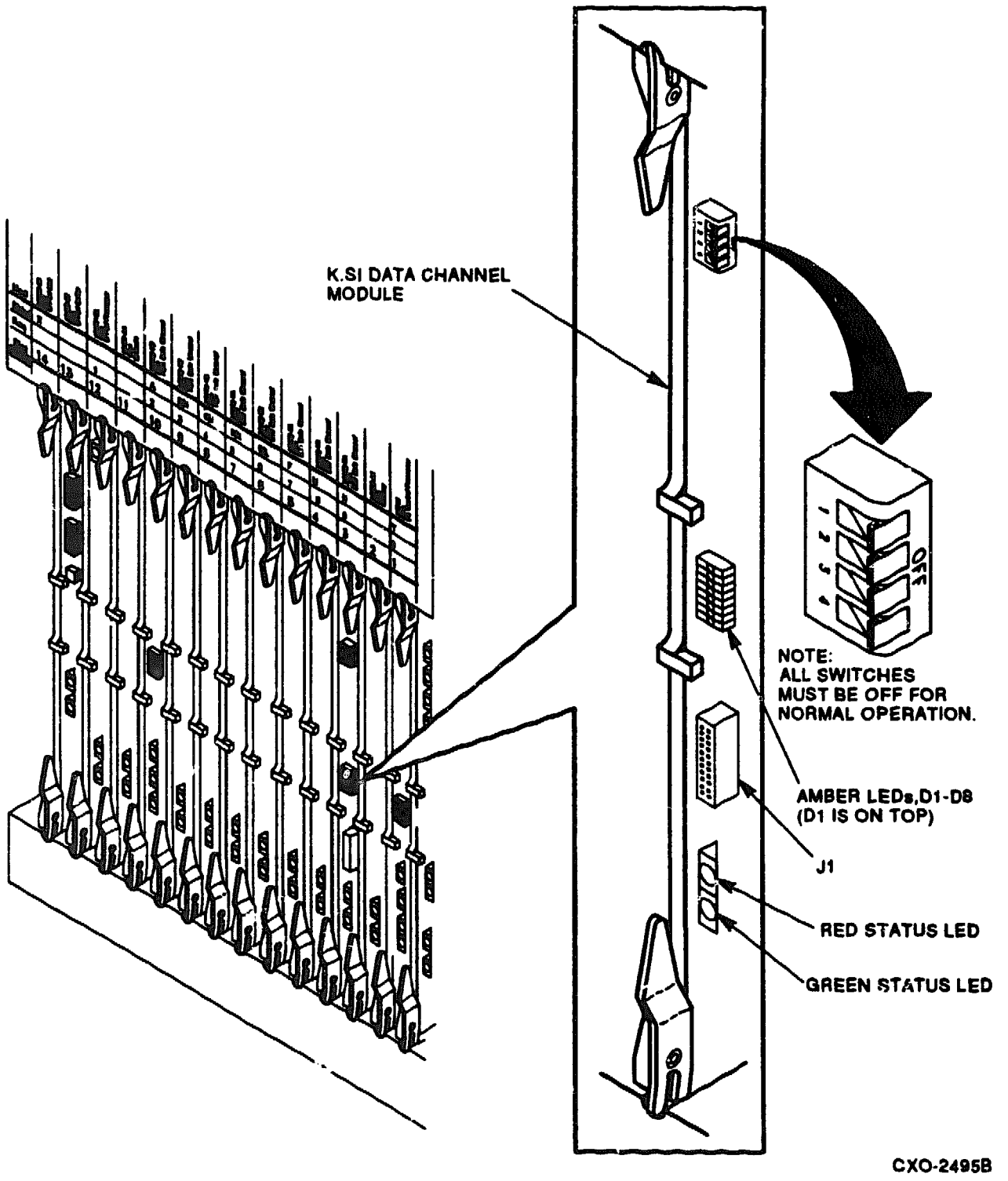


Figure 2–7 K.si Module (L0119-YA/YB) Switches

Table 2–5 Logic Module Switches

Module	Switch	Setting
LINK (L0100)	S1	Node Address
	S2	Node Address (Must be same as S1)
LINK (L0118–00) LINK2 (L0118–YA)	S1	Node Address
	S2	Node Address (Must be same as S1)
	S3	S3-1 = On if cluster size > 16, otherwise Off (See Section 3.5.1.2) S3-2 = Normally Off. Delta time S3-3 = Normally Off. Quiet slot S3-4 = Normally On. Slot count
PILA (L0109) PILA2 (L0125–00)	S1	H/W rev. Do not change except by FCO.
K.pli (L0107–YA)	S1	H/W rev. Do not change except by FCO.
K.pli2 (L0124–AA)	S1	Not used
	S2	Repeats failing internal diagnostics. Mfg only.
	S3	Detects CI path failure. Mfg only.
	S4	Local diagnostic. Mfg only.
K.si 4-port (L0119–YA) K.si 8-port (L0119–YB)	S1	S1-1 — Normally Off. Loop on error. Mfg only. S1-2 — Normally Off. Burn in. Mfg only. S1-3 — Normally Off. Ext loop. Mfg or field use. S1-4 — Normally Off. Ext clock. Mfg only.
P.ioc (L0105–00) P.ioj (L0111–00) P.ioj (L0111–YA) P.ioj (L0111–YC) P.ioj (L0111–YD)	S1	Serial number. Mfg only.
M.std2 (L0117–00)	S1	RX33 timing. Mfg only.
M.std4 (L0123–AA)	S1	RX33 timing. Mfg only.

2.7 HSC Power Controller

The HSC controller contains two types of power controller units. The HSC power controller is a general-purpose, single-phase ac power controller that controls and distributes ac power to various ac-input devices in the HSC cabinet. This power controller is installed in the HSC60 and HSC90 controllers.

The 881 power controller is similar to the HSC power controller, except that it uses three-phase ac input power. This model power controller is used in the HSC40 and HSC70, as well as the HSC50 (modified) controller.

The major external difference between the two power controllers is that the HSC power controller has a round grommet hole for the power cords, while the same hole on the 881 power controller is rectangular. The illustrations in this manual show the HSC power controller.

HSC power controller has the following features:

- Controls large amounts of ac power with low level signals
- Provides ac power distribution to single-phase loads on a three-phase system (881 power controller only)
- Protects data equipment from electrical noise
- Disconnects ac power for servicing and in case of overload
- Local and remote switching
- Switched receptacles only
- Convection cooling
- Rack mounting
- AC line filtering
- Power control bus inputs
- Power control bus delayed output to allow sequencing of other controllers

HSC power controllers intended for 50 Hz 240 Vac operation have a power cord that plugs into a socket in the back panel. These power controllers are supplied with one of the various line cords listed in Table 2–6 for specific service in each country or area.

Table 2–6 Line Cord Part Numbers for Various Countries

Line Cord Part Number	Service
17-00199-10	Central Europe
17-00198-05	Australia
17-00364-06	Italy
17-00209-05	Europe (IEC309 plug and harmonized cordage)
17-01256-01	220 Vac service in U.S., Canada, and Japan (IEC309 plug with UL/CSA cord)

2.7.1 Operating Instructions

The two basic controls on the HSC power controller are the circuit breaker and the BUS/OFF/ON switch. These and all but one of the other controls are located on the front panel of the controller, as shown in Figure 2–8.

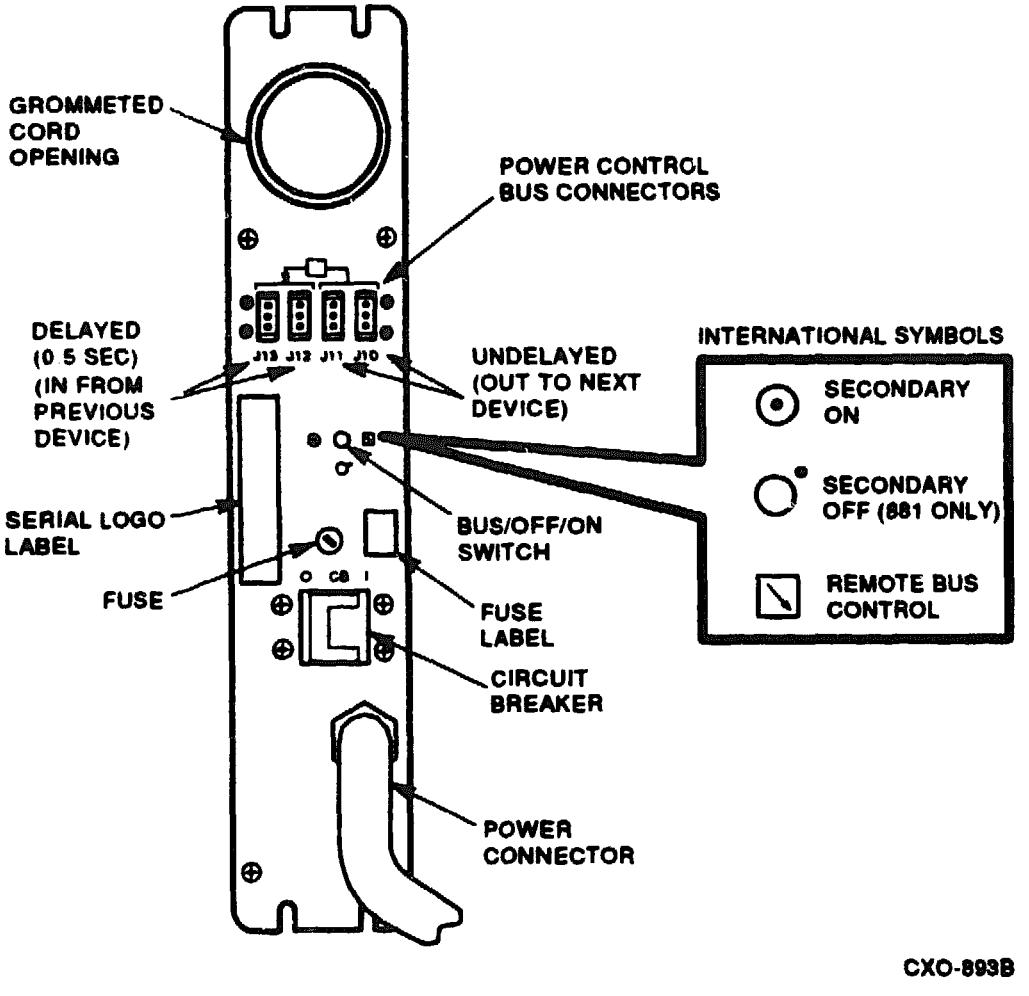


Figure 2–8 HSC Power Controller—Front Panel Controls

The operator controls are described in the following list:

- **HSC power controller circuit breaker**—Controls the ac power to all outlets. It also provides overload protection for the ac line loads and is unaffected by switching the BUS/OFF/ON control.
- **Fuse**—Protects the ac distribution system from an overload of the power control bus circuitry. The fuse is located on the front panel of the power controller.
- **Power control bus connections**—Used if control bus connections to another cabinet are required. Power control bus connectors are J10, J11, J12, and J13. Connectors J10 and J11 are not delayed. Connectors J12 and J13 are delayed.
- **BUS/OFF/ON switch**—There are two positions of this switch on the HSC power controller, and three positions for the 881 power controller. Assuming the circuit breaker for the power controller is on, the ac outlets are:

- Energized when the BUS/OFF/ON switch is in the SECONDARY ON position.
- De-energized when the BUS/OFF/ON switch is in the SECONDARY OFF position. (881 power controller only)
- In the 881 power controller, the center position of the switch de-energizes the ac outlets. The REMOTE BUS CONTROL position of this switch is intended for remote sensing of power control bus instructions. The switch is left in the on position when the power control bus is not used.

- **TOTAL OFF connector**—A two-pin male connector on the rear panel of the power controller (Figure 2–9). It removes power from the HSC controller whenever the air flow sensor detects system air-flow loss or an over temperature condition. To reset the TOTAL OFF connector, cycle the circuit breaker off, and then back on again.

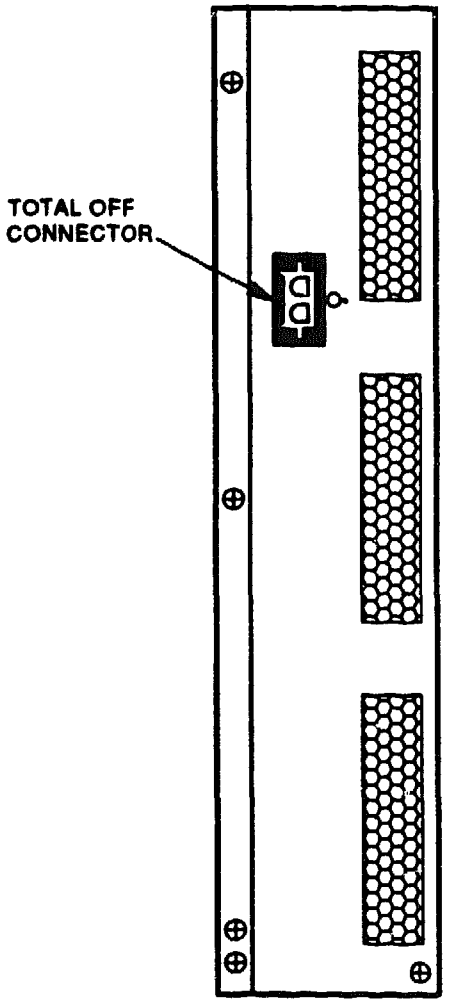


Figure 2–9 HSC Power Controller Rear Panel

2.8 HSC50 Power Controller

The 60 Hz power controller is shown in Figures 2–10 and 2–12. For the 50 Hz unit, refer to Figures 2–11 and 2–13. A physical description of the power controller follows.

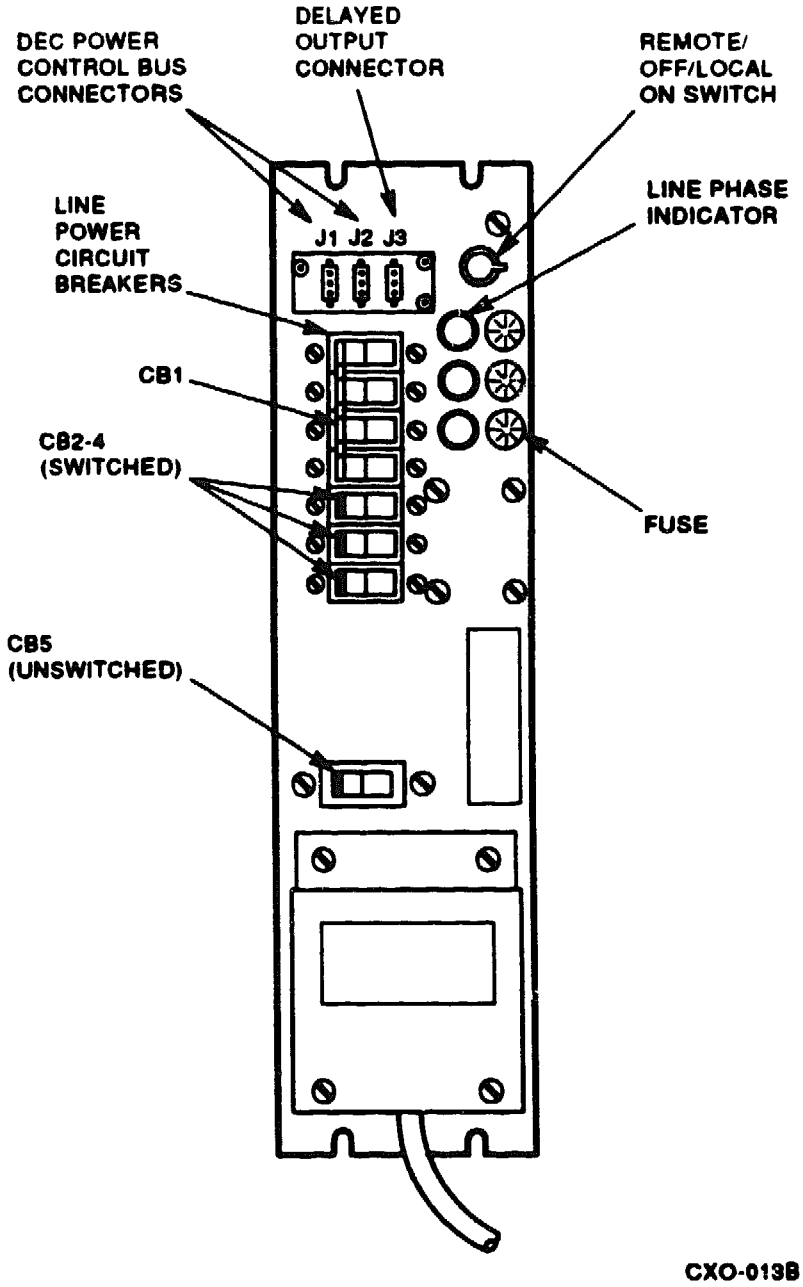


Figure 2–10 HSC50 Power Controller (60 Hz)—Front View

2.8.1 Line Phase Indicators

Three Line Phase indicators display the status of incoming line power. If any phase drops, the indicator for that phase goes off.

2.8.2 Fuses

The three line phases are fused to protect the HSC50 circuitry. These fuses are located beside the Line Phase indicators as shown in Figures 2–10 and 2–11.

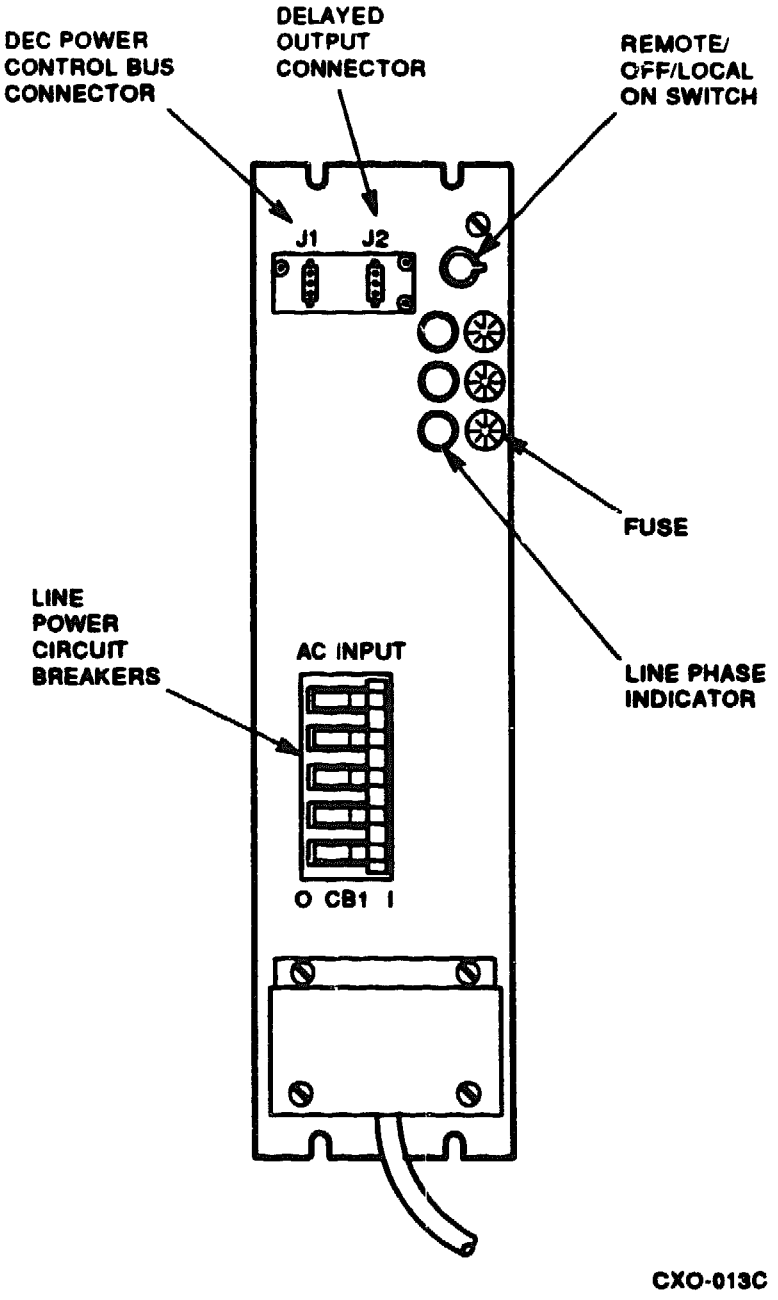


Figure 2–11 HSC50 Power Controller (50 Hz)—Front View

2.8.3 Remote/Off/Local On Switch

When REMOTE/OFF/LOCAL ON switch is in the OFF position, the power controller does not route ac line power to the switched or unswitched outlets.

With the switch in the LOCAL ON position, ac power is routed to the switched or unswitched outlets of the power controller.

When the switch is in the REMOTE position, the routing of ac power is dependent upon the power control bus signals.

2.8.4 Circuit Breakers (60 Hz)

Five power controller circuit breakers perform the following functions:

- CB1—Protects from incoming power surges
- CB2-4—Protects the switched outlets as shown in Figure 2–10
- CB5—Protects the unswitched outlets

2.8.5 Circuit Breakers (50 Hz)

The 50 Hz unit contains one circuit breaker, as shown in Figure 2–11. CB1 on this unit protects all circuits.

2.8.6 Power Controller (60 Hz)—Rear View

The switched outlets, shown in Figure 2–12, are protected by CB2-4 (Figure 2–10) and the unswitched outlets by CB5. These outlets are currently unused.

A three-pin male connector (J8) is located on the back of the power controller (Figure 2–12). J8 removes power from the HSC controller whenever the air flow sensor detects system air-flow loss or an over-temperature condition. To reset the TOTAL OFF, cycle the circuit breaker off and then back on again.

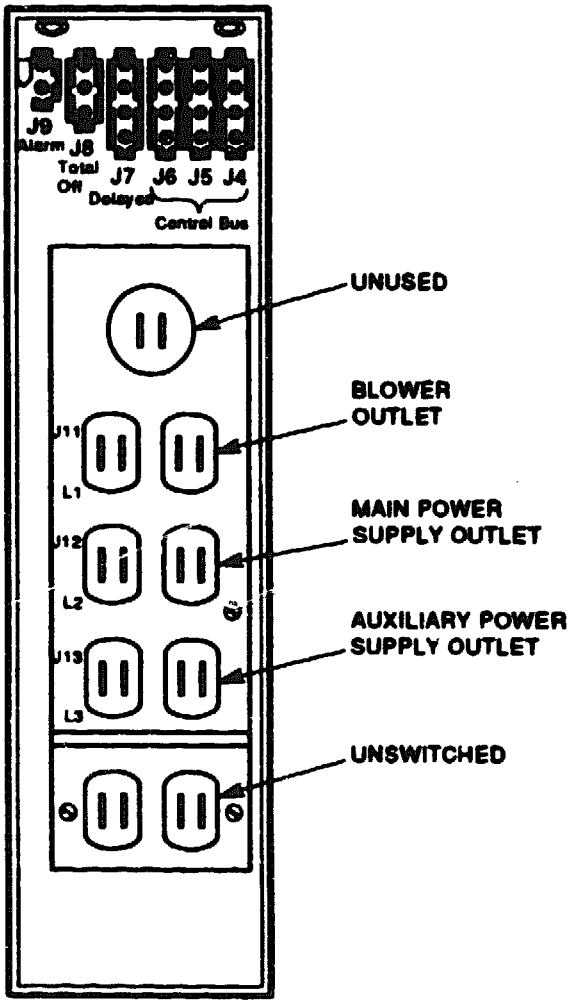


Figure 2–12 HSC50 Power Controller (60 Hz)—Rear View

2.8.7 Power Controller (50 Hz)—Rear View

The outlets shown in Figure 2–13 are protected by CB1 (Figure 2–11). Connector J3, shown at the top of the 50 Hz power controller rear view, connects the air flow sensor.

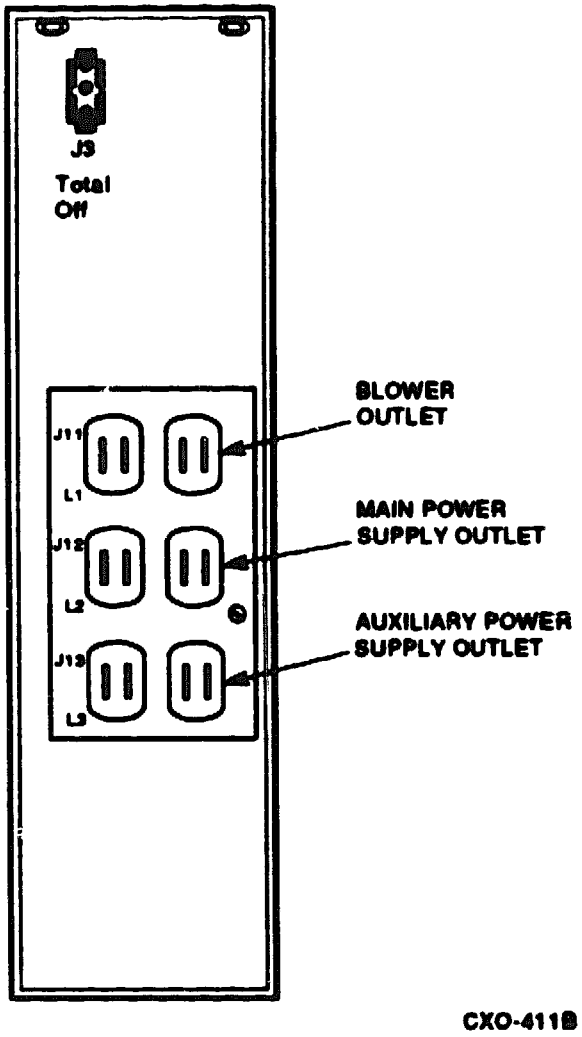
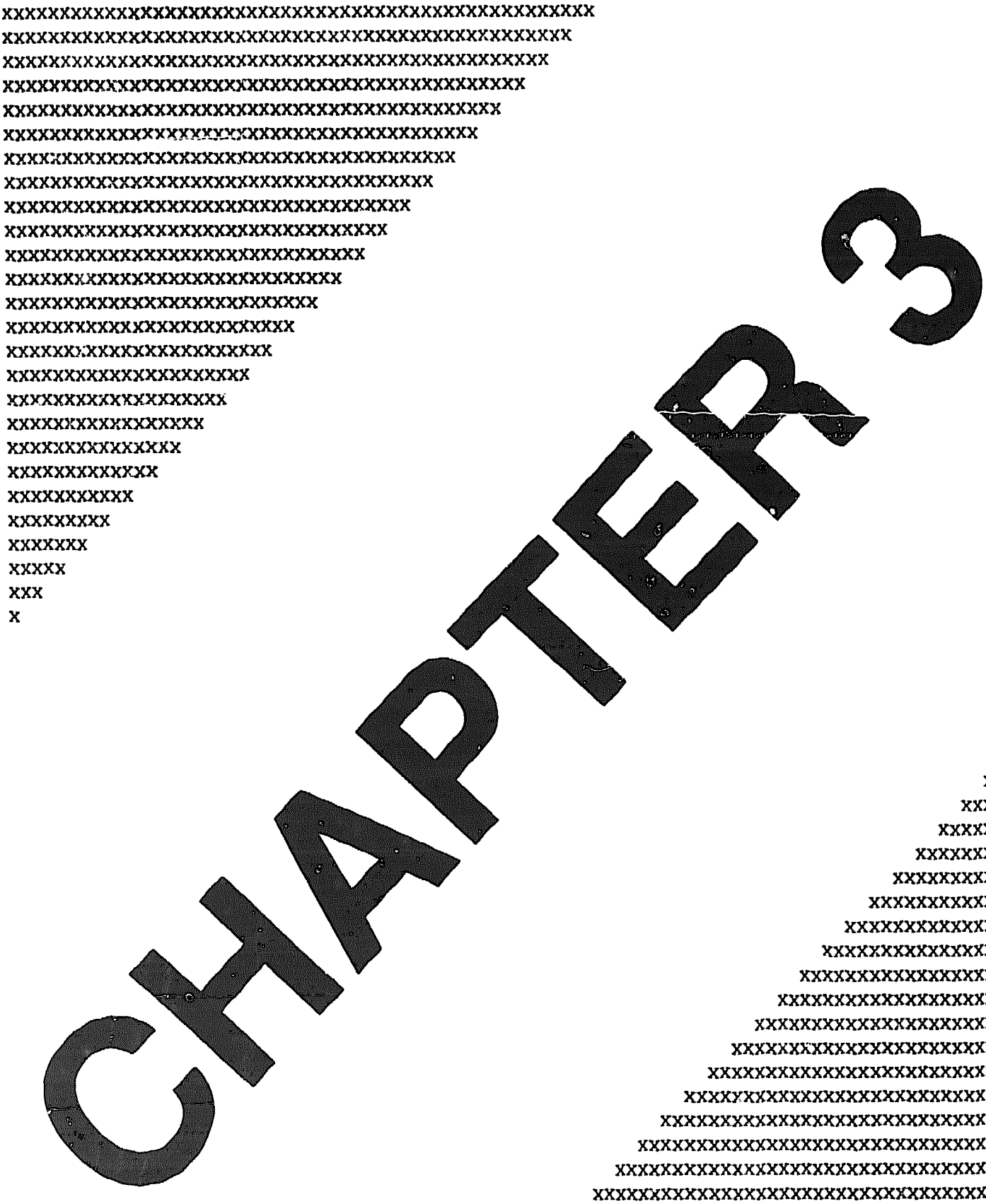


Figure 2–13 HSC50 Power Controller (50 Hz)—Rear View


CHAPTER 3

3
Removal and Replacement Procedures

3.1 Introduction

This chapter emphasizes conditions that must be met when replacing field replaceable units (FRUs), including the following information:

- Safety precautions
- HSC controller failover
- FRU overviews
- Jumper configurations
- Switch configurations
- Test sequence to perform after FRU replacement

Observe the safety and electrostatic discharge (ESD) precautions in this section before starting removal and replacement procedures.

This chapter covers the following replaceable HSC controller subunits and modules:

Modules:

Port link module (LINK and LINK2)
Port buffer module (PILA and PILA2)
Port processor module (K.pli and K.pli2)
I/O control processor module (P.ioj and P.ioc)
Disk data channel module (K.sdi)
Tape data channel module (K.sti)
Data channel module (4-port and 8-port K.si)
Cache module (M.cache)
Memory module (M.std2 and M.std4)
Memory module (M.std)

Subunits:

RX33 disk drive
TU58 tape drive
Operator control panel
Air flow sensor
Blower
Power controller
Main power supply
Auxiliary power supply

3.2 Safety Precautions

Because hazardous voltages exist inside the HSC controller, service must be performed only by qualified people. Serious bodily injury or equipment damage can result from improper servicing. Observe the following safety steps before servicing the HSC controller:

1. Turn off the dc and ac power to the HSC controller before removing or installing internal parts or cables.
2. To ensure absolute safety, disconnect the ac plug from its receptacle after removing power from the HSC controller.
3. Remove and replace heavy subunits with care.
4. Use the Velostat (anti-static) kit (part number 29-11762) strap provided when removing and replacing logic modules.

3.3 Taking the HSC50 Controller Offline for Maintenance

This section describes how to take an HSC controller offline for performing maintenance. A cluster may be configured with a single or with multiple HSC controllers.

3.3.1 Single HSC50 Controller in a Cluster

If there is only one HSC controller in the cluster, use the following procedure:

1. Notify the system manager that the HSC controller is being taken offline and the drives attached to it will not be available. The customer may want to personally dismount the drives in the next step.
2. Dismount the drives connected to the HSC controller or shut down the system.
3. Place the Online switch in the OUT position.
4. Take the HSC controller offline with *one* of the following methods:
   - Turn off the dc and ac power to the HSC controller.
   - Press the Init switch to reboot the HSC controller.

3.3.2 Multiple HSC Controllers in a Cluster

Most VMS system clusters have primary and secondary paths established between the host and drives. If the HSC controller is the primary path, fail over to the secondary path occurs and the drives remain available to the host. Use the following procedure when taking an HSC controller offline from a cluster with multiple HSCs:

1. Notify the system manager that you are taking the HSC controller offline. The customer may want to personally dismount the drives in the next steps.
2. Enter the SETSHO command SHOW TAPE to determine which tape drives are online to the HSC controller. Dismount these tape drives using the appropriate VMS commands.
3. Enter the SETSHO command SHOW DISK to determine which disk drives are online to the HSC controller undergoing maintenance. The online drives must be removed, failed over to the alternate HSC controller, or dismounted.
4. Dismount single-ported disk drives using the appropriate VMS commands.
5. On all dual-ported disk drives, make sure that both A and B port select switches on the drives are pressed in. Deselect the active port on the drive by pressing and releasing the illuminated port select switch.

6. Verify that the illuminated switch turns off and the alternate port switch illuminates. Actual failover time depends on the server timeout and may require 1 minute or more, depending on activity. When the alternate port light illuminates, fail over to the other HSC controller is successful.
7. Enter the SETSHO command SHOW DISK to verify that all online drives have failed over to the alternate HSC controller.
8. If failover did not occur, reselect the ports on the drive and check the connections between the drives and the HSC controller.
9. After all tapes and disks have been failed over, take the HSC controller offline using *one* of the following methods:
   - Turn off the dc and ac power to the HSC controller, or
   - Place the Offline switch in the OUT position, or
   - Press the Init switch to reboot the HSC controller.

3.4 Removing and Replacing Field Replaceable Units

The following sections describe procedures for removing and replacing FRUs in HSC or HSC50 controllers.

3.4.1 Removing HSC Controller Power

Before removing/replacing an FRU, turn off the power to the HSC controller. Following are the methods for removing dc and ac power from an HSC controller:

1. Set the DC power switch on the side of the RX33 housing to the OFF position (Figure 3–1).

   WARNING
   Ensure the OCP Signal/Power line indicator is connected; otherwise the power indicator on the OCP can show power off when the power is on.

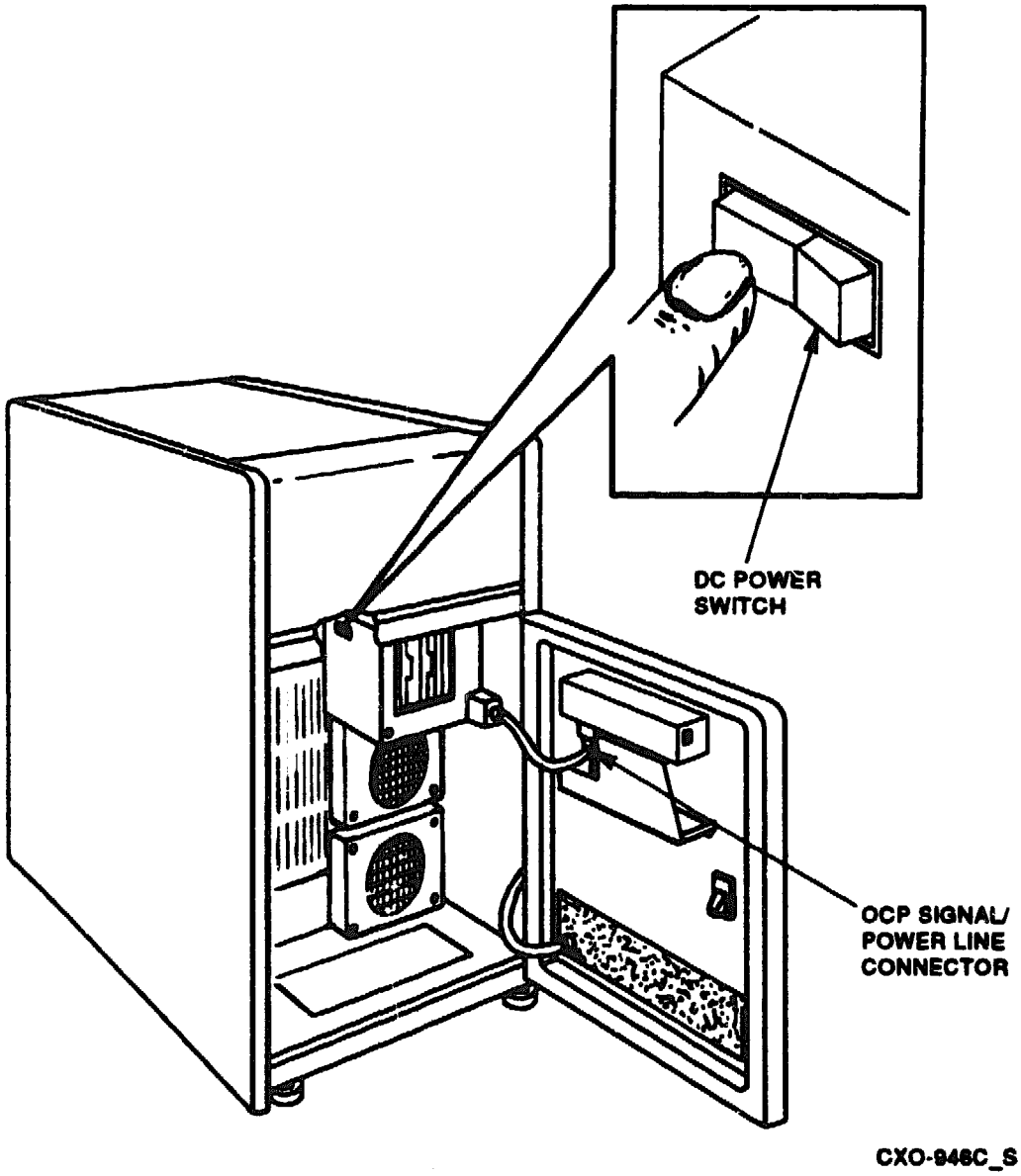


Figure 3–1 HSC DC Power Switch

2. Place the main power switch CB1 on the HSC power controller in the OFF position (Figure 3–2). To ensure safety precautions, unplug the ac power plug from the ac socket.

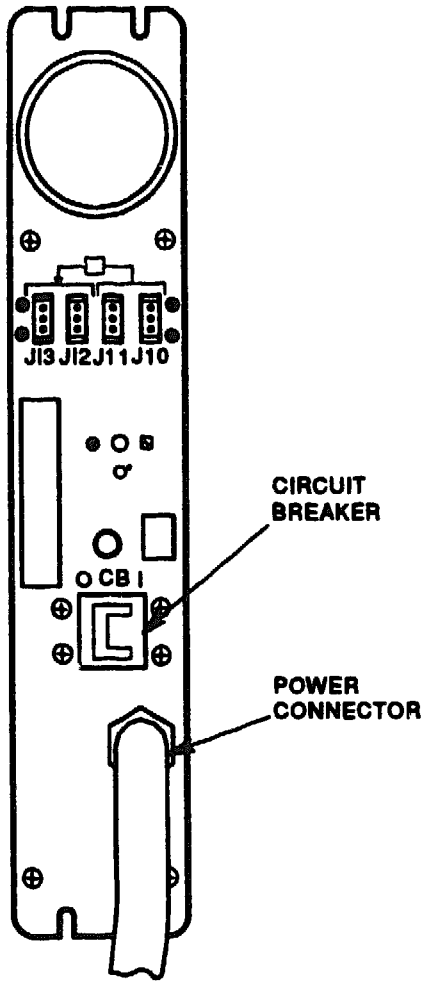


Figure 3–2 HSC Power Controller Circuit Breaker

3.4.2 Removing HSC50 Controller Power

Following are the steps for removing dc and ac power from an HSC50 controller:

1. Set the DC power switch on the maintenance access panel to the OFF position (Figure 3–3).

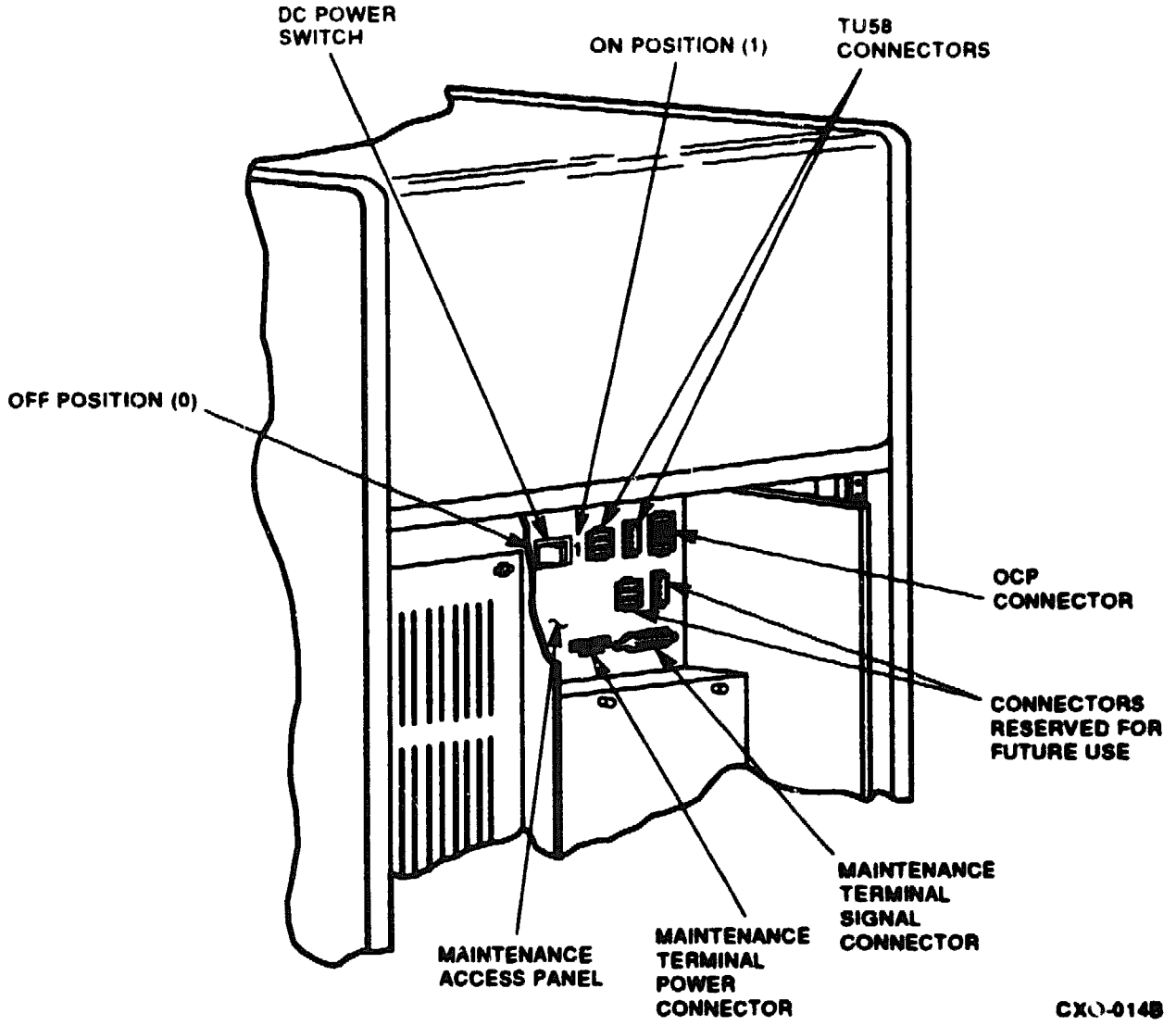


Figure 3–3 HSC50 DC Power Switch

2. Place the main power switch CB1 on the power controller in the OFF position (Figure 3–2) for the HSC50 (modified) and the line power circuit breakers (Figure 3–4) for the HSC50 controller. For safety, unplug the ac power plug from the ac socket.

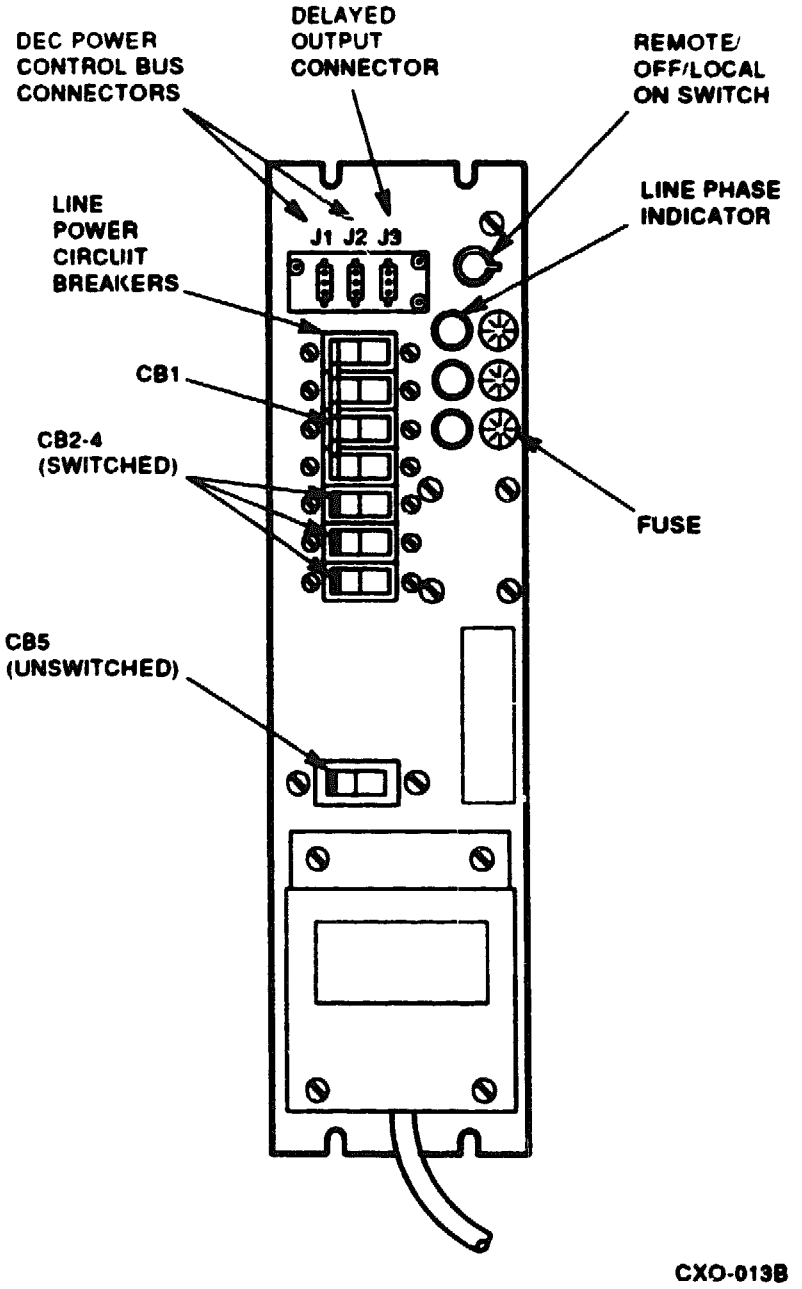


Figure 3–4 HSC50 Line Power Circuit Breakers

3.4.3 Removing Field Replaceable Units

Figure 3–5 shows the sequence for removing FRUs in the HSC controller:

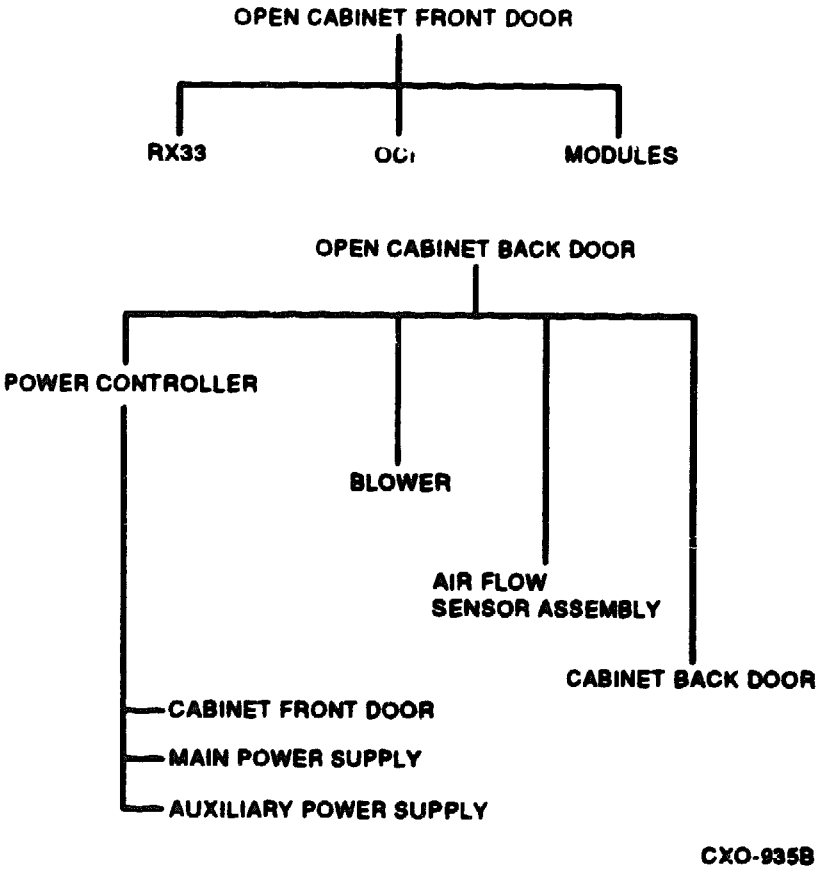


Figure 3–5 HSC Controller FRU Removal Sequence

Figure 3–6 shows the FRU removal sequence for an HSC50 controller.

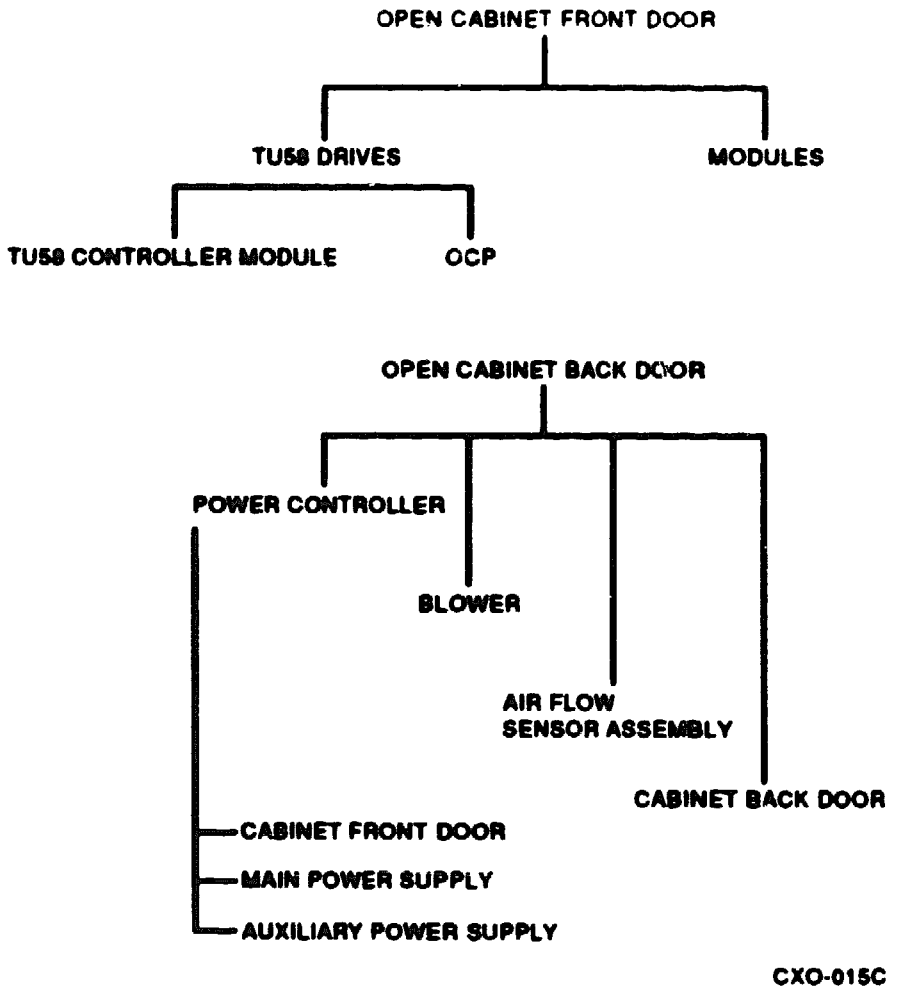


Figure 3–6 HSC50 Controller FRU Removal Sequence

3.4.4 Removing the HSC Cabinet Front Door

The FRUs accessed through the front door include the RX33 drives, the OCP, and the logic modules. To remove the front door, use the following procedure

1 Unlock the cabinet front door and lift the latch to open the door

CAUTION
When performing the following steps, take care not to damage the front spring fingers.

2. Remove HSC controller power by setting the DC power switch to the 0 position.
3. Disconnect the ground wire from the door.
4. Disconnect the OCP signal/power line connector at the bottom of the OCP shield (Figure 3–7).

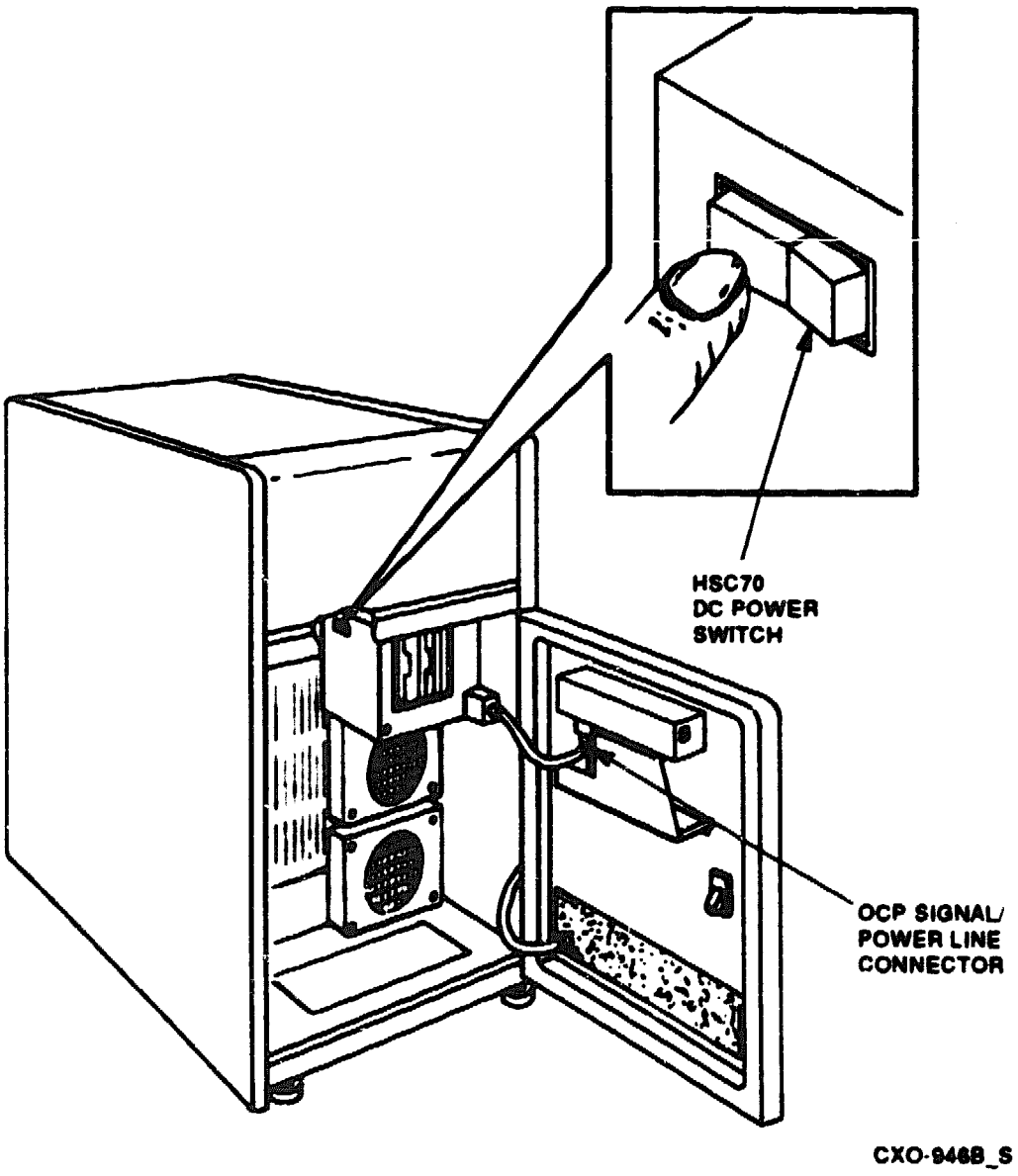


Figure 3–7 HSC OCP Signal/Power Line Connector

5. Pull down on the spring-loaded rod on the top hinge inside the cabinet to disengage the door, then lift the door off its bottom pin.

Reverse the removal procedure to replace the front door.

3.4.5 Removing the HSC50 Cabinet Front Door

The FRUs accessed through the front door include the TU58 tape drives, the OCP, and the logic modules. To remove the front door, use the following procedure:

1. Open the cabinet front door by turning the key clockwise.

   CAUTION
   When performing the following steps, take care not to damage the front spring fingers.

2. Disconnect the ground wire from the door.
3. Remove the maintenance access panel cover by loosening the four captive screws.

   NOTE
   Some HSC50 controllers have a hinged maintenance access panel with only one captive screw.

4. Remove HSC50 controller power by setting the DC power switch to the 0 position.
5. Remove the plastic cable duct cover.
6. Disconnect the cables from the maintenance access panel connectors shown in Figure 3–8.

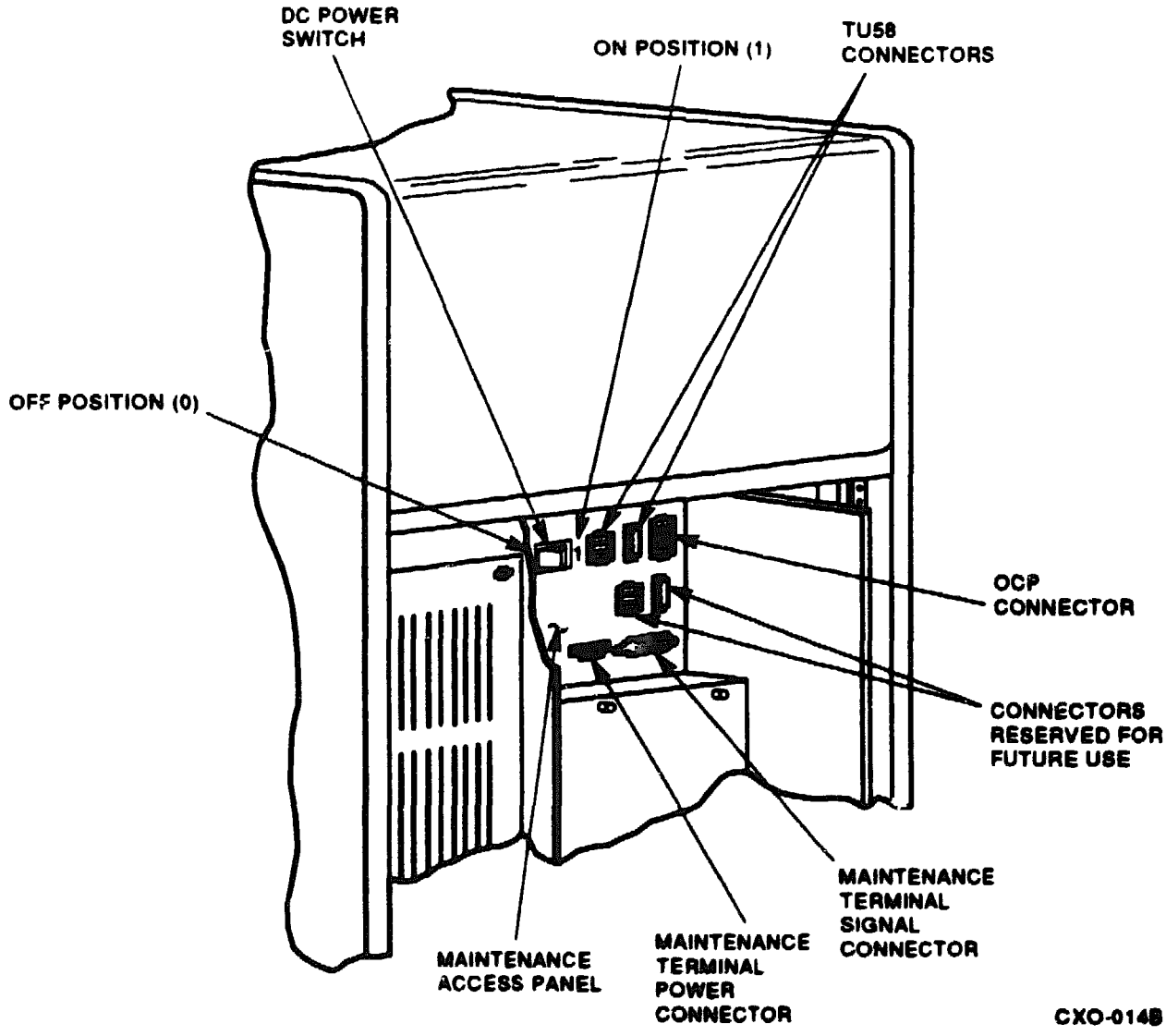


Figure 3–8 HSC50 Maintenance Access Panel Connectors

7. Pull down on the spring-loaded rod on the top hinge inside the cabinet to disengage the door, then lift the door off its bottom pin.

Reverse the removal procedure to replace the front door.

3.4.5 Removing the HSC Cabinet Back Door

The FRUs accessed through the back door include the power controller, blower, air flow sensor assembly, main power supply, and auxiliary power supply. To remove the back door, use the following procedure:

1. Open the back door with a 5/32-inch hex wrench.
2. Pull down on the spring-loaded rod on the top hinge inside the cabinet to disengage the door, then lift the door off its bottom pin.

Reverse the removal procedure to replace the back door.

3.5 Removing and Replacing Modules

This section contains procedures for removing and replacing modules. Refer to Figure 3–9 for the HSC controller, and Figure 3–10 for the HSC50 controller when removing the card cage cover.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

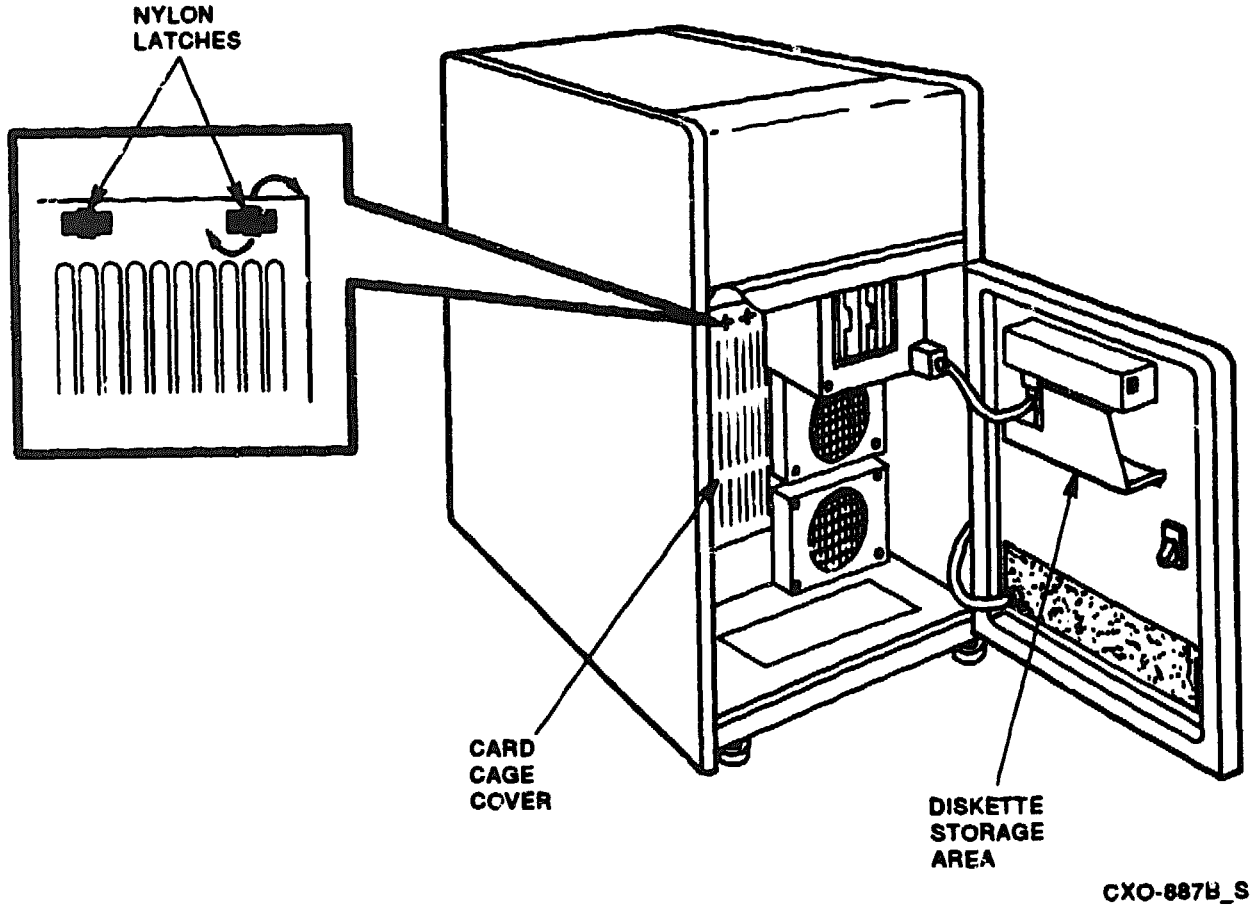


Figure 3–9 HSC Card Cage Cover Removal

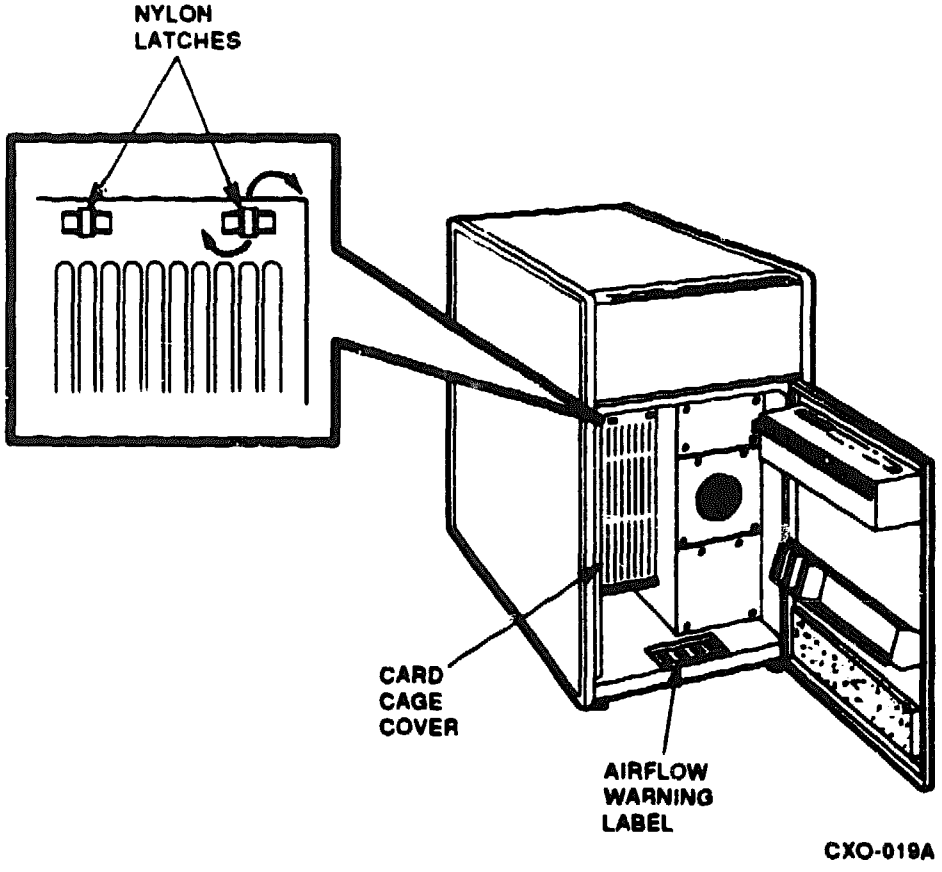


Figure 3–10 HSC50 Card Cage Cover Removal

WARNING
Because hazardous voltages exist inside the HSC controller, service must only be performed by qualified people. Bodily injury or equipment damage can result from improper servicing procedures.

3.5.1 Removing and Replacing the Port Link Module (LINK and LINK2)

The port link module (LINK) is a part of the host interface module set (K.ci). In this section, the term port link is used to refer to LINK modules (L0100-E2 and LO118-00) and the LINK2 module (L0118-YA), unless otherwise noted. With all configuration switches and jumpers in default positions, the L0118 is functionally identical to the L0100 or L0100-E2.

CAUTION
Do not attempt to handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller cabinet. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.1.1 Removing the Port Link Module

Use the following procedure to remove the port link module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller or shut down the system.
3. Set the DC power switch to the 0 (off) position.

   On the HSC controller, the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
4. Turn the two nylon latches on the card cage cover one-quarter turn.
5. Pull the HSC card cage cover up and out.
6. Locate the port link module in slot number 14 of the card cage. This can be verified by the module utilization label.
7. Move the door latch plate attached to the left side of the cabinet frame away from the module removal path. In the HSC cabinet, the latch plate is swivel mounted. Lift the plate slightly and press it flat against the cabinet frame. Remove the port link module.

3.5.1.2 Setting the Replacement Port Link Module Switches

S1 and S2 are the node address switches on the port link module. The node address switches on the replacement module must be set identically to the switch settings on the removed port link module. The L0100-E2 and L0118 port link modules also have an additional switch pack (S3). This section contains information on how to locate and set these switches when replacing the LINK and LINK2 modules.

The switch configurations and their significance is as follows:

S1/S2—Node number
S3-1—Cluster size (GT15)
S3-2, S3-3—Delta time/quiet slot
S3-4—Quiet slot count

Figure 3–11 shows the LINK module (L0100) node address switches.

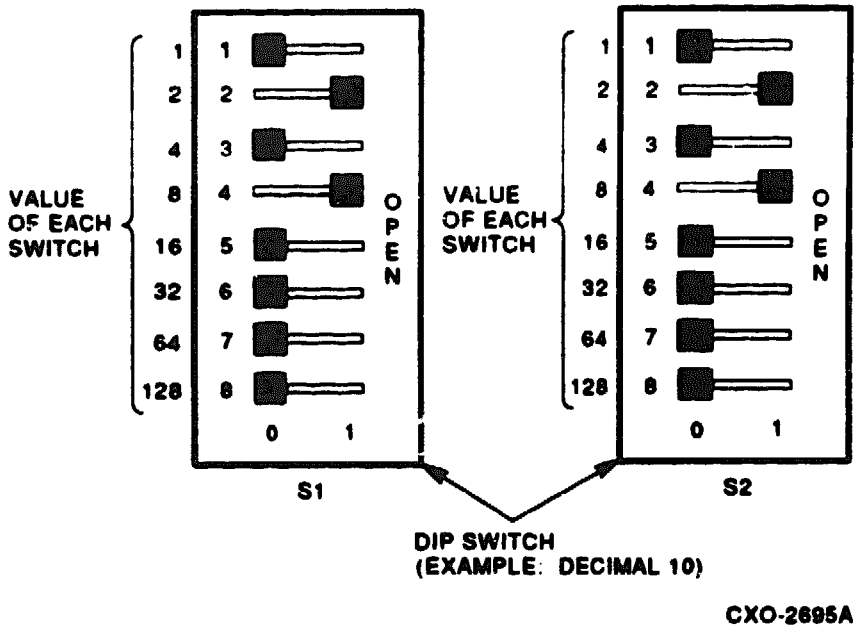


Figure 3–11 LINK Module (L0100) Node Address Switches

Figure 3–12 shows the LINK module (L0100-E2/L0118) node address switches.

Incorrect switch and/or jumper settings on the CI modules in both the HSC controllers and the CI host nodes can cause various cluster disturbances, including:

- Disks in Mount Verification
- Many virtual circuit (VC) closures, resulting in shadow copy initiation on shadowed disks
- Various VMS bugchecks, most commonly CLUEXIT

These disturbances are caused by CI collisions brought about by mismatched CI communications mechanisms. There are two mechanisms involved:

- Slot count timing (also called "quiet time")
- Cluster size

Settings for these mechanisms are selected by switch positions on the L0100/L0118 LINK modules in HSC controllers and older VAX host systems, and by backplane jumpers for CIBCA and CIXCD CI port adapters on newer VAX hosts.

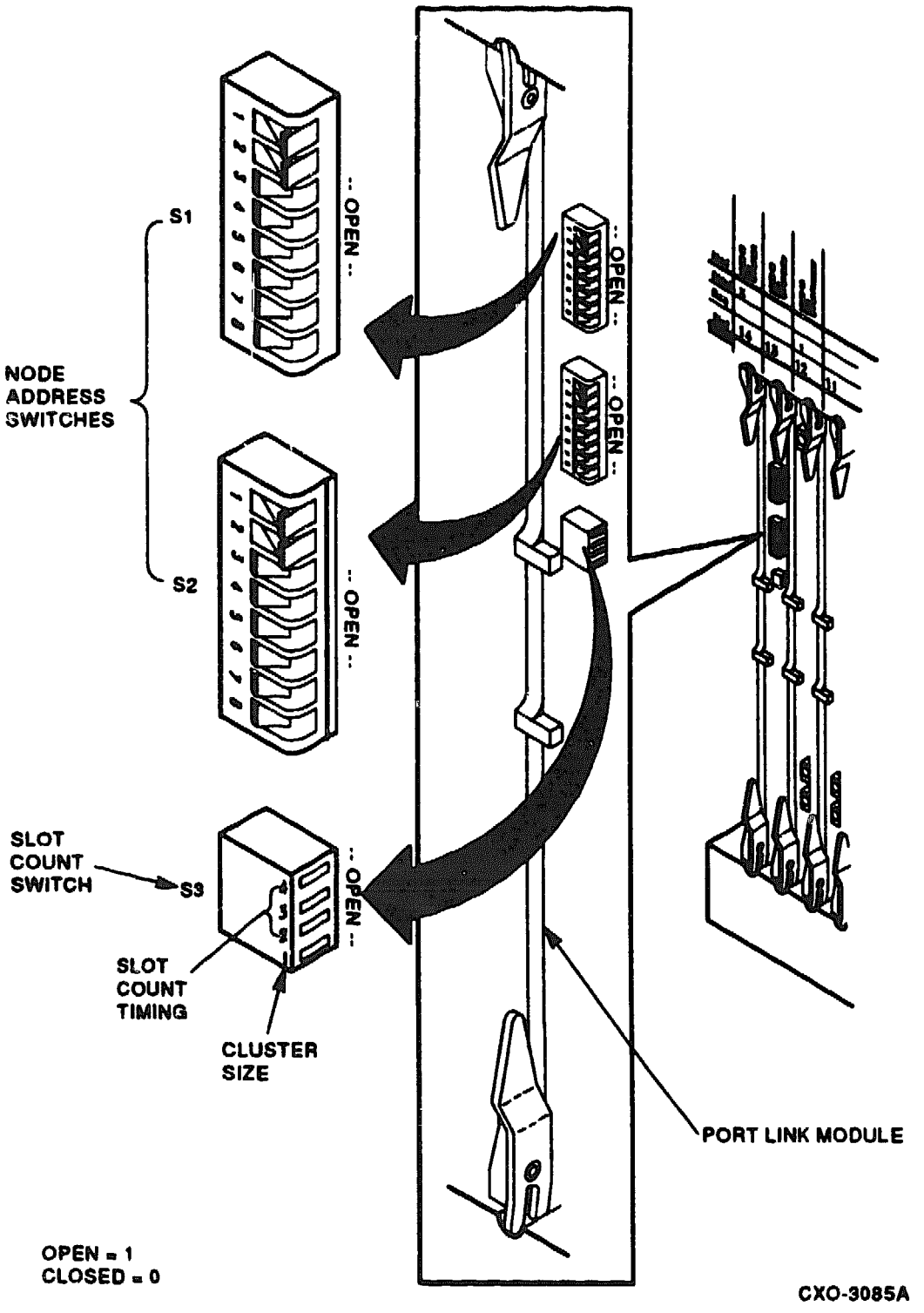


Figure 3–12 LINK Module (L0100-E2/L0118) Node Address Switches

Slot count timing has two possible settings: 7 or 10. At the time of HSC controller installation, all LINK and CI adapter modules in the cluster must be set to a consistent value to avoid the cluster disturbances mentioned above.

It is highly recommended that the slot count timing for all CPU and HSC controller nodes within a cluster be set to a value of 10 (not 7). HSC60 and HSC90 controllers, as well as recently manufactured HSC40 and HSC70 controllers, are shipped with their LINK modules set to a slot count timing of 10.

However, LINK modules for previously installed HSC controllers or CI port adapter modules in host systems may still be set at a slot count timing of 7. If your cluster does not contain a CIXCD adapter and is operating without problems at a slot count timing of 7, you may set the HSC60 or HSC90 controller LINK module to 7 when installing or replacing the LINK module, and defer resetting the entire cluster to a slot count timing of 10 until a more convenient time.

If your cluster contains a CIXCD, all LINK and CI adapter modules should already be set to 10, since the CIXCD does not support a slot count timing of 7.

To assist you with setting the slot count timing in your cluster, Table 3–1 lists LINK and adapter module switch and jumper settings.

In addition, the cluster size parameter must be consistent throughout the cluster at a value of either 16 or 32. If all nodes in your cluster are numbered in the range of 0 to 15, you may select a cluster size of either 16 or 32. If your cluster has any node numbered in the range of 16 to 31, you must select a cluster size of 32. Table 3–1 also contains a list of LINK and adapter module switch and jumper settings to select the appropriate cluster size.

Table 3–1 L0118 LINK Module and CI Adapter Module Switch and Jumper Settings

Adapter Type	Host System	LINK Module	Function	Switch/Jumper Setting
CI750	VAX-11/750	L0100 Rev E[1,2]	Slot=7	S3–1=Open
CI780	VAX-11/78x, VAX 86x0		Slot=10	S3–1=Closed
CIBCI	VAX 82x0, VAX 83x0		Clu_size=16	Fixed
	VAX 87x0, VAX 8800			
	HSC40, HSC50, HSC70	L0118 Rev B[3]	Slot=7	S3–4=Open
			Slot=10	S3–4=Closed
			Clu_size=16	S3–1=Open
			Clu_size=32	S3–1=Closed
	HSC60, HSC90	L0118–YA	Slot=7	S3–4=Open
			Slot=10	S3–4=Closed
			Clu_size=16	S3–1=Open
			Clu_size=32	S3–1=Closed
CIBCA–Ax, CIBCA–Bx[4,5]	VAX 82x0, VAX 83x0	T1025	Slot=7	Jumper E11–41=Out
	VAX 85x0, VAX 8700	T1046	Slot=10	Jumper E11–41=In
	VAX 88x0, VAX 6000		Clu_size=16	Jumper D30–60=Out
			Clu_size=32	Jumper D30–60=In
CIXCD-xx[5]	VAX6000, VAX9000	T2080	Slot=7	Not Supported
			Slot=10	Jumper E15–45=In
			Clu_size=16	Jumper D15–45=Out
			Clu_size=32	Jumper D15–45=In

[1]L0100 Rev "D" modules are not supported.

[2]On L0100 Rev "E" modules, S3-2 serves no function.

[3]On L0118 modules, all on-module jumpers must be left in their default positions, and S3-2 and S3-3 must remain open.

[4]For CIBCA options, all referenced jumpers are located on the backplane slot for the PORT (T1015/T1045) module, *not* the slot allocated to the LINK (T1025/T1046) module. For CIBCA options, all reference jumpers are on the backplane slot for the PORT (T1015 or T1045 module).

[5]For CIBCA and CIXCD options, install *only* those backplane jumpers listed and those required to specify the node address.

Locate the slot count switch (S3) on the L0118–xx Port LINK module. Set the slot count switch as follows:

1. Set the cluster size on S3-1. Switch S3-1 can be set to open (1) or closed (0) if all nodes in the cluster have a node number of 15 or less. Set S3-1 to Closed (0) if any node in the cluster has a node number of 16 or greater. Refer to Table 3–1 for a listing of LINK module switch and jumper settings for various VAXcluster configurations.
2. Set the slot count timing switch to the proper value for the cluster by using the settings for S3-2, S3-3, and S3-4 (either 7 or 10) given in Table 3–1. Refer to Figure 3–12 for the location of the slot count switch pack.

   Table 3–2 lists the settings of the switches as Open or Closed on the LINK module for slot counts of 7 and 10. The table also lists two additional reserved settings for S3. These settings should be used only as directed by Digital Customer Services.

Table 3–2 L0118 LINK Module S3 Switch Slot Count Timing Settings

Slot Count	S3-2	S3-3	S3-4	Comment
7	Open	Open	Open	
10	Open	Open	Closed	Default
Reserved #1	Open	Closed	Open	Slot count=11
Reserved #2	Open	Closed	Closed	Slot count=14

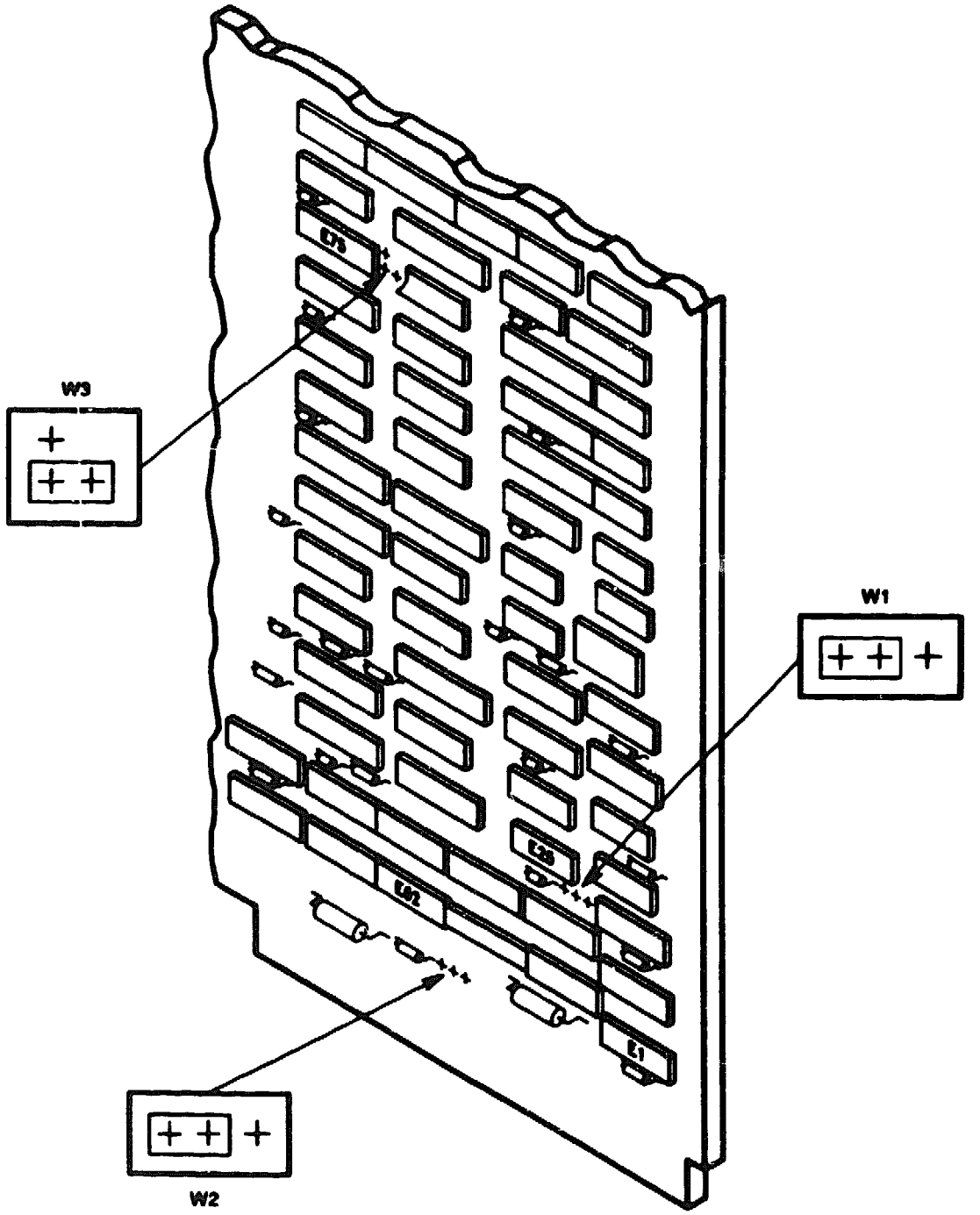
NOTE
When setting the S3 switches, Open= 1 and Closed= 0. Remember that S3-1 is used to set the cluster size and is not related to the slot count timing settings.

3.5.1.3 Setting the Replacement Port Link Module Jumpers

The port link jumper configurations are as follows:

W1—Extender head, Default = Not used
W2—Active hub, Default = Not used
W3—Extender ACK timeout, Default = Not used
W4—Cluster size (GT32), Default = Less than 32

Figure 3–13 shows the LINK module (L0100) jumpers.

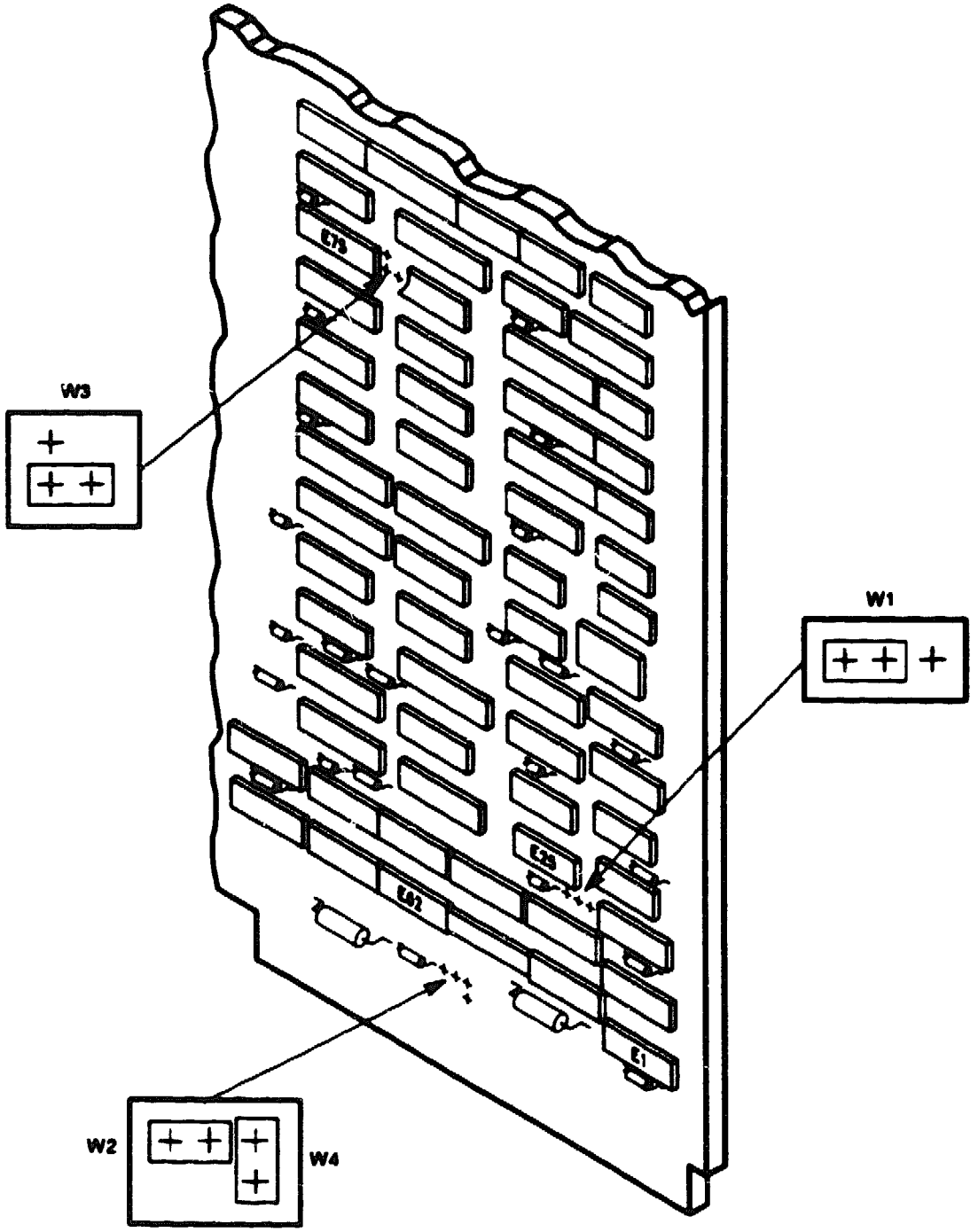


NOTE: BOXES INDICATE THE DEFAULT JUMPER POSITIONS.

CXO-1910B

Figure 3–13 LINK Module (L0100) Jumper Configuration

Figure 3–14 shows the LINK module (L0118-B1) jumpers.

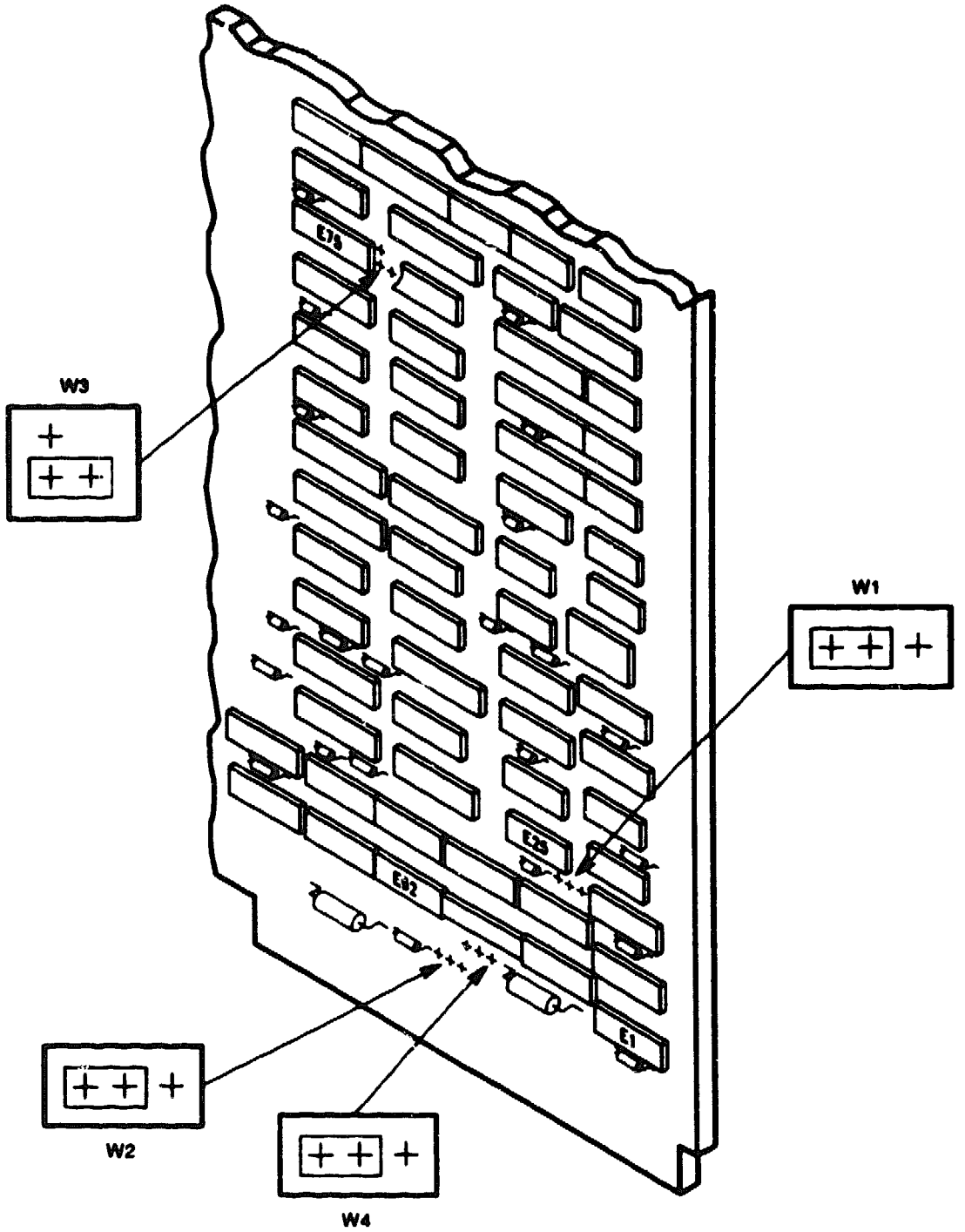


NOTE BOXES INDICATE THE W1 AND W3 FAULT JUMPER POSITIONS.
THE DEFAULT FOR JUMPERS W2 AND W4 IS "OUT"

CXO-1911B

Figure 3–14 LINK Module (L0118-B1) Jumper Configuration

Figure 3–15 shows the LINK module (L0118-00 Rev 2/L0118-YA) jumpers.



NOTE BOXES INDICATE THE DEFAULT JUMPER POSITIONS.

CXO-1912B

Figure 3–15 LINK Module (L0118-00 Rev 2/L0118-YA) Jumper Configuration

3.5.1.4 Replacing the Port Link Module

This section provides the port link module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

1. Install the port link module in slot number 14 of the card cage. This can be verified by the module utilization label.
2. Move the door latch plate attached to the left side of the cabinet frame away from the module installation path. In the HSC cabinet, the latch plate is swivel mounted. Lift the plate slightly and press it flat against the cabinet frame. Install the port link module and return the plate to its locked position.
3. Pull the card cage cover down and in.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Set the DC power switch to the 1 (on) position.

   On the HSC controller, the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.

3.5.1.5 Testing the Port Link Module

Perform the following tests to verify correct port link operation as part of the K.ci host interface module set.

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and perform the following tests:
   - Offline bus interaction test
   - Offline K test selector
   - Offline K/P memory test
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure that both A and B paths are present to all hosts.

3.5.2 Removing and Replacing the Port Buffer Module (PILA and PILA2)

The port buffer module (PILA and PILA2) is a part of the host interface module set (K.ci). In this section, the term PILA refers to both the PILA (L0109) and the PILA2 (L0125) modules. The port buffer module connects with the port link module through a set of interconnect port link signals.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.2.1 Removing the Port Buffer Module

Use the following procedure to remove the port buffer module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller or shut down the system.
3. Set the DC power switch to the 0 (off) position.

   On the HSC controller, the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Pull the card cage cover up and out.
6. Locate the port buffer in slot number 13 of the card cage. This can be verified by the module utilization label.
7. Remove the port buffer module.

3.5.2.2 Setting the Replacement Port Buffer Module Switches

The port buffer module has factory-set dual in-line pack (DIP) switches to indicate the hardware revision level. Do not change DIP switch positions, except as directed by an FCO. On newer port buffer modules the DIP switch has been replaced with a DIP shunt.

Figure 3–16 shows the port buffer module switch.

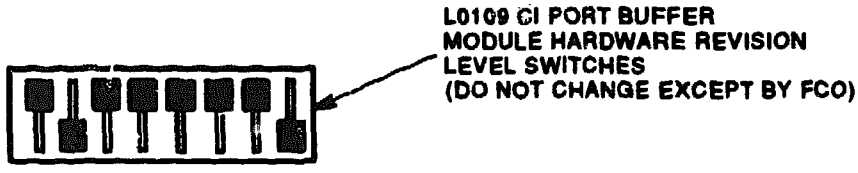


Figure 3–16 L0109 Hardware Revision Level Switch

3.5.2.3 Replacing the PILA Module

This section provides the port buffer module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

1. Install the port buffer module in slot number 13 of the card cage. This can be verified by the module utilization label.
2. Pull the card cage cover down and in.
3. Turn the two nylon latches on the module cover plate one-quarter turn.
4. Set the DC power switch to the 1 (on) position.

   On the HSC controller, the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.

3.5.2.4 Testing the PILA Module

Perform the following tests to verify correct port buffer module operation as part of the K.ci host interface module set:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline bus interaction test
   - Offline K test selector test
   - Offline K/P memory test
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure that both A and B paths are present to all hosts.

3.5.3 Removing and Replacing the Port Processor Module (K.pli and K.pli2)

The port processor module (K.pli and K.pli2) is a part of the host interface module set (K.ci and K.ci2). In this section, the term port processor refers to both the K.pli (L0107-YA) and the K.pli2 (L0124-AA) modules, except as noted. The port processor module interfaces with the port link module indirectly through the port buffer module.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.3.1 Removing the Port Processor Module

Use the following procedure to remove the port processor module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller or shut down the system.
3. Set the DC power switch to the 0 (off) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Pull the HSC controller card cage cover up and out.
6. Locate the port processor module in slot number 12 of the card cage. This can be verified by the module utilization label.

7. Remove the port processor module.

3.5.3.2 Setting the Replacement Port Processor Module Switches

The K.pli (L0107-YA) module has factory-set dual inline pack (DIP) switches to indicate the hardware revision level. Do not change DIP switch positions, except as directed by a Field Change Order (FCO). On newer K.pli modules the switch pack has been deleted.

Figure 3–17 shows the K.pli module switchpack.

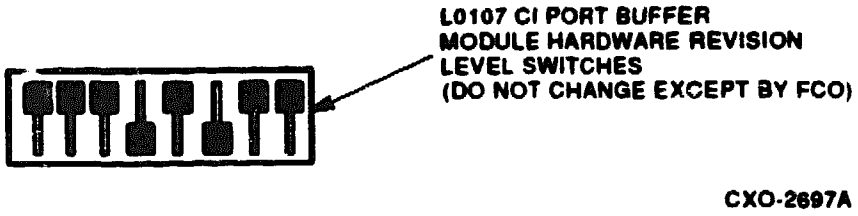


Figure 3–17 K.pli (L0107-YA) Hardware Revision Level Switch

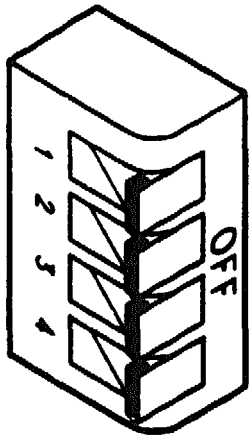
The K.pli2 (L0124-AA) module has a switchpack containing four switches. Table 3–3 shows the names and functions of these switches.

Figure 3–18 shows the K.pli2 module switchpack.

NOTE
The four switches must be in the OFF position to prevent errors during initialization and normal operation.

Table 3–3 K.pli2 (L0124-AA) Module Switchpack Functions

Switch Number	Switch Name	Function Description	Normal Position
SW1	n/a	This switch is not used.	n/a
SW2	Loop on error	K.pli2 internal diagnostics continually execute any failing internal diagnostics.	n/a
SW3	Path fault intolerant	If enabled, the internal CI path diagnostics indicate a failure if a fault is detected on either CI path.	OFF
SW4	Local diagnostics	Enables only those internal diagnostics that directly relate to the K.pli2 module. This test excludes the port buffer and port link module diagnostics.	OFF



CXO-2693A

Figure 3–18 K.pll2 (L0124-AA) Module Switchpack

3.5.3.3 Replacing the Port Processor Module

This section provides the port processor module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

1. Install the port processor module in slot number 12 of the card cage. This can be verified by the module utilization label.
2. Replace the port processor module.
3. Pull the card cage cover down and in.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Set the DC power switch to the 1 (on) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.

3.5.3.4 Testing the Port Processor Module

Run the following tests to verify correct port processor operation as part of the K.ci host interface module set.

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline bus interaction test
   - Offline K test selector test
   - Offline K/P memory test
3. Place the Secure/Enable switch in the ENABLE position.

4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to and ensure both A and B paths are present to all hosts.

3.5.4 Removing and Replacing the I/O Control Processor Module (P.ioj and P.ioc)

The P.ioj module (L0111-00, L0111-YA, L0111-YC, and L0111-YD) uses a PDP–11 ISP (J–11) processor. The P.ioc module (L0105) uses a PDP–11 ISP (F–11) processor. Both contain memory management and memory interfacing logic. These processors execute their respective HSC controller internal software. In this section, the term P.ioj/c refers to all P.ioj and P.ioc modules, except as noted.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.4.1 Removing the P.ioj/c Module

Use the following procedure to remove the P.ioj/c module. Observe safety and ESD precautions before starting the module removal procedure.

1. Enter Ctrl/Y to get the HSC> prompt. Enter the SETSHO command SHOW SYSTEM and save the printout for reference.
2. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
3. Dismount or fail over any drives connected to the HSC controller.
4. Set the DC power switch to the 0 (off) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
5. Turn the two nylon latches on the module cover plate one-quarter turn.
6. Pull the card cage cover up and out.
7. Locate the P.ioj/c module in slot number 1 of the card cage. This can be verified by the module utilization label.
8. Remove the P.ioj/c module.

3.5.4.2 Setting the Replacement P.ioj/c Module Jumpers

The P.ioj/c modules have factory-set jumpers. Each module has a unique serial number that matches the pattern of the jumpers. *Do not reconfigure these serial number jumpers.*

L0111-00 and L0111-YA modules with a revision level of F or higher have a jumper to identify the HSC controller type. The location of this jumper is shown in Figure 3–19. Check the replacement module and configure the jumper as follows:

- If the system is an HSC40, the replacement module is an L0111-YA and the jumper must be installed between pins 101 and 102. W1 and W2 should have no connection.
- If the system is an HSC60, the replacement module is an L0111-YD and the jumper must be installed between pins 101 and 102. W1 should have a connection, W2 should have no connection.

- If the system is an HSC70, the replacement module is an L0111-00 and the jumper must be installed between pins 101 and 103. W1 and W2 should have no connection.
- If the system is an HSC90, the replacement module is an L0111-YC and the jumper must be installed between pins 101 and 103. W1 should have a connection, W2 should have no connection.

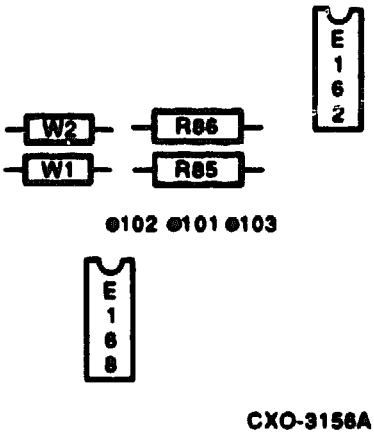


Figure 3–19 Location of HSC Controller Type Jumpers on L0111 Rev F Modules

After installing the jumper, you will get the following indications on booting the HSC:

Module/Configuration	HSC40/HSC60	HSC70/HSC90
L0111-00/YC module with correct jumper configuration	Console error message	Normal operation
L0111-YA/YD module with correct jumper configuration	Normal operation	Console error message
L0111-00/YC module incorrectly configured as -YA	No indication	Console error message
L0111-YA/YD module incorrectly configured as -00	Console error message	Red module indicators 5 through 8 stay lit

The P.ioc module (L0105) also has a baud rate jumper. When the P.ioc module is replaced, set baud rate jumper W3 to match the console terminal or duplicate the jumper configuration of the P.ioc module being replaced.

Figure 3–20 shows the P.ioc module jumper location.

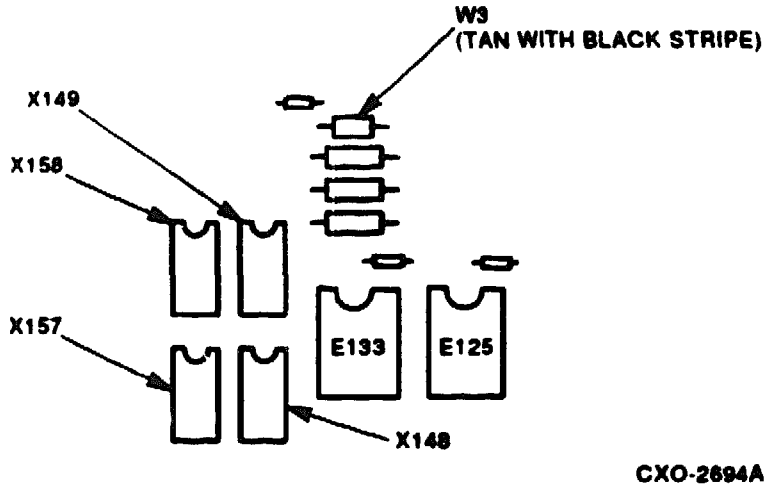


Figure 3–20 P.ioc (L0105) Baud Rate Jumper

Set the baud rate jumper as follows:

For 9600 baud, leave jumper W3 intact.
For 300 baud, cut one elbow angle on the W3 lead and spread slightly to avoid contact with the cut edges.

3.5.4.3 Replacing the P.ioj/c Module

This section provides P.ioj/c module replacement procedure. Observe safety and ESD precautions before starting module replacement procedures.

1. Install the P.ioj/c module in slot number 1 of the card cage. This can be verified by the module utilization label.
2. Pull the card cage cover down and in.
3. Turn the two nylon latches on the module cover plate one-quarter turn.
4. Set the DC power switch to the 1 (on) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.

   NOTE
   Once the host system recognizes an HSC controller, the Online indicator may show that the HSC controller is alternately going online and offline. This is because there is a discrepancy between the node name or ID of the HSC controller and the one recognized by the host for that HSC controller. The HSC controller is allowed to function only if the old node name is equal to the new node name and the old ID is equal to the new ID.

5. Enter Ctrl/Y to get the HSC> prompt, and enter the SETSHO command SHOW SYSTEM. Compare this printout with the one saved during removal.

   If the printout for the node name/ID is different, enter the SETSHO commands SET NAME or SET ID to change the node name/ID so it is the same as in the saved printout.

3.5.4.4 Testing the P.ioj/c Module

When booting the HSC controller with the offline diagnostic media, the P.ioj/c ROM bootstrap verifies the basic integrity of the P.ioj/c module.

Perform the following to verify correct P.ioj/c module operation:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline cache test (P.ioj only)
   - Offline bus interaction test
   - Offline K test selector test
   - Offline K/P memory test
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.

3.5.5 Removing and Replacing the Disk Data Channel Module (K.sdi)

The K.sdi module connects the HSC controller to the SDI. K.sdi operation is controlled by an onboard microprocessor with a programmed read-only memory (PROM). Commands and responses pass between the K.sdi microprocessor and other internal HSC controller processes through control memory.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.5.1 Removing the K.sdi Module

Use the following procedure to remove the K.sdi module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.
3. Set the DC power switch to the 0 (off) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Pull the card cage cover up and out.

6. Check the module utilization label above the card cage for the location of the K.sdi module. The module slots are numbered from right to left when viewed from the front.
7. Remove the K.sdi module.

3.5.5.2 Replacing the K.sdi Module

This section provides the K.sdi module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

1. Check the module utilization label above the card cage for the location of the module. The module slots are numbered from right to left when viewed from the front.
2. Replace the K.sdi module.
3. Pull the card cage cover down and in.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Set the DC power switch to the 1 (on) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.

3.5.5.3 Testing the K.sdi Module

Perform the following tests to verify correct K.sdi operation:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline bus interaction test
   - Offline K test selector test
   - Offline K/P memory test
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.
7. Enter the SETSHO command SHOW DISK to verify that all applicable drives are present.
8. Execute the disk drive integrity test ILDISK. Refer to Chapter 5 for a test description and procedure.

3.5.6 Removing and Replacing the Tape Data Channel Module (K.sti)

The K.sti module is an interface between the HSC controller and the standard tape interface (STI). K.sti operation is controlled by an onboard microprocessor with a programmed read-only memory (PROM). Commands and responses pass between the K.sti microprocessor and other internal HSC controller processes through control memory.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.6.1 Removing the K.sti Module

Use the following procedure to remove the K.sti module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.
3. Set the DC power switch to the 0 (off) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Pull the card cage cover up and out.
6. Check the module utilization label above the card cage for the location of the module. The module slots are numbered from right to left when viewed from the front.
7. Remove the K.sti module.

3.5.6.2 Replacing the K.sti Module

This section provides the K.sti module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

1. Check the module utilization label above the card cage for the location of the module. The module slots are numbered from right to left when viewed from the front.
2. Replace the K.sti module.
3. Pull the card cage cover down and in.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Set the DC power switch to the 1 (on) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.

3.5.6.3 Testing the K.sti Module

Perform the following to verify correct K.sti operation:

1 Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures

CAUTION
The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline bus interaction test
   - Offline K test selector test
   - Offline K/P memory test
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.
7. Run the tape drive integrity test ILTAPE. Refer to Chapter 5 for a test description and procedure.

3.5.7 Removing and Replacing the Data Channel Module (4-Port K.si and 8-Port K.si)

The 4-port K.si (L0119-YA) data channel module is a direct replacement for the K.sdi (L0108-YA) disk data channel or K.sti (L0108-YB) tape data channel modules.

The 8-port K.si (L0119-YB) data channel adds more 4 disk data channels to the 4-port K.si data channel module. The 8-port K.si module is installed in the HSC60 and HSC90 controllers only, and cannot be used with tape drive devices. In this section, the term K.si refers to both the 4-port and 8-port data channel modules, except as noted.

NOTE
The 4-port K.si data channel initializes only with HSC controller Version 3.90 or higher software. Do not use the K.si module with HSC system software with a version level lower than 3.90. Versions lower than 3.90 will cause initialization failure.

The 8-port K.si data channel module is used with HSC software Version 6.0 and higher only.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.7.1 Removing the K.si Module

Use the following procedure to remove the K.si module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.
3. Set the DC power switch to the 0 (off) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Pull the card cage cover up and out.
6. Check the module utilization label above the card cage for the location of the module. The module slots are numbered from right to left when viewed from the front.
7. Remove the K.si module.

3.5.7.2 Setting the Replacement K.si Module Switches

The K.si has a switchpack containing four switches. Table 3–4 describes the names and functions of the switches. SW1 is on the top of the switchpack.

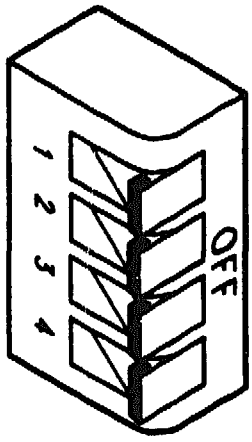
NOTE

The four switches must be in the OFF position to prevent errors during initialization and normal operation.

Table 3–4 K.si Switchpack Functions

Switch Number	Switch Name	Function Description	Normal Position
SW1	MFG	Provides loop on error and single port external loop.	OFF
SW2	Burn in	Continuous loop. Assumes external loop and clock.	OFF
SW3	Ext loop	Loops on all ports; for manufacturing or field use.	OFF
SW4	Ext clock	Substitutes external clock; for manufacturing use only.	OFF

Figure 3–21 shows the K.si module switchpack.



CXO-2693A

Figure 3–21 K.si Switchpack

3.5.7.3 Configuration of Requestors While Replacing the K.si Module

To obtain maximum performance from the HSC controller, physically configure the tape and disk requestors according to the following guidelines:

- Each K.si, K.sdi, or K.sti module in the HSC backplane has a requestor priority number according to its backplane slot. You can greatly enhance the performance of the HSC controller if the attached devices are arranged according to their transfer speeds.
- Attach the slower devices to the lower priority requestors and the faster devices to the higher priority requestors. Do this while you have the HSC controller offline for K.si installation.
- With the introduction of faster devices, such as the TA90 tape drive and RA90 disk drive, backplane configuration has become especially important. Failure to configure the devices properly could result in data bus overrun, EDC errors, and significant performance loss. Refer to the *HSC Controller User Guide* for a discussion of performance issues.

Table 3–5 shows the relative device speeds.

Table 3–5 Relative Speeds of Various Requestors

Device	Relative Speed
TA90/TA91 tape drive	Fastest
RA9x disk drive	.
ESE20 storage element (including enhanced ESE20)	.
RA82 disk drive	.
RA81 disk drive	.
RA60 disk drive	.
RA70 disk drive	.
RA80 disk drive	.
Non-TA90/TA91 tape drives	Slowest

Requestor priority ascends from Requestor 2, with the lowest priority, through the highest requestor number on the HSC controller. Note that requestor priority levels are all relative; that is, the individual requestor numbers have no intrinsic speed characteristic. If you have only one drive in your system, you will not get better performance by placing it on a high priority requestor instead of on a low priority requestor.

If it is necessary to mix TA90/TA91 tape drives with slower tape drives on a requestor, this mixing should be done on the highest priority requestor.

When configuring, it is recommended that you leave blank slots where possible to allow for add-on drives without having to move existing cables.

3.5.7.4 Replacing the K.si Module

This section provides the K.si module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

1. Refer to Table 3–5 and verify that the K.si data channel requestors are arranged according to the transfer speeds of their attached devices.
2. Check the module utilization label above the card cage for the location of the module. The module slots are numbered from right to left when viewed from the front.
3. Install the K.si module. If you are installing a new K.si data channel requestor, install the K.si in the card cage. Attach the label accompanying the K.si module to the appropriate location of the module utilization label chart.
4. If you are planning to run the recommended external loop test, disconnect the SDI cables to the bulkhead of the requestor slot for the installed K.si. Install the loopback connectors (part number 70-22953-01), and refer to the section on K.si external loop tests.
5. Pull the card cage cover down and in.
6. Turn the two nylon latches on the module cover plate one-quarter turn.
7. Set the DC power switch to the 1 (on) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.

3.5.7.5 K.si Module External Loop Test

Run the K.si External Loop Test before you initialize and configure the K.si to ensure that there are no hidden problems with the installation. Loopback connectors (part number 70-22953-01) are required for this test. These connectors are not included with the HSC controller.

The HSC controller must be offline to run this test.

1. Set SW3 of the K.si switch pack to the ON position (SW1 is at the top of the switch pack). All other switches on the switch pack must be set to OFF.
2. If you have not already done so, open the rear door and remove any SDI cables from the bulkhead of the requestor slot being tested. The 8-port K.si in slot 6, bulkheads E and L, is being tested in the example in this section.
3. Install four or eight loopback connectors to the bulkhead.
4. Set the DC power switch to 1 to restore dc power to the card cage.

5. Press and release the Init switch on the OCP to run the automatic loopback test as part of the powerup diagnostics. The following system messages appear:

```
INIPIO-I Booting...

    HSCxx Version VX.00 DD-MMM-YYYY HH:MM:SS System HSC009

Copyright 1982 Digital Equipment Corporation.  All Rights Reserved.
```

6. If the HSC controller shows an error on boot, check that the loopback connectors are seated and that the K.si modules are fully seated in the backplane.

7. Remove the system media and insert the offline diagnostic media into the load device.

8. Press and release the Init switch on the OCP.

   The load device drive-in-use LED should light within a few seconds, indicating the bootstrap is loading the offline diagnostic loader to program memory.

   The offline diagnostic loader indicates it has been loaded properly by displaying the following:

```
HSC OFL Diagnostic Loader, Version Vnnn
Radix=Octal,Data Length=Word,Reloc=00000000
ODL>
```

   The offline loader is now ready to accept commands.

9. Enter the TEST K command and run microdiagnostics 11, 12, 13, and 14. The following example shows the diagnostics run for Requestor 6. Perform these tests for each requestor installed in your system, with the loopback connectors installed for the module under test. The number of passes shown is for this example; you may perform more or fewer passes.

```
ODL> TEST K [RETURN]
```

   The test responds with:

```
HSC OFL K Test Selector Version nnn
Requestor # of K (1 thru 9) [] ? 6 [RETURN]
Test # (1 thru 17) (0) [] ? 11 [RETURN]
# of passes to perform (D) [1] ? 10 [RETURN]

    End of Pass # 0000001, 00000 Errors, 00000 Total Errors
      .
      .
      .
    End of Pass # 0000010, 00000 Errors, 00000 Total Errors

Re-use parameters (Y/N) [Y] ?  N [RETURN]
Requestor # of K (1 thru 9) [] ? 6 [RETURN]
Test # (1 thru 17) (0) [] ? 12 [RETURN]
# of passes to perform (D) [1] ? 10 [RETURN]

    End of Pass # 0000001, 00000 Errors, 00000 Total Errors
      .
      .
      .
    End of Pass # 0000010, 00000 Errors, 00000 Total Errors

Re-use parameters (Y/N) [Y] ?  N [RETURN]
Requestor # of K (1 thru 9) [] ? 6 [RETURN]
Test # (1 thru 17) (0) [] ? 13 [RETURN]
# of passes to perform (D) [1] ? 5 [RETURN]
```

```
    End of Pass # 0000001, 00000 Errors, 00000 Total Errors
    End of Pass # 0000002, 00000 Errors, 00000 Total Errors
    End of Pass # 0000003, 00000 Errors, 00000 Total Errors
    End of Pass # 0000004, 00000 Errors, 00000 Total Errors
    End of Pass # 0000005, 00000 Errors, 00000 Total Errors

Re-use parameters (Y/N) [Y] ? N [RETURN]
Requestor # of K (1 thru 9) [] ? 6 [RETURN]
Test # (1 thru 17) (O) [] ? 14 [RETURN]
# of passes to perform (D) [1] ? 5 [RETURN]

    End of Pass # 0000001, 00000 Errors, 00000 Total Errors
    End of Pass # 0000002, 00000 Errors, 00000 Total Errors
    End of Pass # 0000003, 00000 Errors, 00000 Total Errors
    End of Pass # 0000004, 00000 Errors, 00000 Total Errors
    End of Pass # 0000005, 00000 Errors, 00000 Total Errors

Re-use parameters (Y/N) [Y] ? N [RETURN]
```

The following output is an example of a loopback test failure message:

```
Requestor # of K (1 thru 9) [] ? 6 [RETURN]
Test # (1 thru 17) (O) [] ? 11 [RETURN]
# of passes to perform (D) [1] ? 5 [RETURN]

    ORTS>00:01 T#000 E#008 U-000
    O  K Timed-Out During Init
      K-Status = 370
         End of Pass # 0000001, 00001 Errors, 00001 Total Errors
```

10. If you receive a failure message, check that the loopback connectors are securely installed. Remove the K.si module and try it in a different slot. If these steps fail, replace the K.si module. Be sure to run the tests again after replacing the K.si module.
11. Set SW3 of the K.si switchpack to the OFF position.
12. Install or replace all SDI cables on the HSC controller bulkhead.

3.5.7.6 Initializing the K.si Module

The K.si is by default a disk data channel after initial installation or on first boot of the HSC software. This default can result in a mismatch between the K.si configuration and the devices attached to a 4-port K.si (the 8-port K.si can only be used with disk drive devices). The mismatch results in a series of device errors displayed on the HSC console, leading to the mismatched device(s) being declared inoperative by the HSC controller.

This mismatch can happen under the following conditions:

- After initial installation of the K.si and the attached devices are tape drives.
- After initial installation of HSC software.
- When replacing tape formatters with disk drives after the 4-port K.si has been configured for tape formatters.
- When replacing disk drives with tape formatters after the 4-port K.si has been configured for disk drives.
- When the 8-port K.si module is used with attached tape drives.

3.5.7.7 Correcting K.si Module Configuration Problems

To correct configuration problems, connect the data channel to the proper drive or use the following procedure to reconfigure the K.si:

1. Press the Init switch on the OCP. The HSC controller displays the following message to signify that initialization has started:

```
INIPIO-I Booting...

    HSCxx Version X.00 DD-MMM-YYYY HH:MM:SS System HSC009

Copyright 1982 Digital Equipment Corporation.  All Rights Reserved.
```

NOTE
The term HSCxx refers to the HSC controller model that is receiving the K.si module.

2. After initialization, enter the SETSHO command SHOW REQUESTORS to show the status of the requestors. In the following example, the 4-port K.si modules are in Requestors 2, 3, 4, 5, 7, and 8, and an 8-port K.si module is in Requestor 6. Note that the 4-port K.si modules are shown in the Type column as K.si modules, and the 8-port K.si module is shown as a K.si/8. Also, the 8-port K.si module is listed in the Microcode Loaded column as **8disk**, while the 4-port K.si microcode is listed as **disk** or **tape**.

   This example SHOW REQUESTORS display shows a configuration of requestors in the HSC backplane that may not be advisable for a given HSC controller installation.

```
Ctrl/Y
HSCxx> SHOW REQUESTORS [RETURN]
Req     Status  Type        Version                    Microcode Loaded
0       Enabled P.ioj
1       Enabled K.ci        MC- 73 DS- 3 Pila-64 K.pli-15   CI
2/A     Enabled K.si        MC- 42 DS- 3               disk
3/B     Enabled K.sdi       MC- 42 DS- 3               n/a
4/C     Enabled K.sdi       MC- 42 DS- 3               n/a
5/D     Enabled K.si        MC- 12 DS- 4               disk
6/E     Enabled K.si/8      MC- 17 DS- 3               8disk
7/F     Enabled K.sdi       MC- 42 DS- 3               n/a
8/M     Enabled K.si        MC- 42 DS- 3               disk
9/N     Enabled Empty
SETSHO-I Program Exit
```

3. Change the configuration of Requestors 2 and 8 to tape data channels. Enter reconfiguring commands as shown, then reinitialize the system.

NOTE
Ensure the system load media is write enabled.

```
Ctrl/Y
HSCxx> RUN SETSHO [RETURN]
SETSHO> ENABLE REBOOT [RETURN]
SETSHO-S The HSC will reboot on exit.
SETSHO> SET REQUESTOR 2/TYPE=TAPE [RETURN]
SETSHO> SET REQUESTOR 8/TYPE=TAPE [RETURN]
SETSHO> EXIT [RETURN]
SETSHO-Q Rebooting HSC, type Y to continue, CTRL/Y to abort: Y

INIPIO-I Booting...

    HSCxx Version X.00 DD-MMM-YYYY HH:MM:SS      System HSC009

Copyright 1982 Digital Equipment Corporation.  All Rights Reserved.
```

This configuration is retained on the boot media to ensure that the K.si module comes up in the proper data channel configuration when the HSC controller is rebooted. If you have a K.si configured as a tape data channel and you attach disk drives, you can reconfigure it using the above procedure and specifying TYPE=DISK or, for the 8-port K.si module, TYPE=8DISK. The *HSC Controller User Guide* contains complete information on the SETSHO command SET REQUESTOR.

4. Use the SHOW REQUESTORS command again to verify the current configuration of the K.si modules:

```
Ctrl/Y
HSCxx> SHOW REQUESTORS RETURN
Req     Status  Type        Version                    Microcode Loaded
0       Enabled P.ioj
1       Enabled K.ci        MC- 73 DS- 3 Pila-64 K.pli-15   CI
2/A     Enabled K.si        MC- 17 DS- 3               tape
3/B     Enabled K.sdi       MC- 42 DS- 3               n/a
4/C     Enabled K.sdi       MC- 42 DS- 3               n/a
5/D     Enabled K.si        MC- 12 DS- 4               disk
6/E     Enabled K.si/8      MC- 12 DS- 4               8disk
7/F     Enabled K.sdi       MC- 42 DS- 3               n/a
8/H     Enabled K.si        MC- 17 DS- 3               tape
9/N     Enabled Empty
SETSHO-I Program Exit
```

3.5.7.8 K.si Module New Boot Microcode

When changing to a new boot media, you must power down the HSC controller to clear the old microcode from the K.si. A power-down interval of about 15 seconds is adequate. After powering up again, reboot and use the following procedure:

1. Enter the SETSHO command SHOW REQUESTORS to check the existing configuration and verify necessary changes.
2. Enter the SET REQUESTOR command for each K.si in the HSC controller to set the HSC controller configuration on the new boot media.

Table 3–6 describes the conditions that determine if new K.si microcode is loaded.

Table 3–6 K.si Module New Microcode Load Conditions

Action	New Microcode Load
Using the SET REQUESTOR n/TYPE=xxxx command and allowing the HSC controller to automatically reboot when exiting SETSHO	Yes
Using the SET REQUESTOR n/TYPE=xxxx command and not rebooting by issuing a Ctrl/C to exit SETSHO.	No
Booting the system after a total power fail or after turning off the HSC controller.	Yes
Changing requestor modules. This action requires power down of the HSC controller.	Yes
Changing to new boot media of same version HSC software.	Yes—The new microcode is loaded when the new media is first booted.
Changing to new boot media of different version HSC software.	Yes
Using the SET SCT CLEAR command.	Yes—With media that has been previously booted, hold the Fault switch until the *INIPIO-I Booting...* message appears.
Holding in the Fault switch while pushing in the Init switch. This action clears the system configuration table (SCT).	No

3.5.7.9 Testing the K.si Module (After Initialization)

The K.si module is one of the K requestor interface modules. Perform the following to verify correct K.si operation:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline bus interaction test
   - Offline K test selector test
   - Offline K/P memory test

3.5.7.10 Completing the Installation Procedure

Complete the K.si module installation procedure as follows:

1. Place the Secure/Enable switch in the ENABLE position.
2. Boot the HSC controller with the system media by pressing and releasing the Init switch.
3. Bring the HSC controller online by pressing and releasing the the Online switch.
4. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.
5. If the K.si is configured as a disk data channel, run the disk drive integrity test ILDISK. Refer to Chapter 5 for test description and procedure.
6. If the K.si is configured as a tape data channel, run the tape drive integrity test ILTAPE. Refer to Chapter 5 for test description and procedure.

3.5.8 Removing and Replacing the 32-Mbyte Cache Module (M.cache)

The M.cache module (L0121–AA) option is available for the HSC60 and HSC90 controllers. This procedure explains how to remove, replace, and test the M.cache.

3.5.8.1 Software Version Requirement

The M.cache initializes only with Version 6.00 or higher software. Earlier software versions are not compatible with the M.cache module.

CAUTION

Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.8.2 Removing the M.cache Module

Use the following procedure to remove the M.cache module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.
3. Set the DC power switch to the 0 (off) position. On the HSC controller, the DC power switch is located on the upper left side of the RX33 disk drive housing.
4. Locate the M.cache module in slot 11 of the card cage.
5. Remove the M.cache module.

3.5.8.3 Replacing the M.cache Module

This section describes the M.cache module replacement procedure. Observe safety and ESD precautions before starting the module removal procedure.

1. Verify that the new M.cache module has a jumper installed between pins 1 and 2. If the jumper is installed between pins 3 and 4, move it to pins 1 and 2. Refer to Figure 3–22 for the location of the jumper.
2. Install the M.cache module in slot 11 of the card cage.
3. If not already done, attach the label accompanying the M.cache module to the appropriate location on the module utilization label chart.
4. Pull the card cage cover down and push in.
5. Turn the two nylon latches on the module cover plate one-quarter turn to the left.
6. Set the DC power switch to the 1 (on) position. On the HSC controller, the DC power switch is located on the upper left side of the RX33 disk drive housing.

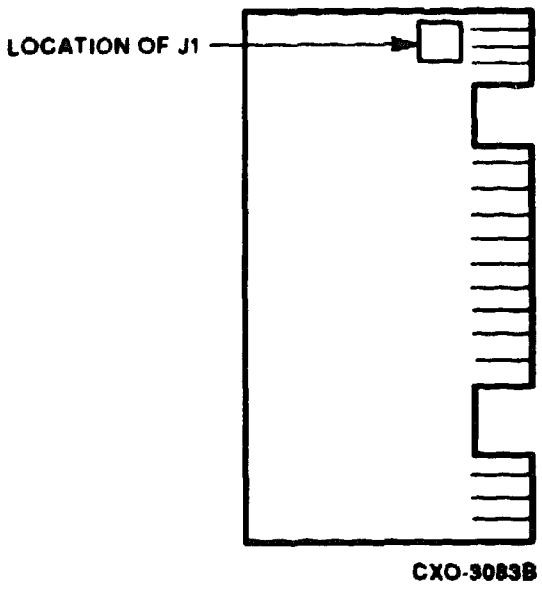


Figure 3–22 Location of M.cache Module Jumper J1

3.5.8.4 Testing the M.cache Module

This section covers the offline and device integrity tests to be performed after replacing the M.cache module.

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and perform the following tests:
   - Offline bus interaction test
   - Offline M.cache test
3. Set the Secure/Enable switch to the SECURE position.
4. Remove the offline diagnostic diskette and install the HSC software diskette.
5. Boot the HSC controller by pressing and releasing the the Init switch. The HSC controller displays the following boot message on the console:

```
INIPIO-I Booting...

    HSCxx Version VX.00 DD-MMM-1990 17:00:41    System HSC009

Copyright 1982 Digital Equipment Corporation. All Rights Reserved.
```

   The HSC controller model and the system name are site specific. The results of the power-up diagnostics test of the M.cache module will be displayed on the terminal.

As part of the self test diagnostics, there will be activity on the board LED indicators. Disregard this activity unless an indicator stays on for more than 60 seconds. The following table lists the indicator functions.

Table 3–7 M.cache Module Indicator Functions

Color	Function
Green	Board status—Indicates the operating software is running and the self-test microdiagnostics have successfully completed. D1 of 3-LED pack.
Yellow	Indicates that the module is running self test diagnostics. D2 of 3-LED pack
Red	Board status—Indicates an inoperable module, except during initialization when it comes on during module testing. D3 of 3-LED pack
Amber	LED pack D1–D8—Indicates module status as follows: D1—Single bit ECC error detected D2—Multiple bit ECC error detected D3—High byte data memory parity error detected D4—Low byte data memory parity error detected D5—Functional state machine active D6—Diagnostic state machine active D7—M.cache module waiting to be enabled D8—Pattern compare failure detected

6. Before testing the M.cache module itself, you must test the cache interface on the M.st4 memory module. To do this, refer to Chapter 5 and run the device integrity test ILMEMY. This diagnostic was automatically run as a result of normal power up, but re-running it now will display further information about memory status.
7. Refer to Chapter 5 and run the device integrity test ILCACH. This diagnostic was automatically run as a result of normal power up, but rerunning it now displays further information about M.cache status.
8. Activate the M.cache module functionality as shown in the following example: Activate the M.cache module functionality as shown in the following example:

```
[SETVC]
HSC> SHOW SETSHO [RETURN]
SETSHO> SET SERVER DISK/CACHE [RETURN]
SETSHO-I You must EXIT SETSHO to update the drive cache state.
SETSHO> SET D8 CACHE [RETURN]
SETSHO> EXIT
SETSHO-I Program Exit
[SETVC]
HSC> SHOW SERVER CACHE
Cache Status
        Supervisor mode initialized
        Cache hardware present
        ILCACH run
        Cache tests good
        Cache Size Threshold: 8. blocks
        ERASE Purge Threshold: 256. blocks
        WRITE Threshold: 8. blocks
        Transfer Defined Extent size: 16. blocks
SETSHO-I Program Exit
```

3.5.9 Removing and Replacing the HSC Memory Module (M.std2 and M.std4)

Memory modules M.std2 (L0117A) and M.std4 (L0123-AA) are used in the HSC controller only. In this section, the term memory module refers to both the M.std2 and M.std4 modules, except where indicated. The memory module contains three independent systems memories, each residing on a different bus in the HSC controller. In addition, the memory module contains the RX33 diskette controller.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.9.1 Removing the Memory Module

Use the following procedure to remove the memory module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.
3. Set the DC power switch to the 0 (off) position.

   On the HSC controller the DC power switch is located on the side of the RX33 housing.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Pull the card cage cover up and out.
6. Locate the memory module in slot number 2 of the card cage. This can be verified by the module utilization label.
7. Remove the memory module.

3.5.9.2 Replacing the Memory Module

This section provides the memory module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

CAUTION
The switch pack on the memory module is factory set to calibrate the RX33 diskette controller. Do not change the setting of this switch pack; the switch settings are unique to each module and cannot be restored outside of the manufacturing environment.

1. Install the memory module in slot number 2 of the card cage. This can be verified by the module utilization label.
2. Replace the memory module.
3. Pull the card cage cover down and in.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Set the DC power switch to the 1 (on) position. On the HSC controller the DC power switch is located on the side of the RX33 housing.
6. Enter Ctrl/C to get the HSC> prompt.
7. Enter the SET MEMORY ENABLE ALL command.

8. After the HSC controller reboots, enter the SHOW MEMORY command. Check that the available memory is equal to the maximum memory, except for 32 (decimal) words, which are disabled for lock functionality.

3.5.9.3 Testing the Memory Module

Perform the following to verify correct memory module operation:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline bus interaction test
   - Offline K/P memory test
   - Offline memory test
   - Offline refresh test
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS and ensure both A and B paths are present to all hosts.
7. Run the memory integrity test ILMEMY. Refer to Chapter 5 for a test description and procedure.

3.5.10 Removing and Replacing the HSC50 Memory Module (M.std)

The HSC50 controller memory module (L0106) contains three separate and independent systems memories, each residing on a different bus within the HSC50 controller.

CAUTION
Do not handle HSC controller modules unless you have taken proper precautions against electrostatic discharge (ESD). When handling modules, wear the ESD grounding wrist strap provided inside the front door of the HSC controller. Do not put modules on anything other than a properly grounded antistatic work surface.

3.5.10.1 Removing the M.std Module

Use the following procedure to remove the M.std module. Observe safety and ESD precautions before starting the module removal procedure.

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.
3. Set the DC power switch to the 0 (off) position.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Pull the card cage cover up and out.

6. Locate the M.std module in slot number 2 of the card cage. This can be verified by the module utilization label.
7. Remove the M.std module.

3.5.10.2 Replacing the M.std Module

This section provides the M.std module replacement procedure. Observe safety and ESD precautions before starting the module replacement procedure.

1. Install the M.std module in slot number 2 of the card cage. This can be verified by the module utilization label.
2. Replace the M.std module.
3. Pull the card cage cover down and in.
4. Turn the two nylon latches on the module cover plate one-quarter turn.
5. Set the DC power switch to the 1 (on) position.

   On the HSC50 controller, the DC power switch is located on the maintenance access panel.
6. Enter Ctrl/C to get the HSC> prompt.
7. Enter the SET MEMORY ENABLE ALL command.
8. After the HSC50 controller reboots, enter the command SHOW MEMORY. Check that the available memory is equal to the maximum memory, except for 32 (decimal) words, which are disabled for lock functionality.

3.5.10.3 Testing the M.std Module

Run the following tests to verify correct M.std operation.

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.
2. Refer to Chapter 6 for test descriptions and procedures and run the following tests:
   - Offline bus interaction test
   - Offline K/P memory test
   - Offline memory test
   - Offline refresh test
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.
7. Run the memory integrity test ILMEMY. Refer to Chapter 5 for a test description and procedure.

3.6 Removing and Replacing Subunits

This section contains procedures for removing and replacing subunits.

WARNING:
Because hazardous voltages exist inside the HSC controller service must be performed only by qualified people. Bodily injury or equipment damage can result from improper servicing procedures.

3.6.1 Removing and Replacing the RX33 Disk Drive

Two RX33 disk drives are used to load the HSC software or offline diagnostics. The RX33 disk drives are mounted in the HSC controller cabinet. A cover plate ensures proper air flow and cooling. When removing and replacing the RX33, avoid snagging the cables attached to the rear of the drive. After replacing an RX33, always replace the cover plate.

3.6.1.1 Removing the RX33 Disk Drive

Use the following procedure to remove the RX33 disk drive:

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.

3. Turn off the DC power switch, located on the side of the RX33 housing as shown in Figure 3–23.

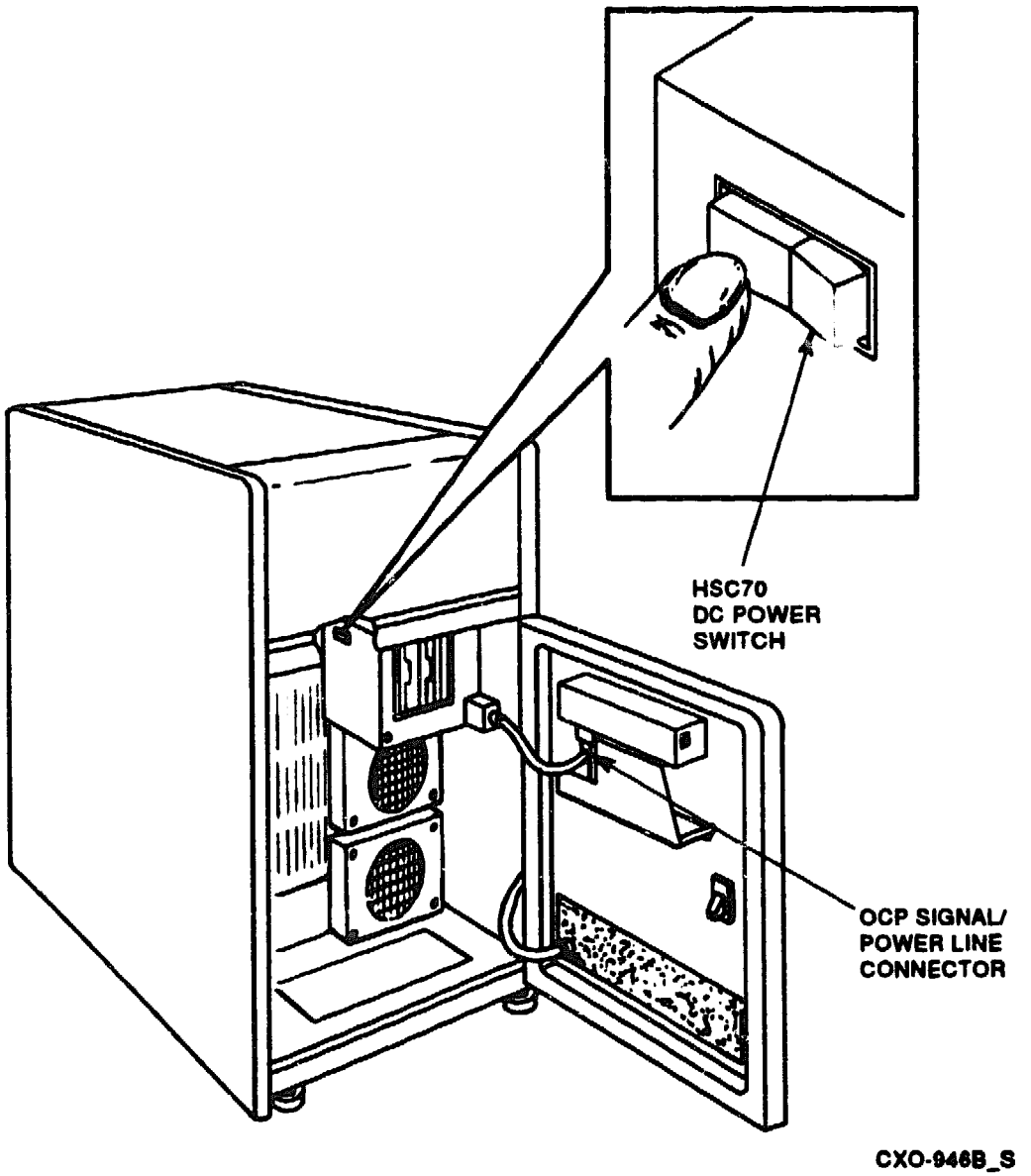


Figure 3–23 HSC DC Power Switch

4. Rotate the four fasteners on the RX33 cover plate one-quarter turn and remove the cover plate, shown in Figure 3–24.

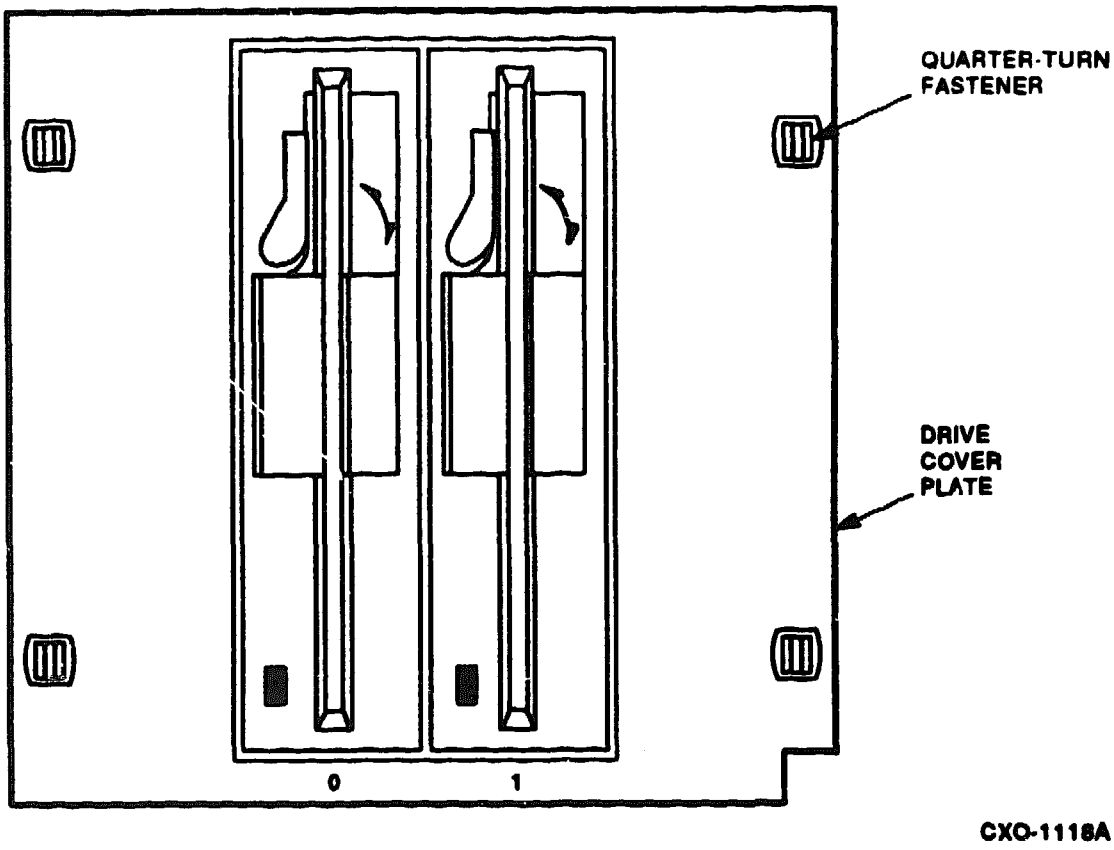


Figure 3–24 Removing the RX33 Cover Plate

5. Loosen the two captive screws holding the drive assembly and mounting plate to the cabinet frame.

CAUTION
Avoid snagging the cables attached to the rear of the drives during the next step.

6. Carefully slide the drive assembly out until the housing is cleared.
7. Support the drive assembly with one hand and remove the flat ribbon cables and power cables from the rear of the drives.
8. Determine whether drive 0 or drive 1 should be replaced.

9. Loosen the captive screws on the drive to be replaced and remove the drive from the drive assembly as shown in Figure 3–25.

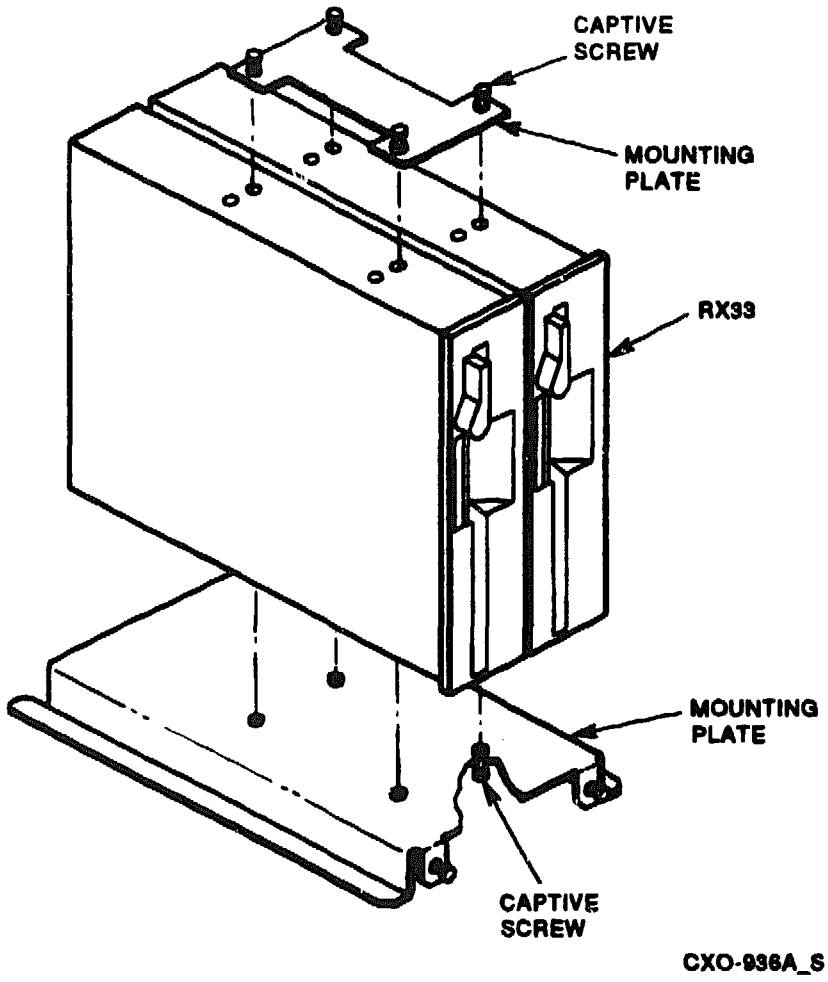


Figure 3–25 RX33 Disk Drive Removal

3.6.1.2 Setting the RX33 Disk Drive Jumpers

Replacement RX33 drives are not configured for the HSC controller. Two identical jumpers (part number 12-18783-00) must be added. If no extra jumpers are available, remove the jumpers from the defective drive. Correct jumper configuration is necessary for the operation of the replacement RX33 drive.

If replacing drive 0, be sure to insert jumper DS0. If replacing drive 1, be sure to insert jumper DS1.

The RX33 module may be revision A1 or A3. Table 3–8 shows the jumper differences and configurations for both revisions when the drive is used in an HSC controller.

Table 3–8 RX33 Jumper Description

Rev A1 Name	Rev A3 Name	Description	Status In or Out
FG	FG	Frame ground	In
HG		Hi gain	In
LG		Lo gain	Out
I	SI	Speed, mode 1 Dual speed	Out
II	II	Speed, mode 2 360 RPM only	In
DS0	D0	Drive select 0	In to select drive 0
DS1	D1	Drive select 1	In to select drive 1
DS2	D2	Drive select 2	Out
DS3	D3	Drive select 3	Out
U1	U0	Selects mode of operation for loading the heads and lighting the bezel LED [1]	In
U2	U1	See U1/U0 above	In
HL	HL	Not applicable to HSC controller use	Out
IU	IU	Not applicable to HSC controller use	Out
	ML	Motor enable	Out
RE		Recalibration	Out
DC	DC1	Disk changed on pin 34	Out
	DC2	Factory setting	In
	DC3	Not applicable to HSC controller use	Out
	DC4	Not applicable to HSC controller use	Out
RY	RY	Ready on pin 34	In

[1]The HSC controller loads the heads and lights the drive-in-use LED when the DRIVE SELECT n and READY signals are both true.

Figure 3–26 shows the jumper locations for RX33 disk drive with a revision A1 module.

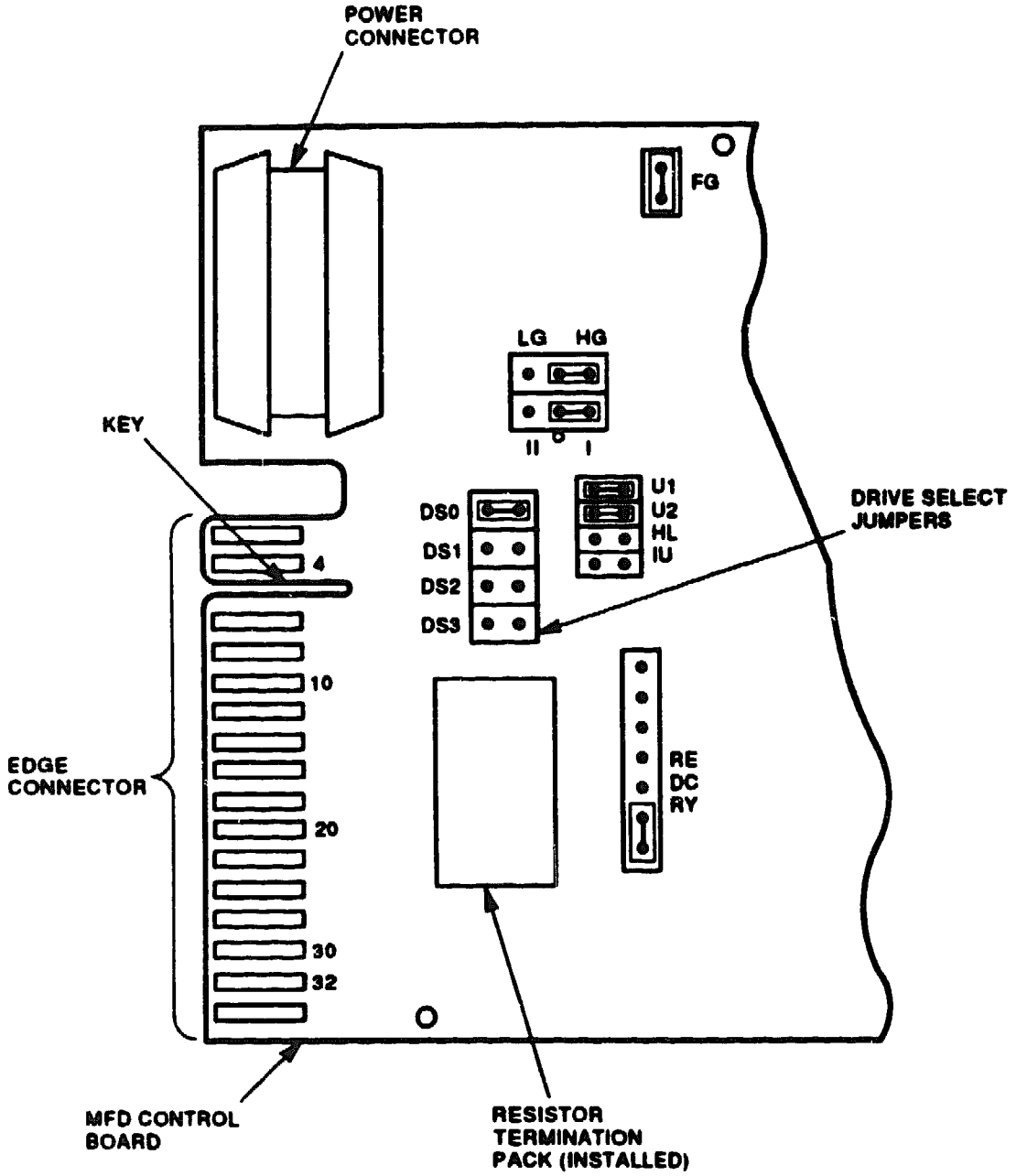


Figure 3–26 Revision A1 Jumper Configurations

Figure 3–27 shows the jumper locations for RX33 disk drive with a revision A3 module.

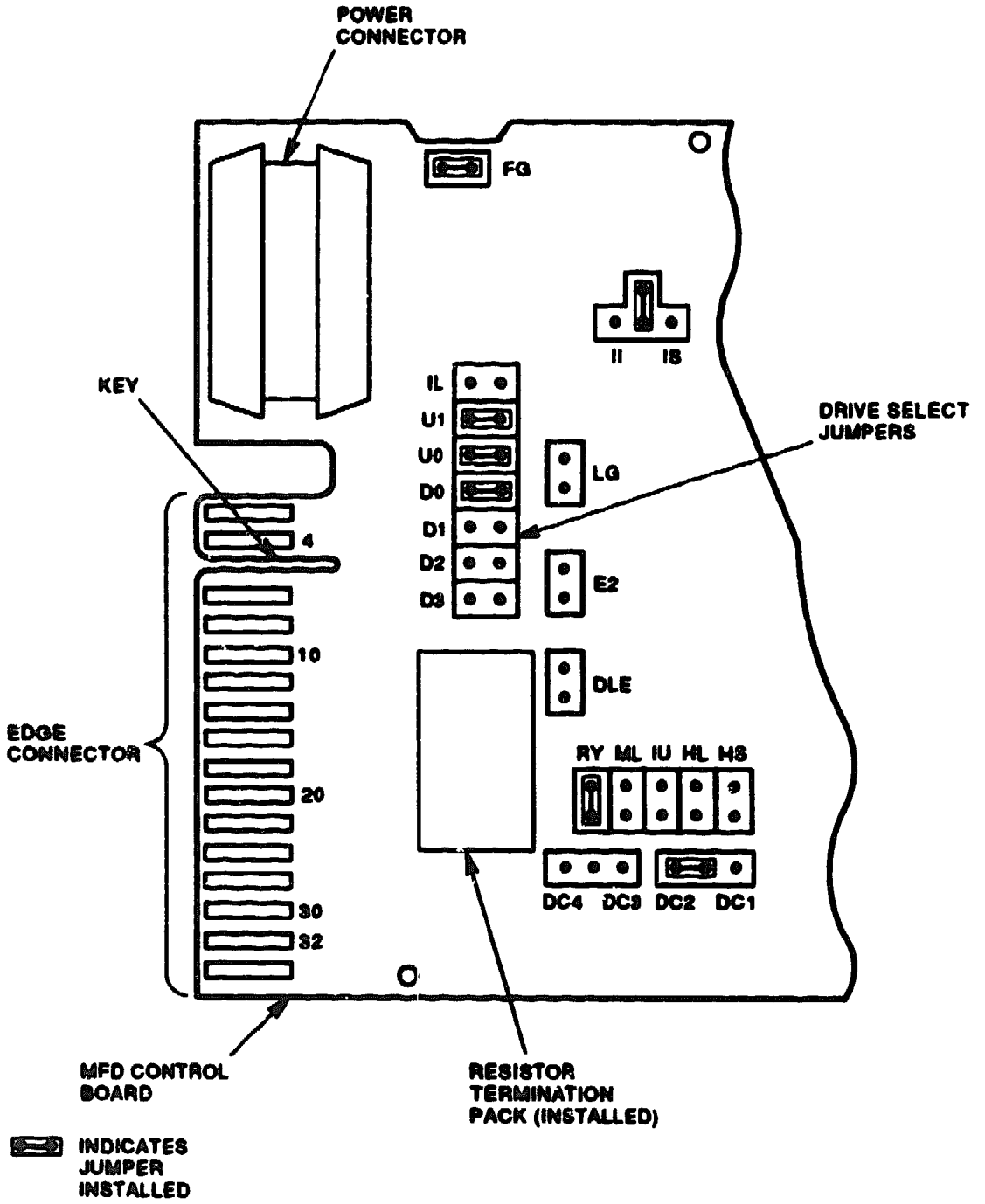


Figure 3–27 Revision A3 Jumper Configurations

3.6.1.3 Replacing the RX33 Disk Drive

Use the following procedure to replace the RX33 disk drive assembly:

1. Replace the drive in the drive assembly and tighten the drive captive screws.
2. Support the drive assembly with one hand and attach the flat ribbon cables and power cables to the rear of the drives.
3. Carefully slide the drive assembly into the drive housing.
4. Replace the cover plate and tighten the captive screws holding the drive assembly.
5. Replace the ac plug in the wall socket and place the main power switch on the power controller in the ON position.
6. The drive-in-use LED lights while the drive is accessed and extinguishes after the drive access is completed or after the drive motor stops.

3.6.1.4 Testing the RX33 Disk Drive

After replacing the RX33 disk drive, use the following procedure to test the drive:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Refer to Chapter 6 for a test description and procedure and run the RX33 offline exerciser OFLRXE.
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.
7. Refer to Chapter 5 for test description and procedure and run the RX33 device integrity test ILRX33.

3.6.2 Removing and Replacing the TU58 Tape Drive

Two TU58 tape drives are used to load the HSC50 software or offline diagnostics. The TU58 tape drives are mounted on the rear of the HSC50 controller front door.

CAUTION
When servicing the TU58 tape drive, avoid bending the tachometer disk mounted on the drive motor shaft. If the disk is bent but not creased, it may be straightened. If the disk cannot be straightened or if it is creased, the TU58 tape drive must be replaced. The disk should not rub against the optical sensor block or dangling wires.

3.6.2.1 Removing the TU58 Tape Drive

Use the following procedure to remove the TU58 tape drive:

1. Notify users that the HSC controller is being taken offline and the drives attached to it will not be available.
2. Dismount or fail over any drives connected to the HSC controller.
3. Remove the maintenance access panel cover by loosening the four captive screws.
4. Turn off the DC power switch, shown in Figure 3–28.

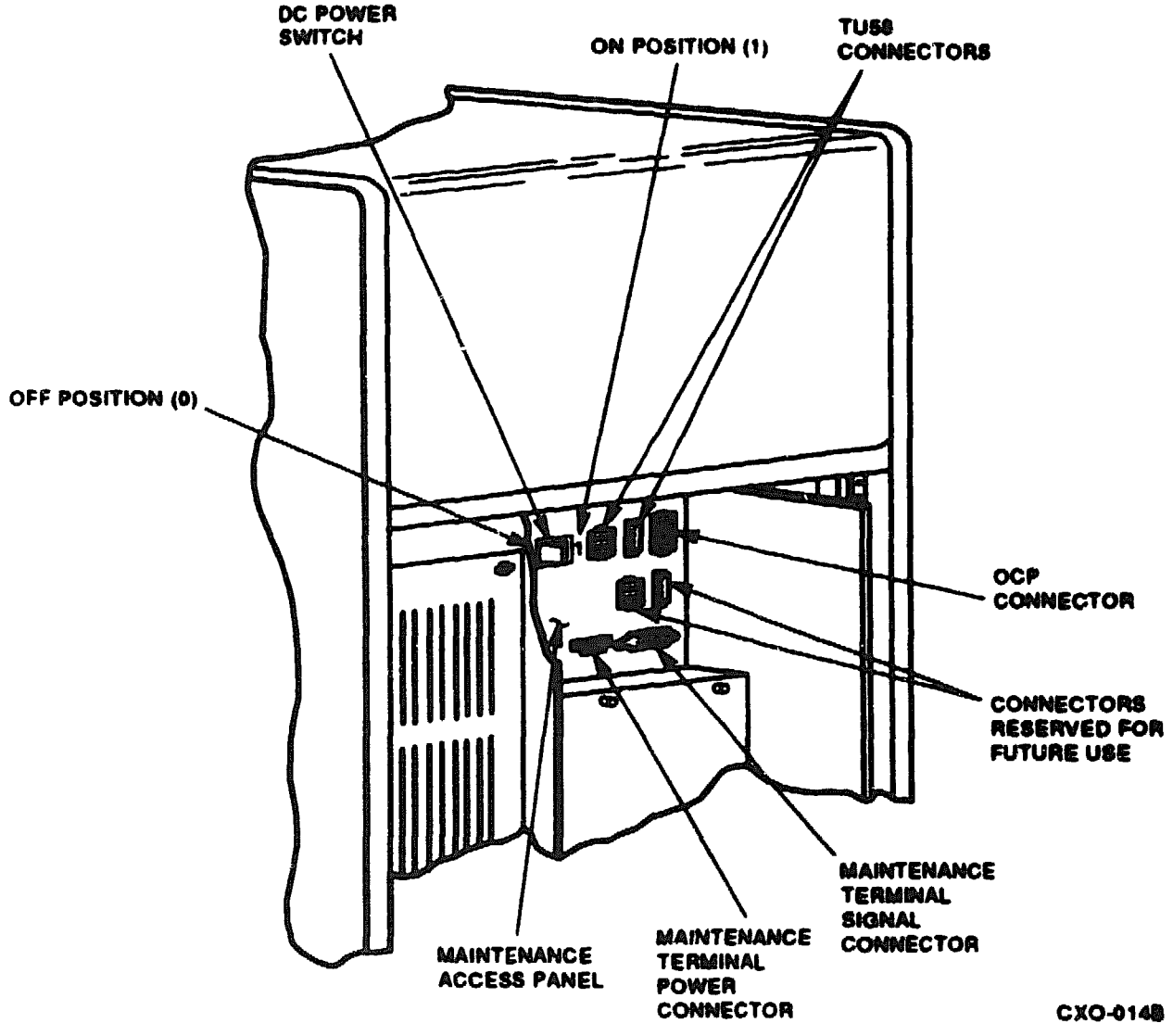


Figure 3–28 HSC50 DC Power Switch

5. Remove the two locknuts on the bottom of the TU58 bezel assembly, shown in Figure 3–29.

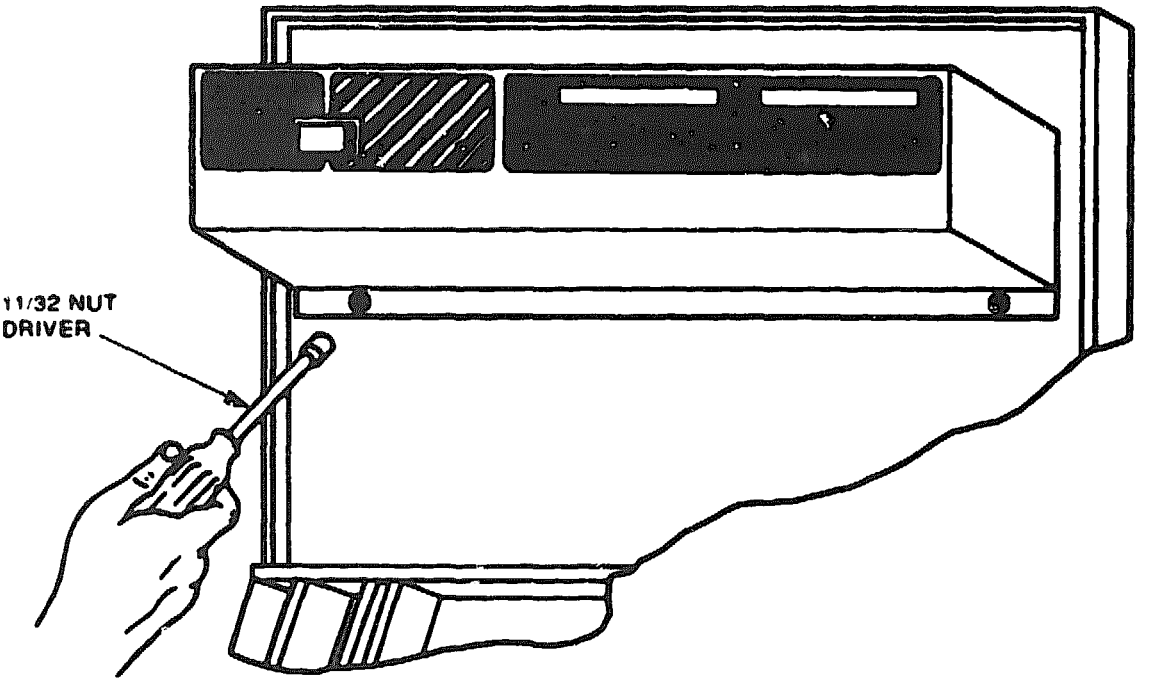


Figure 3–29 Removing the TU58 Bezel Assembly

6. Push the bezel assembly up about 1 inch to clear the mounting hooks from their slots.
7. Pull the bezel assembly back 3 to 4 inches from the door for clearance.

8. Support the bezel assembly with one hand and disconnect J3 and J4 from the OCP, shown in Figure 3–30.

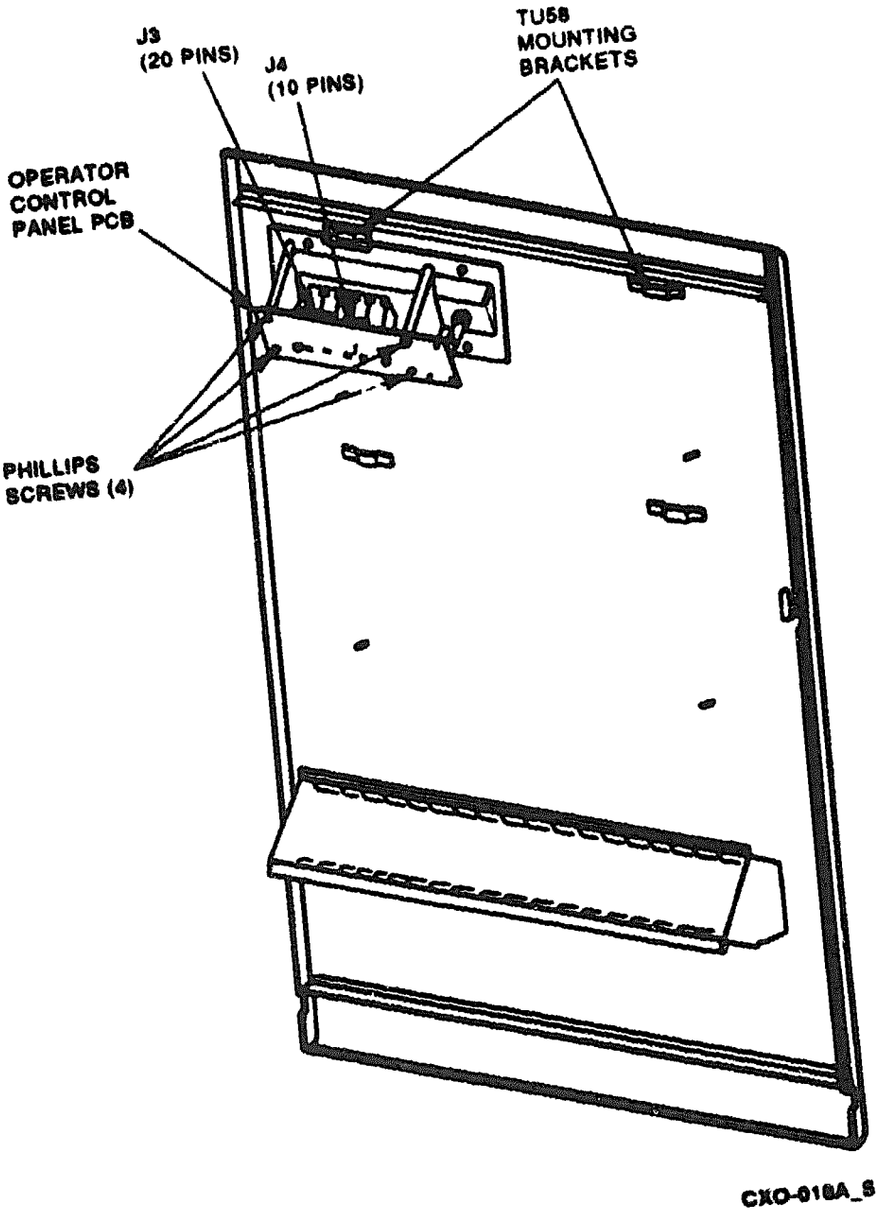


Figure 3–30 Disconnecting the H9C58 OCP Cables

9. Disconnect the cables from the TU58 controller module, shown in Figure 3–31.

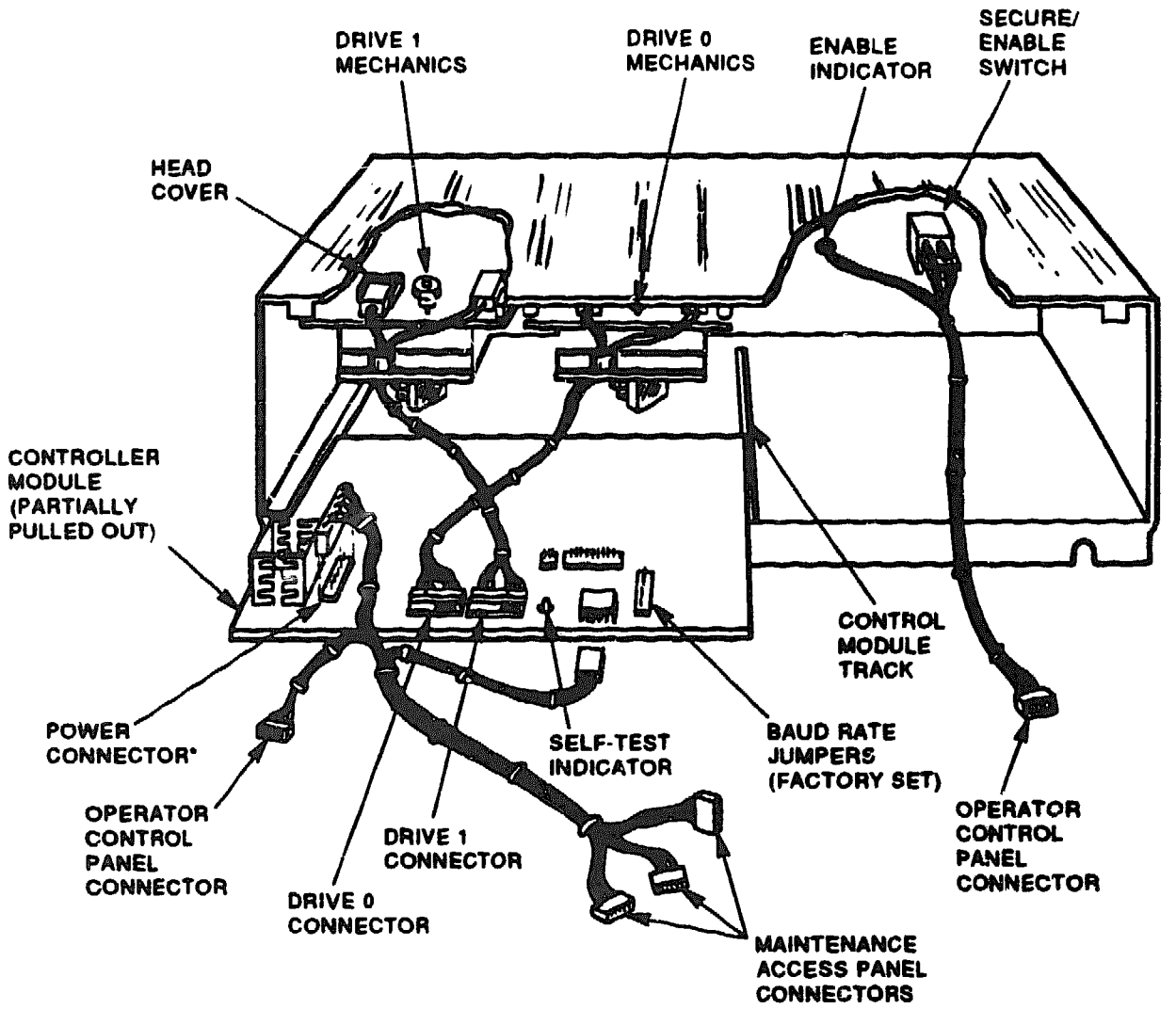


Figure 3–31 Disconnecting the HSC50 TU58 Controller Cables

NOTE
Remove the head cover connector shown in the upper left of Figure 3–31 during operation.

10. Slide the TU58 controller module out of the plastic guides.

3.6.2.2 Setting the TU58 Tape Drive Jumpers

The TU58 baud rate jumpers are factory set. Ensure the baud rate jumper setting on the new module is the same as on the module being replaced.

Figure 3–32 shows the TU58 jumper location.

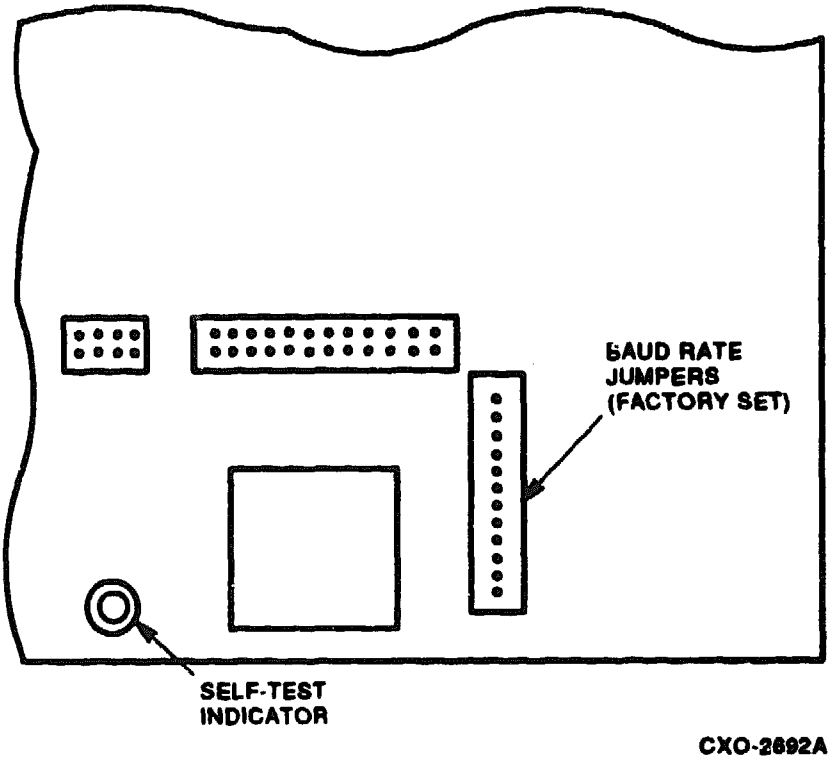


Figure 3–32 TU58 Baud Rate Jumpers

3.6.2.3 Replacing the TU58 Tape Drive

Following is the procedure for replacing the TU58 tape drive:

CAUTION
When servicing the TU58 tape drive, avoid bending the tachometer disk mounted on the drive motor shaft. If the disk is bent but not creased, it may be straightened. If the disk cannot be straightened or if it is creased, the TU58 tape drive must be replaced. The disk should not rub against the optical sensor block or dangling wires.

1. Slide the controller module into the housing on the plastic guides.
2. Connect the cables to the TU58 controller module.
3. Support the bezel assembly with one hand and connect J3 and J4 to the OCP.
4. Attach the bezel assembly to the mounting hooks.
5. Replace the two locknuts on the bottom of the TU58 bezel assembly.
6. Replace the ac plug in the wall socket and place the main power switch on the power controller to the ON position.

3.6.2.4 Testing the TU58 Tape Drive

After replacing the TU58, use the following procedure to test the drive:

1. Place the Secure/Enable switch in the ENABLE position.
2. Boot the HSC controller with the system media by pressing and releasing the Init switch.
3. Bring the HSC controller online by pressing and releasing the the Online switch.
4. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS and ensure both A and B paths are present to all hosts.
5. Run TU58 device integrity test ILTU58. Refer to Chapter 5 for a description and procedure for this test.

3.6.3 Removing and Replacing the HSC Operator Control Panel (OCP)

If any OCP lamp fails, replace the entire OCP.

3.6.3.1 Removing the HSC OCP

Use the following procedure to remove the HSC OCP:

1. Open the front door by turning the key clockwise and lifting the latch.
2. Turn off the DC power switch located on the side of RX33 housing.
3. Remove the four Kepnuts securing the OCP shield to the studs on the front door.
4. Remove the OCP shield.

5. Remove the four screws securing the OCP to the shield shown in Figure 3–33.

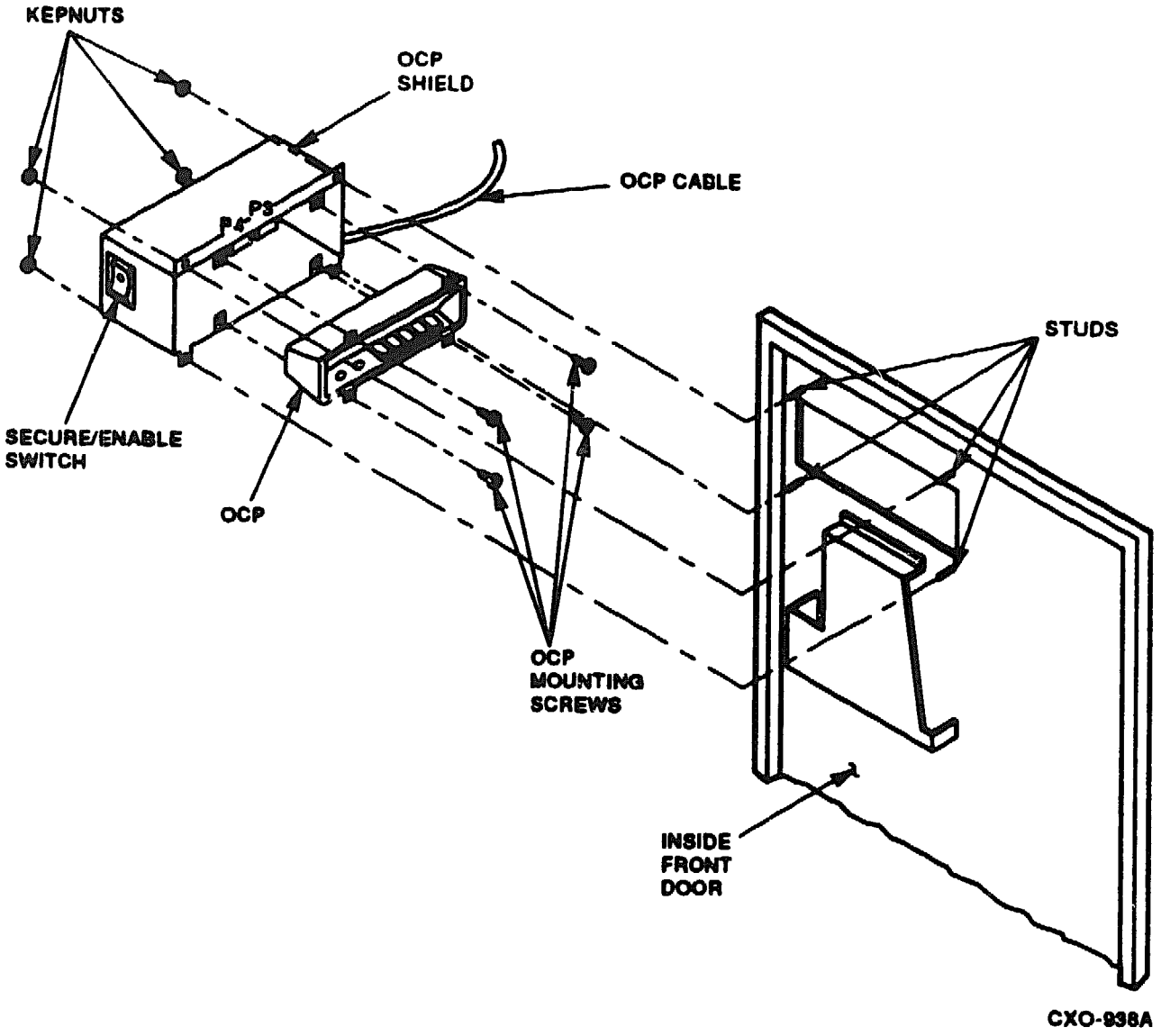


Figure 3–33 Removing the HSC OCP

6. Remove the two connectors from the printed circuit board on the OCP.
7. Pull out the OCP, carefully allowing for indicator and switch clearance.

3.6.3.2 Replacing the HSC OCP

Following is the procedure for replacing the OCP:

1. Replace the two connectors from the printed circuit board on the OCP.
2. Secure the OCP to the shield using the four screws that were removed.
3. Replace the OCP shield.
4. Replace the four Kepnuts securing the OCP shield to the studs on the front door.
5. Turn on the DC power switch located on the side of RX33 housing.

6. Close and secure the front door by turning the key counter-clockwise.

3.6.3.3 Testing the HSC OCP

After replacement, use the following procedure to test the OCP:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   CAUTION
   The offline diskette must be write protected. Place a write-protect tab over the diskette write-enable notch.

2. Run the offline OCP test. Refer to Chapter 6 for a test description and procedures.
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.

3.6.4 Removing and Replacing the HSC50 Operator Control Panel (OCP)

OCP indicators are not field replaceable. If any lamp fails, replace the entire OCP.

3.6.4.1 Removing the HSC50 OCP

Use the following procedure to replace the HSC50 OCP:

1. Open the front door by turning the key clockwise.
2. Remove dc power.
3. Remove the TU58 tape drives. Refer to Section 3.6.2 for this procedure.
4. Remove J3 and J4 from the OCP as shown in Figure 3–34.
5. Remove the four screws from the OCP as shown in Figure 3–34.
6. Carefully pull out the OCP, allowing for indicator and switch clearance.

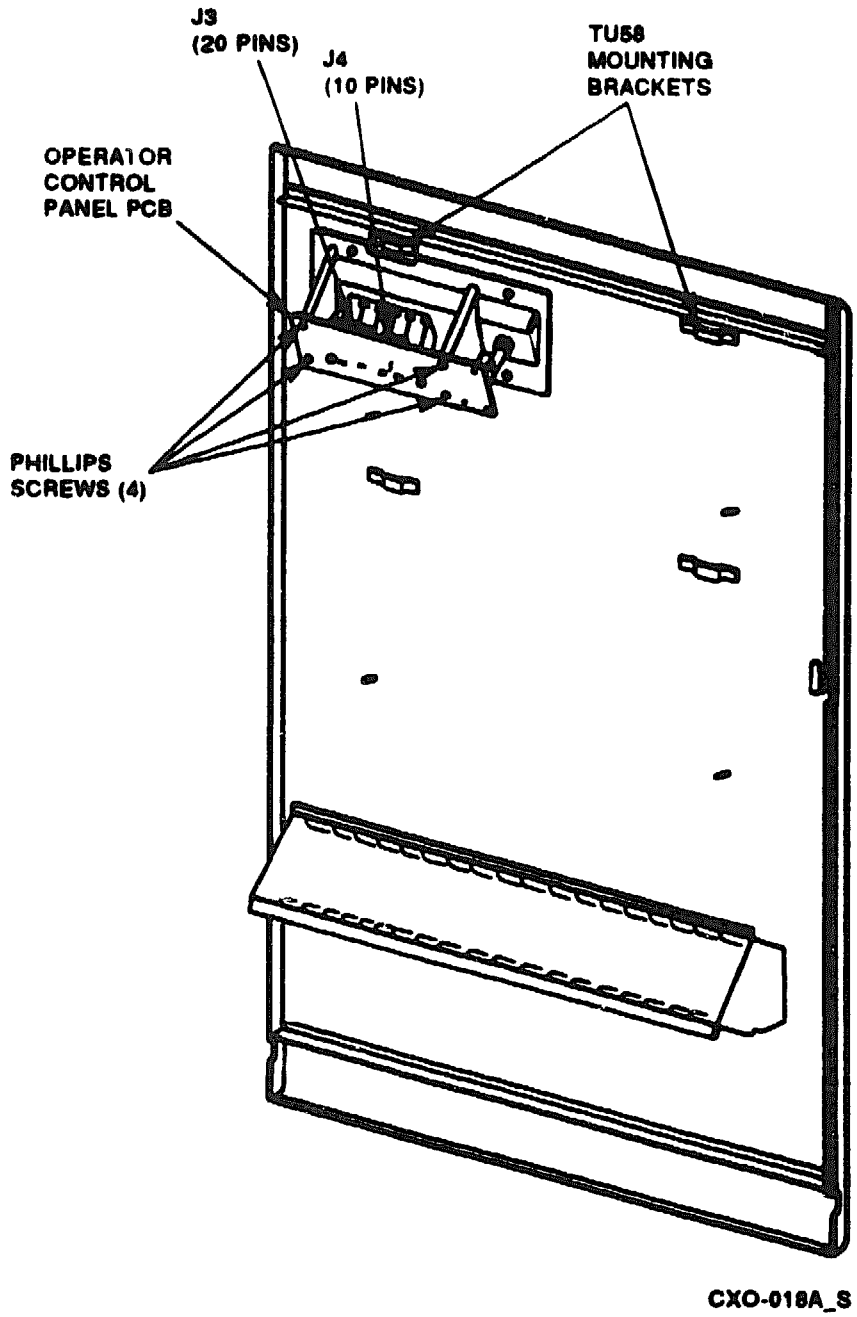


Figure 3–34 Removing the HSC50 OCP

3.6.4.2 Replacing the HSC50 OCP

Following is the procedure for replacing the OCP:

1. Carefully replace the OCP, allowing for indicator and switch clearance.
2. Replace the four OCP screws (Figure 3–34).
3. Connect J3 and J4 to the OCP (Figure 3–34).
4. Replace the TU58 tape drives. Refer to Section 3.6.2 for the procedure.
5. Turn on the dc power.
6. Close the front door by turning the key counterclockwise.

3.6.4.3 Testing the HSC50 OCP

After replacement, use the following procedure to test the OCP:

1. Boot the HSC controller with the offline diagnostic media. Refer to Chapter 6 for boot procedures.

   NOTE
   The offline tape cartridge must be write protected. Slide the write-protect selector to the full right position to enable write protection.

2. Run the offline OCP test. Refer to Chapter 6 for a test description and procedure.
3. Place the Secure/Enable switch in the ENABLE position.
4. Boot the HSC controller with the system media by pressing and releasing the Init switch.
5. Bring the HSC controller online by pressing and releasing the Online switch.
6. Enter the SETSHO command SHOW VIRTUAL_CIRCUITS to ensure both A and B paths are present to all hosts.

3.6.5 Removing and Replacing the HSC Airflow Sensor Assembly

Use the following procedure to remove and replace the HSC airflow sensor:

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off the ac circuit breaker (CB1) on the HSC power controller, as shown in Figure 3–35.
3. Disconnect J70 as shown in Figure 3–36.
4. Remove exhaust duct from the HSC controller.
5. Remove the Phillips head screw that holds the mounting clamp to the duct as shown in Figure 3–36.

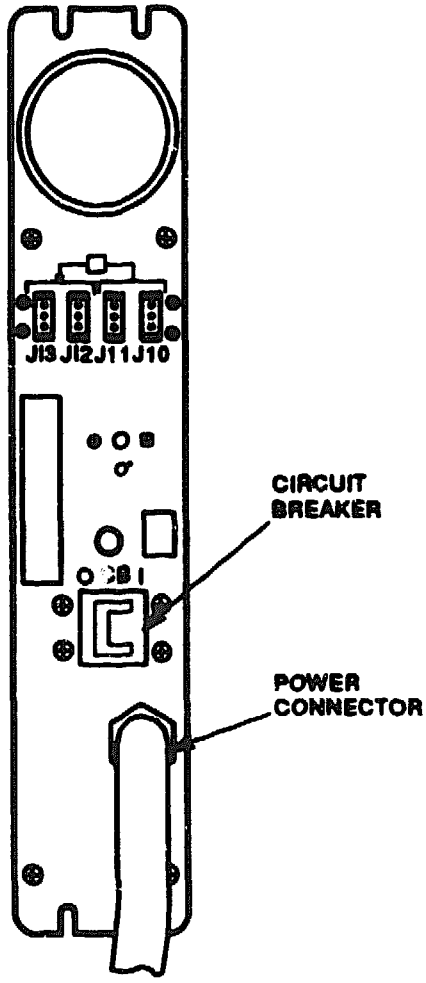


Figure 3–35 HSC Power Controller Circuit Breaker

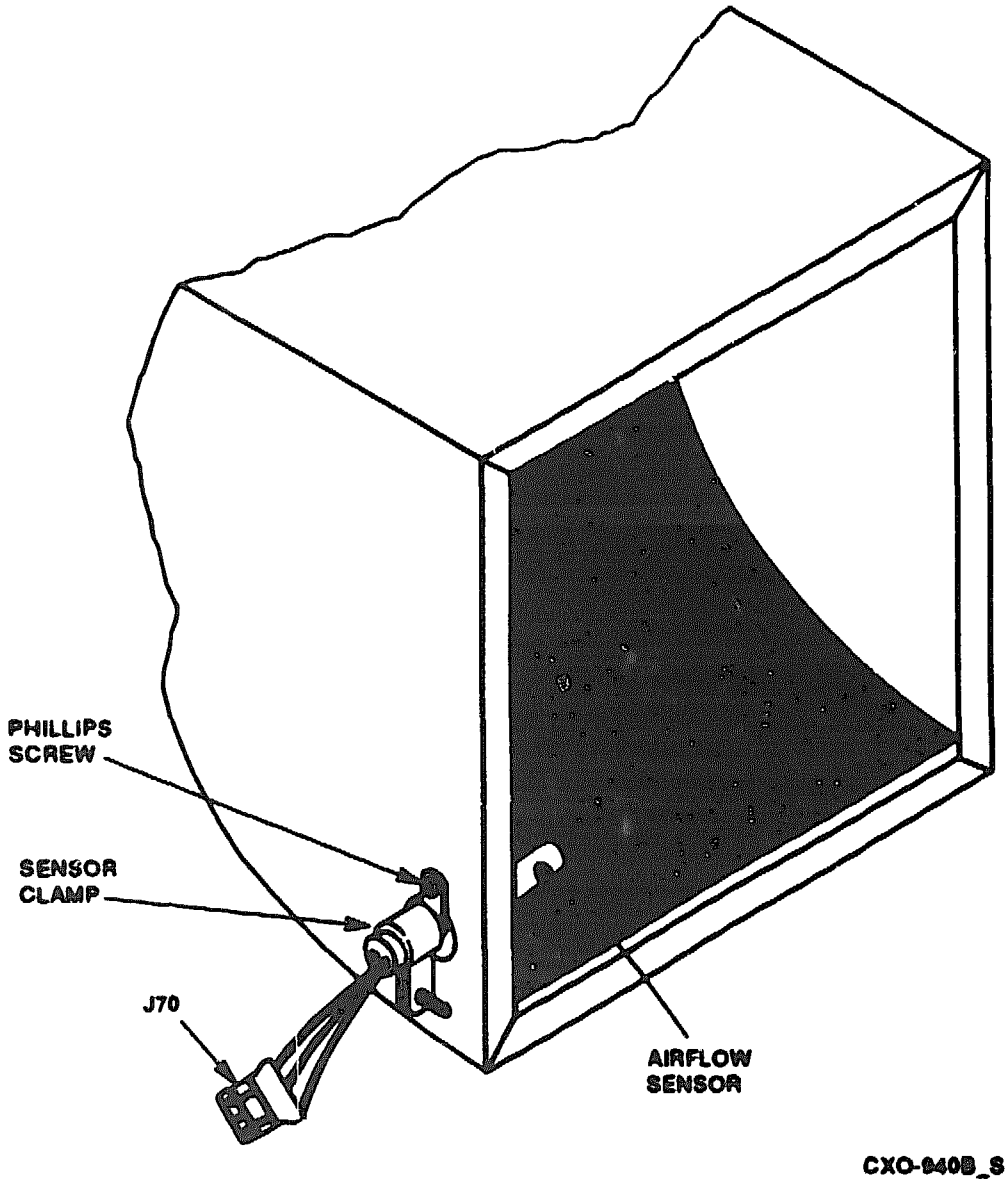


Figure 3–36 Removing and Replacing the HSC Airflow Sensor Assembly

6. Slide the sensor assembly out of the duct.
7. Reverse the removal procedure to replace the airflow sensor assembly. Align the slots in the airflow sensor tip horizontally with the floor. After turning on ac power to the HSC controller, test the new airflow sensor for proper operation by blocking the flow of air.

3.6.6 Removing and Replacing the HSC50 Airflow Sensor Assembly

Use the following procedure to remove and replace the HSC50 airflow sensor assembly:

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off the ac circuit breaker (CB1) on the HSC50 power controller, as shown in Figure 3–37.

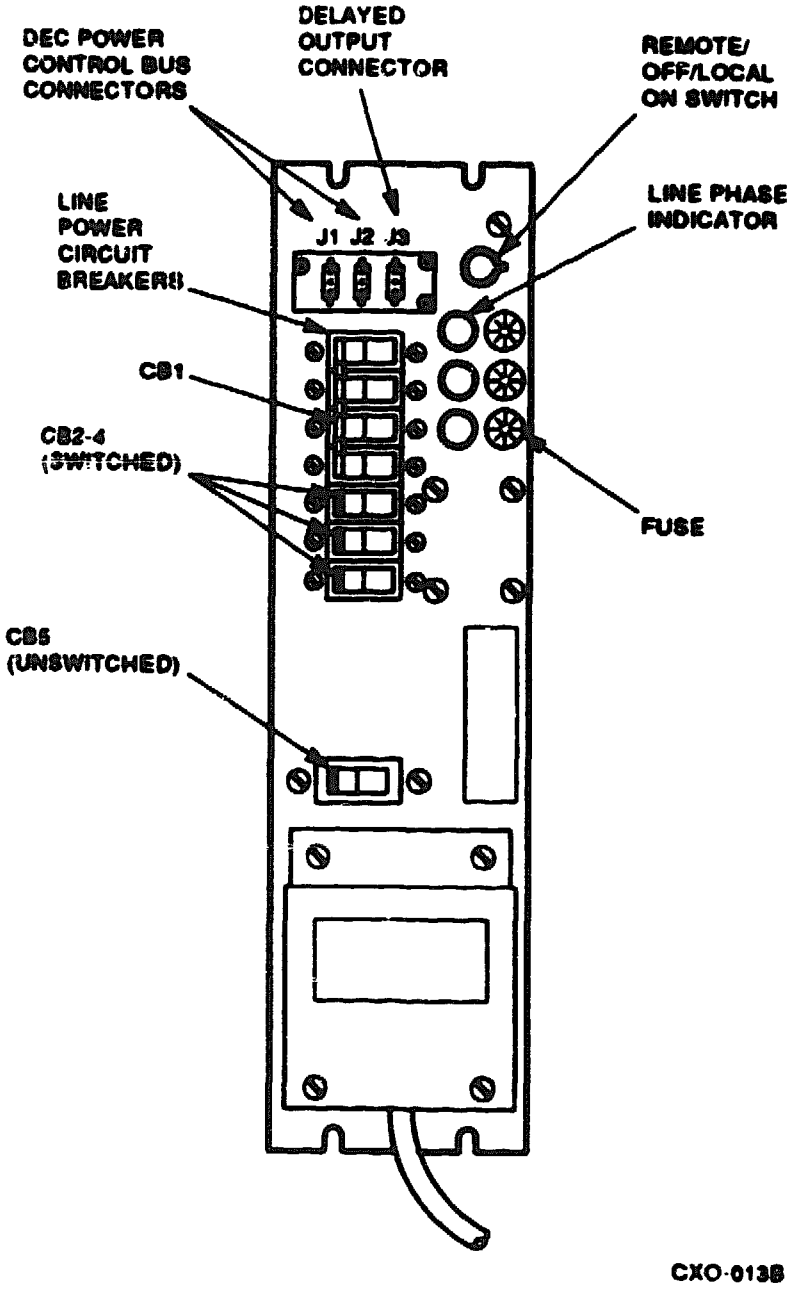


Figure 3–37 HSC50 Power Controller Circuit Breaker

3. Disconnect J70, as shown in Figure 3–38.
4. Remove the Phillips head screw that holds the mounting clamp to the duct, as shown in Figure 3–38

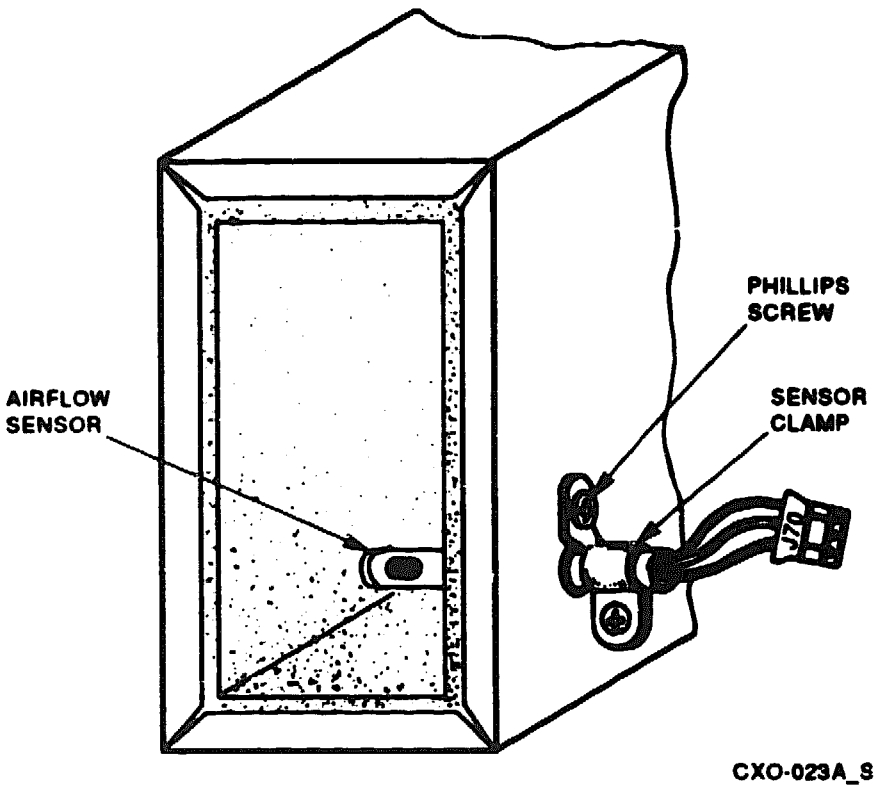


Figure 3–38 Removing and Replacing the HSC50 Airflow Sensor Assembly

5. Slide the sensor assembly out of the duct.
6. Reverse the removal procedure to replace the airflow sensor assembly. Align the slots in the airflow sensor tip horizontally with the floor. Ensure sensor operability by blocking the flow of air. Pinching the sensor should trip CB1.

3.6.7 Removing and Replacing the HSC Blower

The blower, which provides forced air cooling for the cabinet, is removed and replaced with the following procedure:

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off the ac circuit breaker (CB1) on the HSC power controller, as shown in Figure 3–39.

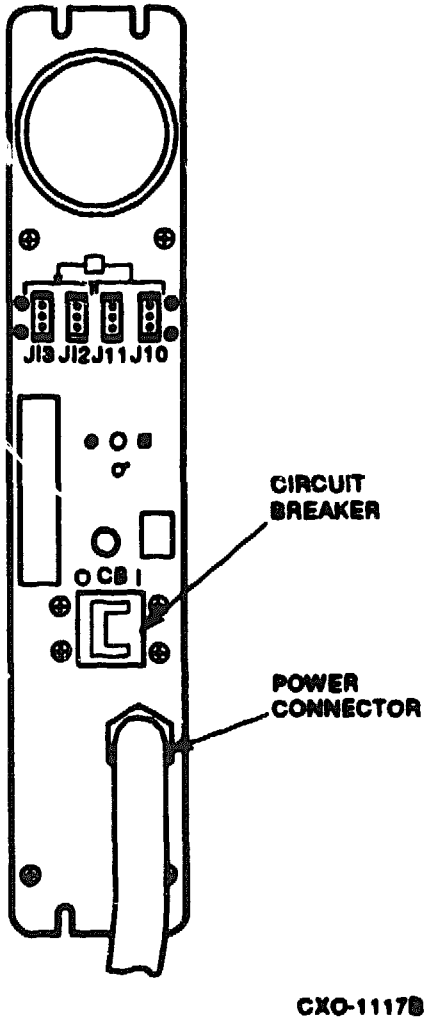


Figure 3–39 HSC Power Controller Circuit Breaker

3. Disconnect the blower power connector, as shown in Figure 3–40.
4. Disconnect the airflow sensor power connector (J70) to allow removal of the exhaust duct, as shown in Figure 3–40.
5. Remove the exhaust duct from the bottom of the blower by lifting up the quick release latch on the right side of the duct and turning the two quarter-turn latches on the inside left of the duct clockwise or counterclockwise, as shown in Figure 3–40. This figure also shows the latch arrangement on the HSC50 (modified) controller.

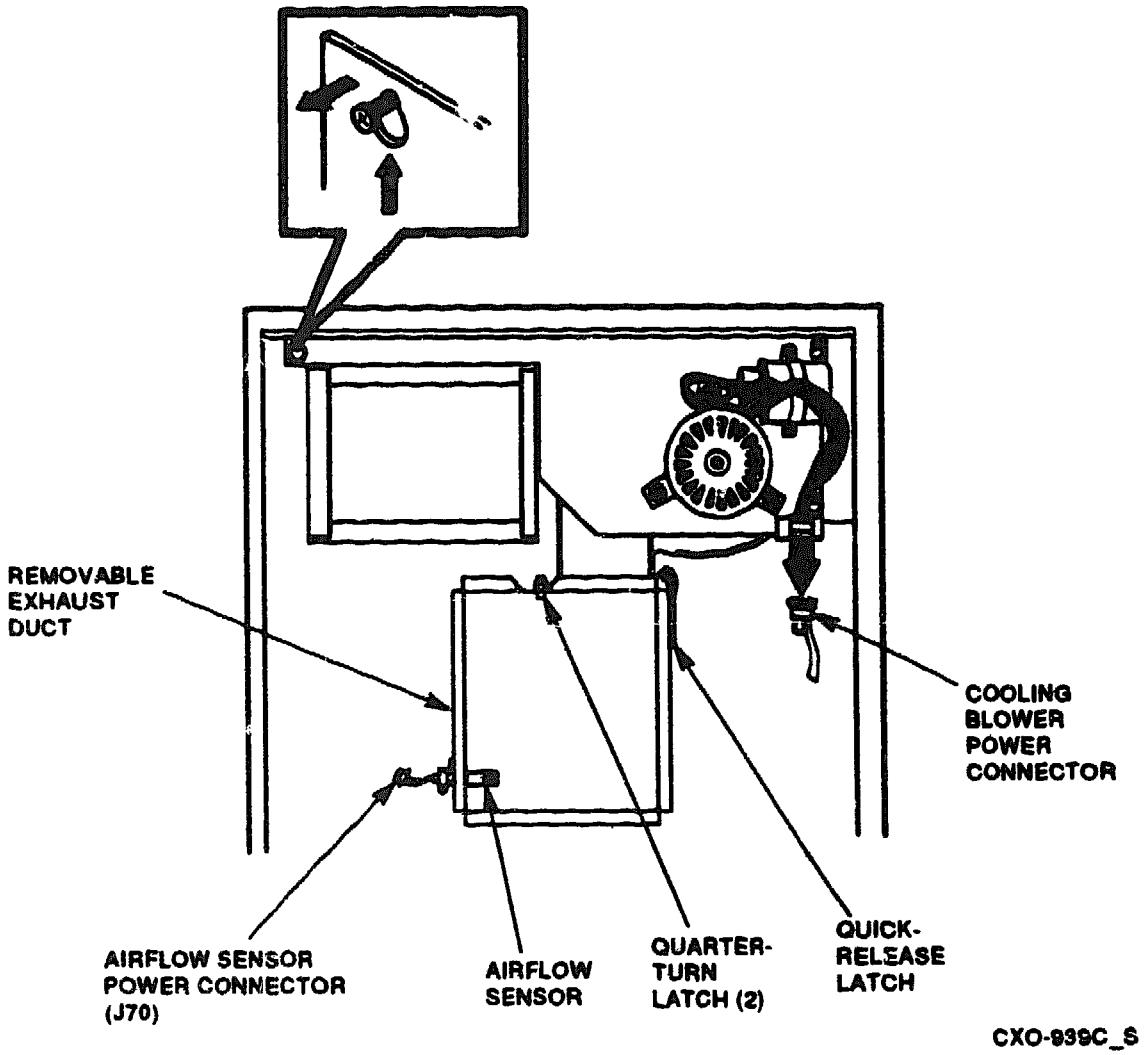


Figure 3–40 Removing and Replacing the HSC Main Cooling Blower Duct

6. Loosen, but do not remove, the three Phillips screws holding the blower mounting bracket to the cabinet.
7. Lift the blower and bracket up and out of the cabinet.
8. Reverse the removal procedure to replace the cooling blower.

3.6.8 Removing and Replacing the HSC50 Blower

The blower, which provides forced air cooling for the cabinet, is removed and replaced using the following procedure:

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off ac power (CB1 on the power controller), as shown in Figure 3–41.

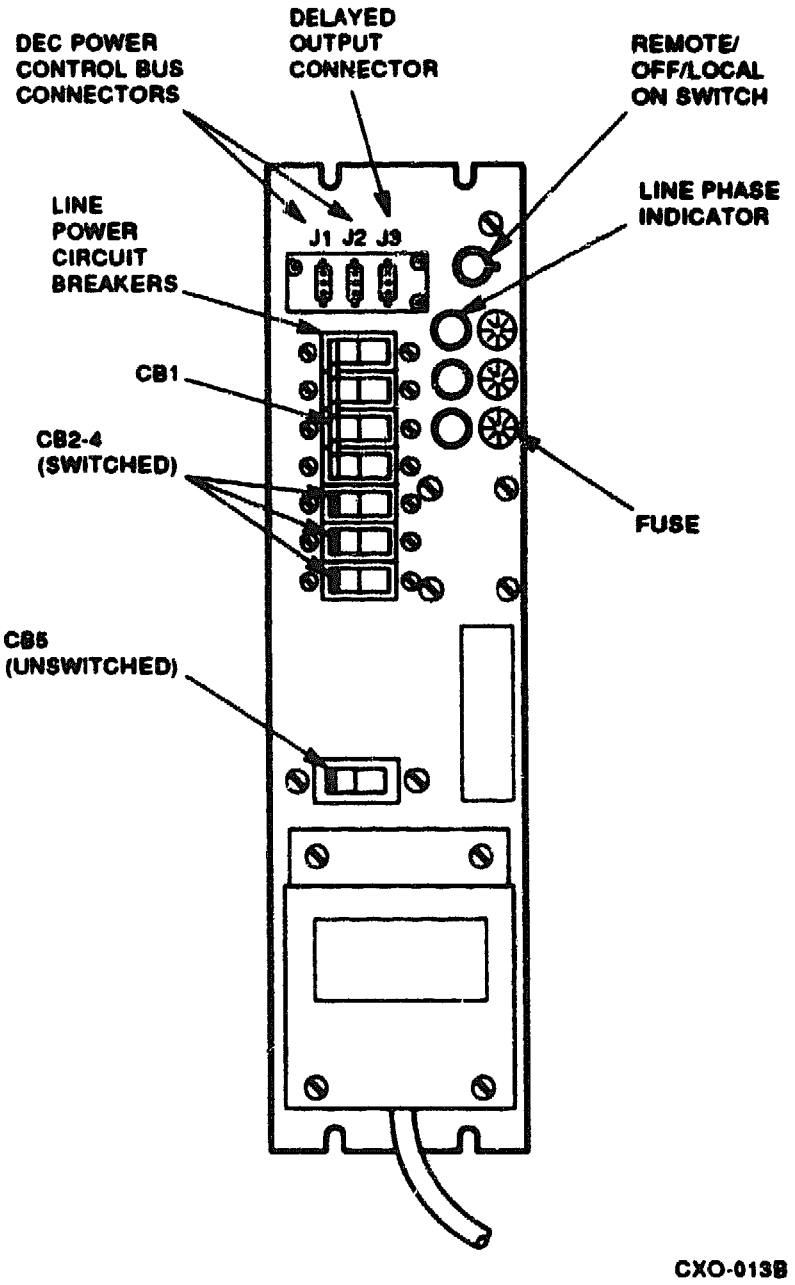


Figure 3–41 HSC50 Power Controller Circuit Breaker

3. Disconnect the blower power connector, as shown in Figure 3–42.
4. Disconnect the airflow sensor power connector (J70) to allow removal of the exhaust duct, as shown in Figure 3–42.
5. Remove the exhaust duct from the bottom of the blower by lifting up the quick release latchee on each side of the duct, as shown in Figure 3–42. For the HSC50 (modified), refer to Figure 3–40 to remove the duct.
6. Loosen, but do not remove, the three Phillips screws holding the blower mounting bracket to the cabinet, as shown in Figure 3–42.

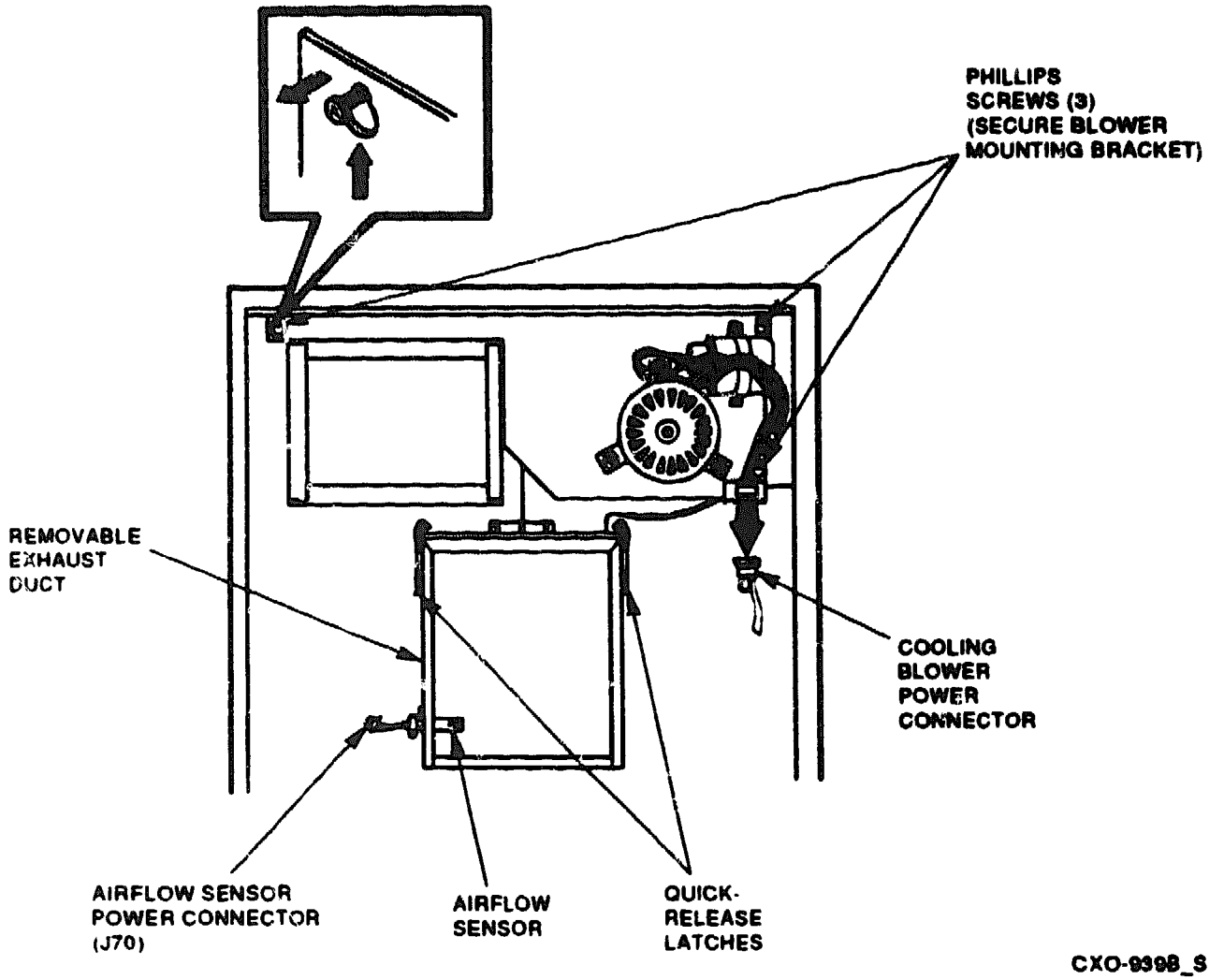


Figure 3–42 Removing and Replacing the HSC50 Blower Duct

7. Lift the blower and bracket up and out of the cabinet.
8. Reverse the removal procedure to replace the blower.

3.6.9 Removing and Replacing the HSC Power Controller

The power controller must be removed to replace a power supply. Use the following procedure to remove and replace the HSC power controller:

1. Open the back door using a 5/32-inch hex wrench.
2. Remove rear door latch to allow clearance for power controller removal.
3. Remove ac power by placing CB1 in the OFF position, as shown in Figure 3–43.

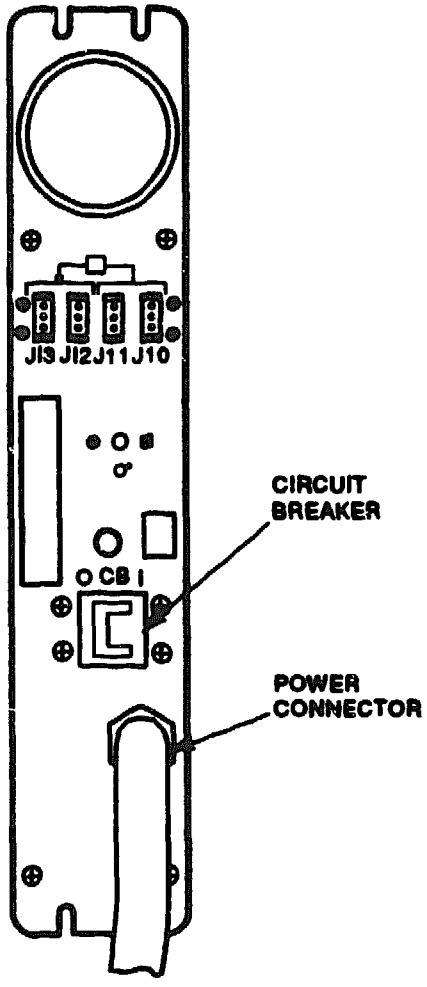


Figure 3–43 HSC Power Controller Circuit Breaker

4. Unplug the power controller from the power source.
5. Remove the two top screws and then the two bottom screws securing the power controller to the cabinet, as shown in Figure 3–44. While removing the two bottom screws, push up on the power controller to take the weight off the screws.

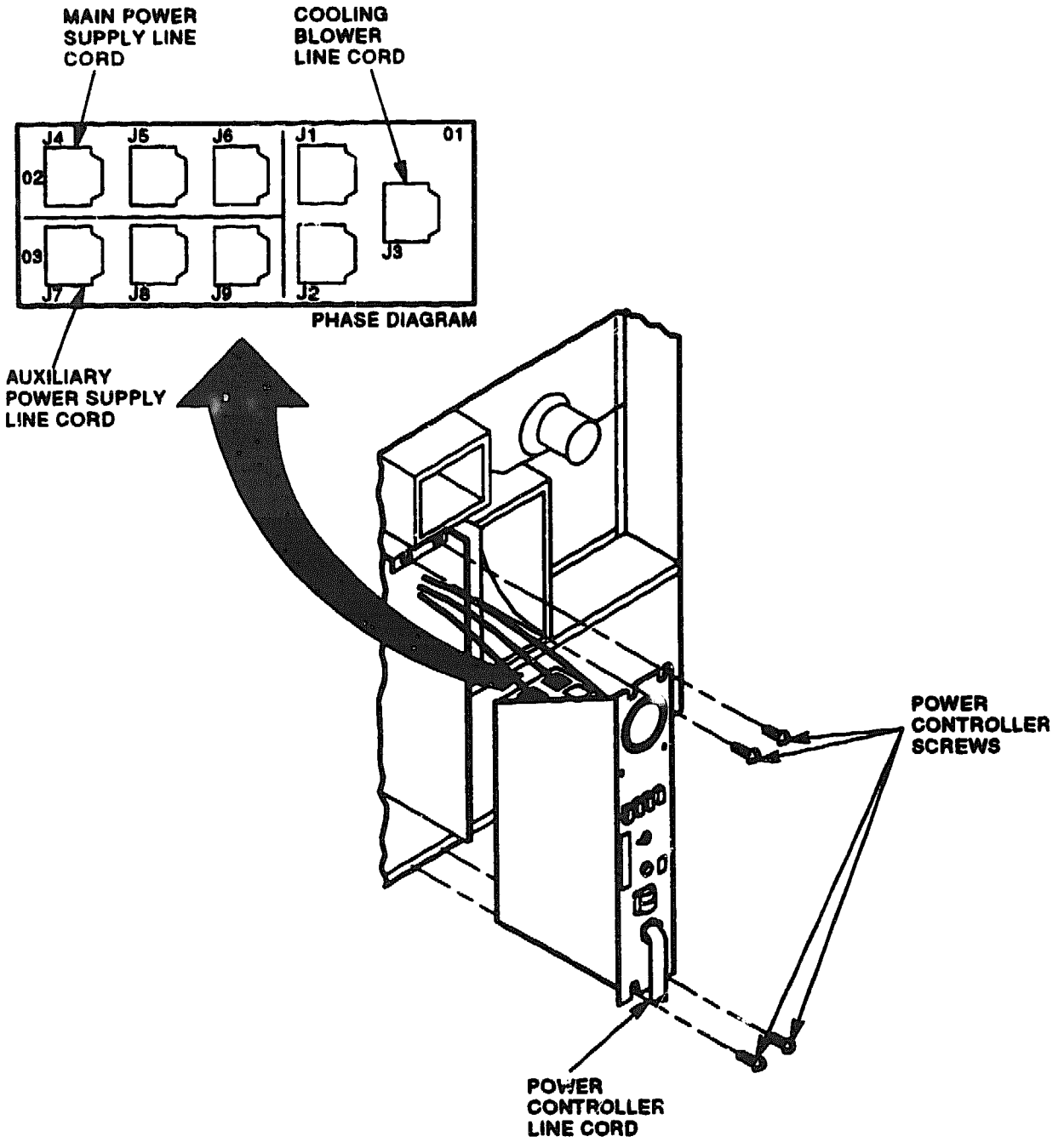


Figure 3–44 Removing and Replacing the HSC Power Controller

CAUTION
Do not pull the power controller out too far because cables are connected to the back and top.

6. Pull the power controller towards you and then out.
7. Remove the power control bus cables from connectors J10, J11, J12, and J13 at the front of the power controller, as shown in Figure 3–43.
8. Disconnect the total off connector at the rear of the power controller, as shown in Figure 3–45.

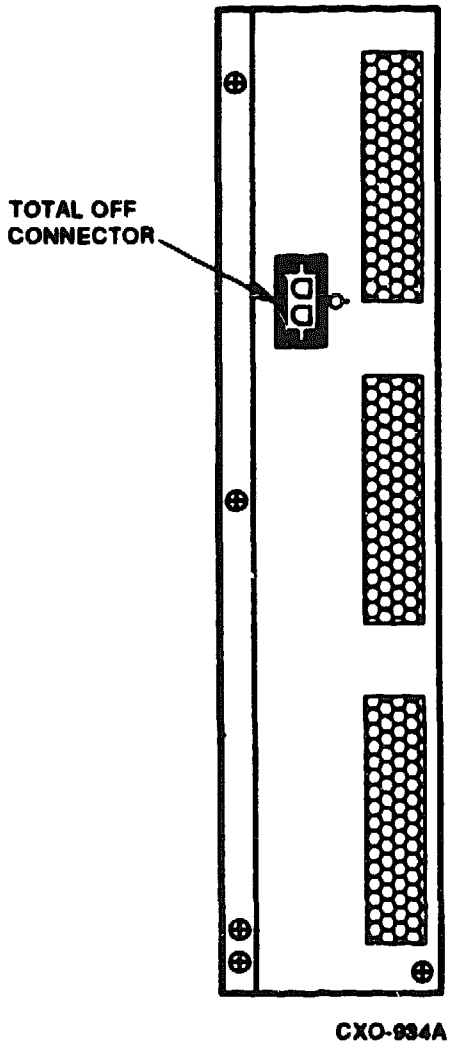


Figure 3–45 HSC Total Off Connector

9. Disconnect all line cords from the top of the power controller.

NOTE
Be sure to rotate the line cord elbow to the vertical position if replacing a defective power controller with a new one. To rotate the elbow, remove the set screw, rotate the elbow to the vertical position, and replace the set screw in the other hole.

10. Reverse the removal procedure to replace the power controller.

NOTE
To ensure proper phase distribution, reconnect the main power supply, auxiliary power supply, and cooling blower line cords as shown in Figure 3–44.

3.6.10 Removing and Replacing the HSC50 Power Controller

The HSC50 power controller must be removed to replace a power supply.

Use the following procedure to remove and replace the HSC50 power controller:

1. Open the back door using a 5/32-inch hex wrench.
2. Remove rear door latch to allow clearance for power controller removal.
3. Turn off ac power (CB1 on the power controller), as shown in Figure 3–46.

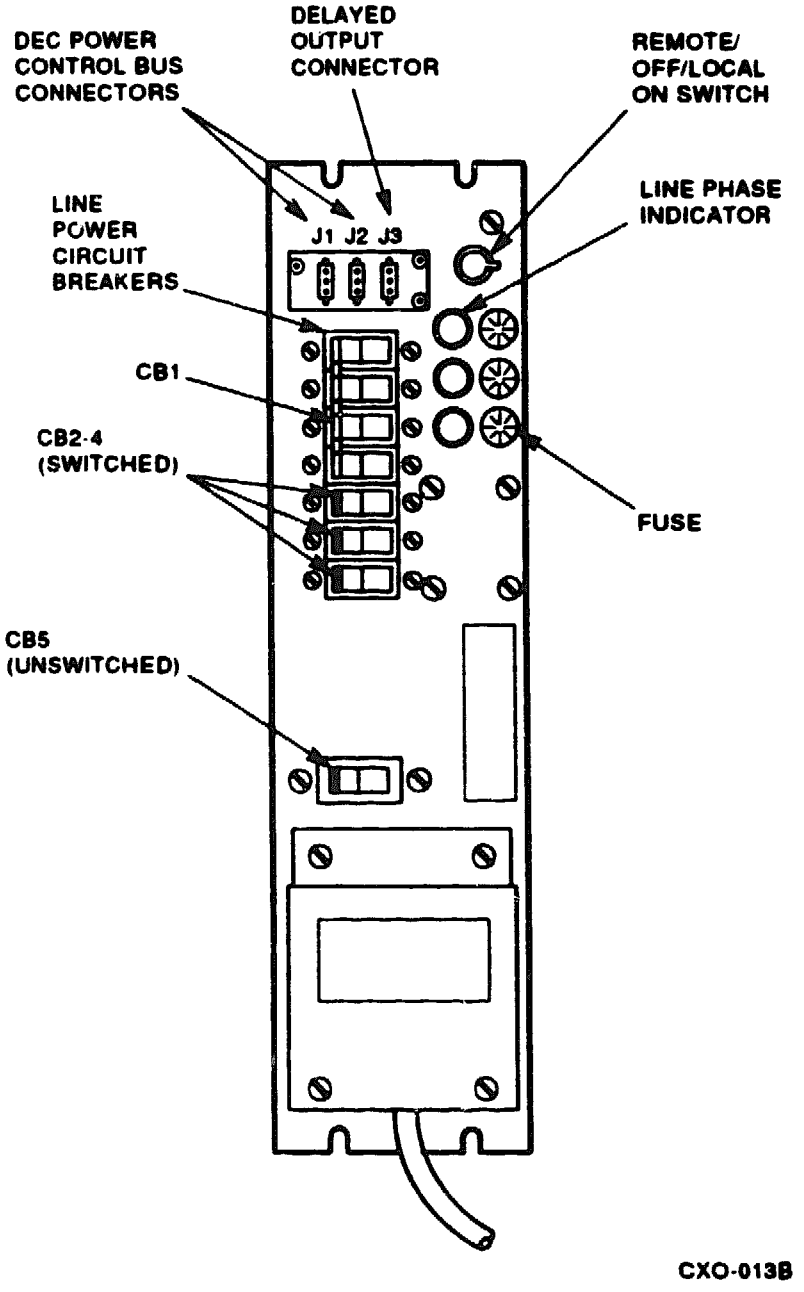


Figure 3–46 HSC50 Power Controller Circuit Breaker

4. Unplug the power controller from the power source.

5. Remove the two top screws and then the two bottom screws securing the power controller to the cabinet as shown in Figure 3–47. While removing the two bottom screws, push up on the power controller to take the weight off the screws.

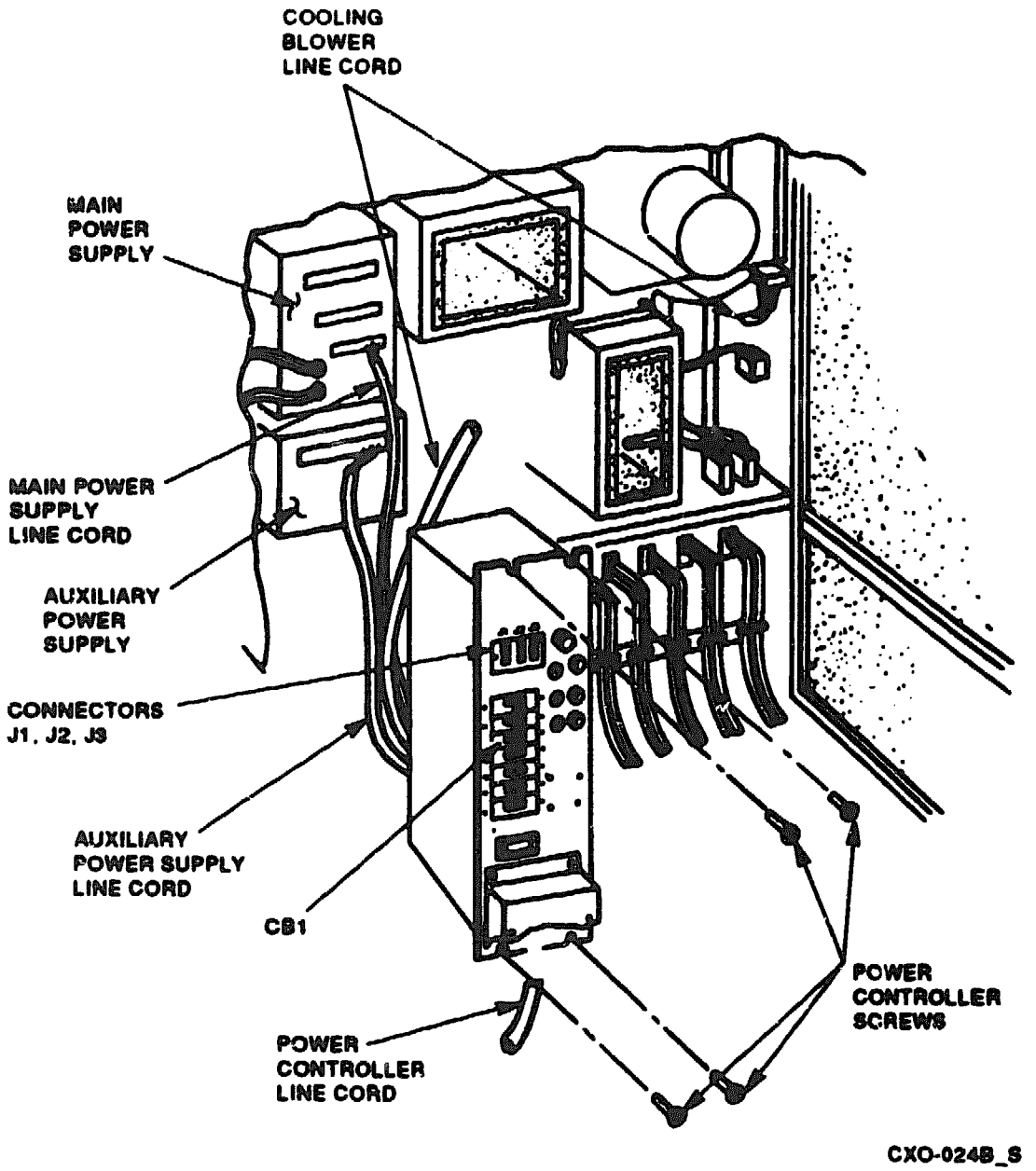


Figure 3–47 Removing and Replacing the HSC50 Power Controller

CAUTION
Do not pull the power controller out too far because cables are connected to the back and top.

6. Pull the power controller towards you and then out.
7. Remove the power control bus cables from connectors J1, J2, and J3 at the front of the power controller as shown in Figure 3–46.

8. Reverse the removal procedure to replace the power controller.

3.6.11 Removing and Replacing the HSC Main Power Supply

Use the following procedure to remove and replace the HSC main power supply:

WARNING
The power supply is heavy. Support it with both hands to avoid dropping it.

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off ac power (CB1 on the power controller), as shown in Figure 3–48.

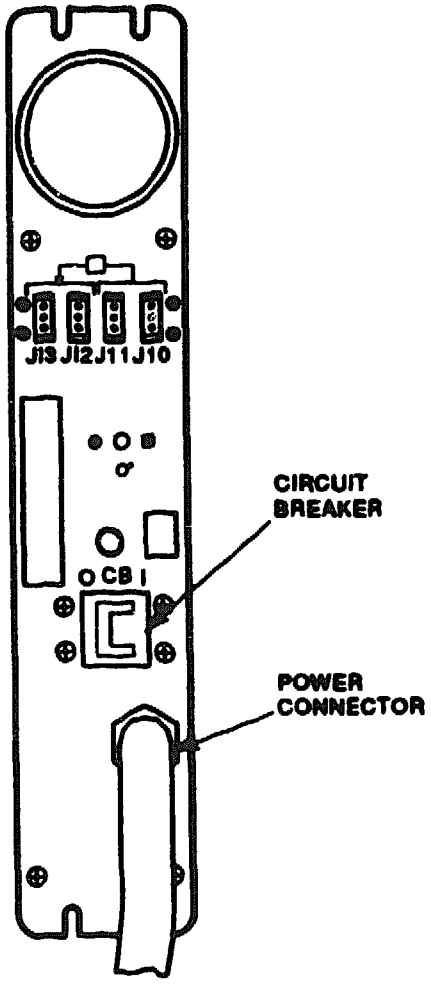


Figure 3–48 HSC Power Controller Circuit Breaker

3. Unplug the power controller from the power source.
4. Remove the front door.
5. Remove the power controller. Refer to Section 3.6.9 to access the back of the power supply.

6. Unplug the main power supply line cord at the power controller.

NOTE
While performing 7 through 15, refer to Figure 3–49.

7 Remove the nut from the –V1 stud (ground) on the back of the power supply.

8. Remove the nut from the +V1 stud (+5 volts) on the back of the power supply.

9. Remove the nut from the –V2 (–5.2 volts) stud on the back of the power supply.

10. Remove the nut from the +V2 (ground) stud.

11. Unplug J31 (+12 Vdc output from the supply to backplane, power fail, and –5 volts sense line).

12. Unplug P32 (+12 Vdc sense line and +5 Vdc sense line).

13. Unplug J33 (to DC power switch).

14. Unplug J34 (remote on/off jumper to auxiliary power supply).

15. Unplug J35 (+12 Vdc power to the airflow sensor).

Figure 3–49 shows the HSC main power supply test points.

WIRE LIST					
COLOR	POSITION	SIGNAL	COLOR	POSITION	SIGNAL
PURPLE	TBI 3 5	12 V	PURPLE	TB1-3-1	12 V SENSE
PURPLE	TBI-3-6	12 V	BLUE	TB1-2-7	ACC
BLACK	TBI-3-3	GND (12 V)	BROWN	TB1-2-6	AC
BLACK			GRN/YEL	TB1-2-5	GND
ORANGE	TBI-2-2	-5 V SENSE	YELLOW	TB1-2-3	ON/OFF (-5, 3 V)
BLACK	TBI-2-1	GND (-5 V SENSE)	ORANGE	TB1-2-2	-5 V SENSE (S2-)
BROWN	TBI-1-4	POWER FAIL	BLUE	TB1-1-3	ON/OFF 5 V
BLACK	TBI-1-2	GND (5 V SENSE)	BLACK	TB1-1-2	GND (5 V SENSE)
RED	TB1-1-1	5 V SENSE	PURPLE	TB1-3-2	12 V
BLACK	TB1-3-4	GND (12 V SENSE)			

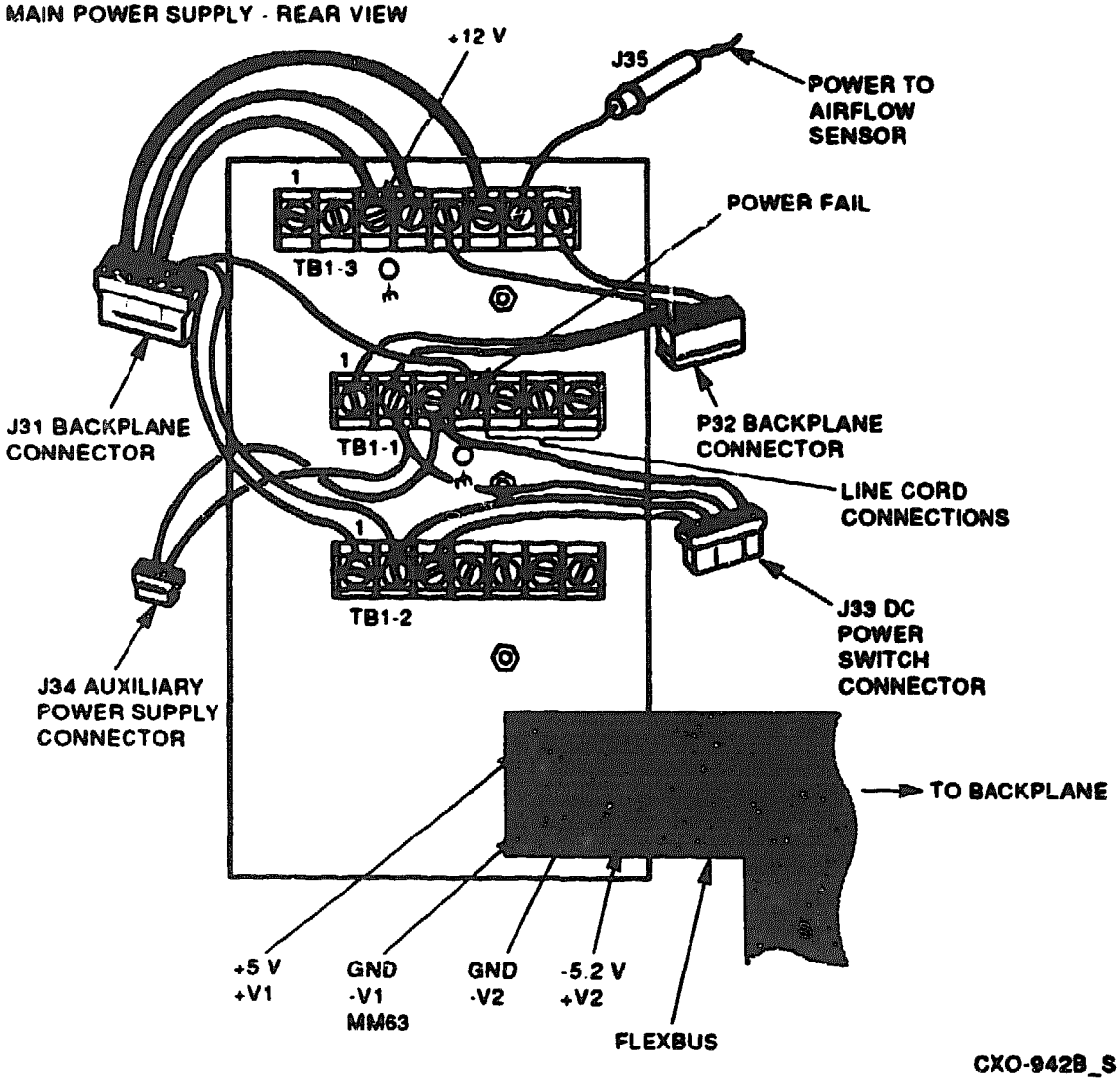


Figure 3–39 HSC Main Power Supply Cables and Test Points

16. Turn the four captive screws on the front of the power supply counterclockwise (Figure 3–50.

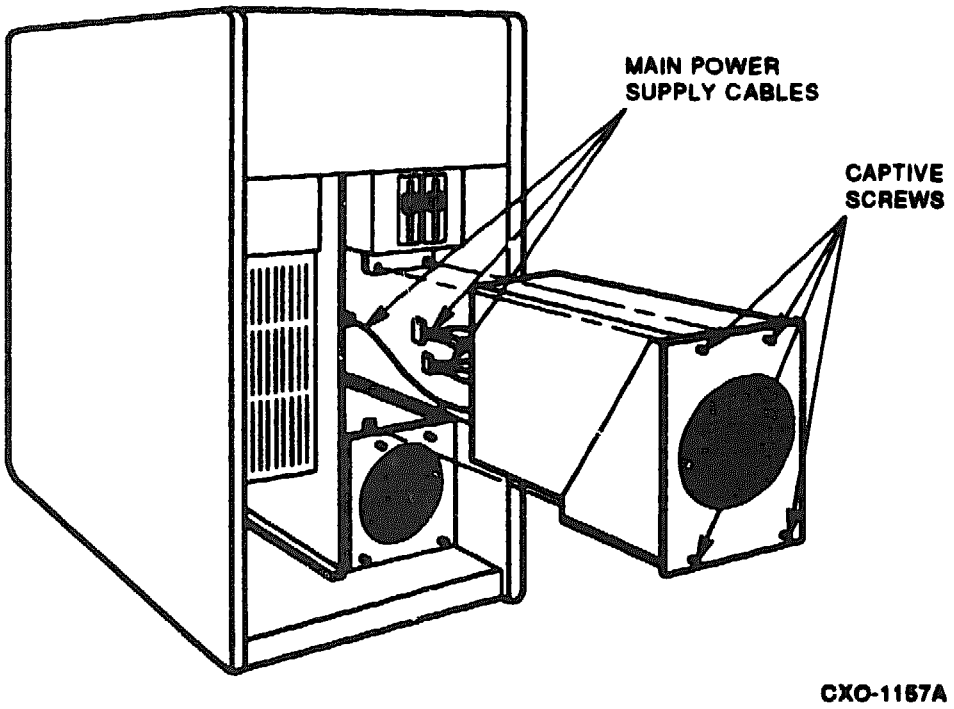


Figure 3–50 Removing and Replacing the HSC70 Main Power Supply

17. Pull the power supply out about an inch. Check the back of the cabinet to ensure the cables and flexbus connectors are clear and will not snag when the supply is completely removed.
18. Carefully pull the power supply all the way out of the cabinet.
19. Remove the power cord from the failing unit and install it on the new power supply.

    NOTE
    Spare power supplies are not shipped with a power cord.

20. Reverse the removal procedure to replace the main power supply.

3.6.12 Removing and Replacing the HSC50 Main Power Supply

Use the following procedure to remove and replace the HSC50 main power supply:

WARNING
The power supply is heavy. Support it with both hands to avoid dropping it.

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off ac power (CB1 on the power controller), as shown in Figure 3–51.

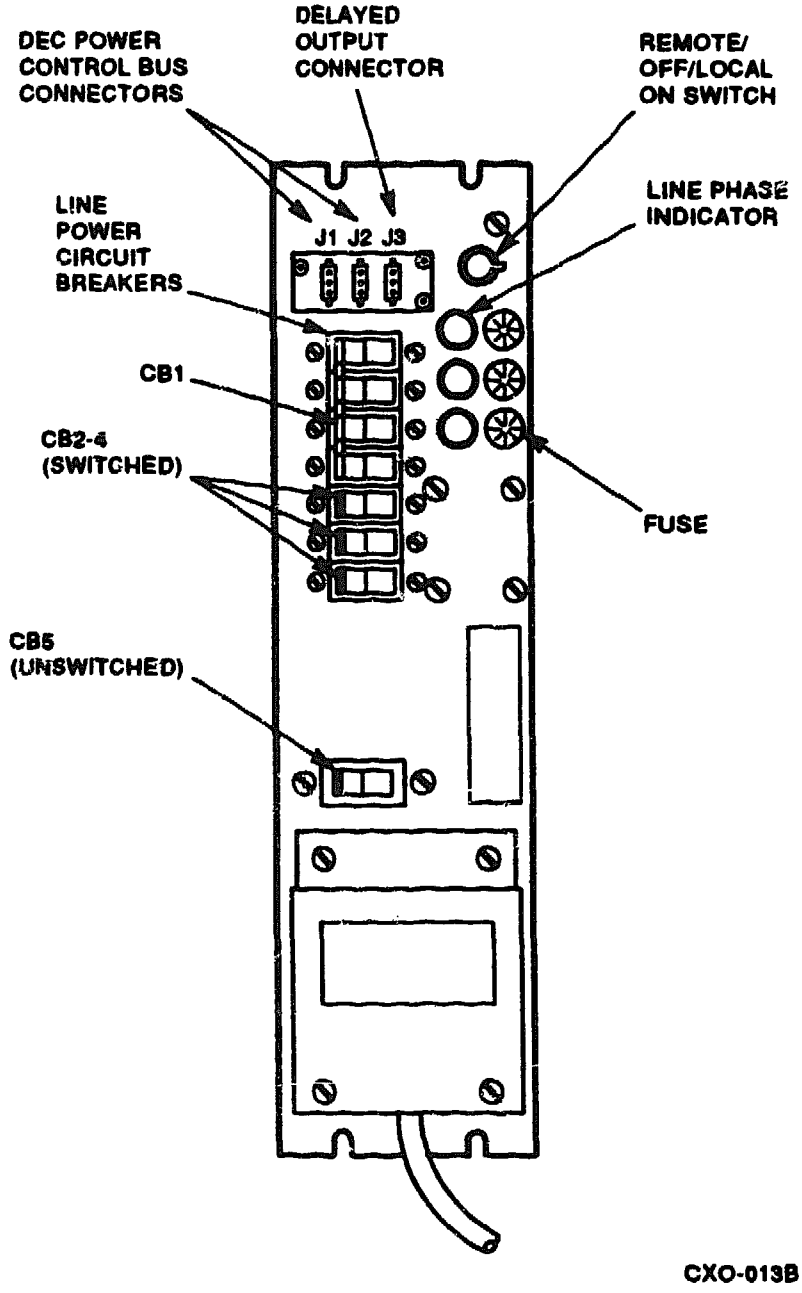


Figure 3–51 HSC50 Power Controller Circuit Breaker

3. Unplug the power controller from the power source.
4. Remove the front door.

5. Remove the power controller. Refer to Section 3.6.10) to access the back of the power supply.

   NOTE
   While performing 6 through 14, refer to Figure 3–52 which shows the HSC50 controller main power supply test points.

6. Unplug the main power supply line cord at the power controller.
7. Remove the nut from the –V1 stud (ground) on the back of the power supply.
8. Remove the nut from the +V1 stud (+5 volts) on the back of the power supply.
9. Remove the nut from the –V2 (–5.2 volts) stud on the back of the power supply as shown in Figure 3–52.
10. Remove the nut from the +V2 (ground) stud on the back of the power supply.
11. Unplug J31 (+12 Vdc output from the supply to backplane, power fail, and –5 volts sense line).
12. Unplug P32 (+12 Vdc sense line and +5 Vdc sense line). Ensure the P32 cable is free to be removed with the power supply.
13. Unplug J33 (to DC power switch).
14. Unplug J34 (remote on/off jumper to auxiliary power supply).
15. Unplug J35 (+12 Vdc power to the airflow sensor).

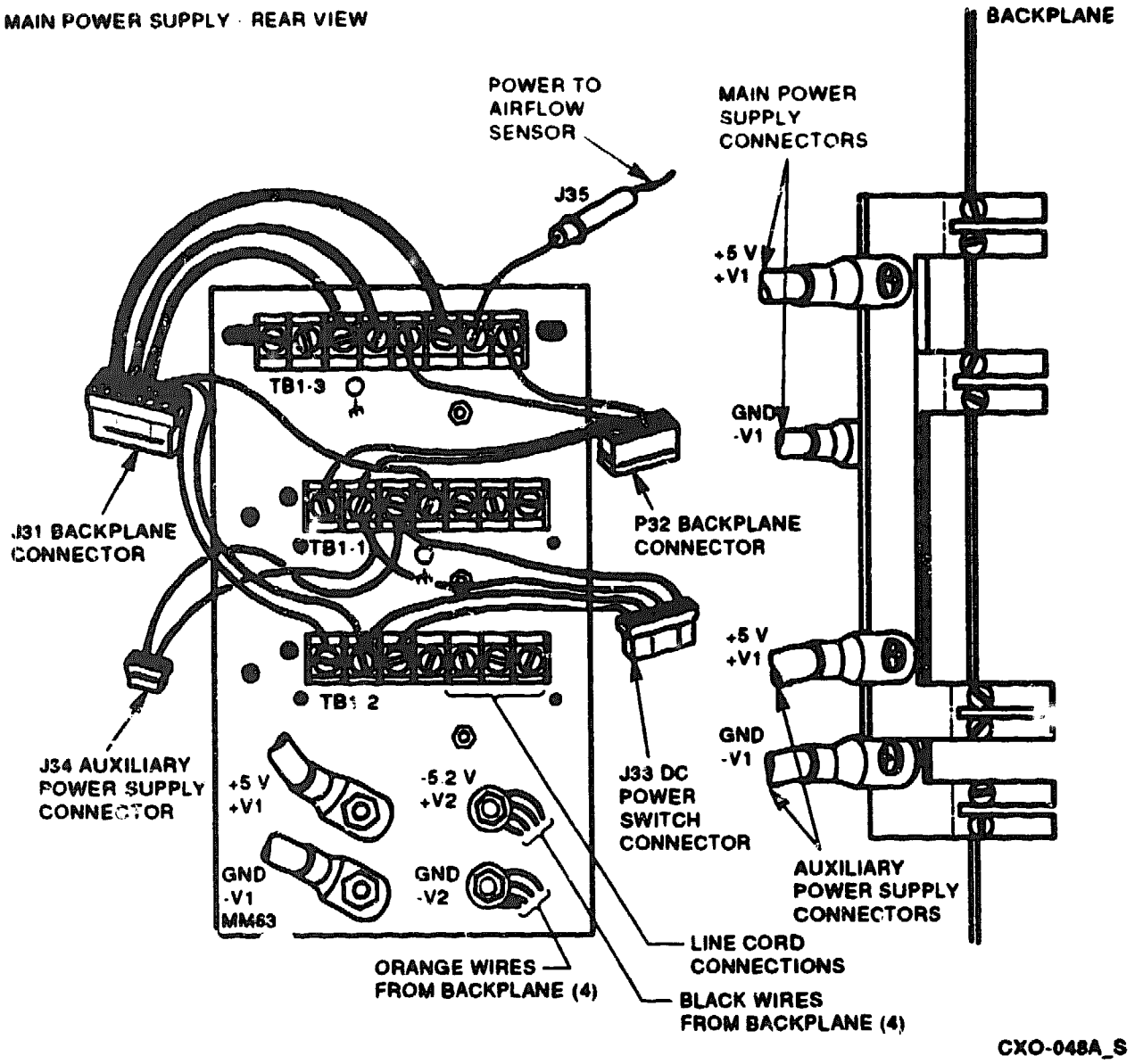


Figure 3–52 HSC50 Main Power Supply Cables and Voltage Test Points

16. Turn the four captive screws on the front of the power supply counterclockwise, as shown in Figure 3–53.

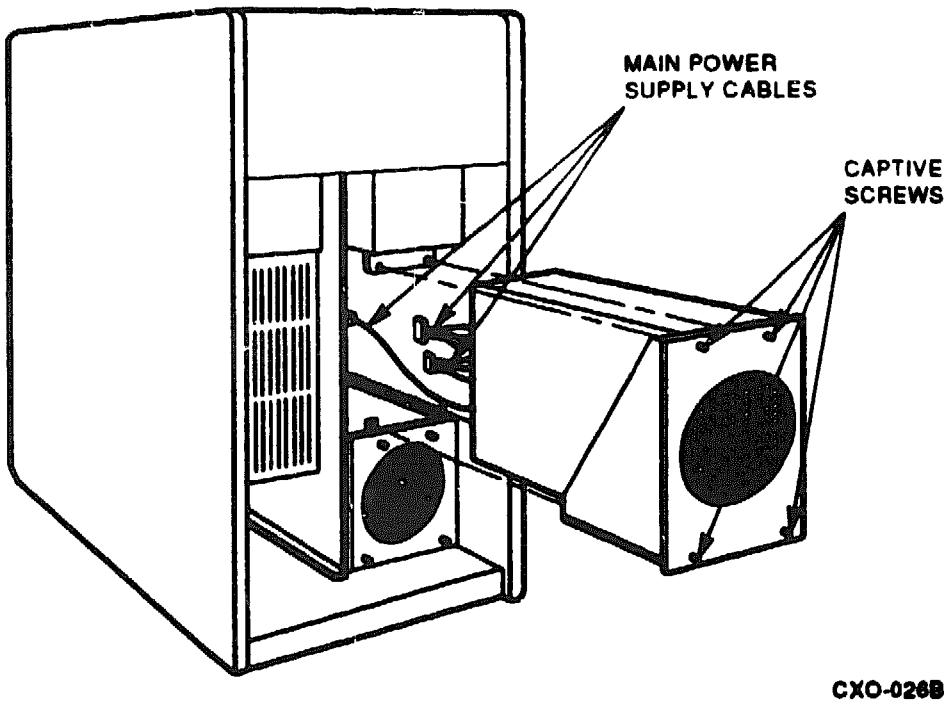


Figure 3–53 Removing and Replacing the HSC50 Main Power Supply

17. Pull the power supply out about an inch. Check the back of the cabinet to ensure the cables are clear and will not snag when the supply is completely removed.
18. Carefully pull the power supply all the way out of the cabinet.
19. Remove the power cord from the failing unit and install it on the new power supply.

    NOTE
    Spare power supplies are not shipped with a power cord.

20. Reverse the removal procedure to replace the HSC50 controller main power supply.

3.6.13 Removing and Replacing the HSC Auxiliary Power Supply

An HSC controller requires an auxiliary power supply if the total module count in the card cage is more than eight. The auxiliary power supply is mounted directly beneath the main power supply.

Use the following procedure to remove and replace the HSC auxiliary power supply:

WARNING
This power supply is heavy. When removing the power supply, support it with both hands to avoid dropping it.

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off ac power (CB1) on the power controller, as shown in Figure 3–54.

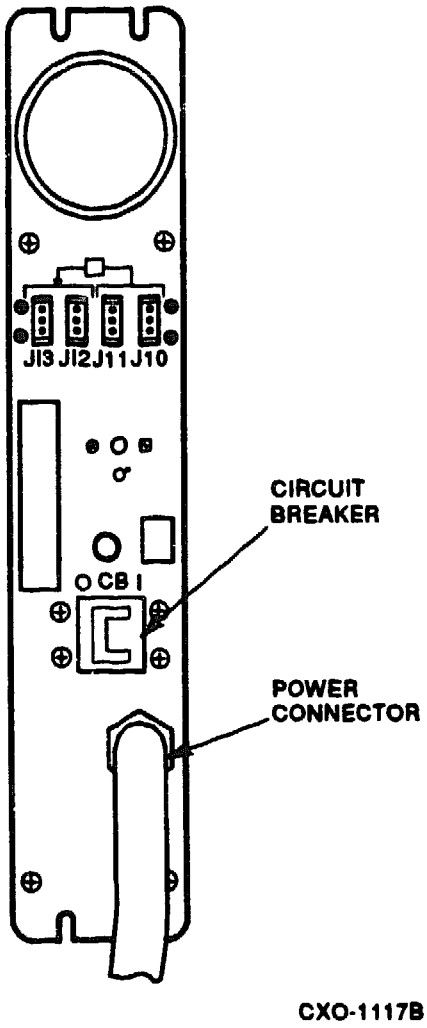


Figure 3–54 HSC Power Controller Circuit Breaker

3. Unplug the power controller from the power source.
4. Remove the front door.
5. Remove the power controller to access the back of the power supply. Refer to Section 3.6.9 for the procedure.
6. Unplug the auxiliary power supply line cord at the power controller.

NOTE
While performing 7 through 10, refer to Figure 3–55.

7. Remove the nut from the +V1 stud (+5 volt) on the back of the power supply.
8. Remove the nut from the –V1 stud (ground) on the back of the power supply.
9. Disconnect J50 (sense line to voltage comparator).
10. Disconnect J51 (dc on/off jumper).

WIRE LIST		
COLOR	POSITION	SIGNAL
BLACK	TBI-2	GROUND (5 V SENSE)
RED	TBI-1	5 V SENSE
BROWN	TBI-4	POWER FAIL
BLUE	TBI-7	ACC
BROWN	TBI-6	AC
GRN/YEL	TBI-5	CHASSIS GROUND
BLUE	TBI-3	ON/OFF
BLACK	TBI-2	GROUND (5 V SENSE)

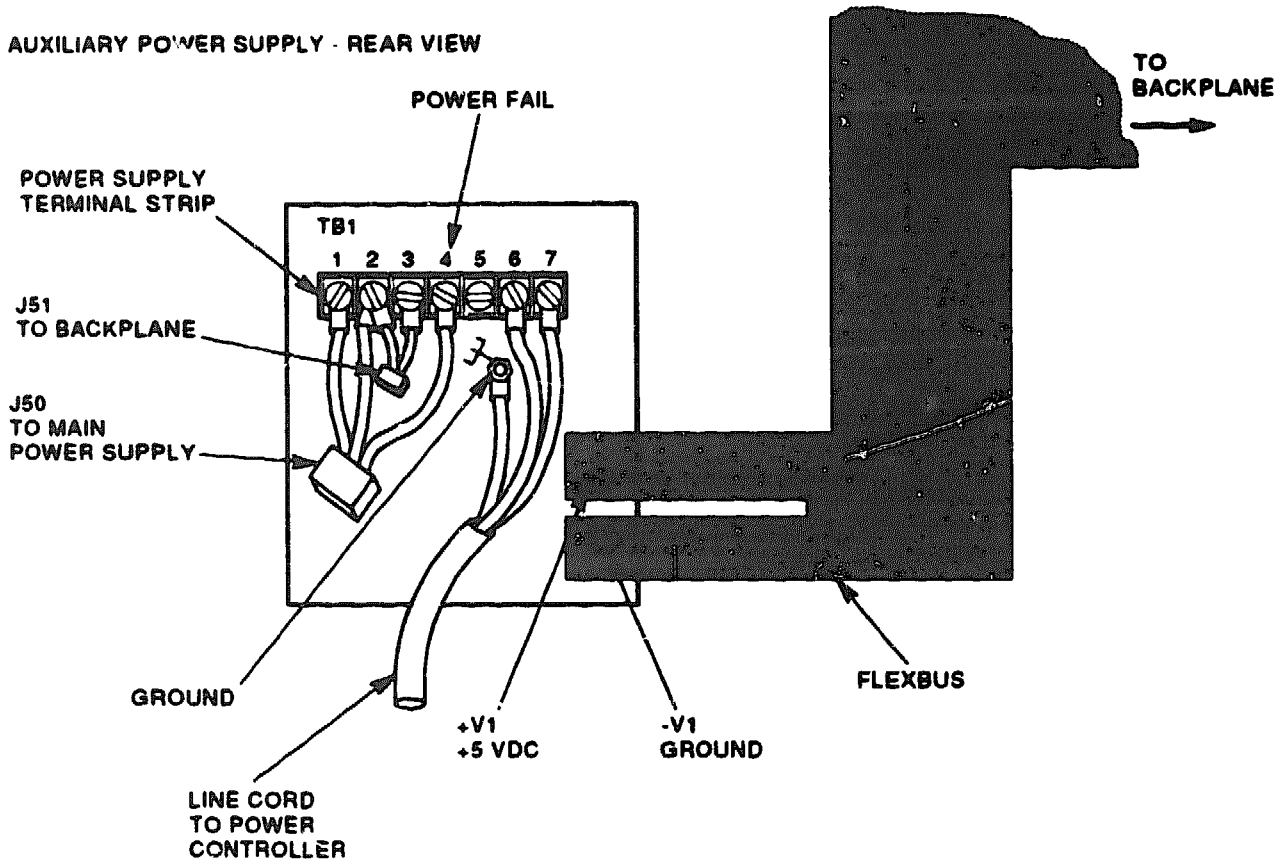


Figure 3–55 HSC Auxiliary Power Supply Cable and Test Points

11. Turn the four captive screws on the power supply counterclockwise, as shown in Figure 3–56.

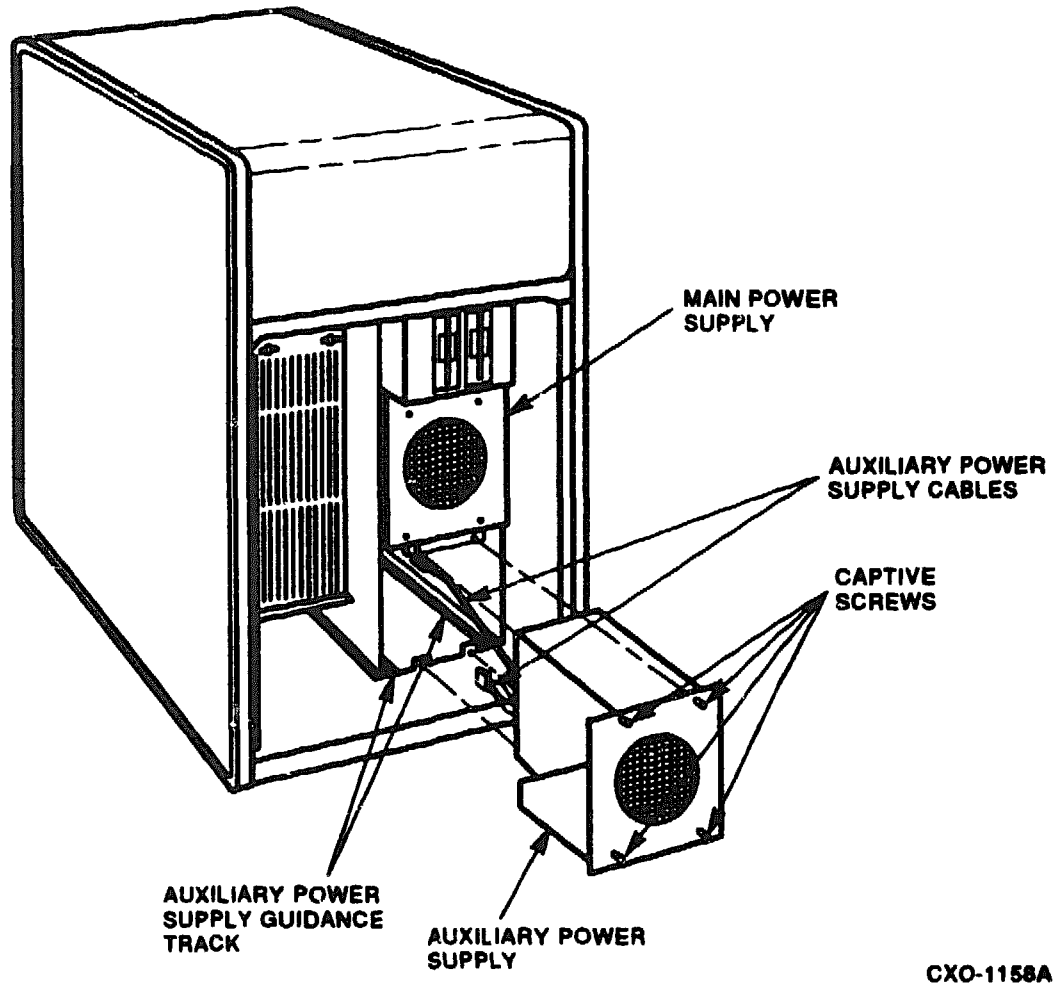


Figure 3–56 Removing and Replacing the HSC Auxiliary Power Supply

12. Pull the power supply out about an inch. Check the back of the cabinet to ensure the cables and flexbus connectors are clear.
13. Carefully slide the power supply out through the front of the HSC controller.
14. Remove the power cord from the failing unit and install it to the new power supply.

NOTE
Spare supplies are not shipped with a power cord.

15. Reverse the removal procedure to replace the HSC auxiliary power supply.

3.6.14 Removing and Replacing the HSC50 Auxiliary Power Supply

An HSC50 controller requires an auxiliary power supply if the total module count in the card cage is more than eight. The auxiliary power supply is mounted directly beneath the main power supply.

Use the following procedure to remove and replace the HSC50 auxiliary power supply:

WARNING
This power supply is heavy. When removing the power supply, support it with both hands to avoid dropping it.

1. Open the back door using a 5/32-inch hex wrench.
2. Turn off the ac circuit breaker (CB1) on the HSC50 power controller, as shown in Figure 3–57.

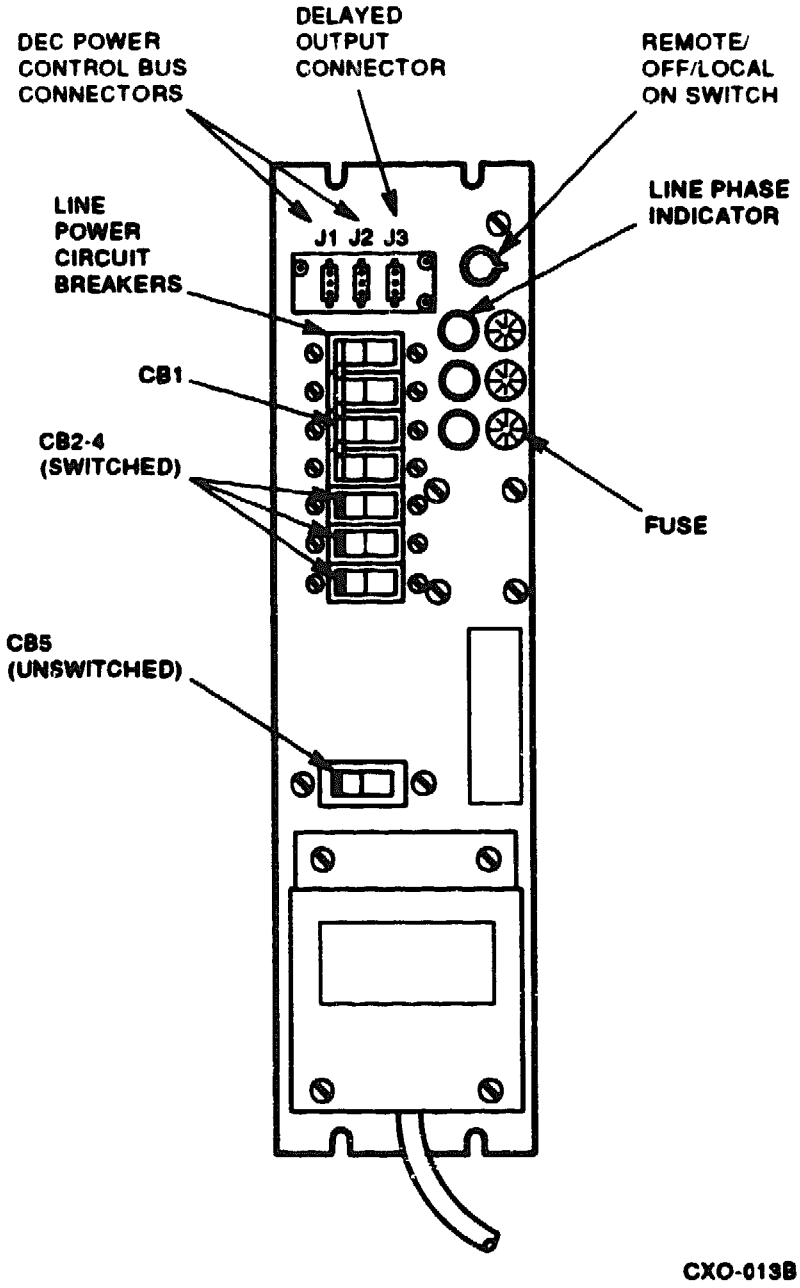


Figure 3–57 HSC50 Power Controller Circuit Breaker

3. Unplug the power controller from the power source.
4. Remove the front door.
5. Remove the power controller to access the back of the power supply. Refer to Section 3.6.10 for the procedure.

6. Unplug the auxiliary power supply line cord at the power controller.

   NOTE
   While performing 7 through 10, refer to Figure 3–58.

7. Remove the nut from the +V1 stud (+5 volt) on the back of the power supply.
8. Remove the nut from the –V1 stud (ground) on the back of the power supply.
9. Disconnect J50 (sense line to voltage comparator).
10. Disconnect J51 (dc on/off jumper).

    Refer to Figure 3–58 for the HSC50 controller auxiliary power supply test points.

WIRE LIST		
COLOR	POSITION	SIGNAL
BLACK	TBI-2	GROUND (5 V SENSE)
RED	TBI-1	5 V SENSE
BROWN	TBI-4	POWER FAIL
BLUE	TBI-7	ACC
BROWN	TBI-6	AC
GRN/YEL	TBI-5	CHASSIS GROUND
BLUE	TBI-3	ON/OFF
BLACK	TBI-2	GROUND (5 V SENSE)

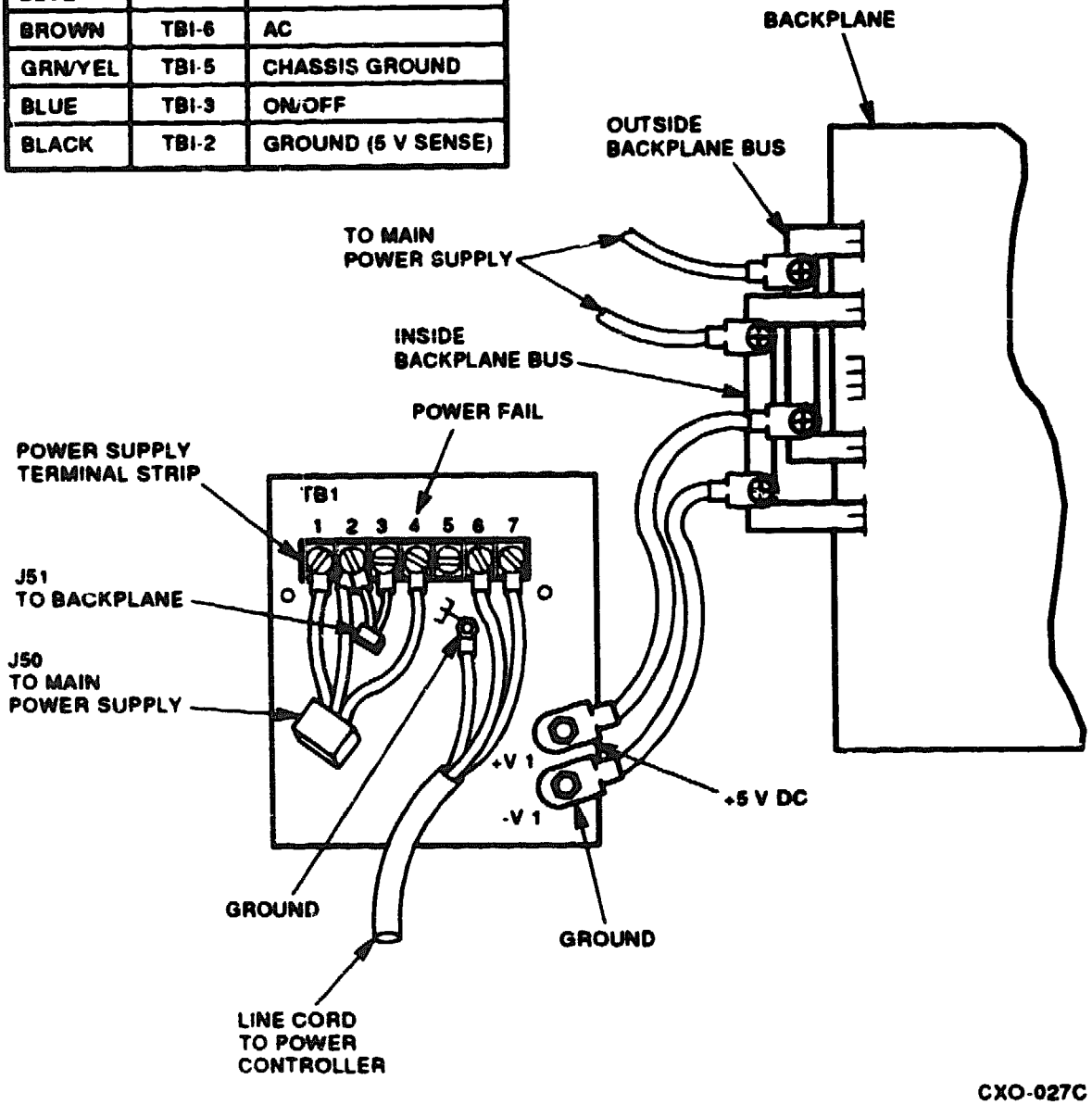


Figure 3–58 HSC50 Auxiliary Power Supply Cable and Voltage Test Points

11. Turn the four captive screws on the power supply counterclockwise, as shown in Figure 3–59.

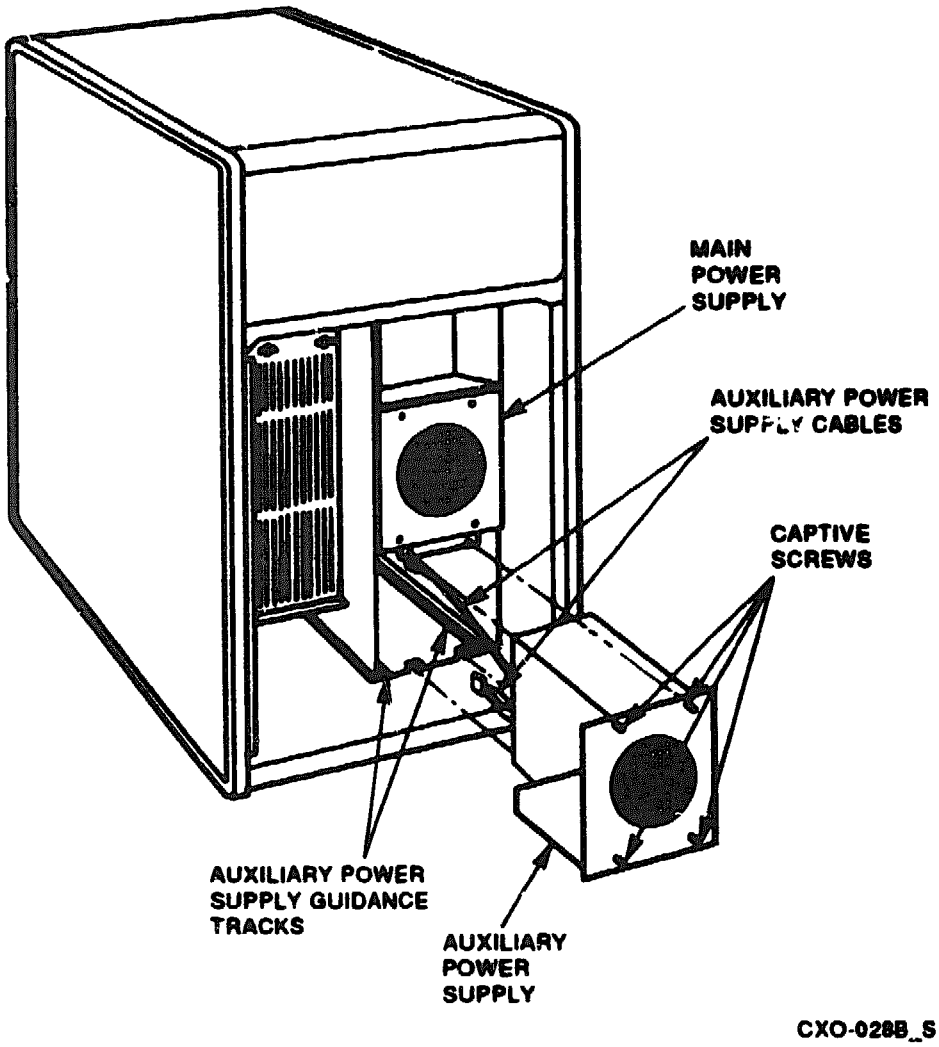


Figure 3–59 Removing and Replacing the HSC50 Auxiliary Power Supply

12. Pull the power supply out about an inch. Check the back of the cabinet to ensure the cables and connectors are clear.
13. Carefully slide the power supply out through the front of the HSC50 controller.
14. Remove the power cord from the failing unit and install it to the new power supply.

    NOTE
    Spare supplies are not shipped with a power cord.

15. Reverse the removal procedure to replace the auxiliary power supply.


CHAPTER 4

4
Initialization Procedures

4.1 Introduction

This chapter contains procedures for connecting the console terminal on the HSC controller and the auxiliary terminal on the HSC50 controller, and initialization procedures for both HSC controller models.

A malfunction during initialization may be reported by a fault code displayed on the operator control panel (OCP). These fault codes are explained in Chapter 8.

4.2 Console/Auxiliary Terminal

The console or auxiliary terminal designated for the HSC controller can be a VTxxx or an LA12 DECwriter. An LAxx printer for hardcopy output can be connected to the VTxxx. Detailed operating information is provided in the appropriate owner manuals accompanying the VTxxx and LAxx models.

NOTE
The VT3xx series terminal can be connected to an RS-232 compatible port only. Connection to another type of port will result in initialization failure and FCC violations.

4.2.1 Console Terminal Connection

Figure 4–1 shows the EIA terminal connectors on the HSC controller rear bulkhead. The console terminal connects to the J60 connector as shown.

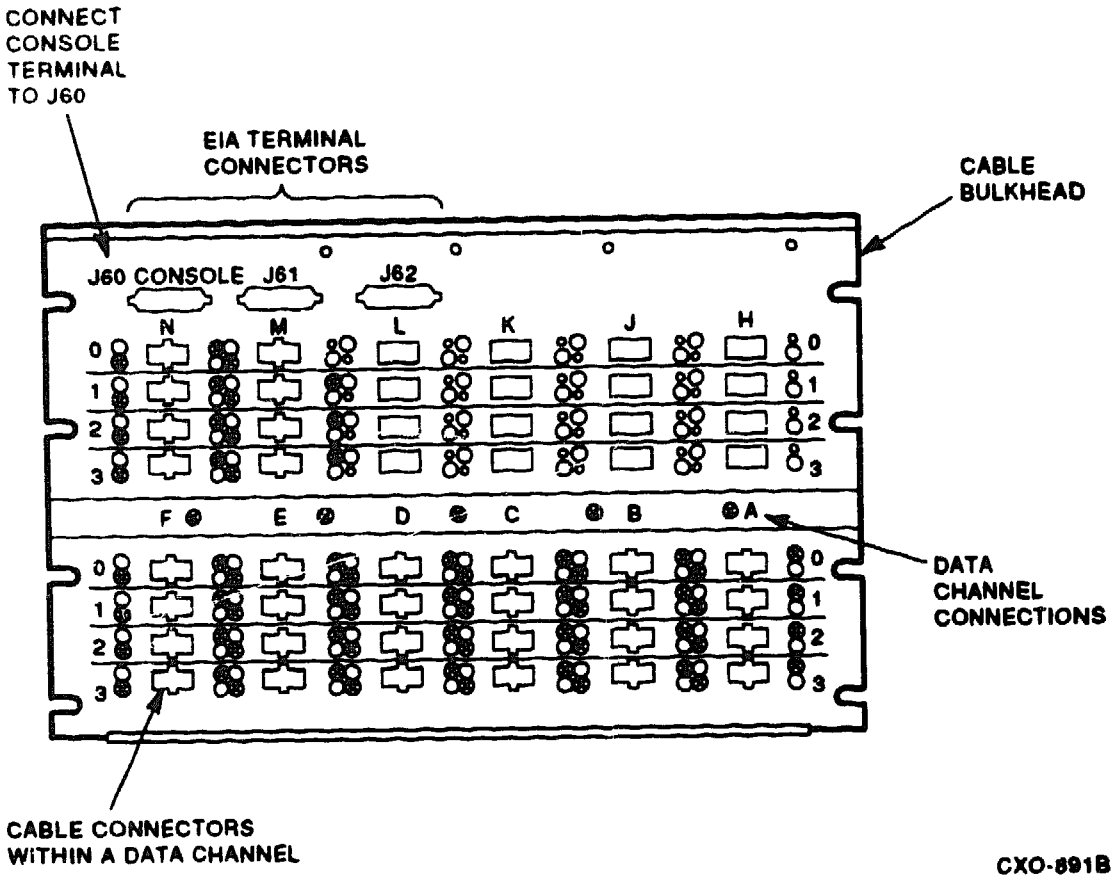


Figure 4–1 Console Terminal Connection

Preferably, power is turned off before the console terminal is installed. However, power can be left on while connecting the terminal. Use the following procedure for installing the console terminal with power on or off:

1. Set the Secure/Enable switch in the SECURE position.
2. Change the terminal state (plug in, remove power, connect EIA line, and so forth).
3. Enter a few spaces on the keyboard.
4. Set the Secure/Enable switch in the ENABLE position if it is necessary to do so at this point.

NOTE
If this procedure is not followed, the HSC controller may enter micro-on-line debugging tool (ODT) mode. This mode is indicated by an @ symbol on the screen. Entering a P (PROCEED) exits this mode.

4.2.2 HSC50 Auxiliary and Maintenance Terminal Connections

Figure 4–2 shows the two ASCII ports on the HSC50 and HSC50 (modified) controllers. The auxiliary terminal can be connected to either the rear or the front ASCII ports. Two terminals *cannot* be connected at the same time.

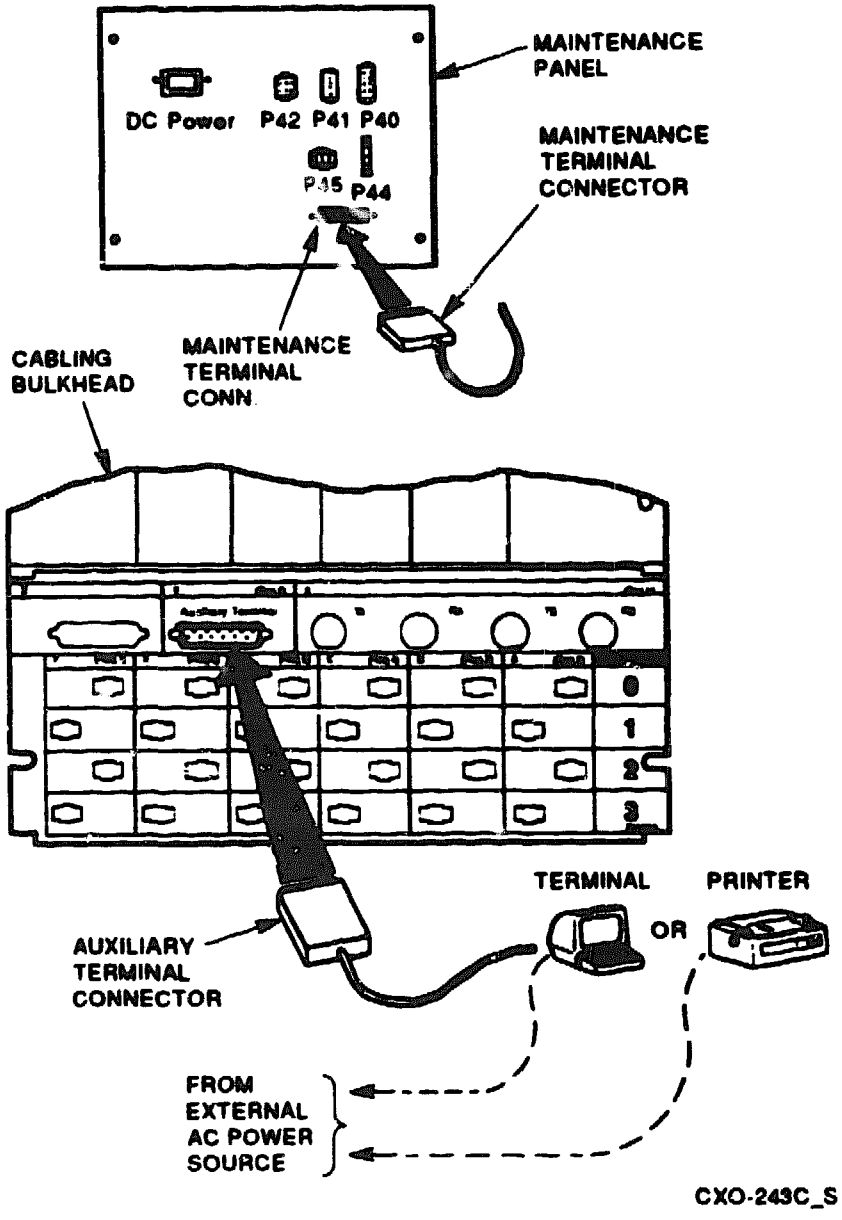


Figure 4–2 Auxiliary or Maintenance Terminal Connection

Preferably, power is turned off before the console terminal is installed. However, power can be left on while connecting the terminal. Use the following procedure for installing the console terminal with power on or off:

1. Set the Secure/Enable switch in the SECURE position.
2. Change terminal state (plug in, remove power, connect EIA line, and so forth).
3. Enter three space characters on the terminal keyboard.

4. If it is necessary to set the Secure/Enable switch in the ENABLE position, do so at this point.

NOTE
If this procedure is not followed, the HSC50 controller may enter micro-on-line debugging tool (ODT) mode. This mode is indicated by an @ symbol on the screen. Entering a P (proceed) should exit this mode.

4.2.3 LA12 Parameters

Detailed information on LA12 terminal installation and operation is found in the *DECwriter Correspondent Technical Manual*.

When an LA12 is used as an auxiliary terminal, the following parameters must be established:

1. Communications:
   - Auto - Ansbk = no
   - Buffer = 1024
   - Comm Port = EIA
   - Disk - HDX = none
   - Echo - Local = no
   - Fault = none
   - G - HDX Start Mode = Rcv
   - H - High Speed (bps) = 9600
   - L - Low Speed (bps) = 300
   - M - Line Prot = FDX - Data Leads
   - O - Rcv Error Ovride = no
   - Parity = 7/M
   - Q - SRTS Polarity = lo
   - Restraint = Xon/Xoff
   - S - Speed Select = hi
   - Turn Char = none
   - U - Power Up = line
   - V - Frequency = bell 103
2. Keyboard:
   - Auto - Linefeed = no
   - Break = no
   - C - Keyclick = no
   - Keypad = normal
   - Language = USA
   - Repeat = yes

3. Printer:
   - A - G0 Char Set = USA
   - B - G1 Char Set = USA
   - C - G2 Char Set = USA
   - D - G3 Char Set = USA
   - End-of-line = wrap
   - Form Length = 264
   - G - Print Cntrl Chars
   - Horiz Pitch (CPI) = 10
   - Newline Char = none
   - Print Force = hi
   - Vertical Pitch (LPI) = 6

4.3 HSC Controller Initialization

This section describes the initialization procedures for the HSC controller using the system diskette. This diskette also contains the software necessary to execute the device integrity tests and the utilities. To boot and run the offline diagnostics from a separate offline diskette, refer to Chapter 7.

System initialization is started by powering on the unit or, if the unit is already on, by pressing and releasing the Init switch with the Secure/Enable switch in the ENABLE position. This initiates the P.io ROM bootstrap tests and then loads the Init P.io test.

NOTE
To run the HSC controller device integrity tests, the system diskette must reside in the RX33 drive. Normally, this diskette resides in RX33 drive 0. However, drive 1 and drive 0 are identical, and disk placement is arbitrary.

Logic in the following areas is tested with the Init P.ioj diagnostic:

- Control processor—The rest of the instruction set not tested by the ROM bootstrap, interrupts, memory management, and the control memory lock-cycle circuitry are included. Detected failures result in an error code display on the OCP. Refer to Chapter 8 for a description of the OCP fault codes.
- Memory—Program, control, and data memories are tested from the I/O control processor. Again, detected failures result in an OCP error code display.
- Host interface and data channels—Module status is collected and placed in a table for the HSC controller operating software initialization process. As each module is enabled, it automatically executes internal microdiagnostics. These internal diagnostics test the following:
  - ROM (sequencer, checksum, parity, and so forth)
  - Special logic unique to that particular module

Upon completion of diagnostics for each module, a status code is passed to the I/O control processor. Status codes for the various modules are discussed in Chapter 5.

If the module diagnostics complete successfully, the status code represents the module type and the green LED is turned on. If the diagnostics fail, the status code indicates the failing microtest. In addition, detected failures cause a red LED to light on that module. K.ci, K.sdi, K.sti, and K.si module failures are also displayed on the console terminal after the boot is completed.

NOTE
Lighting of the red LED on the L0100 or L0118 LINK module in this instance *does not* indicate a failure of the module.

For a detailed description of the boot process, refer to the HSC boot flowchart (Figure 8–17) in Chapter 8.

4.3.1 Init P.io Test (INIPIO)

The INIPIO test completes the P.ioj module and the HSC memory testing previously started by the ROM bootstrap tests. All P.ioj logic not tested by the bootstrap is tested by INIPIO. In addition, the HSC program, control, and data memories are tested.

This test runs in a standalone environment (no other HSC processes are running). If a failure is detected, the failing module is flagged by illumination of the red LED on the module. If the test runs without finding any errors, the HSC software is loaded and started. The Init P.io test is not a repair-level diagnostic. If a repair-level test is needed, run the offline P.io test that provides standard HSC controller error messages.

4.3.2 INIPIO Test System Requirements

To run this test, the following hardware is required:

- P.ioj (processor) module with HSC boot ROM
- K.ci connected to a star coupler or loop-back cables installed
- At least one M.std2 or M.std4 (memory) module
- RX33 controller with at least one working drive
- An HSC system diskette (RX33 media)

4.3.3 INIPIO Test Prerequisites

The INIPIO test is loaded by the HSC ROM bootstrap program. The bootstrap tests the basic J–11 instruction set, the lower 2048 bytes of program memory, an 8 Kword partition in program memory, and the RX33 subsystem used by the bootstrap. When the INIPIO test begins to execute, most J–11 logic has been tested and is considered working. Likewise, the program memory occupied by the test and the RX33 subsystem used to load the test are also considered tested and working. The RX33 diskette is checked to ensure it contains a bootable image.

4.3.4 INIPIO Test Operation

Follow these steps to start the INIPIO test:

1. Insert the HSC system diskette in the RX33 unit 0 drive (left-hand drive).
2. Power on the HSC controller or press and release the Init button on the HSC OCP with the Secure/Enable switch in the ENABLE position. The Init lamp lights and the following occurs:
   - The RX33 drive-in-use LED lights within 10 seconds, indicating the bootstrap is loading the INIPIO test to the program memory.
   - The I/O State indicator is on after diskette motion stops and the INIPIO test begins testing.
   - The INIPIO test displays the following message on the HSC console when it begins:

     ```
     INIPIO-I BOOTING...
     ```

   - HSC software is being loaded when the State indicator flashes rapidly.

- HSC software indicates it has loaded properly when the State indicator blinks slowly.
- The HSC controller displays its name and version indicating it is ready to perform host I/O.

Once initiated, the INIPIO test is terminated only by halting and rebooting the HSC controller. If the test fails to load using the preceding startup procedure, perform the next four steps:

1. Check the OCP fault indicator. If the fault indicator is on, press the fault button once and check the fault code. Refer to Chapter 8 for a description of the OCP fault codes.
2. Boot the diskette from the RX33 unit 1 drive (right-hand drive).
3. Boot using another diskette. If that diskette boots, the original diskette is probably damaged or worn.
4. Boot using the HSC offline diagnostic diskette. This diskette contains the offline P.io test, which provides extensive error reporting features.

The progress of the INIPIO test is displayed in the State LED. Before the test starts, the State LED is off. When the test starts, the State LED is turned on, and the INIPIO-I BOOTING message is displayed on the HSC console. When the test completes with no fatal errors, the State LED begins to blink at a steady rate. If the test detects an error, the Fault lamp on the HSC OCP is lit.

4.4 HSC50 Controller Initialization

To run the HSC50 device integrity tests and utilities, the HSC50 operating software must be initialized with both the system and utilities cassettes loaded in the TU58 drives. Before inserting the system tape into the TU58 drive, check the black RECORD tab. This tab must be in the record position (as indicated by an arrow on the tab) to ensure proper system operation. The utilities tape need not be write-enabled.

NOTE
To run the HSC50 device integrity tests, the system tape must reside in the TU58 tape drive. Normally, this tape resides in TU58 drive 0. Drive 1 and drive 0 are identical, and tape placement is arbitrary.

However, the utilities tape does not contain a bootable image, and if drive 0 contains the utilities tape, the system will try to boot from drive 1.

The HSC50 controller can be initiated by either powering on the unit if it is powered down or, if power is already applied, by pressing and releasing the Init switch with the Secure/Enable switch in the ENABLE position. This causes the P.ioc bootstrap ROM tests to run and then load the Init P.ioc test.

4.4.1 HSC50 Offline Diagnostics Tape

The offline diagnostics tape can be booted in either TU58 tape drive and need not be write enabled. The offline tape can be booted by either powering on the unit or pressing and releasing the Init switch with the Secure/Enable switch in the ENABLE position. This causes the P.ioc bootstrap ROM tests to run and then load the offline P.ioc test.

4.4.2 Init P.ioc Diagnostic

The Init P.ioc test is loaded by the P.ioc ROM bootstrap test each time the HSC50 system tape is booted. This diagnostic completes the testing of the P.ioc module and the HSC50 memories. At the successful completion of these tests, the HSC50 operating software is loaded and started.

Logic in the following areas is tested with the Init P.ioc diagnostic:

- Control processor—The rest of the instruction set not tested by the ROM bootstrap, interrupts, memory management, and the control memory lock-cycle circuitry are included. Detected failures result in an error code display on the OCP. Refer to Chapter 8 for a description of the OCP fault codes.
- Memory—Program, control, and data memories are tested from the I/O control processor module. Again, detected failures result in an OCP error code display.
- Host interface and data channels—Module status is collected and placed in a table for the HSC50 operating software initialization process. As each module is enabled, it automatically executes internal microdiagnostics. These internal diagnostics test the following:
  - ROM (sequencer, checksum, parity, and so forth)
  - Special logic unique to that particular module

Upon completion of diagnostics for each module, a status code is passed to the I/O control processor. Status codes for the various modules are discussed in Chapter 5.

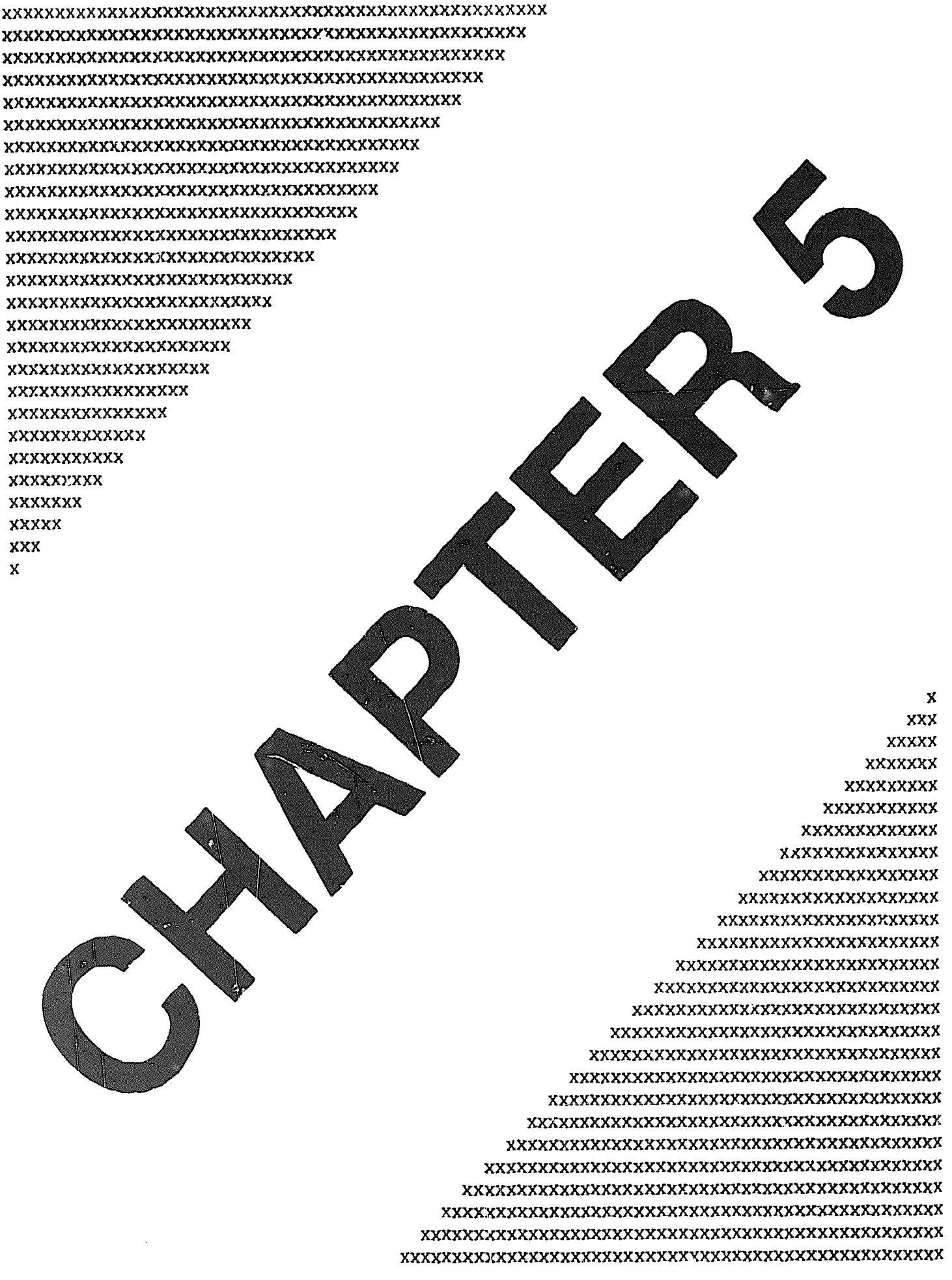
If the module diagnostics complete successfully, the status code represents the module type and the green LED is turned on. If the diagnostics fail, the status code indicates the failing microtest. In addition, detected failures cause a red LED to light on that module. K.ci, K.sdi, K.sti, and K.si module failures are also displayed on the auxiliary terminal after the boot is completed.

NOTE
Lighting of the red LED on the L0100 or L0118 LINK module in this instance *does not* indicate a failure of the module.

For a detailed description of the boot process, refer to the HSC50 boot flowchart (Figure 8–17) in Chapter 8.

4.5 Fault Code Interpretation

All failures occurring during the Init P.io test are reported on the OCP LEDs. When the Fault indicator is lit, pressing the Fault switch results in the display of a failure code in the OCP LEDs. This code indicates which HSC controller module is the most probable cause of the detected failure. The failure code blinks on and off at one second intervals until the HSC controller is rebooted if the fault code represents a fatal fault. A soft fault code is cleared in the OCP by pressing the Fault switch a second time. To restart the boot procedure, press the Init switch. To identify the probable failing module, refer to Chapter 8 for a description of the OCP fault codes.


CHAPTER 5

5
Device Integrity Tests

5.1 Introduction

Device integrity tests executing in the HSC controller do not interfere with normal operation other than with the device being tested, though some performance degradation may be experienced by the HSC controller. The device integrity tests reside on the HSC controller system media disk or HSC50 controller utilities media tape.

The tests described in this chapter are:

- ILRX33—RX33 disk drive integrity tests
- ILTU58—TU58 tape drive integrity tests
- ILMEMY—Memory integrity tests
- ILCACH—Cache memory integrity tests
- ILDISK—Disk drive integrity tests
- ILTAPE—Tape device integrity tests
- ILTCOM—Tape compatibility tests
- ILEXER—Multidrive exerciser

5.1.1 Generic Prompt Syntax

All prompts issued by the HSC controller tests use a generic syntax, as follows:

- Prompts requiring user action or input are followed by a question mark.
- Prompts offering a choice of responses show those choices in parentheses.
- A capital D in parentheses indicates the response should be in decimal.
- Square brackets enclose the prompt default or, if empty, indicate no default exists for that prompt.

5.1.2 Generic Error Message Format

All device integrity tests follow a generic error message format, as follows:

```
>XXXXX-x-tt:tt T#aaa E#bbb  MA-cccccc
<TEXT STRING DESCRIBING ERROR>

   FRU1-dddddd FRU2-dddddd
   MA-cccccc
   EXP-yyyyyy
   ACT-zzzzzz
```

where:

XXXXXX> is the appropriate device integrity test prompt.
x> is the letter indicating the type of integrity test that was initiated:

D> is the demand integrity test.
A> is the automatic integrity test.
P> is the periodic integrity test.

tt:tt is the current time.
aaa is the decimal number denoting the test that failed.
bbb is the decimal number denoting the error detected.
ccc is the unit number of the drive being tested.
FRU1 is the most likely field replaceable unit (FRU).
FRU2 is the next most likely FRU.
dddddd are the names of FRU1 and FRU2.
MA is the media address.
eeeeee is the octal number denoting offset within the block.
yyyyyy is the octal number denoting data expected.
zzzzzz is the octal number denoting data actually found.

The first line of the error message contains general information about the error. The second line describes the nature of the error. Lines 1 and 2 are mandatory and appear in all error messages. Line 3 and any succeeding lines display additional information and are optional.

5.2 ILRX33—RX33 Disk Drive Device Integrity Tests

The ILRX33 exerciser tests either of the RX33 disk drives attached to the HSC controller. ILRX33 runs concurrently with other HSC controller processes and uses the services of the HSC control program and the diagnostic execution monitor (DEMON).

ILRX33 performs several writes and reads to verify the RX33 disk drive internal data paths and read/write electronics.

A scratch diskette is not required. ILRX33 does not destroy any data on the HSC software media.

The exerciser tests only the RX33 disk drive, the RX33 disk drive controller on the memory module, and the data path between the Pico module and the RX33 disk drive. All other system hardware is assumed to be working properly.

ILRX33 verifies only a particular RX33 disk drive and controller combination is working or failing. Therefore, the test should not be used as a subsystem troubleshooting aid. This test does not support flags. If the test indicates a drive or controller is not operating correctly, replace the drive and/or controller.

5.2.1 System Requirements

Hardware and software requirements include:

- Proj (processor) module with boot ROMs
- M.std2/M.std4 memory/disk controller module
- RX33 disk drive controller with at least one working drive
- HSC controller system media
- Console terminal

5.2.2 Operating Instructions

Enter Ctrl/Y to get the HSCxx> prompt. Then, enter either RUN ILRX33 or RUN DXn:ILRX33 to initiate the tests.

NOTE
The term DXn: refers to the RX33 disk drives (DX0: or DX1:).

If ILRX33 cannot load from the specified diskette, try loading the test from the other diskette. For example, if RUN ILRX33 fails, try RUN DXn:ILRX33.

5.2.3 Test Termination

ILRX33 can be terminated by entering Ctrl/Y. The test automatically terminates after reporting an error; however, if the error displayed is Retries Required, the test continues.

5.2.4 Parameter Entry

The device name of the RX33 disk drive to be tested is the only parameter sought by this test. When the test is invoked, the following prompt is displayed:

```
Device Name of RX33 to test (DX0:, DX1:, LB:) [] ?
```

NOTE
The string LB: indicates the RX33 disk drive last used to boot the control program.

One of the indicated strings must be entered. If one of these strings is not entered, the test displays the message Illegal Device Name and the prompt is repeated.

5.2.5 Progress Reports

At the end of the test, the following message is displayed:

```
ILRX33>D>tt:tt Execution Complete
```

where:

tt:tt is the current time.

5.2.6 Test Summary

The ILRX33 test summary is contained in the following paragraph.

Test 001, Read/Write Test—Verifies that data can be written to the diskette and read back correctly. All reads and writes access physical block 1 of the RX33 disk drive (the RT–11 operating system volume ID block). This block is not used by the HSC controller operating software.

Initially, the contents of block 1 are read and saved. Three different data patterns are then written to block 1, read back, and verified. The read/write electronics in the drive and the internal data path between the RX33 disk drive controller and the drive are checked. Following the read/write test, the original contents of block 1 are written back to the diskette.

If the data read back from the diskette does not match the data written, a data compare error is generated. The error report lists the media address (MA) in error within the block together with the expected (EXP) and actual (ACT) contents of the word.

5.2.7 Error Message Example

All error messages issued by ILRX33 conform to the HSC generic error message format described in Section 5.1.2. Following is a typical ILRX33 error message:

```
ILRX33>D>00:00 T#001 E#003 U- 50182
ILRX33>D> No Diskette Mounted
ILRX33>D> FRU1-Drive
ILRX33>D>00:00 Execution Complete
```

Additional (optional) lines may be found on some error messages.

5.2.8 Error Messages

This section describes error messages issued by ILRX33. Hints about the possible cause of the error are provided where feasible.

- **Block Number Out of Range**—Indicates the driver detected a request to read a block number outside the range of legal block numbers (0 through 2399 decimal). Because the ILRX33 reads and writes disk block 1, this error message may indicate a software problem.
- **Data Compare Error**—Indicates data subsequently read back:

  ```
  MA -aaaaaa
  EXP-bbbbbb
  ACT-cccccc
  ```

  In this example:
  aaaaaa represents the address of the failing word within the block (512 bytes) that was read.
  bbbbbb represents the data written to the word.
  cccccc represents the data read back from the word.

  Because this test only reads and writes block 1 of the diskette, all failures are related to block 1.

- **Hard I/O Error**—Indicates the program encountered a hard error while attempting to read or write the diskette.
- **Illegal Device Name**—Indicates the user specified an illegal device name when the program prompted for the name of the drive to be tested. Legal device names include DX0:, DX1:, and LB:. After displaying this error, the program again prompts for a device name. Enter one of the legal device names to continue the test.

- **No Diskette Mounted**—Indicates the RX33 disk drive being tested does not contain a diskette. Insert a diskette before repeating the test. If this error is displayed when the drive does contain a diskette, the drive or controller is at fault.
- **Operation Aborted**—Reported if ILRX33 is aborted by entering Ctrl/Y.
- **Retries Required**—Indicates a read or write operation failed when first attempted, but succeeded on one of the retries performed automatically by the driver software. This error normally indicates the diskette media is degrading and the diskette should be replaced.
- **Unknown Status STATUS=xxx**—Indicates ILRX33 received a status code it did not recognize. The octal value xxx represents the status byte received. RX33 disk drive reads and writes are performed for ILRX33 by the control program's driver software. At the completion of each read or write operation, the driver software returns a status code to the RX33 disk drive test, describing the result of the operation. The test decodes the status byte to produce a description of the error.

  An unknown status error indicates the status value received from the driver did not match any of the status values known to the test. The status value returned (xxx) is displayed to help determine the cause of the problem. Any occurrence of this error should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Write-Protected**—Indicates the RX33 disk drive being tested contains a write-protected diskette. Try again with a write-enabled diskette. If the diskette is already write-enabled, the RX33 disk drive or controller is faulty.

5.3 ILTU58–TU58 Tape Drive Device Integrity Test

ILTU58 tests either of the TU58 tape drives attached to the HSC50 controller. This test runs concurrently with other HSC controller processes and uses the services of the control program and the DEMON. The test can be initiated with only the system tape installed.

Because the operating system tests the TU58 tape drive every time it is used, ILTU58 performs only minimal testing. Several read and write operations are performed to test the internal data paths and the read/write circuitry of the TU58 tape drive.

A scratch tape is not required. This test does not destroy any data on the HSC software cassette.

ILTU58 tests only the TU58 tape drive and the data path between the P.ioc module and the TU58 tape drive. All other system hardware is assumed to be working properly.

ILTU58 verifies that only a particular TU58 tape drive and controller combination is working or failing. Therefore, the test should not be used as a troubleshooting aid. This test does not support flags. If the test indicates that a drive or controller is not operating correctly, replace the drive and/or controller.

5.3.1 System Requirements

Hardware and software requirements include:

- P.ioc module
- M.std memory/disk controller module
- TU58 tape drive controller with at least one working drive
- HSC system media

5.3.2 Operating Instructions

Enter Ctrl/Y to get the HSCxx> prompt. Then enter RUN ILTU58 or RUN DDn::ILTU58 to initiate the tests.

5.3.3 Test Termination

ILTU58 can be terminated by entering Ctrl/Y.

5.3.4 Error Messages

This section describes the error messages issued by ILTU58.

- **Bad Opcode**—Indicates the program encountered an illegal opcode.
- **Bad Record**—Indicates the program encountered a bad record while attempting to read or write the cassette tape.
- **Bad Unit #**—Indicates the diagnostic interface could not find the unit number specified. The drive may have been offline.
- **Data Compare Error**—Indicates that data subsequently read back did not match data written. The test writes a pattern to block 1, then reads block 1 and checks that the pattern read is the same as the pattern written. If the patterns differ, this error message is displayed.

  Because this test only reads and writes block 1 of the cassette tape, all failures occur while trying to access physical block 1.
- **End of Medium**—Indicates the end of the cassette tape.
- **Failed Self-Test**—Indicates the TU58 internal diagnostic test failed.
- **Hard I/O Error**—Indicates the program encountered a hard error while attempting to read or write the cassette tape.
- **Illegal Device Name**—Indicates the user specified an illegal device name when prompted for the name of the drive to be tested. After displaying this error, the program again prompts for a device name. Enter a legal device name to continue the test.
- **No Cassette Mounted**—Indicates the drive does not have a cassette. Insert a cassette tape then repeat the test. Otherwise, the drive or the controller is faulty.
- **Operation Aborted**—Reported if the test is interrupted by entering Ctrl/Y.
- **Retries Required**—Indicates a read or write operation failed in the first attempt but succeeded on one of the retries. This message may also mean that the tape media is degrading and should be replaced.
- **Seek Error**—Indicates a seek error status was set after a SEEK command.
- **Unknown Status**—Indicates ILTU58 received a status code it did not recognize. This status code is displayed to help determine the cause of the problem.
- **Write Protected**—Indicates the drive being tested contains a write-protected tape. Try again with a write-enabled tape. If the tape is not write-protected, then the drive or controller is faulty.

5.4 ILMEMY—Memory Integrity Tests

The memory integrity test is designed to test HSC controller data buffers. This test can be initiated automatically or on demand. It is initiated automatically to test data buffers that produce a parity or nonexistent memory (I) error when in use by any of the K modules.

ILMEMY tests only data memory buffers. Control program memory errors typically cause a reboot of the HSC controller.

Buffers that fail the memory test are removed from service. They are sent to the disabled buffer queue.

NOTE
The contents of the disabled buffer queue are lost during a reboot of the HSC controller. As a result, all bad memory locations are lost.

Buffers sent twice to this test are also sent to the disabled buffer queue even if they did not fail the test. Buffers that pass the memory test and have not been tested previously are sent to the free buffer queue for further use by the control program.

When the test is initiated on demand, any buffers in the disabled buffer queue are tested and the results of the test are displayed on the terminal from which the test was initiated.

This test runs concurrently with other HSC controller processes and uses the services of the control program and the DEMON.

NOTE
If an I/O control processor module or a memory module fails during the periodic memory tests, the FACILITY section of the crash code displays PRMEMY, which indicates the failure occurred during the periodic tests.

5.4.1 System Requirements

Hardware requirements include:

- Ioj/c (processor) module
- At least one M.std2/4 memory module (HSC controller) or the M.std memory module (HSC50 controller)
- RX33 disk drive controller with one working drive (HSC controller) or TU58 tape drive controller with one working drive (HSC50 controller)
- A console terminal to start ILMEMY on demand.

This program only tests data buffers located in the HSC controller data memory. All other system hardware is assumed to be working.

Software requirements include:

- Control program (system diskette or tape)
- DEMON

5.4.2 Operating Instructions

Enter Ctrl/Y to get the HSCxx> prompt. The keyboard monitor responds with the prompt:

```
HSCxx>
```

Enter RUN dev:ILMEMY to initiate the memory integrity test. This program has no user-supplied parameters or flags.

If the memory integrity test is not contained on the specified device (dev:), an error message is displayed.

5.4.3 Test Termination

ILMEMY can be terminated at any time by entering Ctrl/Y.

5.4.4 Progress Reports

Error messages are displayed as needed. At the end of the test, the following message is displayed (by DEMON):

```
ILMEMY>D>tt:tt Execution Complete
```

where:

tt:tt is the current time.

5.4.5 Test Summary

Test 001 receives a queue of buffers for testing. If the ILMEMY is initiated automatically, the queue consists of buffers from the suspect buffer queue.

When the control program detects a parity or nonexistent memory (NXM) error in a data buffer, the buffer is sent to the suspect buffer queue. While in this queue, the buffer is not used for data transfers. The HSC controller periodic scheduler periodically checks the suspect buffer queue to see if it contains any buffers. If buffers are found on the queue, they are removed and ILMEMY is automatically initiated to test those buffers.

If the ILMEMY test is initiated on demand, it retests only buffers already known as disabled.

If the test is initiated automatically and the buffer passes the test, the program checks to see if this is the second time the buffer was sent to the memory integrity test. If this is the case, the buffer is probably producing intermittent errors. The buffer is retired from service and sent to the disabled buffer queue. If this is the first time the buffer is sent to the memory integrity test, it is returned to the free buffer queue for further use by the control program. In this last case, the address of the buffer is saved in case the buffer again fails and is sent to the memory integrity test a second time.

ILMEMY will terminate when all buffers on the test queue are tested.

5.4.6 Error Message Example

All error messages issued by the ILMEMY conform to the generic error message format described in Section 5.1.2. Following is a typical ILMEMY error message:

```
ILMEMY>A>09:33  T#001 E#000
ILMEMY>A>Tested Twice with no Error (Buffer Retired)
ILMEMY>A>FRU1-M.std2  FRU2-
ILMEMY>A>Buffer Starting Address  (physical) = 15743600
ILMEMY>A>Buffer Ending Address    (physical) = 15744776
ILMEMY>D>09:33 Execution Complete
```

5.4.7 Error Messages

This section describes the error messages issued by ILMEMY.

- **Can't Allocate Timer, Test Aborted**—Indicates the program failed to allocate a timer for SLEEP.
- **Memory Data Error**—Indicates the wrong data was read while testing a buffer. The buffer is retired from service and sent to the disabled buffer queue.
- **Memory Parity Error**—Indicates a parity error occurred while testing a buffer. The buffer is retired from service and sent to the disabled buffer queue.
- **NXM Trap (Buffer Retired)**—Indicates an unknown address or memory location is being referenced. The buffer is retired from service and its address is sent to the disabled buffer queue.
- **Returned Buffer to Free Buffer Queue**—Indicates a buffer failed during use by the control program but that no error was detected. Because this is the first time the buffer was sent to the memory integrity test, it is returned to the free buffer queue for further use by the control program. The address of the buffer is stored by the memory integrity test in case the buffer fails again when in use by the control program.
- **Tested Twice with No Error**—Indicates the buffer under test passed the memory test. However, this is the second time the buffer was sent to the memory test and passed it. Because the buffer has a history of two failures while in use by the control program, yet does not fail the memory test, intermittent failures on the buffer are assumed. The buffer is retired from service and sent to the disabled buffer queue.

5.5 ILCACH—Cache Memory Integrity Tests

The ILCACH test is designed to test the M.Cache hardware module. ILCACH can be invoked in three ways:

- ILCACH is always initiated at HSC controller power-up if the boot code determines that an M.cache module is available and properly connected to the M.std4 memory module.
- The cache server software can automatically invoke the ILCACH test if the M.cache module exceeds error thresholds.
- ILCACH may be run on demand at the HSC console.

When ILCACH is initiated at HSC controller power-up, it verifies the results of the M.cache module self-test. The M.cache module self-test checks all of the cache and data memory resident on the module. If there are no memory errors, the ILCACH exerciser runs a series of tests to verify the operation of the portions of the M.cache module that the self-test does not verify.

If the M.cache module self-test reports an error, the ILCACH exerciser performs two tasks:

- It determines if the M.cache module is usable.
- If the module is usable, ILCACH verifies the cache memory to determine what portions of it are usable. The result of this test is a Good Cache List, which is sent to the Cache Server software for further processing.

ILCACH is started automatically by the cache server software when the server determines that the M.cache module has exceeded its error thresholds. ILCACH tests all of the functions on the M.cache module and determines if the error that occurred was fatal or if just portions of the on-board memory were recording errors. If the M.cache module has a fatal error, all caching is disabled. If portions of the memory are found to be usable, a new Good Cache List is generated and reported to the cache server software.

When ILCACH is started on demand by a user, the exerciser runs its set of tests, and a new Good Cache List is generated and reported to the cache server software. ILCACH can only be started on demand if the M.cache module is not being used to cache valid data.

ILCACH runs concurrently with other processes in the HSC controller and uses the services of the HSC software control program and DEMON.

5.5.1 System Requirements

Hardware requirements include:

- P.ioj–18 (18-Mhz processor) module
- M.std4 module
- M.cache module
- RX33 disk drive controller with one working RX33 disk drive
- Console terminal from which to start ILCACH on demand

Software requirements include:

- HSC Version 6.0 or higher control program software on an RX33 diskette

NOTE
Earlier software versions are not compatible with the M.cache module.

5.5.2 Operating Instructions

Enter Ctrl/C. The keyboard monitor responds with the prompt:

```
HSC>
```

Enter RUN ILCACH to initiate the M.cache integrity test. This program has no user-supplied parameters or flags.

The following is an example run of ILCACH with no error message:

```
HSC>RUN ILCACH
ILCACH>D>hh:mm Execution Starting
ILCACH>D>hh:mm Execution Complete
```

5.5.3 Test Termination

ILCACH cannot be terminated while running.

5.5.4 Progress Reports

Error messages are displayed as needed. At the end of the test, the following message is displayed (by DEMON):

```
ILCACH>D>hh:mm Execution Complete
```

where:

hh:mm is the current time.

5.5.5 Test Summaries

Test summaries for ILCACH follow:

- **Test 001, Verify M.cache Self-Test**—Verifies that the M.cache module self-test, invoked by INIPIO, returns a successful status.
- **Test 002, DIAGNOSTIC Buffers Test**— Verifies that all of the diagnostic bytes of cache memory can be written and read back. The diagnostic bytes are the 8 bytes at the top of every 32 kilowords. There are a total of 1024 diagnostic buffers. The data written to the diagnostic bytes is generated by the M.cache module pattern generator.
- **Test 003, Cache Data Register Test**—Verifies that the cache data register can be written and read back. Triplets generated by the M.cache module pattern generator are written to the register and then read back.
- **Test 004, CBUS Address Test**— Verifies that the CBUS address register can be correctly read and that it contains the correct value.
- **Test 005, Refresh Rate Test**—Verifies that the cache memory does a refresh cycle every 25 bus cycles. The test writes a sector to M.cache memory, waits 2 seconds, then reads back the sector and checks for errors. The test also verifies that only one sector of data was transferred to check for underwriting or overwriting.

5.5.6 Error Message Example

All error messages issued by ILCACH conform to the generic error message format described in Section 5.1.2. Following is a typical ILCACH error message:

```
ILCACH>A>09:33 T@001 E@000
ILCACH>A>Error detected with REFRESH CYCLE
ILCACH>A>FRU1-MCACHE

ILCACH>D>09:33 Execution Complete
```

5.5.7 Error Messages

This section describes the error messages issued by ILCACH.

- **Cannot Allocate A Timer, Test Aborted**—ILCACH cannot allocate a timer to properly run its tests.
- **ILCACH cannot be aborted via CTRL/Y or CTRL/C**—ILCACH cannot be terminated while running.
- **MCACHE hardware module not present, or not installed correctly**—ILCACH was invoked by the user, but there was no M.cache module installed in the HSC controller, or the M.cache module was incorrectly installed.
- **MCACHE Memory Address Error**—This error is displayed in the form:

  ```
  MCACHE Memory Address Error.
  Expected Address = xxxxxxxx
  Actual Address   = yyyyyyyy
  ```

  This error occurs when Test 004, CBUS Address Test, finds that the cache memory address did not match the expected value.
- **MCACHE Module is unusable. Caching will be disabled**—The M.cache module is unusable due to errors found in the ILCACH test

- **MCACHE must be disabled. Use SET SERVER DISK/NOCACHE to disable cache**—The user has attempted to run ILCACH on an M.cache module that is still online to the cache server.
- **More than 50% of CACHE is bad.**—More than 50% of the memory on the M.cache module has single bit ECC errors. No caching will be done on this module.
- **Status Word Not Expected Value**—The M.cache module status word did not contain the expected value. ILCACH reports the returned status word and the associated error:

```
ILCACH>A>09:33 T#001 E#001
ILCACH>A>MCACHE Detected Error
ILCACH>A>FRU1-MCACHE
ILCACH>A>MCACHE Status Word = 006377
ILCACH>A>Summary Error Bit
ILCACH>A>Multi-bit ECC Error

ILCACH>D>09:33 Execution Complete
```

- **Timed out reading the MCACHE Status Register**—The M.cache module state machine is not processing any cache commands.
- **Unable to transfer one sector from CACHE to DATA memory**—The M.cache module is either overwriting or underwriting one sector's worth of information to data memory.
- **Unsupported invocation of ILCACH**—ILCACH was invoked incorrectly.
- **MCACHE Memory Address Error**—ILCACH Test 04 found an M.cache module address that did not match the expected value. This error is reported in the following form:

```
Expected Address = xxxxxxxx
Actual Address   = xxxxxxxx
```

- **Between 25% and 50% of CACHE is bad**—One 8 megabyte bank of memory on the M.cache module is bad. The M.cache module is still usable but one-fourth of it is marked bad.

5.6 ILDISK—Disk Drive Integrity Tests

ILDISK isolates disk drive-related problems to a disk drive, including the Enhanced Mode ESE20 storage element, or to the SDI cable, or to a disk data channel module

ILDISK runs in parallel with disk I/O from a host CPU. However, the drive being diagnosed cannot be online to any host. ILDISK can be initiated upon demand through the console terminal or automatically by the control program when an unrecoverable disk drive failure occurs.

ILDISK is automatically invoked by default whenever a drive is declared inoperative, with one exception: if a drive is declared inoperative while in use by an integrity test or utility.

Automatic initiation of ILDISK can be inhibited by entering the SETSHO command SET AUTOMATIC DIAGNOSTICS DISABLE. If the SET AUTOMATIC DIAGNOSTICS command is entered and DISABLE is specified, ILMEMY (a test for suspect buffers) is also disabled. For this reason, leaving ILDISK automatically enabled is preferable.

The tests performed vary, depending on whether the disk drive is known to the HSC controller disk server

If the disk drive is unknown to the disk server, it is either unable to communicate with the HSC controller or was declared inoperative when it failed while communicating with the HSC controller.

In this case, because the drive cannot be identified by unit number, the user must supply the requestor number and port number of the drive. Then the SDI verification tests can execute. The SDI verification tests check the path between the K.sdi/K.si and the disk drive and command the drive to run its integrity tests. If the SDI verification tests fail, the most probable FRU is identified in the error report. If the SDI verification tests pass, presume the drive is the FRU.

If the drive is known to the disk server, that is, identifiable by unit number, the Read/Write/Format tests are performed in addition to the SDI verification tests. If an error is detected, the most probable FRU is identified in the error report. If no errors are detected, presume the FRU is the drive.

To find the drives known to the disk and tape servers, enter the SETSHO command SHOW DISKS or SHOW TAPES.

5.6.1 System Requirements

Hardware requirements include:

- Disk drive
- Disk data channel, connected by an SDI cable

The software requirements for this test reside on the system media and include:

- HSC controller executive (CRONIC)
- ILDISK.DIA program
- DEMON
- K.sdi/K.si microcode (installed with the K.sdi/K.si module)

The test assumes the I/O control processor module and the memory module are working.

Refer to the disk drive documentation to interpret errors that occur in the drive's integrity tests.

5.6.2 Operating Instructions

The following steps are used to initiate ILDISK.

NOTE
To prevent access from another HSC controller, deselect the alternate port switch on the drive to be tested. The alternate port switch is the drive port switch allowing alternate HSC controller access to the drive.

Enter Ctrl/Y to get the HSCxx> prompt. The keyboard monitor responds with the prompt:

```
HSCxx>
```

Enter RUN dev:ILDISK to initiate the disk drive integrity tests. Wait until ILDISK is read from the system software load media into the program memory.

Enter parameters after ILDISK is started. Refer to Section 5.6.5 for the parameter entries.

5.6.3 Availability

If the software media containing ILDISK is not loaded when the RUN ILDISK command is entered, an error message is displayed. Insert the software media containing ILDISK and repeat Section 5.6.2.

5.6.4 Test Termination

ILDISK is terminated by entering Ctrl/Y or Ctrl/C. Test termination may not take effect immediately because certain parts of the program cannot be interrupted. An example would be during SDI commands. If an SDI DRIVE DIAGNOSE command is in progress, interfering with the disk drive at this time can cause the program to wait 2 minutes before aborting.

When ILDISK is aborted, it sends the message:

```
Execution Aborted
```

5.6.5 Parameter Entry

When run on demand, ILDISK first prompts:

```
DRIVE UNIT NUMBER (U) [] ?
```

Enter the unit number of the disk drive being tested. Unit numbers are in the form Dnnnn, where nnnn is a decimal number between 0 and 4094, corresponding to the number printed on the drive unit plug. Terminate the unit number response by pressing Return.

ILDISK attempts to acquire the specified unit through the diagnostic interface. If the unit is acquired successfully, ILDISK next prompts for the drive integrity test to be executed.

If the acquire fails, one of the following conditions is encountered:

- The specified drive is unavailable. This indicates the drive is connected to the HSC controller, but is currently online to a host CPU or an HSC controller utility. Online drives cannot be diagnosed. ILDISK repeats the prompt for the unit number.
- The specified drive is unknown to the disk functional software. Drives are unknown for one of the following reasons:
  - The drive and/or disk data channel port is broken and cannot communicate with the disk functional software.
  - The drive was previously communicating with the HSC controller but a serious error occurred, and the HSC controller has ceased communicating with the drive (marked the drive as inoperative).

  In either case, ILDISK prompts for a requestor number and port number. Refer to Section 5.6.6.

After receiving the unit number (or requestor and port), ILDISK prompts:

```
RUN A SINGLE DRIVE DIAGNOSTIC (Y/N) [N] ?
```

Answering N causes the drive to execute its entire integrity test set. Answering Y executes a single drive integrity test. If a single drive integrity test is selected, the test prompts:

```
DRIVE TEST NUMBER (H) [] ?
```

Enter a number (in hex) specifying the drive integrity test to be executed. Consult the appropriate disk maintenance or service manual to determine the number of the test to perform. Entering a test number not supported by the drive results in an error generated in test 05.

The test prompts for the number of passes to perform:

```
# OF PASSES TO PERFORM (1 to 32767) (D) [1] ?
```

Enter a decimal number between 1 and 32767, specifying the number of test repetitions. Pressing Return without entering a number runs the test once.

5.6.6 Specifying Requestor and Port

To test drives unknown to the disk functional software, specify the requestor number and port number. The requestor number is any number 2 through 9 (HSC controller) or 2 through 7 (HSC50 controller) specifying the disk data channel connected to the drive under test.

The port number is 0 through 7; it specifies which of eight disk data channel ports is connected to the drive under test. The requestor number and port number can be determined in one of two ways:

- By tracing the SDI cable from the desired disk drive to the bulkhead connector, then tracing the bulkhead connector to a specific port on one of the disk data channels.
- By using the SHOW DISKS command to display the requestor and port numbers of all known drives. To use this method, exit ILDISK by entering Ctrl/Y. Enter SHOW DISKS at the HSCxx> prompt.

  The SHOW DISKS command displays a list of all known drives including the requestor number and port number for each drive. Each disk data channel has four or eight possible ports to which a drive can be connected. By inference, the port number of the unknown unit must be one not listed in the SHOW DISKS display (assuming the unknown drive is not connected to a defective disk data channel). A defective disk data channel illuminates the red LED on the lower front edge of the module. Refer to Chapter 2.

After a requestor number and port number are supplied to ILDISK, the program checks to ensure the specified requestor and port do not match any drive known to the HSC controller software. If the requestor and port do not match a known drive, ILDISK prompts for the number of passes to perform, as described in Section 5.6.5. If the requestor and port do match a known drive, ILDISK reports an error.

5.6.7 Progress Reports

ILDISK produces an end-of-pass report at the completion of each pass of the integrity test. One pass of the program can take several minutes, depending upon the type of drive being diagnosed.

5.6.8 Test Summaries

Test summaries for ILDISK are as follows.

- **Test 00, Parameter Fetching**—This test fetches the user-selected parameters. The user is prompted to supply a unit number and/or a requestor and port number. This part of ILDISK also prompts for the number of passes to perform.
- **Test 01, Run K.si/K.sdi Microdiagnostics**—Commands the disk data channel to execute two of its resident microdiagnostics. The revision level of the disk data channel microcode must be up to date to execute the microdiagnostics. The microdiagnostics executed are the partial SDI test (K.sdi test 7) and the SERDES/RSGEN test (K.sdi/K.si test 10).
- **Test 02, Check for Clocks and Drive Available**—Issues a command to interrogate the real-time drive state of the drive. This command does not require an SDI exchange, but the real-time status of the drive is returned to ILDISK. The real-time status should indicate the drive is supplying clocks and the drive should be in the Available state.
- **Test 03, Drive Initialize Test**—Issues a DRIVE INITIALIZE command to the drive under test. This checks both the drive and the controller real-time state line of the SDI cable. The drive should respond by momentarily stopping its clock, then restarting it.

- **Test 04, SDI Echo Test**—First ensures the disk data channel microcode supports the ECHO command. If not; a warning message is issued and the rest of Test 04 is skipped. Otherwise, the test directs the disk data channel to conduct an ECHO exchange with the drive. An ECHO exchange consists of the disk data channel sending a frame to the drive and the drive returning it. An ECHO exchange verifies the integrity of the write/command data and the read/response data lines of the SDI cable.

- **Test 05, Run Drive Integrity Tests**—Directs the drive to run its internal integrity test. The drive is commanded to run a single integrity test or its entire set of integrity tests, depending upon user response to the prompt:

```
Run a Single Drive Diagnostic ?
```

  Before commanding the drive to run its integrity tests, the drive is brought online to prevent the drive from giving spurious Available indications to its other SDI port. The drive integrity tests are started when the disk data channel sends a DIAGNOSE command to the drive. The drive does not return a response frame for the diagnose until it is finished performing integrity tests. This can require two or more minutes. While the disk data channel is waiting for the response frame, ILDISK cannot be interrupted by Ctrl/Y.

- **Test 06, Disconnect From Drive**—Sends a DISCONNECT command to the drive and then issues a GET LINE STATUS internal command to the K.sdi/K.si to ensure the drive is in the Available state. The test also expects Receiver Ready and Attention are set in drive status and Read/Write Ready is not set.

- **Test 07, Check Drive Status**—Issues a GET STATUS command to the drive to check that none of the drive's error bits are set. If any error bits are set, they are reported and the test issues a DRIVE CLEAR command to clear the error bits. If the error bits fail to clear, an error is reported.

- **Test 08, Drive Initialize**—Issues a command to interrogate the Real-Time Drive State of the drive. The test then issues a DRIVE INITIALIZE command to ensure the previous DIAGNOSE command did not leave the drive in an undefined state.

- **Test 09, Bring Drive On Line**—Issues an ONLINE command to the drive under test. Then a GET LINE STATUS command is issued to ensure the drive's real-time state is proper for the online state. Read/Write Ready is expected to be true; Available and Attention are expected to be false.

- **Test 10, Recalibrate and Seek**—Issues a RECALIBRATE command to the drive. This ensures the disk heads start from a known point on the media. Then a SEEK command is issued to the drive, and the drive's real-time status is checked to ensure the SEEK did not result in an Attention condition. Then another RECALIBRATE command is issued, returning the heads to a known position.

- **Test 11, Disconnect From Drive**—Issues a DISCONNECT command to return the drive to the Available state. Then the drive's real-time status is checked to ensure Available, Attention, and Receiver Ready are true, and Read/Write Ready is false.

- **Test 12, Bring Drive On Line**—Attempts to bring the disk drive to the online state. Test 12 is executed only for drives known to the disk functional software. Test 12 consists of the following steps:

  1. GET STATUS—ILDISK issues an SDI GET STATUS command to the disk drive.
  2. ONLINE—ILDISK directs the diagnostic interface to bring the drive online.

If the GET STATUS and the ONLINE commands succeed, ILDISK proceeds to Test 13. If the GET STATUS and the ONLINE commands fail, ILDISK goes directly to Test 17 (termination). Note the online operation is performed through the diagnostic interface, invoking the same software operations a host invokes to bring a drive online. An online operation at this level constitutes more than just sending an SDI ONLINE command. The factory control block (FCT) and replacement control block (RCT) of the drive also are read and certain software structures are modified to indicate the new state of the drive. If the drive is unable to read data from the disk media, the online operation fails. If Test 12 fails, ILDISK skips the remaining tests and goes to Test 17.

- **Test 13, Read Only I/O Operations Test**—Verifies that all read/write heads in the drive can seek and properly locate a sector on each track in the drive read-only diagnostic block number (DBN) space. DBN space is an area on all disk media devoted to diagnostic or integrity test use.

  Test 13 attempts to read at least one sector on every track in the read-only area of the drive's DBN space. The sector is checked to ensure it contains the proper data pattern. Bad sectors are allowed, but there must be at least one good sector on each track in the read-only area. After each successful DBN read, ILDISK reads one logical block number (LBN) to further enhance seek testing. This ensures the drive can successfully seek to and from the DBN area from the LBN area of the disk media. ILDISK performs Test 14 when Test 13 completes.

- **Test 14, I/O Operations Test (Read/Write 512 byte format)**—Checks to see if the drive can successfully write a pattern and read it back from at least one sector on every track in the drive read/write DBN area. Read/write DBN space is an area on every disk drive devoted to diagnostic or integrity test read/write testing.

  Bad sectors are allowed, but at least one sector on every track in the read/write area must pass the test. After Test 14 completes, ILDISK goes to Test 16.

- **Test 16, Format Test**—This test will only be executed if ILDISK did not encounter any errors during the previous tests. If previous errors were detected, ILDISK goes directly to Test 17. In Test 16, ILDISK formats blocks 0 and 1 in the drive's read/write DBN space. After formatting blocks 0 and 1, ILDISK checks that at least one of these blocks can be read without error. After Test 16 completes, ILDISK goes to Test 17.

- **Test 17, Terminate ILDISK**—The ILDISK termination routine performs the following steps:

  1. If the drive is unknown to the disk functional software, or if the SDI verification test failed, go to step 5 of this test.
  2. An SDI CHANGE MODE command is issued to the drive. The CHANGE MODE command directs the drive to disallow access to the DBN area.
  3. The drive is released from exclusive integrity test use. This returns the drive to the Available state.
  4. The drive is reacquired for exclusive integrity test use. This is to allow looping if more than one pass is selected.
  5. If more passes are left to perform, the test is reinitiated.
  6. If no more passes are left to perform, ILDISK releases the drive, returns all acquired structures, and terminates.

5.6.9 Error Message Example

All error messages issued by ILDISK conform to the generic error message format described in Section 5.1.2. The following is a typical ILDISK error message:

```
ILDISK>D>Drive Diagnostic Detected Fatal Error
ILDISK>D>FRU(s) Drive    FRU(s)
ILDISK>D>Requestor Number 04
ILDISK>D>Port Number 03
ILDISK>D>Test  0025 Error  007F
ILDISK>D>End Of Pass  00001
```

5.6.10 Error Messages

This section describes the error messages issued by ILDISK.

- **512-Byte Format Failed**—The program attempted to perform a 512-byte format to the first two sectors of the first track in the read/write DBN area. No errors were detected during the actual formatting operation, but subsequent attempts to read either of the reformatted blocks failed. The specific error detected is identified in the error report.
- **Attention Not Set in Available Drive**—The SDI verification routine executed a command to interrogate the real-time drive state line of the drive and found Attention was not asserted even though the drive is Available.
- **Attention Set After SEEK**—The SDI verification routine issued a SEEK command to the drive which resulted in an unexpected Attention condition. The drive status is displayed with the error report. Refer to the service manual for that drive.
- **Attention Set in On-Line Drive**—The SDI verification routine issued an ONLINE command to the drive. The drive entered the online state, but an unexpected Attention condition was encountered.
- **Available Not Set In Available Drive**—The SDI verification routine executed a command to interrogate the real-time drive state line of the drive. ILDISK found Available was not set in a drive that should be Available.
- **Available Set in On-Line Drive**—The SDI verification routine issued an ONLINE command to the disk drive. Then a command was issued to interrogate the real-time drive state line of the drive. The line status indicates the drive is still asserting Available.
- **Can't Acquire Drive State Area**—ILDISK cannot perform the low-level SDI tests because it cannot acquire the drive state area for the drive. The drive state area is a section of the K Control Area used to communicate with the drive through the SDI interface. To perform the SDI tests, ILDISK must take exclusive control of the drive state area; otherwise, the operational software may interfere with the tests. The drive state area must be in an inactive state (no interrupts in progress) before it can be acquired by ILDISK. If the drive is rapidly changing its SDI state and generating interrupts, ILDISK may be unable to find the drive in an inactive state.
- **Can't Acquire Specified Unit**—ILDISK was initiated automatically to test a disk drive declared inoperative. When initiated by the disk functional software, ILDISK was given the requestor number, port number, and unit number of the drive to test. ILDISK successfully acquired the drive by unit number, but the requestor and port number of the acquired drive did not match the requestor and port given when ILDISK was initiated. This indicates the HSC controller is connected to two separate drives with the same unit number plugs. To prevent inadvertent interaction with the other disk drive, ILDISK performs only the low-level SDI tests on the unit specified by the disk functional software. Read/write tests are skipped because the drive must be acquired by unit number to perform read/write transfers.

- **Can't Read Any Sector on Track**—As part of Test 13, ILDISK attempts to read a pattern from at least one sector of each track in the read-only area of the drive DBN space. (DBN space is an area on every disk drive reserved for diagnostic or integrity test use.) All drives have the same pattern written to each sector in the read only DBN space.

  During the read process, ILDISK detected a track that does not contain any sector with the expected pattern. Either ILDISK detected errors while reading, or the read succeeded but the sectors did not contain the correct pattern. The error information for the last sector accessed is supplied in the error report. The most likely cause of this error is a disk media error. If Test 14 also fails, the problem may be in the disk read/write electronics, or the DBN area of the disk may not be formatted correctly. To interpret the MSCP status code, refer to Section 5.6.11.

- **Can't Write Any Sector on Track**—As part of Test 13, ILDISK attempts to write a pattern to at least one sector of each track in the read/write area of the drive DBN space. DBN space is an area on every disk drive reserved for diagnostic use only.

  During the write process, ILDISK detected a track with no sector that passed the read/write test. That is, ILDISK could not write a pattern and read it back successfully on any sector on the track. The error information for the last sector accessed is identified in the error report. The most probable cause of this error is a disk media error.

  If Test 13 also failed, the problem could be in the disk read/write electronics, or the DBN area of the disk may not be formatted correctly. To interpret the MSCP status code, refer to Section 5.6.11.

- **Change Mode Failed**—ILDISK issued an SDI CHANGE MODE command to the drive and the command failed. The drive is presumed to be the failing unit because the SDI interface was previously verified.

- **Command Failure**—The SDI verification test detected a failure while attempting to send an SDI command to the drive. One of the following errors occurred:

  - Did Not Complete—The drive did not respond to the command within the allowable time. Further SDI operations to the drive are disabled.

  - K.sdi Detected Error—The K.sdi/K.si detected an error condition while sending the command or while receiving the response.

  - Unexpected Response—The SDI command resulted in an unexpected response from the drive. This error can be caused by a DIAGNOSE command if a single drive integrity test was selected, and the drive does not support the specified test number.

- **DCB Not Returned, K Failed for Unknown Reason**—The SDI verification test directed the disk data channel to execute one of its microdiagnostics. The microdiagnostic completed without reporting any error, but the disk data channel did not return the dialog control block (DCB). All drives connected to the disk data channel may now be unusable. The disk data channel is the probable FRU and the HSC controller probably will have to be rebooted.

- **DDUSUB Initialization Failure**—The diagnostic interface did not initialize. Error 01 is not recoverable and is caused by:

  - Insufficient memory to allocate buffers and control structures required by the diagnostic interface.

  - The disk functional software is not loaded.

- **Drive Acquired But Can't find Control Area**—The disk drive was acquired, and ILDISK obtained the requestor number and port number of the drive from the diagnostic interface. However, the specified requestor does not have a control area. This indicates a software problem and should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.

- **Drive Can't Be Brought On Line**—A failure occurred when ILDISK attempted to bring the specified drive online. One of the following conditions occurred:
  - Unit Is Offline—The specified unit went to the Off-Line state and now cannot communicate with the HSC controller.
  - Unit Is In Use—The specified unit is now marked as in use by another process.
  - Unit Is a Duplicate—Two disk drives are connected to the HSC controller, both with the same unit number.
  - Unknown Status from DDUSUB—The diagnostic interface returned an unknown status code when ILDISK attempted to bring the drive on line.
- **Drive Clear Did Not Clear Errors**—When ILDISK issued a GET STATUS command, error bits were set in the drive response. Issuing a DRIVE CLEAR failed to clear the error bits. The drive is the probable FRU.
- **Drive Diagnostic Detected Error**—The SDI verification test directed the disk drive to run an internal integrity test. The drive indicated the integrity test failed, but the error is not serious enough to warrant removing the drive from service. The test number and error number for the drive are displayed (in hex) in the error report. For the exact meaning of each error, refer to the service manual for that drive.
- **Drive Diagnostic Detected Fatal Error**—The SDI verification test directed the disk drive to run an internal integrity test. The drive indicated the integrity test failed and the error is serious enough to warrant removing the drive from service. The test and error number are displayed (in hex) in the error report. For the exact meaning of each error, refer to the service manual for that drive.
- **Drive Disabled Bit Set**—The SDI verification test issued an SDI GET STATUS command to the drive under test. The drive disabled bit was set in the status returned by the drive, indicating the drive detected a serious error and is now disabled.
- **Drive online in enhanced ESE mode.**—An ESE20 storage element, capable of running in enhanced mode, has been brought online in enhanced mode for ILDISK tests.
- **Drive online in normal mode.**—An ESE20 storage element, capable of running in enhanced mode, has been brought online in normal mode for ILDISK tests.
- **Drive online in normal mode. HSC variants not currently enabled.**—ILDISK attempted to bring an ESE20 storage element online in enhanced mode. However, the HSC controller has not been enabled to support the enhanced (variant) mode of operation. Refer to the *HSC Controller User Guide* for information on using the SETSHO command SET SERVER DISK/VARIANT_PROTOCOL to enable enhanced mode operations on the HSC controller.
- **Drive online in normal mode. Requested variant is not supported.**—ILDISK tried to bring an ESE20 storage element online in enhanced mode. However, some component of the HSC controller does not support the enhanced mode of operation. Verify that the ESE20 is attached to a K.si data channel module that is configured with disk microcode by using the SETSHO commands SHOW DISK and SHOW REQUESTORS. Refer to the *HSC Controller User Guide* for information on using these SETSHO commands.

  The ESE20 storage element cannot be run in enhanced mode on a K.sdi disk data channel module. If the ESE is attached to a properly configured K.si module, and this message is still being sent, there may be a software problem. Submit an SPR with the HSC console log and any other information pertinent to the HSC controller configuration.
- **Drive online in normal mode. Retry operation later.**—ILDISK attempted to bring an ESE20 storage element online in enhanced mode. However, the drive indicated that the enhanced mode of operation cannot currently be enabled.

The ESE20 does not allow enhanced mode operations to be enabled while it is restoring data from its data retention system (this restoration takes approximately 10 minutes on an ESE20). If, during the restoration period, the ESE20 storage element receives a request from the HSC controller to bring the drive online in enhanced mode the ESE responds by issuing this message. Retry the operation after the data restore operation is completed.

- **Drive Spindle Not Up to Speed**—ILDISK cannot continue testing the drive because the disk spindle is not up to speed. If the drive is spun down, it must be spun up before ILDISK can completely test the unit. If the drive appears to be spinning, it may be spinning too slowly or the drive may be returning incorrect status information to the HSC controller.
- **Drive Transfer Queue Not Empty Before Format**—ILDISK found a transfer already queued to the K.sdi/K.si when the format test began. ILDISK should have exclusive access to the drive at this time, and all previous transfers should have been completed before the drive was acquired. To avoid potentially damaging interaction with another disk process, ILDISK aborts testing when this condition is detected.
- **Drive Unavailable**—The selected disk drive is not available for ILDISK.
- **Drive Unknown to Disk Functional Code**—The disk drive selected is not known to the disk functional software. The drive may not be communicating with the HSC controller, or the disk functional software may have disabled the drive due to an error condition. ILDISK prompts the user for the drive's requestor and port. Refer to Section 5.6.6 for information on specifying requestor and port.
- **Drive Went Off Line**—The drive previously acquired by the integrity test is now unknown to the disk functional code. This indicates the drive spontaneously went offline or stopped sending clocks and is now unknown. Restart the test using the requestor and port numbers instead of drive unit number.
- **Duplicate Unit Detected**—At times during the testing sequence, ILDISK must release, then reacquire the drive under test. After releasing the drive and reacquiring it, ILDISK noted the requestor and port numbers of the drive it was originally testing do not match the requestor and port numbers of the drive just acquired. This indicates the HSC controller is connected to two separate drives with the same unit number. If this error is detected, ILDISK discontinues testing to prevent inadvertent interaction with the other disk drive.
- **Echo Data Error**—The SDI verification test issued an SDI ECHO command to the drive. The command completed, but the wrong response was returned by the drive. The SDI set and the disk drive are the probable FRUs.
- **Echo Framing Error**—The framing code (upper byte) of an SDI ECHO command response is incorrect. The expected and actual ECHO frames are displayed with the error message. The K.sdi/K.si module cable and the drive are the probable FRUs.
- **Error Bit Set in Drive Status Error Byte**—The SDI verification test executed an SDI GET STATUS command to the drive under test. The error byte in the returned status was nonzero, indicating one of the following conditions:
  - Drive error
  - Transmission error
  - Protocol error
  - Initialization integrity test failure
  - Write lock error

  For the exact meaning of each error, refer to the service manual for that drive.

- **Error Reading LBN**—As part of Test 13, ILDISK alternates between reading DBNs and LBNs. This tests the drive's ability to seek properly. The error indicates an LBN read failed. The drive is the probable FRU.
- **Error Releasing Drive**—ILDISK attempted to release the drive under test. The release operation failed. One of the following conditions occurred:
  - Could Not Disconnect—An SDI DISCONNECT command to the drive failed. Check the drive port lamp to see if the drive has been allocated to an alternate HSC controller.
  - Unknown Status from DDUSUB—The diagnostic interface returned an unknown status code. This indicates a software error and should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Error Starting I/O Operation**—ILDISK detected an error when initiating a disk read or write operation. One of the following conditions occurred:
  - Invalid Header Code—ILDISK did not supply a valid header code to the diagnostic interface. This indicates a software error and should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
  - Could Not Acquire Control Structures—The diagnostic interface could not acquire sufficient control structures to perform the operation. Retry ILDISK during lower HSC controller activity if this condition persists.
  - Could Not Acquire Buffer—The diagnostic interface could not acquire a buffer needed for the operation. Retry ILDISK during lower HSC controller activity if this condition persists.
  - Unknown Status from DDUSUB—The diagnostic interface returned an unknown status code. This indicates a software error and should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Error in DCB on Completion**—The SDI verification test directed the disk data channel to execute one of its microdiagnostics. The microdiagnostic completed without reporting any error, but the disk data channel returned the dialog control block (DCB) with an error indicated. The disk data channel is the probable FRU.
- **Failed To Reacquire Unit**—In order for ILDISK to allow looping, the drive under test must be released then reacquired. (This method is required to release the drive from the online state.) The release operation succeeded, but the attempt to reacquire the drive failed. One of the following conditions occurred:
  - Drive Unknown to Disk Functional Code—A fatal error caused the disk functional software to declare the drive inoperative, so the drive unit number is not recognized. You must now test the drive by specifying requestor and port number.
  - Drive Unavailable—The specified drive is not available for integrity test use. The drive may be allocated to an alternate HSC controller. Check the drive port lamp to see if this caused the error.
  - Unknown Status from DDUSUB—This indicates a software error and should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Failure While Updating Drive STATUS**—When in the process of returning the drive to the same mode as ILDISK originally found it in, an error occurred while performing an SDI GET STATUS command. In order to ensure the disk functional software is aware of this mode change, ILDISK calls the diagnostic interface routines to perform a GET STATUS on the drive. These routines also update the disk functional software information on the drive to reflect the new mode.

This error indicates that the drive status update failed. The diagnostic interface returns one of three different status codes with this error:

- DRIVE ERROR—The GET STATUS command could not be completed due to an error during the command. If informational error messages are enabled (through a SET ERROR INFO command), an error message describing the failure is displayed on the console terminal.
- BAD UNIT NUMBER—The diagnostic interface could not find the unit number specified. The drive may have spontaneously transitioned to the Off-Line state (no clocks) since the last ILDISK operation. For this reason, the unit number is unknown when the diagnostic interface tries to do a GET STATUS command.
- UNKNOWN STATUS FROM DDUSUB—*Refer* to the listing for this error.

- **Format DRAT Was Not Returned to Completion Queue**—The K.sdi/K.si module failed to complete a format operation. A format operation consists of a read followed by a format. The read completed successfully, and the fragment request block (FRB) for the format was returned by the K.sdi/K.si module with no error indicated. However, the disk rotational access table (DRAT) for the format operation was never returned, indicating a probable K.sdi/K.si module failure. After reporting this error, the format test aborts.
- **Format Operation Timed Out**—The K.sdi/K.si module failed to complete a format operation. A format operation consists of a read followed by a format. The read completed successfully, but after waiting a 16-second interval, the format was not complete. A change in drive state may prevent formatting, the drive may no longer be sending sector/index information to the K.sdi/K.si module, or the K.sdi/K.si module may be unable to sample the drive state. The format test aborts on this error to prevent damage to the existing disk format.
- **Format Tests Skipped Due to Previous Error**—To prevent possible damage to the existing disk format, ILDISK does not attempt to format if any errors were detected in the tests preceding the format tests. This error message informs the user that formatting tests will not be performed.
- **I/O Operation Lost**—While ILDISK was waiting for a disk read or write operation to complete, the diagnostic interface notified ILDISK that no I/O operation was in progress. This error may have been induced by a hardware failure, but it actually indicates a software problem, and the error should be reported by a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Init Did Not Stop State Line Clock**—The SDI verification test sent an SDI INITIALIZE command to the drive. When the drive receives this command, it should momentarily stop sending state line clock to the disk data channel. The disk data channel did not see the state line clock stop after sending the initialize. The drive is the most probable FRU.
- **Insufficient Memory, Test Not Executed**—The SDI verification test could not acquire sufficient memory for control structures. The SDI verification test could not be executed. Use the SETSHO command SHOW MEMORY to display available memory. If any disabled memory appears in the display, consider further testing of the memory module. If no disabled memory is displayed, and no other integrity test or utility is active on this HSC controller, submit an Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Insufficient Resources to Perform Test**—This error indicates further testing cannot complete due to lack of required memory structures. To perform certain drive tests, ILDISK needs to acquire timers, a dialog control block (DCB), free control blocks (FCBs), data buffers, and enough control memory to construct two disk rotational access tables (DRATs). If any of these resources are unavailable, testing cannot be completed. Under normal conditions, these resources should always be available.

- **Invalid Requestor or Port Number Specified**—The requestor number given was not in the range 2 through 9 (HSC controller) or 2 through 7 (HSC50 controller), or the port number given was not in the range 0 through 7. Specify requestor and port numbers within the allowable ranges.
- **K Microdiagnostic Did Not Complete**—The SDI verification test directed the disk data channel to execute one of its microdiagnostics. The microdiagnostic did not complete within the allowable time. All drives connected to the disk data channel may now be unusable (if the microdiagnostic never completes) and the HSC controller will probably have to be rebooted. The disk data channel module is the probable failing FRU.
- **K Microdiagnostic Reported Error**—The SDI verification test directed the disk data channel to execute one of its microdiagnostics. The microdiagnostic completed and reported an error. The disk data channel is the probable FRU.
- **K.sdi Detected Error During Format**—The K.sdi/K.si module detected an error during a format operation. Each error bit set in the fragment request block (FRB) is translated into a text message that accompanies the error report.
- **K.sdi Detected Error in Read Preceding Format**—To guarantee the disk is on the correct cylinder and track while formatting, ILDISK queues a read operation immediately preceding the FORMAT command. The read operation failed, so ILDISK aborted the format test. Each error bit set in the fragment request block (FRB) is translated into a text message which accompanies the error report.
- **K.sdi Does Not Support ECHO**—The disk data channel connected to the drive under test does not support the SDI ECHO command because the disk data channel microcode is not the latest revision level. This is not a fatal error, but the disk data channel microcode should be updated to allow for improved isolation of drive-related errors.
- **K.sdi Does Not Support Microdiagnostics**—The K.sdi/K.si module connected to the drive under test does not support microdiagnostics. This indicates the K.sdi/K.si microcode is not at the latest revision level. This is not a fatal error, but the K.sdi/K.si module should probably be updated with the latest microcode to improve error detection capabilities.
- **Not Enough Good DBNs for Format**—In order to guarantee the disk is on the proper cylinder and track, all formatting operations are immediately preceded by a read operation on the same track where the format is planned. This requires the first track in the drive's read/write DBN area to contain at least one good block that can be read without error. This error message indicates that a good block was not found on the first track of the read/write DBN area, so the formatting tests are skipped.
- **Read DRAT Not Returned to Completion Queue**—To guarantee the disk is on the correct cylinder and track while formatting, ILDISK queues a read operation immediately preceding the format command. The read operation apparently completed successfully because the fragment request block (FRB) for the read was returned with no error bits set. However, the disk rotational access table (DRAT) for the read operation was not returned indicating a problem with the K.sdi/K.si module.
- **Read Operation Timed Out**—To guarantee the disk is on the correct cylinder and track while formatting, ILDISK queues a read operation immediately preceding the FORMAT command. The read operation did not complete within 16 seconds indicating the K.sdi/K.si module is unable to sense sector/index pulses from the disk, or the disk is not in the proper state to perform a transfer. ILDISK aborts the format test following this error report.
- **Read/Write Ready Not Set in On-line Drive**—The SDI verification test executed a command to interrogate the real-time drive state line of the drive. The drive should be in the online state, but the READ/WRITE READY bit was not set in the status register.

This could be caused by a failing disk drive, bad Read/Write logic, or bad media.

- **Read/Write Ready Set in Available Drive**—The SDI verification routine executed a command to interrogate the real-time drive state line of the drive and found the AVAILABLE bit asserted. However, Read/Write Ready also was asserted. Read/Write Ready should never be asserted when a drive is in the Available state.
- **Receiver Ready Not Set**—The SDI verification routine executed a command to interrogate the Real-Time Drive State Line of the drive. The routine expected to find Receiver Ready asserted, but it was not.
- **Req/Port Number Information Unavailable**—ILDISK was unable to obtain the requestor number and port number from HSC disk software tables. The drive may have changed state and disappeared while ILDISK was running. This error also can be caused by inconsistencies in software structures.
- **Requestor Does Not Have Control Area**—ILDISK cannot find a control area for the requestor supplied by the user. One of the following conditions exists:
  - The HSC controller does not contain a disk data channel (or other type of requestor) in the specified requestor position.
  - The disk data channel (or other type of requestor) in the specified requestor position failed its initialization integrity tests and is not in use by the HSC controller.

  Open the front door and remove the cover from the card cage. Locate the module slot in the card cage that corresponds to the requestor. Refer to the module utilization label above the card cage to help locate the proper requestor.

  If a blank module (air baffle) is in the module slot, the HSC controller does not contain a requestor in the specified position. If a requestor is in the module slot, check that the red LED on the lower front edge of the module is lit. If so, the requestor failed and was disabled by the HSC controller. If the red LED is not lit, a software problem exists and should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Requestor Selected Is Not a K.sdi**—The requestor specified was not a disk data channel (K.sdi/K.si). Specify a requestor that contains a disk data channel.
- **RUN DRIVE RESIDENT DIAGNOSTICS**—This message accompanies an error message indicating some type of failure while ILDISK was communicating with a disk drive.
- **SDI Enable Variant command failed**—The HSC controller attempted to issue an SDI command to an ESE20 storage element to enable variant operations, but the SDI command failed. Verify that the ESE is available and that all SDI cable connections are secure. Check for other HSC error messages indicating why the SDI command failed.
- **Specified port contains a Known Drive**—The requestor and port specified contain a drive known to the disk functional software. The unit number of the drive is supplied in the report. ILDISK does not allow testing a known drive through requestor number and port number.
- **State Line Clock Did Not Start Up After Init**—The SDI verification test sent an SDI INITIALIZE command to the drive. When the drive receives this command, it should momentarily stop sending state clock to the disk data channel. The disk data channel saw the state clock stop, but the clock never restarted. The drive is the most probable FRU.
- **State Line Clock Not Running**—The SDI verification test executed a command to interrogate the Real-Time Drive State of the drive. The returned status indicates the drive is not sending state line clock to the disk data channel. Either the port, SDI cable, or drive is defective or the port is not connected to a drive.

- **Testing Aborted Ping-Pong Testing Detected**—ILDISK was automatically initiated to test a disk drive declared inoperative by the disk functional code. The disk drive had previously been automatically tested at least twice and somehow was returned to service. Because the tests performed by ILDISK may be causing the inoperative drive to be returned to service, ILDISK does not attempt to test an inoperative drive more than twice. On all succeeding invocations of ILDISK, this message prints and ILDISK exits without performing any tests on the drive.
- **Unexpected Item on Drive Service Queue**—The SDI verification test directed the disk data channel to execute one of its microdiagnostics. The microdiagnostic completed without error, and the disk data channel returned the dialog control block (DCB) with no errors indicated. However, the disk data channel sent the drive state area to its service queue, indicating an unexpected condition in the disk data channel or drive.
- **Unit Selected Is Not a Disk**—The response to the unit number prompt was not of the form Dnnnn. Refer to Section 5.6.5 for the correct prompt format.
- **Unknown Status from DDUSUB**—A call to the diagnostic interface resulted in the return of an unknown status code. This indicates a software error and should be reported through a Software Performance Report (SPR). See Appendix B for detailed information on SPR submission.
- **Wrong Structure on Completion Queue**—While formatting, ILDISK checks each structure returned by the K.sdi/K.si module to ensure the structure was sent to the proper completion queue. This error indicates that one of these structures was sent to the wrong completion queue. This type of error indicates a problem with the K.sdi/K.si microsequencer or a control memory failure.

5.6.11 MSCP Status Codes—ILDISK Error Reports

This section lists some of the MSCP status codes that may appear in ILDISK error reports. All status codes are listed in the octal radix. Further information on MSCP status codes is provided in Appendix C.

007—Compare Error
010—Forced Error
052—SERDES Overrun
053—SDI Command Timeout
103—Drive Inoperative
110—Header Compare or Header Sync Timeout
112—EDC Error
113—Controller Detected Transmission Error
150—Data Sync Not Found
152—Internal Consistency Error
153—Position or Unintelligible Header Error
213—Lost Read/Write Ready
253—Drive Clock Dropout
313—Lost Receiver Ready
350—Uncorrectable ECC Error
353—Drive Detected Error
410—One Symbol ECC Error
412—Data Bus Overrun
413—State or Response Line Pulse or Parity Error
450—Two Symbol ECC Error
452—Data Memory NXM or Parity Error
453—Drive Requested Error Log
510—Three Symbol ECC Error

513—Response Length or Opcode Error
550—Four Symbol ECC Error
553—Clock Did Not Restart After Init
610—Five Symbol ECC Error
613—Clock Did Not Stop After Init
650—Six Symbol ECC Error
653—Receiver Ready Collision
710—Seven Symbol ECC Error
713—Response Overflow
750—Eight Symbol ECC Error

5.7 ILTAPE—TAPE Device Integrity Tests

The following tests can be initiated through ILTAPE:

- **Tape formatter-resident integrity tests.**
- **Functional test of the tape transport.** The three types of tape transport tests are listed below. See Section 5.7.6 for a summary of each.

  Fixed canned sequence
  User sequence supplied at the terminal
  Fixed streamer sequence

- **Full test of the K.sti/K.si interface.** When a full test is selected, the K.sti/K.si microdiagnostics are executed, line state is verified, an ECHO test is performed, and a default set of formatter tests is executed. See the DRIVE UNIT NUMBER prompt in Section 5.7.3 for information on initiating a full test. Detected failures result in fault isolation to the FRU level.

Hardware required to run ILTAPE includes:

- HSC controller with K.sti/K.si
- STI-compatible tape formatter
- TA78, TA81, or other DSA tape drive (for transfer commands only)
- Console terminal
- RX33 disk drive or equivalent (HSC controller)
- TU58 tape device or equivalent (HSC50 controller)

In addition, the I/O control processor, program memory, and control memory must be working.

Software required to run ILTAPE includes:

- HSC controller executive (CHRONIC)
- DEMON
- K.sti/K.si microcode (installed with the K.sti/K.si module)

5.7.1 Operating Instructions

The following steps outline the procedure for running ILTAPE. The test assumes an HSC controller is configured with a terminal and an STI interface. If the HSC controller is not booted, start with step 1. If the HSC controller is already booted, proceed to step 2.

1. Boot the HSC.

   Press the Init button on the OCP. The following message appears:

   ```
   INIPIO-I Booting...
   ```

   The boot process takes about 2 minutes. When booting has completed, the following message is displayed:

   ```
   HSC Version xxxx Date Time  System n
   ```

2. Enter Ctrl/Y to get the HSCxx> prompt.The keyboard monitor responds with the prompt:

   ```
   HSCxx>
   ```

3. Enter RUN DXn:ILTAPE to initiate tape device integrity test program. The following message will appear:

   ```
   ILTAPE>D>hh:mm Execution Starting
   ```

5.7.2 Test Termination

ILTAPE can be terminated by entering Ctrl/C. When you terminate ILTAPE in this fashion, it runs until the current test sequence finishes. This can take several minutes. Certain errors that occur during execution will cause ILTAPE to terminate automatically.

5.7.3 User Dialog

The following paragraphs describe ILTAPE/user dialog during execution of ILTAPE. Note that the default values for input parameters appear within the brackets of the prompt. The absence of a value within the brackets indicates the input parameter does not have a default value.

ILTAPE executes two times for each pass when executing on cache-capable drives. Write Back Caching is disabled for the first pass and enabled for the second pass. When cache is enabled, ILTAPE issues all SDI Level Two caching commands in addition to the normal commands issued for the first pass. You are informed of the enabled/disabled status of cache with appropriate messages.

```
DRIVE UNIT NUMBER (U) []?
```

To run formatter tests or transport tests, enter T*nnn*, where *nnn* is the MSCP unit number (such as T316).

For a full interface test, enter X*m*, where *m* is any number. Typing X instead of T requires a requestor number and slot number. The following two prompts solicit requestor/slot numbers:

```
ENTER REQUESTOR NUMBER (2-9) []?
```

Enter the requestor number. The range includes numbers 2 through 9, with no default value.

```
ENTER PORT NUMBER (0-3) []?
```

Enter the port number. The port number must be 0, 1, 2, or 3 with no default value. After this prompt is answered, ILTAPE executes the K.sti/K.si interface test. At completion of this test, ILTAPE exits and issues an Execution Complete message. You must restart ILTAPE to run additional tests.

If you entered T*nnn* at the Drive Unit Number prompt, ILTAPE issues the following prompt:

```
EXECUTE FORMATTER DEVICE INTEGRITY TEST (Y/N) [Y]?
```

Enter Y or press Return to execute the formatter device integrity tests. Entering N will not test the formatter device.

```
MEMORY REGION NUMBER (H) [0]?
```

This prompt appears if the response to the previous prompt was a Return or Y. A formatter test is named according to the formatter memory region where it executes. Enter the memory region (in hex) in which the formatter test is to execute. ILTAPE continues at the prompt for iterations. Refer to the appropriate tape drive service manual for more information on formatter tests.

If you specify a memory region in the range 8000 through FFFF hexadecimal, you will be further prompted for diagnostic parameters as follows:

```
ENTER FORMATTER DIAGNOSTIC PARAMETERS (Y/N) [N]? Y
PARAMETER 00: 33
PARAMETER 01: 33
.
.
.
PARAMETER 14: 77
PARAMETER 15: 77
IS SCRATCH MEDIA MOUNTED (Y/N) []?
```

Enter up to 15 parameters as shown. If you enter less than 15 parameters, terminate your last entry by pressing Return. This causes the test to skip to the IS SCRATCH MEDIA MOUNTED prompt.

If you do not elect to run the formatter device integrity test, you will get the following prompt:

```
EXECUTE TEST OF TAPE TRANSPORT (Y/N) [N]?
```

To test the tape transport, enter Y. If you enter N or press Return to select the default, ILTAPE exits.

The following prompts appear when you select the tape transport test:

```
IS SCRATCH MEDIA MOUNTED (Y/N) []?
```

This test writes to the tape transport, requiring a mounted scratch tape. Enter Y if a scratch tape is already mounted.

```
Functional Test Sequence Number (0 thru 5) [1]?
```

Select one of five transport tests. The default is 1 (the canned sequence). If you select the canned sequence, the test then skips to the ENTER CANNED SEQUENCE RUN TIME IN MINUTES prompt.

Enter 0 if a new user sequence will be input from the terminal. You are then prompted for the user sequence beginning with the following prompt:

```
INPUT STEP 00:
```

See Section 5.7.4 for a description of user sequences.

You can also enter 2, 3, or 4 to select a user sequence previously input and stored on the HSC device. Enter 5 to select the streaming sequence.

```
ENTER CANNED SEQUENCE RUN TIME IN MINUTES (D) [1]?
```

Answering this prompt determines the time limit for the canned sequence. It appears only if the canned sequence is selected. Enter the total run time limit in minutes. The default is 1 minute.

Still continuing with the canned sequence, if the device under test is not a TA90 tape drive, you are next prompted for density:

```
SELECT DENSITY (0=ALL, 1=1600, 2=6250) [0]?
```

If you select a density that is not supported by the tape drive, or is not on the list of options, you will get an error message and be reprompted for density. The default selection, ALL, tests the drive at 1600 and 6250 bpi in separate passes.

The test now goes on to the speed selection prompt if the drive supports variable speeds. If the drive does not support variable speeds, the test skips to the DATA PATTERN NUMBER prompt.

If you have selected the canned sequence, and the device under test is a TA90 tape drive **without** the optional data compaction board, ILTAPE sets the speed and density prompts automatically and skips to the DATA PATTERN NUMBER prompt.

If the device under test is a TA90 tape drive with the optional data compaction board installed, ILTAPE issues the following density prompt:

```
SELECT DENSITY (0=ALL, 1=Normal, 3=Normal Compacted) [1]?
```

If you select a density that is not supported by the tape drive, or is not on the list of options, you will get an error message and be re-prompted for density. Selecting ALL tests the drive at normal and compacted densities in separate passes. Since the TA90 tape drive operates at fixed speeds, the test now goes on to the DATA PATTERN NUMBER prompt.

The next series of prompts concerns speed selection. The particular prompts depend upon the type of speeds supported (fixed or variable). ILTAPE determines the speed types supported and prompts accordingly.

NOTE
If only a single speed is supported, ILTAPE does not prompt for speed. It runs at the single speed supported.

If fixed speeds are supported, ILTAPE displays a menu of supported speeds, as follows:

```
SPEEDS AVAILABLE:
               (1) ssss ips
               (2) ssss ips
               (3) ssss ips
               (4) ssss ips
SELECT SPEED? (D) [0=AUTOMATIC]?
```

The supported speed in inches per second is shown as *ssss*. The maximum number of supported speeds is 4. Thus, *n* cannot be greater than 4.

To select a fixed speed, enter a number (*n*) corresponding to one of the displayed speeds. The default is the lowest supported speed. ILTAPE continues at the data pattern prompt.

If variable speeds are supported, ILTAPE displays the lower and upper bounds of the supported speeds as follows:

```
VARIABLE SPEEDS AVAILABLE:

     LOWER BOUND = lll ips

     UPPER BOUND = uuu ips
```

To select a variable speed, enter a number within the bounds, inclusively, of the displayed supported variable speeds. The default is the lower bound. The prompt for a variable speed is:

```
SELECT VARIABLE SPEED (D) [0 = LOWEST]?
```

The next prompt asks for the data pattern.

```
DATA PATTERN NUMBER (0,1,2,3,4) [3]?
```

Choose one of five data patterns. The data patterns are defined as follows:

0—User supplied
1—All zeros
2—All ones
3—Ripple zeros (default)
4—Ripple ones

If you enter 1, 2, 3, or 4, the test skips to the SELECT RECORD SIZE prompt. If your response is 0, the following prompt appears:

```
HOW MANY DATA ENTRIES (1-16) []?
```

Enter the number of unique words in the data pattern. Up to 16 words are permitted.

```
DATA ENTRY (H) []?
```

Enter the data pattern word (in hex), for example, ABCD (hexadecimal). This prompt repeats until the data words specified in the previous prompt are exhausted.

```
SELECT RECORD SIZE (GREATER THAN 0) (D) [8192]?
```

NOTE
The Record Size prompt does not appear if you selected the streaming sequence (choice 5 at the Functional Test Sequence Number prompt).

Enter the desired record size in decimal bytes. The default is 8192 bytes. The maximum record size that can be specified is 12288.

```
ITERATIONS (D) [1]?
```

Enter the number of times the selected tests are to run. After the number of iterations is entered, the selected tests begin execution. Errors encountered during execution cause the display of appropriate messages.

5.7.4 User Sequences

To test/exercise a tape transport, write a sequence of commands at the terminal. This sequence may be saved on the HSC controller load device and recalled for execution at a later time. Up to three user sequences can be saved.

Following is a list of supported user sequence commands:

WRT—Write one record
RDF—Read one record forward
RDFC—Read one record forward with compare
RDB—Read one record backward
RDBC—Read one record backward with compare
FSR—Forward space one record
FSF—Forward space one file
BSR—Backspace one record
BSF—Backspace one file
REW—Rewind
RWE—Rewind with erase
UNL—Unload (after rewind)
WTM—Write tape mark
ERG—Erase gap
C*nnn* —Counter set to *nnn* (0 = 1000.)
D*nnn* —Delay *nnn* ticks (0 = 1000.)

BR*nn*—Branch unconditionally to step *nn*
DB*nn*—Decrement counter and branch if nonzero to step *nn*
TM*nn*—Branch on Tape Mark to step *nn*
NT*nn*—Branch on NO Tape Mark to step *nn*
ET*nn*—Branch on EOT to step *nn*
NE*nn*—Branch on NOT EOT to step *nn*
QUIT—Terminate input of sequence steps

To initiate the user sequence dialog, enter 0 in response to the prompt:

```
Functional Test Sequence Number (0 thru 5) [1]?
```

The paragraphs that follow describe the ILTAPE user dialog during a new user sequence.

```
INPUT STEP  nn
```

Enter one of the user sequence commands listed previously. ILTAPE keeps track of the step numbers and automatically increments them. Up to 50 steps may be entered. Typing QUIT in response to the INPUT STEP prompt terminates the user sequence. At that time, the following prompt appears:

```
Store Sequence as Sequence Number (0,2,3,4) [0]?
```

The sequence entered at the terminal may be stored on the HSC controller load device in one of three files. To select one of these files, enter 2, 3, or 4. Once stored, the sequence may be recalled for execution at a later time by referring to the appropriate file (entering 2, 3, or 4 in response to the sequence number prompt).

Entering the default indicates the user sequence just entered should not be stored. In this case, the sequence cannot be run at a later time.

An example of entering a user sequence follows:

```
INPUT STEP  00  REW   ;Rewind the tape
INPUT STEP  01  C950  ;Set counter to 950
INPUT STEP  02  WRT   ;Write one record
INPUT STEP  03  ET07  ;If EOT branch to step 7
INPUT STEP  04  RDB   ;Read backward one record
INPUT STEP  05  FSR   ;Forward space one record
INPUT STEP  06  DB02  ;Decrement counter, branch
                      ;to step 2 if nonzero
INPUT STEP  07  REW   ;Rewind the tape
INPUT STEP  08  QUIT  ;Terminate sequence input
STORE SEQUENCE AS SEQUENCE NUMBER (0,2,3,4) [0]? 3
```

This sequence writes a record, reads it backwards, and skips forward over it. If an EOT is encountered prior to writing 950 records, the tape is rewound and the sequence terminates. Note, the sequence is saved on the HSC controller load device as sequence number 3 and can be recalled at a later execution of ILTAPE.

The following density prompts are issued if a user-defined sequence is selected. The differences between these density prompts and the canned sequence prompts is that the choice ALL cannot be selected. Only one pass with one density can be run for the user sequences.

If the device under test is not a TA90 tape drive, you are prompted for density as follows:

```
SELECT DENSITY (1=800, 2=1600, 3=6250) [3]?
```

If the device under test is a TA90 tape drive with the optional data compaction board installed, you are prompted for density as follows:

```
SELECT DENSITY (1=Normal, 3=Normal Compacted) [1]?
```

If you select a density that is not supported by the tape drive, or not on the list of options, ILTAPE issues an error message and you are reprompted for density.

For TA90 tape drives without the data compaction board installed, the density prompt is skipped, since there is only one density to choose from.

5.7.5 Progress Reports

When transport testing is finished, a summary of soft errors appears on the terminal upon completion of the test. The format of this summary is:

```
Soft Error Summary:

Unit  Media  Double  Double  Single  Single  Other  Other  Other
N     Error  Trkerr  Trkrev  Trkerr  Trkrev  Err A  Err B  Err C
T020  000001 00000   00000   00000   00000   000000 00002  00000
```

Successful completion of a formatter test is indicated by the following message on the terminal:

```
TEST nnnn DONE
```

where:

nnnn is the formatter test number.

When an error is encountered, an error message is printed on the terminal.

5.7.6 Test Summaries

The following sections summarize the tests run by ILTAPE.

5.7.6.1 Interface Test Summary

This portion of ILTAPE tests the STI of a specific tape data channel and port. It also performs low-level testing of the formatter by interfacing to the K.sti/K.si drive service area (port) and executing various Level 2 STI commands. The testing is limited to dialog operations; no data transfer is done. The commands issued are DIAGNOSE, READ MEMORY, GET DRIVE STATUS, and READ LINE STATUS.

K.sti/K.si microdiagnostics are executed to verify the tape data channel. A default set of formatter tests (out of memory region 0) is executed to test the formatter, and an echo test is performed to test the connection between the port and the formatter.

Failures detected are isolated to the extent possible and limited to tape data channels, the STI set, or the formatter. The STI set includes a small portion of the K.sti/K.si module and the entire STI (all connectors, cables, and a small portion of the drive). The failure possibilities of the STI set are:

- STI cables or connectors (most probable)
- Formatter
- K.sti/K.si module (least probable)

When the STI set is identified as the FRU, replacement should be in the order indicated in the preceding list.

5.7.6.2 Formatter Test Summary

Formatter tests are executed out of a formatter memory region selected by the user. Refer to the tape drive service manual for a description of the formatter tests. Failures detected identify the formatter as the FRU.

5.7.6.3 User Sequence Test Summary

User sequences are used to exercise the tape transport. The particular sequence is totally user-defined. Refer to Section 5.7.4.

5.7.6.4 Canned Sequence Test Summary

The canned sequence is a fixed routine for exercising the tape transport. The canned sequence first performs a quick verify of the ability to read and write the tape at all supported densities. Using a user-selected record size, the canned sequence then writes, reads, and compares the data written over a 200-foot length of tape. Positioning over this length of tape is also performed. Finally, random record sizes are used to write, read, compare, and position over a 50-foot length of tape. Errors encountered during the canned sequence are reported at the terminal.

5.7.6.5 Streaming Sequence Test Summary

The streaming sequence is a fixed sequence that attempts to write and read the tape at speed (without hesitation). The entire tape is written, rewound, and read back. This test may be terminated at any time by entering Ctrl/Y.

5.7.7 Error Message Example

All error messages issued by ILTAPE conform to the generic error message format described in Section 5.1.2. An example of an ILTAPE error message follows:

```
ILTAPE>D>09:31 T # 011 E # 011 U-T00101
ILTAPE>D>COMMAND FAILURE
ILTAPE>D>MSCP WRITE MULTIPLE COMMAND
ILTAPE>D>MSCP STATUS:   000000
ILTAPE>D>POSITION    001792
```

The test number reflects the state level where ILTAPE was executing when an error occurred. This number does not indicate a separate test that can be called. Table 5–1 defines the ILTAPE test levels.

Table 5–1 ILTAPE Test Levels

Test Number	ILTAPE State
0	Initialization of tape software interface
1	Device (port, formatter, unit) acquisition
2	STI interface test in execution
3	Formatter tests executing in response to Diagnostic Request (DR) bit
4	Tape transport functional test
5	User-selected formatter test executing
6	Termination and cleanup

The optional text is dependent upon the type of error.

5.7.8 Error Messages

This section describes the error messages issued by ILTAPE.

- **AVAILABLE Set in Online Drive**—After successful completion of an ONLINE command to the formatter, the AVAILABLE bit is set.
- **Chosen Density Is Not Supported**—You have selected a density that is not supported by the drive under test.
- **Command Failure**—A command failed during execution of ILTAPE. The command in error may be one of several types, such as an MSCP or Level 2 STI command. The failing command is identified in the optional text of the error message. For example:

```
ILTAPE>D>MSCP READ COMMAND
ILTAPE>D>MSCP STATUS:  nnnnnn
```

- **DCB Not Returned, K Failed for Unknown Reason**—During the STI interface test, the requestor failed for an undetermined reason and the dialog control block (DCB) was not returned to the completion queue.
- **Data Compare Error**—During execution of the user or canned sequence, ILTAPE encountered a software compare mismatch on the data written and read back from the tape. The software compare is actually carried out by a subroutine in the diagnostic interface, TDUSUB. The results of the compare are passed to ILTAPE. The text of the error message identifies the data in error.
- **EDC Error**—During execution of the user or canned sequence, ILTAPE encountered an EDC error on the data written and read back from the tape. This error is actually detected by the diagnostic interface, TDUSUB, and reported to ILTAPE. The text of the error message identifies the data in error.
- **Echo Data Error**—Data echoed across the STI interface was incorrectly returned.
- **Error in DCB on Completion**—During the STI interface test, an error condition was returned in the DCB.
- **Formatter Device Integrity Test Detected Error**—A test running in the formatter has detected an error. Any error text from the formatter is displayed.
- **Formatter Device Integrity Test Detected Fatal Error**—A test running in the formatter has detected a fatal error. Any error text from the formatter is displayed.
- **Formatter State Not Preserved Across Init**—The state of the formatter prior to a formatter initialize was not preserved across the initialization sequence.
- **Init Did Not Stop State Line Clock**—During the STI interface test, after execution of a formatter INITIALIZE command, the state line clock did not drop for the time specified in the STI specification.
- **Initialization Failure**—Tape path software interface cannot be established due to insufficient resources (buffers, queues, timers, and so forth).
- **Insufficient Resources to Acquire Specified Device**—During execution, ILTAPE was unable to acquire the specified device due to a lack of necessary resources. This condition is identified to ILTAPE by the tape functional code through the diagnostic interface, TDUSUB. ILTAPE has no knowledge of the specific unavailable resource.
- **Insufficient Resources To Acquire Timer**—ILTAPE was unable to acquire a timer from the system; insufficient buffers are available in the system to allocate timer queues.

- **Invalid Multiunit Code from GUS Command**—After a unit number is input to ILTAPE and prior to acquiring the unit, ILTAPE attempts to obtain the unit's multiunit code through the GET UNIT STATUS command. This error indicates a multiunit code of zero was returned to ILTAPE from the tape functional code. Because a multiunit code of zero is invalid, this error is equivalent to a device unknown to the tape subsystem.
- **Invalid Requestor/Port Number**—Selected requestor number or port number is out of range or requestor selected is not known to the system.
- **K Microdiagnostic Did Not Complete**—During the STI interface test, the requestor microdiagnostic timed out.
- **K Microdiagnostic Reported Error**—During the STI interface test, an error condition was reported by the K microdiagnostics.
- **K.STI DOES NOT SUPPORT MICRODIAGNOSTICS** — While doing the inter-tape verification routine, it was determined that the revision level was too low.
- **Load Device Error—File Not Found**—During the user sequence dialog, ILTAPE was unable to locate the sequence file associated with the specified user sequence number. Ensure load device media is properly installed. The program reprompts for a user sequence number. To break the loop of reprompts, enter Ctrl/Y.
- **Load Device Read Error**—While attempting to read a user sequence from the load device, a read error was encountered. Ensure a sequence has been stored on the load device as identified by the user sequence number. The program reprompts for a user sequence number. To break the loop of reprompts, enter Ctrl/Y.
- **Load Device Write Error—CHECK IF WRITE LOCKED**—An error occurred while attempting to write a user sequence to the HSC controller load device. Check to see if the load device is write protected. The prompt calls for a user sequence number. To break the loop of reprompts, enter Ctrl/Y.
- **PATTERN WORD ERROR** — During the execution of a user or canned sequence, the pattern word compared to the data on tape did not match. The software compare is actually carried out by a subroutine in the diagnostic interface, TDUSUB. The results of the compare are passed to ILTAPE. The text of the error message identifies the data in error.
- **Read Memory Byte Count Error**—The requested byte count used in the read (formatter) memory command is different from the actual byte count received.

```
EXPECTED COUNT: xxxx     ACTUAL COUNT: yyyy
```

- **Receiver Ready Not Set**—After issuing an ONLINE command to the formatter, the Receiver Ready signal was not asserted.
- **Requested Device Is Busy**—Selected device is online to another controller or host.
- **Requested Device Unknown**—Device requested is not known to the tape subsystem.
- **Requestor Not A K.sti**—Selected requestor is not known to the system as a tape data channel.
- **Selected Unit Not a Tape**—Selected drive is not known to the HSC controller as a tape.
- **State Line Clock Did Not Start Up After Init**—During the STI interface test, after execution of a formatter INITIALIZE command, the state line clock did not start up within the time specified in the STI specification.
- **State Line Clock Not Running**—During the STI interface test, execution of an internal command to interrogate the real-time formatter state line of the drive indicated the state line clock is not running

- **Tape write protected—Test Terminating**—You have mounted a scratch tape that is write protected.
- **Timeout Acquiring Drive Service Area**—While attempting to acquire the drive service area (port) in order to run the STI interface test, a timeout occurred. If this happens, the tape functional code is corrupted. ILTAPE invokes a system crash.
- **Unable to Release Device**—Upon termination of ILTAPE or upon an error condition, the device(s) could not be returned to the system.
- **Unexpected Item on Drive Service Queue**—During the STI interface test, an unexpected entry was found on the drive service queue.
- **Unit Unknown or On Line to Another Controller**—The device identified by the selected unit number is either unknown to the system or online to another controller. Verify the selected unit number is correct and run ILTAPE again.
- **UNIT WENT OFFLINE OR AVAILABLE** — During the execution of a user sequence, the drive state is checked and found to be available or offline. Check the drive and assure that it remains online for the duration of the test.
- **Unknown Status from TDUSUB**—An unknown status was returned from the tape diagnostic interface.

5.8 ILTCOM—Tape Compatibility Test

ILTCOM tests the tape compatibility of different tape drives. The tapes tested may have been written on different systems with different STI-compatible tape drives connected to an HSC controller through the STI bus.

A compatibility tape consists of file groups (called bunches) of specific data pattern records. ILTCOM may generate, modify, read, or list a compatibility tape. Data read from the compatibility tape is compared to the expected pattern.

Each bunch contains a header record and several data records of different sizes and is terminated by a tape mark. The last bunch on a tape is followed by an additional tape mark (thus forming logical EOT).

There is a total of 199 records in each bunch: one header record followed by 198 data records. The header record contains 48 (decimal) bytes of 6-bit encoded descriptive information, as follows:

Table 5–2 ILTCOM Header Record

Field	Description	Length	Example
1	Drive type	6 bytes	TA78
2	Drive serial number	6 bytes	123456
3	Processor type	6 bytes	HSC
4	Processor serial number	6 bytes	123456
5	Date	6 bytes	093083
6	Comment [1]	18 bytes	Comment

[1]ILTCOM can read, but cannot generate, a comment field.

The data records are arranged as follows:

- 66 records, 24 (decimal) bytes in length. These records sequence through 33 different data patterns. The 1st and 34th records contain pattern 1, the 2nd and 35th records contain pattern 2, and so forth, through the 33rd and 66th records containing pattern 33.

- 66 records, 528 (decimal) bytes in length. These records sequence through the 33 data patterns as described above.
- 66 records, 12,024 (decimal) bytes in length. These records sequence through the 33 data patterns in the same manner as the preceding data records.

The data patterns used by ILTCOM are shown in Table 5–3.

Table 5–3 ILTCOM Data Patterns

Pattern Number	Pattern	Description
1	377	Ones
2	000	Zeros
3	274, 377, 103, 000	Peak shift
4	000, 377, 377, 000	Peak shift
5	210, 104, 042, 021	Floating one
6	273, 167, 356, 333	Floating zero
7	126, 251	Alternate bits
8	065, 312	Square pattern
9	000, 377	Alternate frames
10	001	Track 0 on
11	002	Track 1 on
12	004	Track 2 on
13	010	Track 3 on
14	020	Track 4 on
15	040	Track 5 on
16	100	Track 6 on
17	200	Track 7 on
18	376	Track 0 off
19	375	Track 1 off
20	373	Track 2 off
21	367	Track 3 off
22	3o7	Track 4 off
23	337	Track 5 off
24	277	Track 6 off
25	177	Track 7 off
26	207, 377, 370, 377	Bit peak shift
27	170, 377, 217, 377	
28	113, 377, 264, 377	
29	035, 377, 342, 377	
30	370, 377, 207, 377	
31	217, 377, 170, 377	
32	264, 377, 113, 377	
33	342, 377, 035, 377	

5.8.1 System Requirements

The hardware requirements necessary to run ILTCOM include:

- An HSC controller with K.sti/K.si
- STI-compatible tape formatter
- Tape drive

Because ILTCOM is not diagnostic in nature, all of the necessary hardware is assumed to be working. Errors are detected and reported, but fault isolation is not a goal of ILTCOM.

ILTCOM software requirements include:

- CHRONIC
- DEMON
- K.sti/K.si microcode
- TFUNCT
- TDUSUB

5.8.2 Operating Instructions

The following steps outline the procedure for running ILTCOM. ILTCOM assumes the HSC controller is configured with a terminal, an STI interface, and a TA78 tape drive (or STI-compatible equivalent). If the HSC controller is already booted, go to step 2. If the HSC controller needs to be booted, start with step 1.

1. Boot the HSC controller.

   Press the Init button on the OCP. The following message appears:

   ```
   INIPIO-I Booting...
   ```

   The boot process can take several minutes, then the following message appears:

   ```
   HSC Version xxxx Date Time System n
   ```

2. Enter Ctrl/Y to get the HSCxx> prompt. The keyboard monitor responds with the prompt:

   ```
   HSCxx>
   ```

3. Enter RUN DXn:ILTCOM to initiate tape compatibility device integrity test program. The following message will appear:

   ```
   ILTCOM>D>hh:mm Execution Starting
   ```

5.8.3 Test Termination

ILTCOM is terminated normally by selecting the exit function (EXIT) or by entering Ctrl/Y or Ctrl/C. Certain errors that occur during execution cause ILTCOM to terminate automatically.

5.8.4 Parameter Entry

ILTCOM allows writing, reading, listing, or modifying compatibility tapes. The following describes the user dialog during the execution of ILTCOM:

```
DRIVE UNIT NUMBER (U) []?
```

Enter the tape drive MSCP unit number (such as T21). If the device under test is a TA90 tape drive, with or without the optional data compaction board installed, ILTCOM prompts the user for density as follows:

```
Density (1=Normal, 3=Normal Compacted) [1]?
```

The default density is Normal. If you select Normal Compacted density and the drive under test does not support this mode, you will get an error message.

If the device under test is not a TA90 tape drive, ILTCOM prompts for density as follows:

```
SELECT DENSITY FOR WRITES (1600,6250) (d) []?
```

There is no default, you must enter a density.

ILTCOM automatically sets speed for all types of drives, including the TA90 tape drive.

```
SELECT FUNCTION (WR=WRITE,REA=READ,ER=ERASE,LI=LIST,REW=REWIND,EX=EXIT) []?
```

Enter the function by using the characters that uniquely identify the desired function (for instance, REA for read).

The subsequent dialog is dependent upon the function selected.

- **Write**—The write function writes new bunches on the compatibility tape. Bunches are either written one at a time or over the entire tape. Bunches are written from the current tape position. If the write function is selected, the following prompt occurs:

  ```
  PROCEED WITH INITIAL WRITE (Y/N) [N]?
  ```

  Enter Y to proceed with the initial write. The default is no, in which case program control is continued at the function selection prompt. If the response is yes, the following prompt occurs:

  ```
  WRITE ENTIRE TAPE (Y/N) [N]?
  ```

  Enter Y if the entire tape is to be written. Writing of bunches begins at the current tape position and continues to physical EOT. Enter the default N if the entire tape is not to be written. In this case, only one bunch is written from the current tape position. This prompt only appears on the initial write selection. After the bunch has been written, control continues at the function selection prompt.

- **Read**—The read function reads and compares the data in the bunches with an expected (predefined) data pattern. As the reads occur, the bunch header information is displayed at the terminal. The format of the display is shown in the following example:

  ```
  BUNCH   01 WRITTEN BY TA78  SERIAL NUMBER 002965
  ON A HSC SERIAL NUMBER 005993 ON 09-18-84
  ```

  The number of bunches to be read is user selectable. All reads are from beginning of tape (BOT). If the read function is selected, the following prompt appears:

  ```
  READ HOW MANY BUNCHES (D) [0=ALL]?
  ```

  Enter the number of bunches to be read. The default (0) causes all bunches to be read. After the requested number of bunches have been read and compared, control continues at the function selection prompt.

- **List**— The list function reads and displays the header of each bunch on the compatibility tape from BOT. The display is the same as the one described under the read function. The data contents of the bunches are *not* read and compared. After listing the tape bunch headers, control continues at the function selection prompt.

- **Erase**—The erase function erases a user-specified number of bunches from the current tape position toward BOT. ILTCOM backs up the specified number of tape marks and writes a second tape mark (logical EOT). This effectively erases the specified number of bunches from the tape. Thus, for example, if the current tape position is at bunch 5 and the user wishes to erase two bunches, three bunches are left on the tape after the ERASE command completes.

  ILTCOM does not allow the user to erase all bunches. At least one bunch must remain. For example, with five bunches on the tape, only four bunches can be erased.

  If the erase function is selected, the following prompt appears at the terminal:

  ```
  ERASE HOW MANY BUNCHES FROM CURRENT POSITION (D) [0]?
  ```

Enter the number of bunches to be erased. The default of 0 results in no change in tape contents or position. Control continues at the function selection prompt.

- **Rewind**—The rewind function rewinds the tape to BOT.
- **Exit**—The exit function rewinds the tape and exits the tape compatibility program ILTCOM.

5.8.5 Test Summaries

ILTCOM writes, reads, and compares compatibility tapes upon user selection. The testing that takes place looks for compatibility of tapes written on different drives (and systems).

Incompatibilities due to data compare errors or unexpected formats are reported as they are found. ILTCOM makes no attempt to isolate any faults found during execution; it merely reports incompatibilities and other errors as they occur.

5.8.6 Error Message Example

All error messages issued by ILTCOM conform to the generic error message format described in Section 5.1.2. An example of an ILTCOM error message follows:

```
ILTCOM>D>09:29 T 000 E 003 U-T00100
ILTCOM>D>COMMAND FAILURE
ILTCOM>D>OPTIONAL TEXT
```

where:

Ennn is an error number.
U-T*xxxxx* indicates the TMSCP unit number.

The optional text is dependent upon the type of error. Some error messages contain the term *object count* in the optional text. Object count refers to tape position (in objects) from BOT.

5.8.7 Error Messages

This section describes the error messages issued by ILTAPE.

- **Can't Find End of Bunch**—The compatibility tape being read or listed has a bad format.
- **Chosen density is not supported**—You have selected a density that is not supported by the drive under test.
- **Command Failure**—A command failed during execution of ILTCOM. The command in error may be one of several types (MSCP level, STI Level 2, and so forth). The failing command is identified in the optional text of the error message. For example:

```
ILTCOM>D>tt:tt T 000 E 003 U-T00030
ILTCOM>D>COMMAND FAILURE
ILTCOM>D>MSCP READ COMMAND
ILTCOM>D>MSCP STATUS:  nnnnnn
```

- **Data Compare Error**—A data compare error has been detected. The actual and expected data are displayed in the optional text of the error message. For example:

```
ILTCOM>D>tt:tt T 000 E 011 U-T00030
ILTCOM>D>DATA COMPARE ERROR
ILTCOM>D>EXPECTED DATA: XXXXXX  ACTUAL DATA: YYYYYY
ILTCOM>D>NUMBER OF FIRST WORD IN ERROR:  nnnnn
ILTCOM>D>NUMBER OF WORDS IN ERROR:  mmmmm
ILTCOM>D>OBJECT COUNT = cccccc
```

- **Data EDC Error**—An EDC error was detected. Actual and expected values are displayed in the optional text of the error message.
- **Device is Unknown**—User selected a drive not known to the system as a tape.
- **Error Releasing Drive**—After completion of execution or after an error condition, the tape drive could not successfully be returned to the system.
- **Insufficient Resources to Acquire Drive**—ILTCOM was unable to acquire the specified device due to lack of system resources. Try again later.
- **Invalid User Selection**—The selected unit is unknown to the HSC controller.
- **Specified Unit Cannot Be Brought On Line**—The selected unit is offline, online to another controller, or not available.
- **TDUSUB Initialization Failure**—Tape path cannot be established due to insufficient resources.
- **Unknown Status from TDUSUB**—An unknown error condition returned from the software interface TDUSUB.

5.9 ILEXER—Multidrive Exerciser

ILEXER exercises the various disk drives and tape drives attached to the HSC controller. The exerciser is initiated upon demand. Drives to be tested are selected by the operator. The exerciser issues random READ, WRITE, and COMPARE commands to exercise the drives. The results of the exerciser are displayed on the terminal from which it was initiated.

ILEXER automatically enables write-back caching when executing on a cache-capable disk drive. This action is transparent to you.

The reports given by ILEXER do not provide any analysis of the errors reported, nor explicitly call out a specific FRU. This is strictly an exerciser.

ILEXER runs with other processes on the HSC controller. It is loaded from the RX33 disk drive or TU58 tape drive and uses the services of the DEMON and the control software.

5.9.1 System Requirements

For the ILEXER program to run, the following hardware and software items must be available.

Hardware requirements include:

- Console terminal
- P.ioj/c (processor) module with boot ROMs
- K.sdi, K.sti, and/or K.si data channel module
- Memory module
- RX33 disk drive (HSC controller) or TU58 tape drive (HSC50 controller)
- SDI compatible disk drive and/or STI compatible tape drive

Software requirements include:

- Control program (system diskette or tape)
- DEMON
- K.si, K.sdi, and/or K.sti microcode
- Disk and/or tape functional code

- Error handler
- Diagnostic Interface to disk and/or tape functional code

Tests cannot be performed on drives if their respective interfaces are not available (K.sdi, K.sti, or K.si).

5.9.2 Operating Instructions

Enter Ctrl/Y to get the HSCxx> prompt. The keyboard monitor responds with the prompt:

```
HSCxx>
```

Enter RUN DXn:ILEXER to initiate the multidrive exerciser. The system loads the program from the specified local load media. When the program is successfully loaded, the following message is displayed:

```
ILEXER>D>hh:mm Execution Starting
```

where:

hh:mm is the current time.

ILEXER then prompts for parameters. After all prompts are answered, the execution of the test continues. Error reports and performance summaries are returned from ILEXER.

When ILEXER has run for the specified time interval, reported any errors found, and generated a final performance summary, the exerciser concludes with the following message:

```
ILEXER>D>hh:mm Execution Complete
```

5.9.3 Test Termination

ILEXER terminates normally when it completes the exercise on each selected drive, reports any errors found, and displays the final performance summary. All resources, including the drive being tested, are released. The operator may terminate ILEXER before normal completion by entering Ctrl/Y. The following output is displayed, plus a final performance summary:

```
ILEXER>D>hh:mm DIAGNOSTIC ABORTED
ILEXER>D>PLEASE WAIT -- CLEARING OUTSTANDING I/O
```

Certain parts of ILEXER cannot be interrupted, so entering Ctrl/Y may have no effect for a brief moment and may need repetition. Whenever ILEXER is terminated, whether normally or by operator abort, ILEXER always completes any outstanding I/O requests and prints a final performance summary.

5.9.4 Parameter Entry

The parameters in ILEXER follow the format:

```
PROMPT DESCRIPTION (DATATYPE) [DEFAULT]?
```

where:

PROMPT DESCRIPTION explains the type of information ILEXER needs from the operator. The DATATYPE is the form ILEXER expects and can be one of the following:

Y/N—Yes/no response
D —Decimal number

U —Unit number (see form below)
H —Number (in hex)

DEFAULT is the value used if a Return is pressed for that particular value. If a default value is not allowed, it appears as [ ]

NOTE
Entering Ctrl/Z at any time during parameter input selects the default values for the remaining parameters.

The first prompt after starting ILEXER is:

```
DRIVE UNIT NUMBER (U) [] ?
```

Enter the unit number of the drive to be tested. This prompt has no default. Unit numbers are either in the form Dnnnn or Tnnnn, where nnnn is a decimal number between 0 and 4094 that corresponds to the number printed on the drive's unit plug. The D or T indicates either a disk drive or tape drive, respectively. Terminate the unit number by pressing Return. ILEXER attempts to acquire the specified unit through the HSC controller Diagnostic Interface. If the unit is acquired successfully, ILEXER continues with the next prompt. If the acquire fails with an error, one of the following conditions was encountered:

- The specified drive is unavailable. This indicates the drive is connected to the HSC controller but is currently online to a host CPU or an HSC controller utility. Online drives cannot be exercised. ILEXER repeats the prompt for the unit number.
- The specified drive is unknown to the disk functional software. Drives are unknown for one of the following reasons:
  - The drive and/or K.sdi/K.si port is broken and cannot communicate with the disk functional software.
  - The drive was communicating with the HSC controller when a serious error occurred and the HSC controller ceased communicating with the drive.

  In either case, ILEXER asks the operator if another drive will be selected. If so, it asks for the unit number. If not, ILEXER begins to exercise the drives selected. If no drives are selected, ILEXER terminates.

When a disk drive is specified, one set of prompts is presented. When a tape drive is selected, an entirely different set of prompts is presented.

If a nondefaultable parameter is encountered, the following message appears:

```
ILEXER>D>hh:mm Nondefaultable Parameter
```

Select up to 12 drives to be exercised: either all disk drives, all tape drives, or a combination of the two.

5.9.5 Disk Drive Prompts

The following prompts are presented if the drive selected for test is a disk drive:

```
ACCESS USER DATA AREA (Y/N) [N]?
```

If this prompt is answered with an N or Return, testing is confined to the disk area reserved for diagnostics or integrity tests (DBN area). The multidrive exerciser continues with the TERMINATE TEST ON THIS DRIVE FOLLOWING INITIAL WRITE prompt.

Answering Y to this and the next prompt directs ILEXER to perform testing in the user data area.

CAUTION
It is the operator's responsibility to see that the data contained there is either backed up or of no value.

```
ARE YOU SURE (Y/N) [N]?
```

Answering N causes the DBN area to be exercised. Answering Y allows the exercise to take place in the user data area of the disk.

```
DO YOU WANT BBR (Y/N) [Y]?
```

Answer N if you suspect the drive is bad. If you are positive the drive is good, answer Y to enable BBR.

```
START BLOCK NUMBER (D) [0]?
```

This value specifies the starting block of the area ILEXER exercises when the user data area is selected. If block 0 is specified, ILEXER begins with the first LBN on the disk.

```
END Block NUMBER (D) [0=MAX]?
```

This parameter specifies the ending block of the area ILEXER exercises when the user data area is selected. If block 0 is specified as the ending block, ILEXER exercises up to the last LBN on the disk.

```
INITIAL WRITE TEST AREA (Y/N) [N]?
```

Answering Y to this prompt causes ILEXER to write the entire test area before beginning random testing. If the prompt is answered with an N or a Return, the prompt immediately following is omitted.

```
TERMINATE TEST ON THIS DRIVE FOLLOWING INITIAL WRITE  (Y/N) [N]?
```

This question allows an initial write on the drive and terminates the test at that point. The default answer (N) permits this initial write. After completing the initial write, the test continues to exercise the drive.

NOTE
The following prompts specify the test sequence for that part of the test following the initial write portion. Even if the operator requests read-only mode, the drive will not be write protected until after any initial write has been completed.

```
SEQUENTIAL ACCESS (Y/N) [N]?
```

The operator has the option of requesting all disk data access be performed in a sequential manner.

```
READ ONLY (Y/N) [N]?
```

If answered N, the operator is asked for both a pattern number and the possibility of write-only mode. If the answer is Y, ILEXER does not prompt for write-only mode, but only asks for a data pattern number if an initial write was requested.

```
DATA PATTERN NUMBER (0-15) (D) [15]?
```

The operator has the option of selecting one of 16 disk data patterns. Selecting data pattern 0 allows the user to specify a pattern with a maximum of 16 words. The default data pattern (15) is the factory format data pattern.

```
WRITE ONLY (Y/N) [N]?
```

This option permits only write operations on a disk. This prompt is not displayed if read-only mode is selected.

```
DATA COMPARE (Y/N) [N]?
```

If this prompt is answered with an N or a Return, data read from the disk is not checked; for example, disk data is not compared to the expected pattern. If the prompt is answered with a Y, the following prompt is issued. The media must have been previously written with a data pattern in order to do a data compare.

```
DATA COMPARE ALWAYS (Y/N) [N]?
```

Answering Y causes ILEXER to check the data returned by every disk read operation. Answering with an N or a Return causes data compares on 15 percent of the disk reads.

NOTE
Selection of data compares significantly reduces the number of disk sectors transferred in a given time interval. This can degrade performance on other drives not being tested; do not do data compares unless absolutely necessary.

```
ANOTHER DRIVE (Y/N) []?
```

Answering Y permits selection of another drive for exercising. This prompt has no default. Answering N causes ILEXER to prompt:

```
MINIMUM DISK TRANSFER LENGTH IN SECTORS (1 TO 400) [10]?
MAXIMUM DISK TRANSFER LENGTH IN SECTORS (1 TO 400) [10]?
```

These prompts request the range of size in sectors of each data transfer issued to the disk drives. The default disk transfer length is 10 sectors. If data compares are selected, the maximum transfer length is 35 sectors.

Once the preceding parameters are entered, ILEXER continues with the global user prompts listed in Section 5.9.7.

5.9.6 Tape Drive Prompts

ILEXER displays the following prompts if the drive selected is a tape drive:

```
Do you wish to enable enhanced protocol (Y/N  [Y]?
```

This prompt is issued if you have selected a tape drive that supports enhanced protocol. If you answer Y or a Return, your test is run in the default enhanced protocol. Answering N runs the test in normal protocol.

```
IS A SCRATCH TAPE MOUNTED (Y/N) []?
```

Answering N results in a reprompt for the drive unit number. Answering Y displays the next prompt.

```
ARE YOU SURE (Y/N) [N]?
```

If the answer is N, the operator is reprompted for the drive unit number. If answered with a Y, the following prompt is displayed.

```
DATA PATTERN NUMBER (16-22) (D) [21]?
```

Seven data patterns are available for tape. The default pattern (pattern 21) is defined in Section 5.9.8.

If the device under test is a TA90 tape drive, with or without the optional data compaction board installed, ILEXER prompts the user for density as follows:

```
Density (1=Normal, 3=Normal Compacted) [1]?
```

The default density is Normal. If you select Normal Compacted density and the drive under test does not support this mode, you will get an error message.

ILEXER automatically sets speed for all types of drives, including the TA90 tape drive.

```
SELECT AUTOMATIC SPEED MANAGEMENT (Y/N) [N]?
```

Either Automatic Speed Management (if the feature is supported) or a tape drive speed is selected at this point. If the choice is Automatic Speed Management, the available speeds are not displayed.

```
ILEXER>D>FIXED [VARIABLE] SPEEDS AVAILABLE:
```

This is an informational message identifying the speeds available for the tape drive. If the speeds are fixed, the value is presented. If the speed is variable within a range, the range is listed, and the next prompt asks the operator to select a speed. See the tape drive user documentation for available speeds.

```
SELECT FIXED [VARIABLE] SPEED (D) [1]?
```

This prompt allows selection of variable speed for the tape drive selected. See the tape drive user documentation for available speeds.

```
RECORD LENGTH IN BYTES (1 to 12288) (D) [8192]?
```

Response to this prompt specifies the size in bytes of a tape record. Maximum size is 12 Kbytes. The default value is 8192 and the standard record-length size for 32-bit systems. Constraints on the diagnostic interface prohibit selection of the maximum allowable record length of 64 Kbytes.

```
DATA COMPARE (Y/N) [N]?
```

Answering N results in no data compares performed during a read from tape. Answering Y causes the following prompt.

```
DATA COMPARE ALWAYS (Y/N) [N]?
```

Answering Y selects data compares to be performed on every tape read operation. Answering N causes data compares to be performed on 15 percent of the tape reads.

```
ANOTHER DRIVE (Y/N) []?
```

If answered with a Y, the prompts beginning with the prompt for DRIVE UNIT NUMBER are repeated. If answered with an N, the global prompts in Section 5.9.7 are presented. This prompt has no default, allowing the operator to default all other prompts and set up another drive for this pass of ILEXER.

5.9.7 Global Prompts

The following prompts are presented to the operator when no more drives or drive-specific parameters are to be entered into the testing sequence. These prompts are global in the sense that they pertain to all the drives.

```
RUN TIME IN MINUTES (1 TO 32767) [10]?
```

The minimum run time is one minute and the default is ten minutes. After the exerciser has executed for that period of time, all testing terminates and a final performance summary is displayed.

```
]]HARD ERROR LIMIT (D) [20]?
```

The number of hard errors allowed for the drives being exercised can be specified. The limit can be set from 0 to 20. When a drive reaches this limit, it is removed from any further exercising on this pass of ILEXER. Hard errors include the following types:

- Tape drive BOT encountered unexpectedly
- Invalid MSCP response received from functional code
- UNKNOWN MSCP status code returned from functional code
- Write attempted on write-protected drive
- Tape formatter returned error
- Read compare error
- Read data EDC error
- Unrecoverable read or write error
- Drive reported error
- Tape mark error (ILEXER does not write tape marks)
- Tape drive truncated data read error
- Tape drive position lost
- Tape drive short transfer occurred on read operation
- Retry limit exceeded for a tape read, write, or read reverse operation
- Drive went OFFLINE or AVAILABLE unexpectedly

The prompt next calls for:

```
NARROW REPORT (Y/N) [N]?
```

Answering Y presents a narrow report which displays the performance summaries in 32 columns. The default display, selected by answering N or pressing the Return key, is 80 columns. The format of this display is described in further detail in Section 5.9.12. This report format is intended for small hand-held terminals.

```
ENABLE SOFT ERROR REPORTS (Y/N) [N]?
```

Answering Y enables soft error reports. By default, the operator does not see any soft error reports specific to the number of retires required on a tape I/O operation.

Answering N results in no soft error report. Soft errors are classified as those that eventually complete successfully after explicit controller-managed retry operations. They include read, write, and read reverse requested retries.

5.9.8 Data Patterns

The data patterns available for use with ILEXER are listed in the following sections. Note that pattern 0 is a user-defined data pattern. Space is available for a repeating pattern of up to 16 words.

The following are data patterns for disks:

Pattern 0	Pattern 1	Pattern 2	Pattern 3
User Defined	105613	031463	030221

Pattern 4	Pattern 5	Pattern 6	Pattern 7
Shifting 1s	Shifting 0s	Alter 1s,0s	B1011011011011001
000001	177776	000000	133331
000003	177774	000000	
000007	177770	000000	
000017	177760	177777	
000037	177740	177777	
000077	177700	177777	
000177	177600	000000	
000377	177400	000000	
000777	177000	177777	
001777	176000	177777	
003777	174000	000000	
007777	170000	177777	
017777	160000	000000	
037777	140000	177777	
077777	100000	000000	
177777	000000	177777	

Pattern 8	Pattern 9	Pattern 10	Pattern 11
B0101../B1010..	B110...	26455/151322	
052525	155554	026455	066666
052525		026455	
052525		026455	
125252		151322	
125252		151322	
125252		151322	
052525		026455	
052525		026455	
125252		151322	
125252		151322	
052525		026455	
125252		151322	
052525		026455	
125252		151322	
052525		026455	
125252		151322	

Pattern 12	Pattern 13	Pattern 14	Pattern 15
Ripple 1	Ripple 0	Manufacture --	Patterns
000001	177776	155555	155555
000002	177775	133333	133333
000004	177773	155555	066666
000010	177767	155555	155555
000020	177757	133333	133333
000040	177737	155555	066666
000100	177677	155555	155555
000200	177577	133333	133333
000400	177377	155555	066666
001000	176777	155555	155555
002000	175777	133333	133333
004000	173777	155555	066666
010000	167777	155555	155555
020000	157777	133333	133333
040000	137777	155555	066666
100000	077777	155555	155555

The following are data patterns for tapes:

Pattern 16 Alternating one and zero bits 125252 125252	Pattern 17 All ones	Pattern 18 Alternating bytes of all ones	Pattern 19 Alternating bytes of all ones and all zeros
Pattern 20 Alternating two bytes ones and two bytes zeros	Pattern 21 Alternating four bytes ones and four bytes zeros	Pattern 22 Alternating three bytes of ones and one byte zeros	Pattern 23 Alternating bytes of ones and zeros with high byte in pattern number also zero*

*Pattern 23 is used with odd record sizes.

5.9.9 Setting/Clearing Flags

The ENABLE SOFT ERROR REPORT display prompt in Section 5.9.7 allows the operator to inhibit the display of soft error reports. No other error reports can be inhibited.

5.9.10 Progress Reports

ILEXER has three basic forms of progress reports: the data transfer error report, the performance summary, and the communication error report.

- The data transfer error report is printed each time an error is encountered in one of the drives being tested.
- The performance summary is printed when the operator terminates the pass with Ctrl/Y. The performance summary is also printed on a periodic basis during the execution of ILEXER.
- The communication error report is sent to the console terminal any time ILEXER is unable to establish and maintain communications with the drive selected for exercising.

5.9.11 Data Transfer Error Report

The ILEXER data transfer error report is printed on the terminal each time a data transfer error is found during execution of ILEXER. The report describes the nature of the error and all data pertinent to the error found. The data transfer error report is a standard HSC error log message. It contains all data necessary to identify the error. The only exception to this is when the error encountered by ILEXER is a data compare error. In this case, ILEXER has performed a check and found an error during the compare, resulting in an ILEXER error report.

5.9.12 Performance Summary

The performance summary is printed on the terminal when am testing session is manually terminated, or after the specified number of minutes for the periodic performance summary. This report provides statistical data which is tabulated by ILEXER during the execution of this test.

The performance summary presents the statistics which are maintained on each drive. This summary contains:

- The drive unit number
- The drive serial number
- The number of position commands performed
- The number of kilobytes read and written

- The number of hard errors
- The number of soft errors
- The number of software correctable transfers

For tape drives being exercised by ILEXER, an additional report breaks down the software correctable errors into eight different categories.

To set the frequency of report display, enter Ctrl/G while ILEXER is executing. The following prompt is displayed:

```
Interval time for performance summary in seconds (D) [30]?
```

Answer this prompt with a time interval between 1 and 3599 seconds.

NOTE
Entering a value of 1 causes the performance summary to be immediately printed using the previous time interval.

The format of the performance summary follows:

```
                        PERFORMANCE SUMMARY (DEFAULT)

Unit R   Serial    Position   Kbyte      Kbyte    Hard  Soft  Corr.
 No  -   Number   Operations  Read      Written  Error Error Error
Dddd   HHHHHHHHHH dddddddddd ddddddddd ddddddddd ddddd ddddd ddddd
Tddd   HHHHHHHHHH dddddddddd ddddddddd ddddddddd ddddd ddddd ddddd
```

A performance summary is displayed for each disk drive and tape drive active on the HSC controller. The following list explains the performance summary:

- **Unit Number**—The unit number of the drive. D is for disk and T is for tape. The number is reported in decimal.
- **R**—The status of the drive. If an asterisk (*) appears in this field, the drive was removed from the test and the operator was previously informed. If the field is blank, the drive is being exercised.
- **Serial Number**—The serial number (in hex) for each drive.
- **Position**—The number of seeks.
- **Kbyte Read**—The number of Kbytes read by ILEXER on each drive.
- **Kbyte Written**—The number of Kbytes written by ILEXER.
- **Hard Error**—The number of hard errors reported by ILEXER for a particular drive.
- **Soft Error**—The number of soft tape errors reported by the exerciser if enabled by the operator.
- **Correctable Errors**—The number of correctable ECC errors encountered by ILEXER. Only ECC errors above the specific drive ECC error threshold are reported through normal functional code error reporting mechanisms. ECC errors below this threshold are not reported through an error log report, but are included in this count maintained by ILEXER.

If any tape drives are exercised, the following summary is displayed within each performance summary:

```
UNIT  MEDIA  DOUBLE  DOUBLE  SINGLE  SINGLE  OTHER  OTHER  OTHER
NO    ERROR  TRKERR  TRKREV  TRKERR  TRKREV  ERR A  ERR B  ERR C

Tddd  ddddd  ddddd   ddddd   ddddd   ddddd   ddddd  ddddd  ddddd
```

An explanation of the summary columns follows:

- **Unit No**—The unit number of the tape drive being exercised.

- **Media Error**—The number of bad spots detected on the recording media.
- **Double TRKERR**—The number of double-track errors encountered during a read or write forward.
- **Double TRKREV**—The number of double-track errors encountered during a read reverse or write reverse.
- **Single TRKERR**—The number of single-track errors detected during a read or write in the forward direction.
- **Single TRKREV**—The number of single-track errors encountered during a read reverse or write reverse.
- **Other Err A-C**—Reserved for future use.

```
                    PERFORMANCE SUMMARY (NARROW)

ILEXER>D>PER SUM
D[T]ddd
SN HHHHHHHHHHHH
P ddddd
R ddddddddddd
W ddddddddddd
HE ddddd
SE ddddd
SC ddddd
```

This report is repeated for each drive tested.

If tape drives are being tested, the following report is issued for each tape drive following the disk drive performance summaries:

```
ILEXER>D>ERR SUM
ILEXER>D>Tddd
ILEXER>D>ME ddddd
ILEXER>D>DF ddddd
ILEXER>D>DR ddddd
ILEXER>D>SF ddddd
ILEXER>D>SR ddddd
ILEXER>D>OA ddddd
ILEXER>D>OB ddddd
ILEXER>D>OC ddddd
```

5.9.13 Communications Error Report

Whenever ILEXER encounters an error that prevents it from communicating with one of the drives to be exercised, ILEXER issues a standard error report. This report gives details enabling the operator to identify the problem. For further isolation of the problem, the operator should run another test specifically designed to isolate the failure (ILDISK or ILTAPE).

5.9.14 Test Summaries

The test numbers in ILEXER correspond to the module being executed within ILEXER itself. The main module is called MDE, and it calls all other modules.

- **Test number 1, Main Program: MDE**— The multidrive exerciser (MDE) is the main program within ILEXER. It is responsible for calling all other portions of ILEXER. It obtains the buffers and control structures for the exerciser. It verifies that disk or tape functionalities are available before allowing ILEXER to continue.

- **Test number 2, INITT**—INITT is called to initialize drive statistic tables. It obtains the parameters and verifies the values of each one entered. This routine calls INICOD to obtain drive-specific parameters.
- **Test number 3, INICOD**—INICOD is the initialization code for ILEXER. It gets the various parameters for the drives from the operator and fills in the drive statistic tables with initial data for each drive. It also verifies the validity of the input for the parameters. INICOD, in turn, calls ACQUIRE to acquire the disk and/or tape drive.
- **Test number 4, ACQUIRE**—ACQUIRE is responsible for acquiring the drives as specified by the operator. It brings all selected drives online to the controller and spins up the disk drives. Errors reported in this routine cause the removal of the drive from the exercise.
- **Test number 5, INITD**—INITD initializes the disk drives for the exercise. This routine clears all disk access control blocks and invokes the initial write.
- **Test number 6, TPINIT**—TPINIT initializes the tape drives for the exercise. It rewinds all acquired tape drives and verifies the drives are at the BOT. If an error occurs, the drive is removed from the exerciser. TPINIT is also responsible for obtaining buffers for each acquired tape drive.
- **Test number 7, Exerciser**—EXER is the main code of the exerciser. It dispatches to the disk exerciser (QDISK and CDISK) and the tape exerciser (TEXER). It continuously queues I/O commands to disk and tape, and checks for I/O completion. The subroutines EXER calls are responsible for sending commands and checking for I/O completion.

- **Test number 8, QDISK**—QDISK is part of the disk exerciser that selects commands to send to the disk drives. If the initial write is still in progress, it returns to EXER. QDISK calls a routine to select the command to exercise the disk drive. The following scenario is the algorithm used to select the command:
  - If the drive is read only and data compare is not requested, a read operation is queued to the drive.
  - If read only and data compare (occasional) are requested, a read operation is queued along with a random choice of compare/no-compare.
  - If read only and data compare (always) are requested by the operator, a READ-COMPARE command is queued to the drive.
  - If write only is requested, and data compare is not, then a write request is queued to the disk drive.
  - If write only and data compare (occasional) are requested, a write operation is queued along with a random choice of compare/no-compare.
  - If write only and data compare (always) are requested, a WRITE-COMPARE command is queued to the drive.
  - If only data compare (occasional) is requested, then a random selection of read/write and compare/no-compare is done.
  - If only data compare (always) is requested, a COMPARE command is paired with a random selection of read/write.

  QDISK randomly selects the number of blocks for the selected operation.
- **Test number 9, RANSEL**—RANSEL is the part of the tape exerciser that is responsible for sending commands to the tape drives. This routine is called by TEXER, the tape exerciser routine. RANSEL selects a command for a tape drive using a random number generator. Following are some constraints for the selection process:
  - No reads when no records exist before or after the current position.
  - No writes when records exist after the current position.
  - No position of record when no records exist before or after the current position.
  - Reverse commands are permitted on the drive when 16 reverse commands previously have been selected. That is, 1 out of every 16 reverse commands are sent to the drive. Immediately following a reverse command, a position to the end-of-written-tape is performed. The reason for forward biasing the tape is to prevent thrashing.

  The following commands are executed in exercising the tape drives:
  - READ FORWARD
  - WRITE FORWARD
  - POSITION FORWARD
  - READ REVERSE
  - REWIND
  - POSITION REVERSE

  RANSEL randomly selects the number of records to read, write, or skip.

- **Test number 10, CDISK**—CDISK checks for the completion of disk I/O specified by QDISK. CDISK checks the return status of a completed I/O operation and if any errors occur, they are reported.
- **Test number 11, TEXER**—TEXER is the main tape exerciser which selects random writes, reads, and position commands. TEXER processes the I/O once it is completed and reports any errors encountered.
- **Test number 12, EXCEPT**—EXCEPT is the ILEXER exception routine. This is the last routine called by MDE. EXCEPT is called when a fatal error occurs, when ILEXER is stopped with Ctrl/Y, or when the program expires its allotted time. It cleans up any outstanding I/O, as necessary, returns resources, and returns control to DEMON.

5.9.15 Error Message Format

ILEXER outputs four types of error formats:

- Prompt errors
- Data compare errors
- Pattern word errors
- Communication errors

The format of these errors conform to the generic error message format described in Section 5.1.2.

5.9.15.1 Prompt Error Format

Prompt errors occur when the operator enters the wrong type of data or the data is not within the specified range for a parameter. The format is:

```
ILEXER>D>error message
```

The error message is an ASCII string describing the error.

5.9.15.2 Data Compare Error Format

A data compare error occurs when an error is detected during the exercise of a particular drive. The two formats for the data compare error are data word compare error and pattern word error. A data word compare error occurs when the data read does not match the expected pattern. The error message format is:

```
ILEXER>D>hh:mm T#ddd E#dddd U-dddd
ILEXER>D>Error Description
ILEXER>D>MA -- HHHHHHHHHH
ILEXER>D>EXP -- HHHH
ILEXER>D>ACT -- HHHH
ILEXER>D>MSCP STATUS CODE = HHHH
ILEXER>D>FIRST WORD IN ERROR = ddddd
ILEXER>D>NUMBER OF WORDS IN ERROR = ddddd
```

where:

hh:mm is the current system time.
T is the test number in the exerciser.
E corresponds to the error number.
U is the unit number for which the error is being reported.
MA is the media address (block number) where the error occurred.
EXP is the expected data.
ACT is the data (or code) actually received.
MSCP STATUS CODE is the code received from the operation.
FIRST WORD IN ERROR describes the number of the first word found in error.

NUMBER OF WORDS IN ERROR—Once an error is found, the routine continues to check the remainder of the data returned and counts the number of words found in error.

5.9.15.3 Pattern Word Error Format

The format for the pattern word error is slightly different from the data word compare error. A pattern word error occurs when the first data word in a block is not a valid pattern number. The error message format is:

```
ILEXER>D>hh:mm T#ddd E#ddd U-dddd
ILEXER>D>Error Description
ILEXER>D>MA -- HHHHHHHHHH
ILEXER>D>EXP -- HHHH
ILEXER>D>ACT -- HHHH
```

The MSCP status code, first word in error, and number of words in error are not relevant for this type of error. The other fields are as described for the data compare error.

5.9.15.4 Communications Error Format

Communications errors occur when ILEXER cannot establish/maintain communications with a selected drive. The error message appears in the following format:

```
ILEXER>D>hh:mm T#ddd E#ddd U-uddd
ILEXER>D>Error Description
ILEXER>D>Optional Data lines follow here
```

where:

hh:mm is the time stamp.
T is the test number in the exerciser.
E corresponds to the error number.
U is the unit number for which the error is being reported.
Error Description is an ASCII string describing the error encountered.
Optional Data lines—A maximum of eight optional lines per report.

5.9.16 Error Messages

This section lists the informational and error messages and explains the cause of each error. A typical error message is:

```
ILEXER>D>09:32 T#006 E#204 U-T00100
ILEXER>D>Comm Error: TBUSUB call failed
```

Use the E#xxx code to interpret the type of ILEXER error. ILEXER generic errors have error numbers of 99 or less. ILEXER disk errors have error numbers between 100 and 199. ILEXER tape errors have error numbers between 200 and 299.

5.9.16.1 Informational Messages

Informational messages are not fatal to the exerciser and are intended only to:

- Alert the user to incorrect input to parameters
- Indicate missing interfaces
- Provide user information

The informational messages listed by ILEXER are as follows:

- **Disk Interface Not Available**—Indicates the disk functionality is not available to exercise disk drives. This means that the HSC controller's disk functional code is not loaded.

- **Drive online in enhanced ESE mode**—An ESE20 storage element, capable of running in enhanced mode, has been brought online in enhanced mode for ILEXER tests, as requested by the user.
- **Drive online in normal mode**—An ESE20 storage element, capable of running in enhanced mode, has been brought online in normal mode for ILEXER tests, as requested by the user.
- **Drive online in normal mode. HSC variants not currently enabled**—The user requested that an ESE20 storage element be brought online in enhanced mode. However, the HSC controller has not been enabled to support the enhanced (variant) mode of operation. Refer to the *HSC Controller User Guide* for information on using the SETSHO command SET SERVER DISK/VARIANT_PROTOCOL to enable enhanced mode operations on the HSC controller.
- **Drive online in normal mode. Requested variant is not supported.**—ILEXER tried to bring an ESE20 storage element online in enhanced mode on request from the user. However, some component of the HSC controller does not support the enhanced mode of operation. Verify that the ESE20 is attached to a K.si data channel module that is configured with disk microcode by using the SETSHO commands SHOW DISK and SHOW REQUESTOR. Refer to the *HSC Controller User Guide* for information on using these SETSHO commands.

  The ESE20 storage element cannot be run in enhanced mode on a K.sdi disk data channel module. If the ESE20 is attached to a properly configured K.si module, and this message is still being sent, there may be a software problem. Submit an SPR with the HSC console log and any other information pertinent to the HSC controller configuration.
- **Drive online in normal mode. Retry operation later.**—ILEXER attempted to bring an ESE20 storage element online in enhanced mode on request of the user. However, the drive indicated that the enhanced mode of operation cannot be enabled. The ESE20 does not allow enhanced mode operations to be enabled while it is restoring data from its data retention system (this restoration takes approximately 10 minutes on an ESE20). If, during the restoration period, the ESE20 receives a request from the HSC controller to bring the drive online in enhanced mode the ESE20 responds by issuing this message. Retry the operation after the restore operation is completed.
- **Number Must Be Between 0 and 15**—Reported when the user enters an erroneous value for the data pattern on a disk.
- **Pattern Number Must Be Within Specified Bounds**—Reported when the operator tries to specify a disk pattern number for a tape.
- **Please Mount a Scratch Tape**—Appears after an N response to the prompt asking if the scratch tape is mounted on the tape drive to be tested.
- **Please Wait—Clearing Outstanding I/O**—Displayed when the operator enters Ctrl/Y to stop ILEXER. All outstanding I/O commands are aborted at this time.
- **SDI Enable Variant command failed**—The HSC controller attempted to issue an SDI command to an ESE20 storage element to enable variant operations, but the SDI command failed. Verify that the ESE20 is available and that all SDI cable connections are secure. Check for other HSC error messages indicating why the SDI command failed.
- **Starting LBN is Either Larger Than Ending LBN or Larger Than Total LBN on Disk**—Reprompts for the correct values. The operator selected a starting block number for the test that is greater than the ending block number selected, or it is greater than the largest block number for the disk.
- **Tape Interface Not Available**—Indicates the tape functionality is not available to exercise tape drives. This means that the HSC controller's tape functional code is not loaded.

- **You May Enter at Most 16 Words in a Data Pattern**—Reported if the operator specifies more than 16 words for a user-defined pattern. The operator is then reprompted for the value.

5.9.16.2 Generic Errors

The following list indicates the error text and cause of errors displayed by ILEXER. ILEXER generic errors have numbers of 99 or less.

- **Could Not Get Buffers for Transfers**—The buffers required for a tape transfer could not be acquired.
- **Could Not Get Control Block for Timer—Stopping ILEXER**—ILEXER could not obtain a transmission queue for a timer. This should occur only on a heavily loaded system and is fatal to ILEXER.
- **Could Not Get Timer—Stopping ILEXER**—The exerciser could not obtain a timer. Two timers are required for ILEXER. This should only occur on a loaded system and is fatal to ILEXER.
- **Could Not Return Drive to Available State**—The release of the drive from ILEXER was unsuccessful. This is the result of a drive being taken from the test due to reaching an error threshold or going off line during the exercise.
- **Couldn't Get Drive Status—Choose Another Drive**—ILEXER was unable to obtain the status of a drive for one of the following reasons:
  - The drive is not communicating with the HSC controller. Either the formatter or the disk is not on line.
  - The cables to the K.sdi, K.sti, or K.si modules are loose.
- **Disk Functionality Unavailable—Choose Another Drive**—The disk interface is not available. A previous message is printed at the start of ILEXER if any of the interfaces are missing. This error prints when the operator still chooses a disk drive for the exercise.
- **Drive Cannot Be Brought On Line**—ILEXER was unable to bring the selected drive on line. One of the following conditions occurred:
  - The unit went into an Offline state and cannot communicate with the HSC controller.
  - The unit specified is now being used by another process.
  - There are two drives of the same type with duplicate unit numbers on the HSC controller.
  - An unknown status was returned from the diagnostic interface when ILEXER attempted to bring the drive online.
- **Drive Is Unavailable—Choose Another Drive**—This could result from any of the following conditions:
  - The drive port button is disabled for that port.
  - The drive is online to another controller.
  - The drive is not able to communicate with the controller on the port selected.
- **Drive Is Unknown—Choose Another Drive**—The drive chosen for the exerciser is not known to the functional software for that particular drive type. Either the drive is not communicating with the HSC controller, or the drive has been disabled due to an error condition.
- **Invalid Time Entered...Must Be from 1 to 3599**—The user entered an erroneous value to the performance summary time interval prompt.

- **No Disk or Tape Functionality...Exerciser Terminated**—Neither disk nor tape functional software is available to run the exercise. This error condition terminates ILEXER.
- **No Tape Mounted on Unit...Mount and Continue**—The operator specified a scratch tape was mounted on the tape drive selected when it was not mounted. Mount a tape and continue.
- **Record Length Larger than 12K or 0**—The record length requested for the transfer to tape was either greater than 12K or was 0.
- **Tape Functionality Unavailable—Choose Another Drive**—The tape interface is not available. A previous message is printed at the start of ILEXER if any of the interfaces are missing. This error prints when the operator still chooses a tape drive for the exercise.
- **Tape Rewind Commands Were Lost—Cannot Continue**—The drive was unloaded during ILEXER execution.
- **This Unit Already Acquired**—A unit number was specified for testing, but the associated drive has already been acquired.
- **User Requested Write on Write-Protected Unit**—The operator should check the parameters entered and the write protection on the drive to make sure they are consistent.

5.9.16.3 Disk Errors

The following list includes the error text and cause of ILEXER disk errors. ILEXER disk errors have error numbers between 100 and 199.

- **Command Failed—Invalid Header Code**—ILEXER did not pass a valid header code to the diagnostic interface for the HSC controller.
- **Command Failed—No Buffer Available**—The diagnostic interface was unable to obtain buffers to run the exercise. The HSC controller could be overloaded. Try ILEXER when the HSC controller has less I/O activity. If the error still occurs, test the HSC controller memory.
- **Command Failed—No Control Structures Available**—The diagnostic interface could not obtain disk access control blocks to run the exercise. The HSC controller could be overloaded. Try ILEXER when the HSC controller has less I/O activity. If the error still occurs, test the HSC controller memory.
- **Couldn't Put Drive in DBN Space—Removed from Test**—An error or communication problem occurred during the delivery of an SDI command to put the drive in DBN space.
- **Data Compare Error**—Bad data was detected during a read operation.
- **Disk Unit Numbers Must Be Between 0 and 4094 decimal**—The operator specified a disk unit number outside the allowed range of values.
- **Drive No Longer Exercised**—A disk drive reached the hard error limit or the drive went off line to the HSC controller during the exercise.
- **Drive No Longer On Line**—A drive that was being exercised went into an Available state. This could be caused by the operator releasing the port button on the drive. A fatal drive error could also cause the drive to go into this state.

  This error messages identifies the function attempted by ILEXER that caused an error to occur. Error logs do not indicate the operation attempted.
- **Drive Spindle Not Up to Speed—Spin Up Drive and Restart**—The disk drive is not spun up.

- **EDC Error**—Error detection code error: invalid data was detected during a read operation.

NOTE
The following hard failure error messages identify the function attempted by ILEXER that caused an error to occur. Error logs do not indicate the operation attempted.

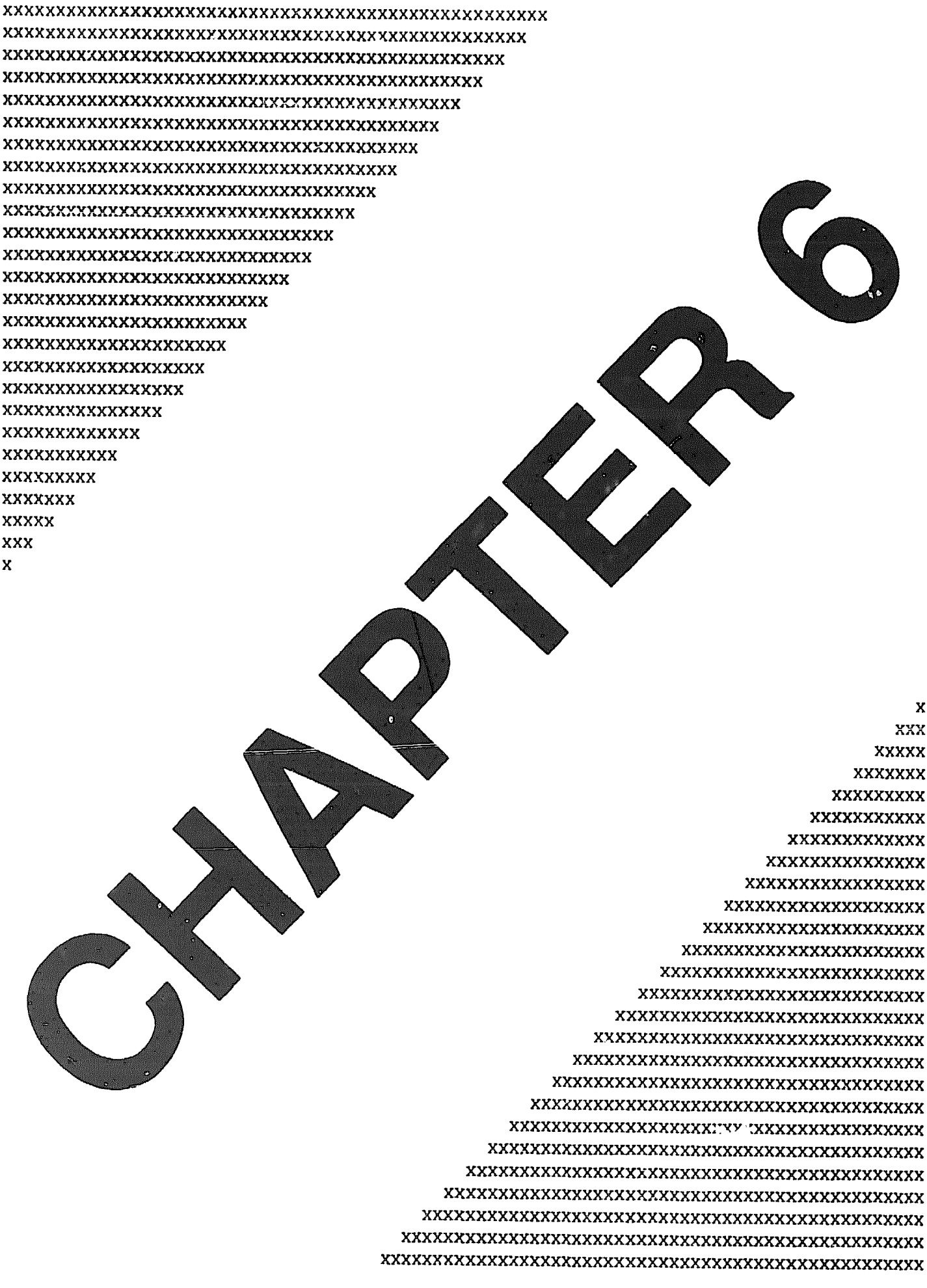
- **Hard Failure on Compare Operation**—A hard failure occurred during a compare of data on the disk drive.
- **Hard Failure on Disk**—A hard error occurred on the disk drive being exercised.
- **Hard Failure on Initial Write Operation**—A hard failure occurred during an initial write to the disk drive.
- **Hard Failure on Read Operation**—A hard failure occurred during a read operation on the disk drive being exercised.
- **Hard Failure on Write Operation**—A hard fault occurred during a write operation on the specified disk drive.
- **No DACB Available—Notify Customer Services, Submit SPR**—This is reported if no DACBs can be acquired. If this happens, contact Customer Services as soon as possible and submit an SPR.
- **Pattern Number Error**—The first two bytes of each sector, which contain the pattern number, did not contain a valid pattern number.
- **Some Disk I/O Failed to Complete**—An I/O transfer did not complete during an allotted time period.
- **Unknown Unit Number Not Allowed in ILEXER**—The operator attempted to enter a unit number of the form X*nnnn*, which is not accepted by ILEXER.
- **Write Requested on Write-Protected Drive**—The operator requested an initial write operation on a drive that was already write protected. The operator should write enable the drive reporting the error or have ILEXER do a read-only operation on the drive.

5.9.16.4 Tape Errors

The following list includes the error text and cause of ILEXER tape errors. ILEXER tape errors have error numbers between 200 and 299.

- **Comm Error: TDUSUB Call Failed**—ILEXER cannot communicate with the drive through interface structures. They have been removed. Either the drive went from online to available, the drive is offline, or there is a fault.
- **Controller Error..Hard Error..Rewinding to Restart**—A communications problem exists between the controller and the formatter.
- **Could Not Set Unit Char...Removing from Test**—The drive is offline and not communicating.
- **Couldn't Get Formatter Characteristics**—A communication problem with the drive is indicated. It could be caused by the unit not being online.
- **Couldn't Get Unit Characteristics**—The drive is not communicating with ILEXER. The unit could be offline.
- **Data Pattern Word Error Defect**—The first two bytes of a record containing the data pattern did not contain a valid pattern number.
- **Data Read EDC Error**—Error detection code error; incorrect data was detected.

- **Drive Error...Hard Error**—The drive unexpectedly transitioned from the online to the available state while being exercised.
- **Drive Went Available...Removing from Test**—During the exercise the drive unexpectedly transitioned from the online to the available state.
- **Drive Went Offline...Removing from Test**—The drive went offline during the exercise. This is caused by the operator taking the drive offline or a hard failure forcing the drive offline.
- **Formatter Error...Hard Error**—A communications problem exists between the formatter and the controller and/or drive.
- **Hard Error Limit Exceeded...Removing Drive from Test**—The drive exceeded the threshold of hard errors determined by a global user parameter (Section 5.9.7). The drive is then removed from the exercise.
- **Read Data Error**—A read operation failed during a data transfer, and no data was transferred.
- **Retry Required on Tape Drive**—A failed read/write operation required a retry before succeeding.
- **Short Transfer Error...Rewinding to Restart**—Less data was received than transferred.
- **Some Tape I/O Failed to Complete**—The drive or formatter stopped functioning properly during a data transfer.
- **Tape Mark Error...Rewinding to Restart**—ILEXER does not write tape marks. This error indicates a drive failure.
- **Tape Position Discrepancy**—The tape position was lost, indicating a hard failure.
- **Tape Position Lost...Rewinding to Restart**—An error occurred during a data transfer or a retry of one.
- **Truncated Record Data Error...Rewinding to Restart**—More data was received than expected, indicating a drive problem.
- **Unexpected BOT Encountered...Will Try to Restart**—The drive is experiencing a positioning problem.
- **Unexpected Error Condition...Removing Drive from Test**—This is caused by TMSCP error conditions, which are not allowed (invalid commands, unused codes, write-protected drive write, and so forth).
- **Unrecoverable Read Error...Rewinding to Restart**—A hard error occurred during a read operation and a data transfer did not take place.
- **Unrecoverable Write Error...Rewinding to Restart**—A hard error occurred during a write operation. The write did not take place.


CHAPTER 6

6
Offline Diagnostics

6.1 Introduction

This chapter describes the offline diagnostics, how to run them, errors that can occur, and summaries of the tests in each diagnostic. Included in the offline diagnostics are:

- ODL—Offline diagnostics loader
- OFLCXT—Offline P.ioj cache test (HSC controller only)
- OBIT—Offline bus interaction test
- OKTS—Offline K test selector
- OKPM—Offline K/P memory test
- OMEM—Offline memory test
- OMCA—Offline memory cache test (HSC controller only)
- OFLRXE—Offline RX33 exerciser (HSC controller only)
- ORFT—Offline refresh test
- OOCP—Offline operator control panel (OCP) test
- WCS LOADER—Offline control store loader

The offline diagnostics contain specific common characteristics, which are discussed in the following three sections. These characteristics are listed below:

- Identical software requirements
- Common load procedure
- Identical bootstrap initialization procedures
- Generic error message format

6.1.1 Software Requirements

All offline diagnostics require boot media containing a bootable image of the diagnostics software programs. For an HSC controller, an RX33 offline diagnostic diskette is required. For an HSC50 controller, a TU58 offline diagnostic tape cassette is required.

6.1.2 Offline Diagnostics Load Procedure

For the HSC controller, the offline diagnostics diskette boots from either RX33 drive and should not be write enabled. This diskette contains the necessary software to run all the HSC offline diagnostics. Booting is done either by powering on or by pressing and releasing the Init switch with the Secure/Enable switch in the ENABLE position. This causes the P.ioj ROM bootstrap tests to run followed by the offline P.ioj test.

The offline diagnostics TU58 cassette boots from either TU58 drive and should not be write enabled. This TU58 cassette contains the necessary software to run all the HSC50 offline diagnostics. Booting is accomplished either by powering on or by pressing and releasing the Init switch with the Secure/Enable switch in the ENABLE position. This causes the P.ioc ROM bootstrap tests to run followed by the offline P.ioc test.

NOTE
For offline diagnostics, the HSC controller must be booted with the Secure/Enable switch in the ENABLE position. If a hardware error occurs during boot, the software executes a halt instruction on certain errors. A halt instruction, even in Kernel mode, is valid only if the Secure/Enable switch is in the ENABLE position. Otherwise, the result can be an illegal instruction trap in addition to the error causing the halt.

For the bootstrap to complete successfully, the following must be operational:

- Basic instruction set of the PDP–11
- First 2048 bytes of program memory plus 8 Kwords of contiguous program memory below address 160000
- RX33 controller and at least one RX33 disk drive containing a diskette with a bootable image for the HSC controller
- TU58 tape drive controller and at least one TU58 tape drive containing a cassette with a bootable image for the HSC50 controller

Before control is turned over to the HSC controller bootstrap ROMs, internal microcode tests execute in the J11 (HSC) or F11 (HSC50) chip sets. Refer to Table 2–4 for definitions of the J11/F11 module (P.ioj/c) LEDs.

6.2 ROM Bootstrap

The P.ioj/c ROM bootstrap verifies the basic integrity of the P.ioj/c module, part of the program memory, and the boot device. The goal of the bootstrap tests is to test enough of the HSC controller to allow further test loading from the boot device.

The bootstrap test is the first step in the HSC controller initialization process. This test is run for every bootstrap or reload of the HSC operating system (CRONIC). The bootstrap is initiated automatically each time the HSC controller is powered on and is initiated by CRONIC when a software reboot is required.

The bootstrap is a PDP–11 program written to execute in a DCJ11/DCF11 CPU in a standalone environment. This means no other software processes coexist with the bootstrap.

Bootstrap failures are reported through the fault indicator mechanism on the OCP, which specifies the module most likely causing the problem. See Chapter 8 for the fault code definitions. An error table is maintained in program memory for addresses 00000400 through 00000412. These addresses contain the reasons for each load device boot failure.

6.2.1 Initialization Instructions

The following procedure lists the operating instructions for the P.ioj/c ROM bootstrap. Refer to Section 6.2.4 if this procedure fails.

1. HSC controller—Insert the offline diagnostics diskette with a bootable image into either RX33 disk drive.
2. HSC50 controller—Insert the offline diagnostics tape with a bootable image into either TU58 drive.
3. Turn power ON.
4. Set the Secure/Enable switch to the ENABLE position, then press the Init switch. The bootstrap initiates automatically.

At this point, the P.ioj/c module executes internal microdiagnostics and then begins to execute from the boot ROM. The Init indicator lights on the HSC operator control panel (OCP) when the bootstrap PDP–11 tests are done. The load device drive-in-use LED lights within 8 to 10 seconds, indicating the bootstrap is attempting to load software into program memory. If the load is successful, the bootstrap transfers control to the first instruction of the image just loaded from the diskette.

6.2.2 Failures

Most bootstrap failures result in lighting the fault indicator on the HSC OCP. When this happens, press the Fault switch momentarily and read the failure code displayed in the OCP indicators. Section 6.2.5 indicates the HSC controller modules most likely causing the bootstrap failure. Momentarily pressing the Init switch on the OCP reinitiates the bootstrap.

The microdiagnostic LEDs on the J11/F11 module indicate if a hard fault exists causing the J11/F11 to hang before control is passed the boot ROM. Section 6.2.5 contains an explanation of these LEDs.

If a failure occurs in the tests of the PDP–11 basic instruction set, the fault indicator mechanism does not report the failure. Instead, the PDP–11 executes a Branch dot (BR .) and does not continue the bootstrap program. A failure of this type is easily detected because the Init indicator does not light. (The Init indicator does light immediately after the basic PDP–11 tests successfully complete.)

When a console terminal is connected to the P.ioj/c, the exact instruction that failed is determined by pressing the terminal break key and noting the address displayed on the terminal. With a bootstrap listing, this address indicates the instruction that failed.

NOTE
The bootstrap does not accept user-modifiable flags.

6.2.3 Progress Reports

The bootstrap does not issue progress reports in the usual sense; however, certain indications of bootstrap progress are evident. These indications are given in the following list:

- **Lamps clear**—Clears all of the HSC OCP indicators. If the indicators fail to clear immediately after the bootstrap is initiated, a failure of the P.ioj/c is probable. (Circuitry on the P.ioj/c module is responsible for initiating the bootstrap program.)
- **Init lamp**—Lights as soon as the basic tests of the PDP–11 instruction set are finished. These tests normally complete within milliseconds after the bootstrap is initiated. Failure of the Init indicator to light indicates a failure in the P.ioj/c PDP–11 processor.
- **RX33 drive-in-use**—Lights as the bootstrap tries to load the Init P.io test (or offline P.ioj test) from the RX33 following the test of the PDP–11 and program memory.

- **State lamp**—Lights when the bootstrap completes and initiates the Init P.ioj/c test (or offline P.ioj/c test). When the State indicator is ON, the Init lamp is OFF.
- **Fault lamp**—Lights during the boot process if the ROM bootstrap tests have detected a fatal error.

6.2.4 Error Information

Specific error codes for the P.ioj/c bootstrap (Codes 21, 22, and 23) are described in detail in Chapter 8.

Because the bootstrap operates in a standalone environment, it does not use the terminal as an error-reporting mechanism. Instead, the HSC OCP indicators are used to report errors and to indicate the module most likely causing the error.

When the bootstrap detects an error, it lights the fault indicator on the OCP. When the Fault switch is pressed, the bootstrap displays a failure code in the OCP indicators. The failure code blinks on and off at one-half second intervals.

6.2.5 Failure Troubleshooting

The ODT program (built into the PDP–11 microcode) contains further information about bootstrap failures. This information is shown in the following list:

- **Init is off, Fault is lit**—A failure was detected after control was passed to the bootable image loaded from the diskette.
- **Init and Fault both lit**—The fault code displays when the fault indicator is momentarily pressed. The program is halted by pressing the break key on the console terminal. If 17772340 is entered, ODT responds by displaying the contents of address 17772340, the test number. Use the test number to refer to the appropriate test in Section 6.2.6.
- **Init and Fault lamps are both off**—Either the bootstrap program was not automatically initiated or the bootstrap PDP–11 instruction test failed.

  Before proceeding, ensure the Secure/Enable switch is set to the ENABLE position. If the switch was not in the ENABLE position when the Init switch was pressed, the HSC controller did not initiate its boot sequence. If the Secure/Enable switch is in the correct position, the J11/F11 microdiagnostics may have failed.

  To check the microdiagnostics, remove the card cage cover and examine the four LEDs on the central edge of the J11/F11 module. At powerup, set all the LEDs and then turn them off as the J11/F11 proceeds through its microdiagnostic sequence.

6.2.6 Bootstrap Test Summaries

This section summarizes the bootstrap tests.

- **Test 0, Basic PDP-11 Instruction Set**—This test verifies the correct operation of a PDP–11 instruction subset. This instruction subset includes only those instructions required for completion of the bootstrap. The following instructions are tested:

  a. Single operand instructions (both word and byte mode):

     ADC, CLR, COM, INC, DEC, NEG, TST, ROR, ROL, ASR, ASL, SWAB, NOP

  b. Double operand instructions (both word and byte modes):

     MOV, CMP, BIT, BIC, BIS, ADD, SUB

c. Branch instructions:

BR, BNE, BEQ, BPL, BMI, BCC (BHIS), BCS (BLO), BGE, BLT, BGT, BLE, BHI, BLOS, BVC, BVS

d. Jump and miscellaneous instructions:

JMP, JSR, RTS, SOB, MTPS, MFPS, CCC, CLN, CLV, CLZ, SEN, SEV, SEZ

e. Addressing modes:

All eight addressing modes

The PDP–11 instruction set test uses two methods of reporting errors. During the initial part of the test, errors result in an infinite program loop at the location of the detected error. During the latter part of the test (when enough instructions have been tested), the fault indicator mechanism is used to report failures. Refer to Section 6.2.2.

- **Test 1, Program Memory (Swap Bank)**—The memory (Swap Bank) HSC memory module includes special logic that permits changing the address range of program memory. This address range is controlled by the Swap Banks bit in the P.ioj/c control and status register (CSR). This test verifies the Swap Banks bit can be set and cleared. (The actual memory switching is not tested; only the setting and clearing of the bit is tested.) A failure in this test indicates the P.ioj/c module must be replaced.

- **Test 2, Program Memory (Vector Area)** – For the HSC control program to function, the first 2048 bytes (addresses 00000000 through 00003777) of program memory must be working. This test verifies the first part of program memory is operating properly. If the test fails, the Swap Banks feature is used, attempting to swap a portion of memory into the 00004000 through 00007777 address range. If the test still fails after Swap Banks has been invoked, a program memory error is reported through the fault indicator mechanism (Section 6.2.2). A failure in this test indicates the M.std2/M.std module must be replaced.

- **Test 3, Program Memory (8-Kword Partition)**—After verifying the first part of program memory is working, the bootstrap tries to find an 8-Kword piece of program memory between address 00004000 and address 00160000. This partition is used to load the Init P.ioj/c test from the load device. If insufficient memory is available, a program memory error is reported through the fault indicator mechanism.

  A failure in this test indicates the M.std2/M.std module must be replaced.

- **Test 4, RX33 Controller Test**—This test verifies basic functionality of the control logic on the M.std2 module. The four controller registers are tested for stuck bits. The DMA hardware is checked for correct cycling and addressing. The interrupt logic is checked to ensure interrupts are properly acknowledged. With the control hardware verified, proceed to the next step, and try to read data from one of the drives.

- **Test 5, RX33 Drive/Interface Test**—The goal of this test is to find a working RX33 drive containing a diskette with a bootable image. Such an image is identified by a PDP–11 NOP instruction in the first word of the image. The intended drive is checked for DRIVE READY from the interface. Then RECAL/VERIFY commands the drive to seek to track 0. This command then reads the diskette header to verify the RECAL command did move the head to track 0.

  After a suitable drive is found, the first eight blocks of the diskette are loaded into the 8-Kword partition found in test 3. The eight blocks loaded consist of the first five blocks of the Init P.ioj/c test (or Offline P.ioj/c test), the RT–11 volume ID block, and the first RT–11 directory segment on the diskette. (The directory blocks are loaded at this time to save directory look-up time in the Init P.ioj/c test or the Offline P.ioj/c test.)

RX33 drive 0 is tested first. A failure with drive 0 causes the bootstrap to proceed to drive 1 and begin the tests again. If neither RX33 drive is working correctly, an RX33 error is displayed by the fault indicators. An error table is maintained in program memory addresses 00000400 through 00000412, which remembers why each rejected RX33 drive failed the boot. Table 6–1 shows the RX33 error table addresses and meanings.

Table 6–1 RX33 Error Table

Address	Meaning
00000400	Contains controller error code (code 1 or code 2)
00000402	RX33 address being accessed, if applicable
00000404	Expected result
00000406	Actual result
00000410	Drive error code, byte-encoded: drive 1/drive 0 (high-byte/low-byte)

NOTE
It is not possible to simultaneously have information in addresses 00000400 and 00000410.

If the boot fails with a RX33 error, the ODT feature of the PDP–11 is used to examine the RX33 error table to determine why each RX33 drive failed the test. (Remember, the bootstrap tries both drives before declaring an error.) Use the following sequence to examine the RX33 error code table.

1. Press the break key on the console terminal.

   The terminal displays the address of the current instruction of the bootstrap, then prompts for input with an @ character.

   NOTE
   Newer I/O control processor modules do not use the break key to enter ODT. Use the SETSHO command SET ODT REBOOT and then enter Ctrl/P to get the ODT prompt. The prompt for these modules is an asterisk (*).

2. Enter the appropriate address, *nnn*.

   The terminal displays the (octal) contents of that address.

3. Press LINEFEED to examine the Table 6–2 controller error and related failure information.

Table 6–2 RX33 Error Code Table

Controller Error	Failure Information
1	NXM occurred while accessing RX33 registers.
2	A bit was stuck in the registers.
3	Force mode interrupt did not occur.
4	DMA test mode hardware error occurred.
5	DMA address counters were wrong after transfer.
6	Incorrect data found after DMA test operation.
7	Data parity was bad after DMA test operation.

Table 6–2 (Cont.) RX33 Error Code Table

Controller Error	Failure Information
10	Drive was not ready (no diskette inserted or door was open).
11	Hard error (CRC or Record Not Found) occurred on RECAL/verify.
12	Track 0 bit was not set after RECAL.
13	SEEK command timeout occurred.
14	Seek error (CRC or Record Not Found) occurred.
15	READ SECTOR command timeout.
16	Hard error (CRC or Record Not Found) occurred on read.
17	Nonbootable image (non-NOP instruction is the first word).

Failure information for both drives in address 00000410 is possible. In this case, nonzero data is in both bytes. Only when failures are detected on both drives does the boot ROM generate a LOADFAL failure code and branch to the fault light routine.

- **Test 6, Transfer Control to Loaded Image**—This part of the bootstrap is not actually a test. However, it is given a test number in case an error occurs in this section of code. The PDP–11 general registers are loaded with certain parameters (CSR and unit of load device, base address, and size of partition, and so forth). The image loaded from the RX33 is initiated by jumping to the first instruction. Any errors occurring in this part of the bootstrap are probably unexpected traps or interrupts caused by intermittent P.ioj/c or M.std2/M.std failures. When the loaded image is started, the State indicator is lit, and the Init indicator is turned off.

6.2.7 Generic Error Message Format

All of the diagnostics use a common method of reporting errors and a common error message format. All errors are reported on the console terminal as they occur. In all offline diagnostics, error messages conform to the HSC controller diagnostic error message format.

The first line of an error message contains general information concerning the error and is mandatory. The second line of an error message consists of text describing the error and also is mandatory. The third and succeeding lines of the message are used for additional information where required, and are optional.

The generic error message format follows:

```
XXXXXX>hh:mm T@aaa E@bbb U-000
 SEEK error detected during positioning operation
 optional line 1
 optional line 2
 optional line 3
```

where:

XXXXXX> is the prompt for the particular diagnostic in question such as OFLCXT> or OBIT>.
hh:mm is the number of hours and minutes since system boot.
aaa is a test number.
bbb is an error number with a range of 1 through 77 (octal).
U-*000* is the unit number.

The final field in the first line appears only in diagnostics where such information is appropriate. Each error number has a unique text string associated with it. For errors that consist of results that did not compare with the expected value, the diagnostic uses the optional lines to show expected/actual (EXP/ACT) data. Errors on data transfers and SEEK commands use the optional lines to print out the LBN, track, sector, and side to help isolate problems with the media or the drive.

6.3 ODL—Offline Diagnostics Loader

The offline diagnostics loader provides a software environment for the HSC offline diagnostics. The loader supports a command language that loads and executes an offline diagnostic from the load device into program memory. The loader command language also permits the display and modification of any address contents in the HSC controller program, data, or control memories.

The software environment provided for offline diagnostics includes a load device driver and a terminal driver. A standard software interface between the diagnostics and the load device and terminal devices takes the place of individual interface routines within the diagnostics. The loader also maintains a timer that keeps track of the relative time since the loader was last booted. This allows diagnostic error messages to be time stamped.

6.3.1 Loader System Requirements

Hardware required to run the offline diagnostics loader includes:

- I/O control processor module with HSC boot ROM
- At least one memory module
- RX33 controller with at least one working drive

  or

- TU58 controller with at least one working drive
- Terminal connected to the I/O control processor console interface

6.3.2 Loader Prerequisites

In the process of loading the offline diagnostics loader, several diagnostics are run. The ROM bootstrap tests the basic PDP–11 instruction set, tests a partition in program memory, and tests the load device used for the boot. Then the bootstrap loads the offline P.ioj/c test, which completes the PDP–11 tests and the remainder of the I/O control processor module tests.

After these tests, the offline diagnostics loader is loaded from the load device to memory, and control is passed to the loader. Because of the sequence of tests that precede the loader, the loader assumes the I/O control processor module and the RX33 are tested and working.

6.3.3 Loader Operating Instructions

Follow these steps to start the offline loader:

1. Insert the HSC offline diagnostics media into the load device.
2. Power on the HSC, or press and release the Init button on the HSC OCP.
3. The load device drive-in-use LED lights within a few seconds, indicating the bootstrap is loading the offline diagnostic loader to program memory.

4. In less than 30 seconds, the offline diagnostics loader indicates it has loaded properly by displaying the following:

```
HSC OFL Diagnostic Loader, Version Vnnn
Radix=Octal,Data Length=Word,Reloc=00000000
ODL>
```

5. The offline loader is now ready to accept commands. Section 6.3.4 contains information on the loader command language.

6.3.4 Loader Commands

The following sections describe the commands recognized by the offline loader.

6.3.4.1 HELP Command

The HELP command supplies an abbreviated list of all commands the loader recognizes. In response to the HELP command, the loader reads the file OFLLDR.HLP from the load device and displays the contents of this file on the HSC console terminal. Section 6.3.5.2 contains a listing of the loader help file.

6.3.4.2 SIZE Command

The offline system sizer is invoked by the SIZE command. The sizer determines the sizes of the HSC controller program, control, and data memories, and the type of requestor in each HSC controller requestor position. The term requestor position refers to the priority of a particular requestor on the data and control memory buses. It does not match the numbering of module slots.

6.3.4.3 TEST Command

The offline diagnostics loader TEST command is used to invoke the various offline diagnostics available on the HSC. The following list shows the particular form of the TEST command used to invoke each diagnostic. In general, the TEST command format allows specification of the system component to be tested; for instance, the TEST MEMORY command invokes the offline memory test.

- **Offline P.ioj Cache Test**—Verifies the full functionality of the P.ioj module cache. The offline cache test is invoked by the TEST CACHE command.
- **Bus Interaction Test**—Invoked by the TEST BUS command. The bus interaction test generates contention on the HSC controller data and control memory buses by two or more Ks simultaneously testing different sections of the control and data memories. Two or more working requestors are required to run this test (including the K.ci).
- **K Test Selector**—Invoked by the TEST K command. The K test selector allows specific requestor microdiagnostics to run.
- **K/P Memory Test**—Invoked by the TEST MEMORY BY K command. The K/P memory test uses one of the HSC requestors to test either data or control memory. This test runs faster than the offline memory test because a requestor is roughly seven times faster than the I/O control processor. Program memory cannot be tested using the K/P memory test as the Ks do not have an interface to the program memory bus.
- **Offline Memory Test**—Invoked by the TEST MEMORY command. This test uses the I/O control processor to test program, control, or data memories. OMEM also tests the single bit error correction logic on the M.std4 module.
- **Offline M.cache Test**—This test is invoked by the TEST MCACHE command. The offline M.cache test checks the optional M.cache module.

- **Offline RX33 Exerciser**—Invoked by the TEST RX command. This test is a combined hardware diagnostic and exerciser for the floppy disk controller circuits on the M.std2 and M.std4 modules, and for the RX33 disk drive itself.
- **Memory Refresh Test**—Invoked by the TEST REFRESH command. This test allows the refresh feature of the memories to be tested.
- **OCP Test**—Invoked by the TEST OCP command. The OCP test checks the HSC controller indicators and switches. The test requires manual intervention by an operator.

6.3.4.4 LOAD Command

The LOAD command loads a program into HSC program memory without starting it. The command format is LOAD <filename>, where <filename> is the name of any file on the HSC OFFLINE diskette. The loader finds the specified file and loads it into program memory. This command patches a program image in before starting execution. After the patch is made, the program can be initiated by entering the START command.

6.3.4.5 START Command

The START command initiates the loader program currently loaded in program memory. The START command can be used in conjunction with the LOAD command, or it may be used to reinitiate the last loaded offline diagnostic. This saves the time required to reload the program from the load device. For example, you have previously entered SIZE to initiate the offline system sizer program and after the sizer completes, you wish to run it again. Entering START restarts the sizer without reloading the program from the load device, saving many seconds of load time.

6.3.4.6 EXAMINE and DEPOSIT Commands

The EXAMINE and DEPOSIT commands are used to display or modify the contents of any location in the HSC program, control, and data memories. Qualifiers (switches) can be used with these commands to display bytes, words, long words, or quad words. The radix (octal, decimal, hex) of the displayed data also can be controlled by qualifiers. Alternately, the SET DEFAULT command can be used to set the default data length and radix for all EXAMINE and DEPOSIT commands. Refer to Section 6.3.4.11 for more information on these commands.

The EXAMINE command:

The EXAMINE command is used to display the contents of any location in the HSC program, data, or control memories. The format of the command is: EXAMINE <address>. The <address> can be a string of digits in the current (default) radix. Certain symbolic addresses also are permitted. Refer to Section 6.3.4.7 for more information on these commands.

In the following example, the user entered a command to examine the contents of location 14017776. (Notice the EXAMINE command can be abbreviated to a single E.) When the loader displays the contents of location 14017776, the address is preceded by a (D) indicating the location is within data memory. The display shows the location contains the value 125252.

```
ODL> E 14017776
  (D) 14017776 125252
```

The DEPOSIT command:

The DEPOSIT command is used to modify the contents of any location in the HSC program, Control, or data memories. The format of the command is: DEPOSIT <address> <data>. The <address> can be a string of digits in the current (default) radix. Certain symbolic addresses also are permitted. Refer to Section 6.3.4.7 for more information on these commands.

In the next example, the user entered a command to store the value 123456 in the contents of address 14017776. The previous contents of this data memory location are replaced with the value specified in the DEPOSIT command (123456).

```
ODL> D 14017776 123456
```

6.3.4.7 EXAMINE and DEPOSIT Symbolic Addresses

The four symbols used as symbolic addresses in a DEPOSIT or EXAMINE command are described in the following list.

- **Asterisk (*)**—This symbol indicates that the loader is to use the same address as used in the last EXAMINE or DEPOSIT command. For example, if the contents of address 16012344 were just examined and the value 1234 is to be deposited into the same address, enter DEPOSIT * 1234 instead of entering DEPOSIT 16012344 1234.

- **Plus sign (+)**—This sign is also used as a symbolic address. This symbol means the loader is to use the address following the last address used by an EXAMINE or DEPOSIT command. When the loader sees a plus sign (+) as an address, it takes the last address used by EXAMINE or DEPOSIT and adds an offset. The offset depends on the current default data length. Refer to Section 6.3.4.11 for more information on using these commands.

  If the current default data length is a byte, the loader adds 1 to the last address. If the default is a word, the loader adds 2 to the last address. The offset is 4 for longword data length and 8 for quadword. This feature is useful when examining a number of items stored in successive locations.

  For example, if you want to examine a table of words beginning at address 14125234, examine the first location by entering EXAMINE 14125234. The next location can now be examined by entering EXAMINE + instead of entering EXAMINE 14125236.

- **Minus sign (–)**—This sign is also used as a symbolic address. It indicates the loader is to use the address preceding the last address used by either command. When the loader sees a minus sign (–) as an address, the loader takes the last address used by an EXAMINE or DEPOSIT and subtracts an offset, depending on the current default data length. Refer to Section 6.3.4.11 for more information on these commands.

  If the current default data length is a byte, the loader subtracts 1 from the last address. If the default is a word, the loader subtracts 2 from the last address. The loader subtracts 4 for longword data length and 8 for quadword. This feature is useful in the same way as the + symbol, but examines a table which starts at the highest address and proceeds down to lower addresses.

  For example, if a table of words that ends at address 14012346 is to be examined, the operator can examine the last location of the table by entering EXAMINE 14012346. The preceding location in the table could now be accessed by entering EXAMINE – instead of entering EXAMINE 14012344.

- **At (@)**—The @ symbol is also used as a symbolic address. This symbol means the loader uses the data from the last EXAMINE or DEPOSIT command as an address. This feature is useful when following linked lists. For example, first examine location 123434 which contains a pointer to a linked list. Now enter EXAMINE @ to examine the location pointed to by the first location.

6.3.4.8 Repeating EXAMINE and DEPOSIT Commands

When troubleshooting memory problems, continuously executing an EXAMINE or DEPOSIT command is sometimes useful. The REPEAT command is used for this continuous execution. Enter REPEAT EXAMINE or DEPOSIT. To stop a repeated command, enter Ctrl/C.

In the following example of repeating a DEPOSIT command, the value 125252 is continuously deposited into address 14017776. The format of the DEPOSIT command does not change. The DEPOSIT command is just preceded by the word REPEAT. The REPEAT command can be abbreviated to RE:

```
REPEAT DEPOSIT 14017776 125252
```

or

```
RE D 14017776 125252
```

By repeating an EXAMINE command, the contents of address 14017776 can be continuously examined. The format of the EXAMINE command does not change. The EXAMINE command is just preceded by the word REPEAT.

```
REPEAT EXAMINE 14017776
```

or

```
RE E 14017776
```

In the examples shown, the contents of location 14017776 are displayed continuously on the terminal. This slows down the repetition of the command and wastes paper on hardcopy devices. Stop output to the terminal by entering Ctrl/O. However, the loader also provides a special EXAMINE command qualifier (/INHIBIT) for suppressing output to the terminal. This qualifier is discussed in Section 6.3.4.10.

6.3.4.9 Relocation Register

The loader provides a relocation register. It can be used to reduce the number of address digits entered for an EXAMINE or DEPOSIT command when all addresses are in either the control or data memories. The contents of the relocation register are added to the address given with an EXAMINE or DEPOSIT command. The relocation register contains a 0 when the loader is initiated, so it normally has no effect on the addresses entered in an EXAMINE or DEPOSIT command.

Use the following example to examine many locations in data memory.

```
ODL> SET RELOCATION:14000000
ODL> EXAMINE 0
  (D) 14000000 123432

ODL> EXAMINE 1234
  (D) 14001234 154323
```

Load the relocation register with the address of the first location in data memory (14000000). When an EXAMINE command with an address of 0 is issued, the loader adds the relocation register to the address given, resulting in the examination of address 14000000. Likewise, when an EXAMINE command with an address of 1234 is issued, the loader displays the contents of location 14001234.

The following example shows how to examine many locations in control memory.

```
ODL> SET RELOCATION:16000000
ODL> EXAMINE 0
  (C) 16000000 125252

ODL> EXAMINE 4320
  (C) 16004320 125432
```

The relocation register is loaded with the address of the first location in control memory (16000000). When an EXAMINE command is issued with an address of 0, the loader adds the relocation register to the address given, displaying the contents of address 16000000. Likewise, when the user enters an EXAMINE command with an address of 4320, the loader displays the contents of location 16004320. You can stop the display by entering Ctrl/C.

6.3.4.10 EXAMINE and DEPOSIT Qualifiers (Switches)

The following list describes the EXAMINE and DEPOSIT qualifiers (switches).

- **/NEXT**—Allows an EXAMINE or DEPOSIT command to work on successive addresses. When used with a valid EXAMINE command, the /NEXT qualifier specifies that after the command location has been displayed, the loader also displays the next number of locations following the first. For example, the command E 1000/NEXT:5 results in the display of locations 1000, 1002, 1004, 1006, 1010, and 1012 (assuming the default data length is a word). The number of the argument can be any value in the current default radix that can be contained in 15 binary bits or less. For instance, if the default radix is octal, the number of the argument can be any value between 1 and 77777.

  The /NEXT qualifier works the same way for the DEPOSIT command, except that the data given with the DEPOSIT command is stored in the location specified and the next number of locations following.

- **/BYTE/WORD/LONG/QUAD**—These qualifier switches are used to control the data length of examined or deposited data. Normally, the loader uses the default data length (Section 6.3.4.11) when data is examined or deposited. However, the data length qualifiers can be used to override the default for a single examine or deposit. For instance, assume the default data length is currently a word, and a byte quantity at address 16001234 is to be examined. Entering EXAMINE 16001234/BYTE would display the proper byte without affecting the default data length.

- **/OCTAL/DECIMAL/HEX**—These qualifier switches can be used with an EXAMINE command to control the radix of the address and data displayed. They are *not* used to control the radix of the address supplied in the EXAMINE command. The radix of the address and data displayed by an EXAMINE command is usually controlled by the current default radix (Section 6.3.4.11), but the /OCTAL/DECIMAL/HEX qualifiers are used to override the default radix for a single EXAMINE command. For example, assume the default radix is octal. Entering EXAMINE 14001234/HEX displays the contents of address 14001234(8) in the hexadecimal radix. The EXAMINE display would be as follows: (D) 30029C HHHH. HHHH represents the contents (hex) of the location displayed. The address is also displayed in hex.

- **/INHIBIT** (abbreviated to /INH)—This qualifier switch inhibits the display of examined data when repeating an EXAMINE command. This is useful both for saving paper on hardcopy devices and for speeding up the EXAMINE operation for scope-loop purposes. For example, the command REPEAT EXAMINE 16012346/INH results in the loader continuously reading the contents of location 16012346 without displaying anything at the console.

6.3.4.11 Setting and Showing Defaults

The SET DEFAULT command is used to change the default radix and/or data length. The default radix controls the radix of parameters supplied with EXAMINE or DEPOSIT commands and the radix of data displayed by the EXAMINE command. The default data length controls the length (byte, word, long, or quad) of data displayed by the EXAMINE command or data stored by a DEPOSIT command.

The default radix may be set to octal, decimal, or hexadecimal. When the offline loader first starts, it sets the default radix to octal. Enter SET DEFAULT HEX to set the default radix to hexadecimal. After the default radix is set, it remains so until another SET DEFAULT command is entered or the loader is rebooted.

The default data length may be set to byte, word, longword, or quadword. When the loader is first started, it sets the default data length to word (16 bits). Enter SET DEFAULT LONG to set the default data length to longword (32 bits). Setting the default data length to longword causes an EXAMINE command to display longword quantities and causes the DEPOSIT command to store longword quantities. (Because the loader is executing in a PDP–11, longwords are stored and retrieved as two successive 16-bit words.) After the default data length is set, it remains so until changed by another SET DEFAULT command or until the loader is rebooted.

6.3.5 Unexpected Traps and Interrupts

When the loader detects an unexpected trap or interrupt, the following message is displayed:

```
Unexpected trap through www, VPC=xxx, PSW=yyy
Error Address = zzz
```

where:
www is the address of the trap or interrupt vector.
xxx is the virtual PC of the loader at the time of trap.
yyy are the contents of PSW at the time of trap.
zzz is the address of the location causing NXM or parity trap.

The first line of the unexpected trap report is issued for all unexpected traps or interrupts. The second line is issued only if the trap was through vector addresses 000004 (NXM trap) or 000114 (parity trap). The address of the vector is a direct clue to the cause of the trap. Refer to Section 6.3.5.1 for a list of the devices and error conditions associated with each vector.

The virtual PC (VPC) of the instruction executing when the trap occurs is sometimes useful in determining the cause of the trap. The VPC can be referenced in the listing to find the instruction causing the trap. The contents of the VPC include the address of the instruction following the instruction executing when the trap occurred. Notify Customer Service to analyze such failures.

NXM traps can be caused by EXAMINE or DEPOSIT commands if an address not contained in a particular HSC controller is specified. For example, if an HSC controller contains only data memory from addresses 14000000 through 14177776, and an EXAMINE or DEPOSIT is tried for address 14200000, the loader reports an NXM trap. In this example, the NXM trap would *not* represent an error condition.

Parity traps can be caused by an EXAMINE command if a user examines an address not initialized with good parity. For example, when the HSC controller memories are powered on, the parity bits are in random states. Thus, if a user examines a location not written since power-on, the location may generate a parity error. This does not constitute an error condition.

However, if a location produces a parity error and that location has been written since power-on, a memory error is indicated.

NOTE
The I/O control processor and Ks have bits allowing them to write bad parity for testing the parity circuit. These bits are for diagnostics engineering purposes only.

6.3.5.1 Trap and Interrupt Vectors

Table 6–3 is a list of trap and interrupt vectors for various devices and error conditions recognized by the I/O control processor PDP–11 processor.

Table 6–3 Trap and Interrupt Vectors

Vector	Device or Error Condition
000004	Nonexistent memory, stack overflow, halt in user mode, and odd address trap
000010	Illegal instruction
000014	BPT instruction
000020	IOT instruction
000024	Power fail interrupt
000030	EMT instruction
000034	TRAP instruction
000060	Console terminal—receiver interrupt
000064	Console terminal—transmitter interrupt
000100	Line clock interrupt
000114	Parity trap
000120	Control bus interrupt—level 4
000124	Control bus interrupt—level 5
000130	Control bus interrupt—level 6
000134	Control bus interrupt—level 7
000230	RX33 interrupt
000250	MMU abort (trap)
000300	SLU (Serial Line Unit) #1, receiver interrupt
000304	SLU (Serial Line Unit) #1, transmitter interrupt
000314	SLU (Serial Line Unit) #2, receiver interrupt
000310	SLU (Serial Line Unit) #2, transmitter interrupt

6.3.5.2 Help File

The help file display is started by entering HELP at the ODL prompt. This file is unique to each version of software, as shown by V*nnn* in Example 6–1. This display is the complete help facility for the offline diagnostics. Exit the help file display by entering Ctrl/C.

```
!
! HSC OFL Diagnostic Loader Help File - Vnnn
! Capital letters = required input, lower case = optional
!
! Commands (terminated by CR):
! 'Examine <address>'              ;'splay data at <address> specified
! 'Deposit <address> <data>'       ;deposit <data> to <address>
!                                  ;<address> = digit string in current
!                                  ;default radix, or:
!                                  ;'*' = use same address as last ex or de
!                                  ;'+' = use address following last address
!                                  ;'-' = use address preceding last address
!                                  ;'@' = use <data> from last ex or de as address
! 'HElp'                           ;print this file
! 'Load <filename>'                ;load file to diagnostic partition
! 'REpeat <command>'               ;repeat specified command until ^C
! 'RUN <filename>'                 ;Do implicit LOAD and START of <filename>
! 'SEt Default <option>,<option>   ;set default radix or data length
!    <options> = Byte,Word,Long,Quad,Hex,Octal,Decimal
! 'SEt Relocation:#'               ;set relocation register to #
!                                  ;relocation register is 22-bit positive #
!                                  ;added to address of all 'Ex' and 'De'
!                                  ;commands.
! 'SEt MCAche ON                   ;Enable the M.Cache board, use DATA MEMORY
!                                  ;from the M.Cache module
! 'SEt MCAche OFF                  ;Disable the M.Cache board, use DATA MEMORY
!                                  ;from the M.Std4 Memory module
! 'SHow'                           ;display defaults and Loader version
! 'SIze'                           ;Size memories and display K status
! 'Start'                          ;start program in diagnostic partition
! 'Test Bus'                       ;load and start the OFL Bus Interaction test
! 'Test K'                         ;load and start the OFL K Test Selector
! 'Test MCache'                    ;load and start the OFL M.CACHE test
! 'Test MEmory'                    ;load and start the OFL Memory Test
! 'Test MEmory By K'               ;load and start the OFL K/P Memory Test
! 'Test OCP'                       ;load and start the OFL OCP Test
! 'Test Refresh'                   ;load and start the OFL Refresh Test
! 'Test Cache'                     ;load and start the OFL cache test (L0111-xx)
! 'Test Rx'                        ;load and start the OFL Rx33 test (L0111-xx)
! 'WCS'                            ;load and start the OFL control store loader
!
!Qualifiers (switches) for 'Ex' and 'De':
! '/Next:#'                        ;repeat Ex or De on next '#' addresses
! '/Byte,/Word,/Long,/Quad'        ;use specified data length instead of default
! '/Octal,/Decimal,/Hex'           ;use specified radix for Ex display
! '/INH'                           ;inhibit display of examined data
! <end of help file>
```

Example 6–1 Example HELP file display

6.4 OFLCXT—Offline P.ioj Cache Test

The offline cache test (OFLCXT) is a diagnostic that runs under the offline loader in a standalone environment. OFLCXT provides in-depth testing of the cache logic on the J11 P.ioj and verifies the full functionality of the onboard cache. Execution time for a single pass is between 16 seconds and 4 minutes, depending on the options selected.

6.4.1 System Requirements

OFLCXT is loaded into memory through the offline loader. This test requires 8 Kwords of memory to run. One-half of this memory space contains the program; the other half is used as a cached buffer. All terminal I/O and handling of the line clock is done by the offline loader.

6.4.2 Operating Instructions

This section contains operating instructions specific to OFLCXT. If the HSC controller is not booted and running the offline loader, see the instructions for booting OFLCXT in Section 6.1.2 and in Section 6.2. To run the offline loader, enter the TEST CACHE command at the ODL> prompt.

This command loads OFLCXT from the media and transfers control to the diagnostic. When it starts, OFLCXT displays the following:

```
HSC OFL CPU CACHE EXERCISER Version nnn
```

where: Version *nnn* is a three-digit version number.

6.4.3 Test Termination

OFLCXT can be terminated by entering Ctrl/Y.

6.4.4 Parameter Entry

Following are the three user-modifiable parameters for OFLCXT. In each case, the default, invoked by a comma (,), is shown in brackets. If no default is possible, the brackets are empty.

- **Select Data Reliability test**—This is the first user-modifiable parameter, an optional selection of the data reliability tests. It is a moving-inversions style test for exercising the RAM array. The offline cache test prints:

  ```
  Run extended cache ram test (Y/N)  [N] ?
  ```

  Selecting this optional test increases test time per pass to about four minutes. It is useful for the manufacturing burn-in and test areas. It is not necessary to run this optional test to fully verify the health of the cache.

- **Leave Cache Enabled**—Determines the cache state at the termination of the diagnostic. OFLCXT prints:

  ```
  Leave cache enabled after successful completion (Y/N) [N] ?
  ```

  This feature allows enabling the cache for further use after running the diagnostic to verify the cache is working. If the diagnostic detects any hard failures in the cache, it is not enabled at the end of the diagnostic. This prevents complications if the cache contains hard failures and is inadvertently turned on.

- **Number of Passes**—Accepts a total number of passes from 1 to 32767 (decimal). The test prompts for this number as follows:

  ```
  # of passes to perform (D) [1] ?
  ```

  Any decimal number up to 32767 can be used. Fatal errors can cause the diagnostic to terminate before the specified number of passes executes.

  At the completion of the total passes requested by the user, the diagnostic prompts:

  ```
  Reuse parameters (Y/N) [Y] ?
  ```

To repeat the last test specified using the parameters, answer this prompt by entering Y or Return. To cause the test to prompt for new parameters, answer the prompt with N.

Use the delete key to delete mistyped parameters before terminating the entry with Return. If an error in a parameter was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.4.5 Progress Reports

OFLCXT provides summary information at the end of each pass. The end-of-pass message is similar to the following:

```
End of Pass 00001, 00000 Errors, 00000 Total Errors
```

The errors field contains the number of errors for the pass. The total errors field contains a running total of errors accumulated since the start of the diagnostic.

For any OFLCXT prompts, use the delete key to delete mistyped parameters before terminating the entry with Return. If an error in a parameter was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.4.6 Test Summaries

Following are summaries of the OFLCXT tests 1 through 16:

- **Test 1, Cache register access test**—Checks for the presence of the necessary cache control/status registers, the cache control register (17777746), the hit/miss register (17777752), and the memory system error register (17777744). To perform further diagnosis, these registers must respond.
- **Test 2, Cache control register bits**—Tests the read/write bits of the cache control register (17777746) for stuck-at faults. In addition, bits (8,11:15), which are write only, are checked for read data of 0. Bits 6 and 10 which cause data and tag parity to be written incorrectly on new data allocated to cache are treated as special cases. After writing/reading each of these bits, the cache is flushed to remove any bad parity locations.
- **Test 3, Force miss action**—Verifies all references made with either bit 3 or bit 2 of the cache control register set that cause a cache miss and leave the cache entry unchanged. To perform this test, first write a test address with bits 3:2 cleared to allocate cache and place a known data pattern into the cache. Then bit 2 is set, and the same test location is written again. With bit 2 set, the cache will not update, and the data in cache is still considered valid. When bit 2 is cleared and the test location is accessed again, the old data from cache is the result. If not, the force miss action of bit 2 did not work. The same sequence is repeated for bit 3, and the same results are expected.
- **Test 4, Hit/miss register, part I**—Checks the basic operation of the hit/miss register in logging hit/miss information on instruction fetches and data reads/writes. The hit/miss register is critical to further cache diagnosis because it is the window into what is actually going on inside the cache.

  First, a test location is allocated with cache enabled. Then cache is bypassed, and the test location is accessed again by a write. This write goes directly to main memory and bypasses the cache. The cache is enabled, and a read access to the test location results in a hit condition in the hit/miss register. Then the test location offset by 8 Kwords is accessed. This results in a miss, since the upper bits of the address (tag) will not match.

- **Test 5, Hit/miss register, part II**—Checks all the combinations of the six bits in the hit/miss register for a single miss at different bit positions. This is done by caching a certain sequence of instructions and executing them, with miss conditions forced at each bit position. At the completion of this test the hit/miss register has been checked for both ones and zeros at each bit position.
- **Test 6, Byte accesses**—Ensures byte references to the cache are handled correctly by the control logic. The first operation is a byte-write to the test location not allocated followed by a byte-read of the test location. The read results in a miss. Then the entire word at the test location is allocated. The upper byte of the test location is modified, and a cache hit is expected. The entire word is also read and compared against the expected result to see if the byte-write occurred. A similar chain of events follows, this time modifying the low byte.
- **Test 7, PDR Cache bypass test**—Tests all of the kernel PDRs <0:7>, as well as the user PDRs. It is very important for the bypass cache bit (bit 15 of any PDR) to work correctly in the multiprocessing environment of the HSC controller.

  PDR bypass is tested by remapping all PDRs to point to control memory. Control memory is written by the MMU writing a data pattern and allocating cache. Control memory windows are used to write control memory to a second pattern without involving the cache control logic. When control memory is read through the MMU with the bypass bit set, the actual control memory content (second pattern) is the result if the bypass bit is actually set. If the old content (first pattern) is read back, the bypass bit is not working. PARs 1, 2, 3, 5, and 6 are tested in this way.

  PARs 0, 4, and 7 are treated as special cases due to programming environment restrictions. They are tested by allocating cache with some location mapped by the PAR/PDR under test and then setting the bypass bit. When the test location is read, the hit/miss register records a hit and then invalidates the location. If the location is written or read again, it results in a miss as long as the bypass bit is set.

  After all the kernel PAR/PDR registers are tested, the program maps user space that is identical to kernel space and switches into user mode to reexecute all the tests. After all user PAR/PDR pairs have been tested, the program swaps back into kernel mode and proceeds to the next test.
- **Test 8, Cache flush action**—Allocates all 4 Kwords of cache, and then executes a flush command by setting bit 8 in the cache control register. The cache control logic then writes every location in cache with the data value 17777746 and resets the valid bit for each location. All 4 Kwords of cache allocated before the flush are read again, and if any location responds with a hit when read, an error is declared.
- **Test 9, Unconditional bypass to main memory**—Checks the correct operation of bit 9 of the cache control register. Bit 9 is used to bypass cache in a fashion similar to the bypass bits in the PAR/PDRs. Any location allocated in cache before the bypass bit is set results in a hit on the first access, and further accesses all show as misses.

  This function is used when it is desirable to temporarily disable the cache in a fashion that does not leave the cache with stale data when reenabled. A test location is allocated, and then the bypass bit is set. The first access of the test location is a hit, and the second is a miss.
- **Test 10, Force tag/data parity errors**—Forces parity errors in the tag and data fields of the cache array to test the parity detection logic. A special diagnostic mode is used, with bit 0 of the cache control register and one of the force parity error bits set. When bit 0 is set, any trap through 114 is disabled on a parity error detected in cache. If a parity trap does occur, an error is declared.

First, tag errors are forced using bit 10 in the cache control register. When this bit is set, locations allocated to cache do so with bad tag parity. When accessed again (resulting in a cache hit), the tag parity error bit is set (bit 5 in the memory system error register). The force data parity error bit (bit 6 of the cache control register) is checked next. After a location is allocated to cache with bad data parity, further reads of that location result in setting the data parity error bits (bits 6:7) of the memory system error register. After using the force bad parity bits, the program flushes the cache to remove these parity errors.

- **Test 11, Abort/interrupt on parity errors**—Uses the force parity error bits in the cache control register to force parity errors in the cache array. Because testing of the detection of such errors has been done, testing of the other logic related to cache data or tag parity errors can be done.

  Different combinations of tag and parity errors are forced, with the cache control register set to interrupt through trap 114, or abort through trap 114 on parity errors. An interrupt through trap 114 sets the correct error bit(s) in the memory system error register. Also, the instruction detecting the parity error completes.

  On an abort through trap 114, the correct error bit(s) is set, but the instruction does not complete. If the parity error is detected on the fetch of the source data, the data in the destination of the instruction is not modified. The PC on the stack after each interrupt or abort instruction is checked against the PC that is expected.

- **Test 12, DMA invalidate**—Modifies a location resulting in the cache acquiring stale data unless cache logic detects the DMA change. The RX33/M.std2 subsystem is used to generate DMA operations to program memory. A DMA write to a program memory location allocated to cache results in a cache miss when it accesses after the DMA write.

- **Test 13, Check blockage of parity error on NXM abort**—Generates simultaneous NXM and parity errors. The NXM trap occurs, overriding the parity error.

- **Test 14, Cache data RAM test**—Tests the cache data RAMs by mapping one PAR and using the cache solely for data storage. A data pattern to detect dual addressing is written to the cache. Failures of the cache data to match the expected data on read-back are considered miscompare errors. The test is first done using word addresses and test values, and then repeated with byte addresses and byte data patterns. Each location allocated is expected to be a hit from cache, and the content is checked as well.

- **Test 15, Tag store RAM test**—Checks the tag bits of the cache array for dual-address errors and stuck-at faults. With the cache flushed and completely deallocated, the first 256 locations of the cache are written with a unique data value in each address. Then the entire cache is read. Only the 256 locations written are cache hits, and only these locations have the expected data pattern. Then the upper address bits are changed so a new combination of tag bits results. This test is repeated 15 times until all of the tag bits have been tested.

- **Test 16, Data RAM reliability test**—Performs a modified moving inversions test on the cache data RAM array. Due to the geometry of the data RAMs, every fourth bit is done concurrently to save time. This results in using the same pattern in both nibbles of the data word. This test must be selected by the user as it does not normally run by default. About four minutes are required to complete one pass of this test.

6.4.7 Error Information

OFLCXT displays the errors detected during execution on the console terminal. Error messages follow the diagnostics generic error message format preceded by an OFLCXT> prompt.

A typical OFLCXT error message format follows:

```
OFLCXT>hh:mm T#aaa E#bbb U-000
 < Text describing error >
 MA-xxxxxxxx
 EXP-yyyyyy
 ACT-zzzzzz
```

where:
hh is the elapsed hours since last bootstrap.
mm is the elapsed minutes.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-*000* is the unit number.
MA-*xxxxxxxx* is the address of location causing the error.
EXP-*yyyyyy* is the data pattern that was expected.
ACT-*zzzzzz* is the data pattern that was actually found.

Each error number has a unique text string associated with it. For errors with results that did not compare with the expected value, the diagnostic uses the optional lines to show expected/actual data.

Soft errors (such as cache parity errors) can accumulate to a point where the diagnostic classes them as fatal. The test then terminates on a fatal error.

6.4.8 Error Messages

The following list describes in detail each possible error message. The errors are listed in numerical order.

- **Error 00, Memory Parity Error, VPC = xxxxxx**—Applicable to all tests. This error can occur at any time during execution of the diagnostic. The virtual PC on the stack is printed to help identify the program area where the error occurred. The content of the error address register is also displayed.

  Both the virtual PC and the error address register content are optional lines. Detection of this error causes the testing to cease. Then the diagnostic returns to the Reuse Parameters prompt.

- **Error 01, NXM Trap, VPC = xxxxxx**—Applicable to all tests. This error causes the diagnostic to return to the Reuse Parameters prompt. Additional data (such as the virtual PC of the instruction that caused the trap and the physical address contained in the error address register) are printed as optional lines.

- **Error 02, Cache Parity Error, VPC = xxxxxx**—Applicable to tests 2 through 16. This error results when a trap through the parity error vector is detected and the cache is enabled. The virtual PC where the error was detected is printed, as well as the content of the error address register. If the 22-bit value in the error address register is 177770024, no main memory error was present. Assume the parity error is from the cache.

- **Error 03, Bit Stuck in Cache Control Register**—Applicable to test 2. This error indicates that a bit is stuck-at-fault in the cache control register. The expected and actual data values are printed as optional lines.

- **Error 04, Forced Miss Operation Failed**—Applicable to test 3. Bit 2 of the cache control register does not prevent the cache from allocating a test location. This could be a problem in the cache control gate array or in the hit/miss compare logic.
- **Error 05, Forced Miss with Abort Failed**—Applicable to test 3. Bit 3 did not prevent the cache from allocating when set. Failures of this nature mean the cache cannot be disabled, and all memory references may be allocating cache regardless of the intent of the code being executed. The cache control gate array or the tag compare logic may be at fault.
- **Error 06, Expected Cache Hit Did Not Occur**—Applicable to tests 4, 6, 9, 12, and 14. These tests did not allocate a given test location to the cache as expected, causing a miss condition in the hit/miss register.
- **Error 07, Expected Cache Miss Did Not Occur**—Applicable to tests 7, 9, and 10. Shows a test location not expected to be allocated, or valid, as a hit on access.
- **Error 10, Value in Hit/Miss Register Incorrect**—Applicable to test 5. Indicates the 6-bit value in the hit/miss register was incorrect after a certain sequence of instructions. The expected values, as well as the actual contents of the hit/miss register, are printed as optional lines.
- **Error 11, Write Byte Operation Caused Cache Update**—Applicable to test 6. A byte operation (on a miss) did not cause cache to deallocate the test location. Thus, when the test location was read back, a cache hit resulted.
- **Error 12, Write Byte Did Not Cause Cache Update**—Applicable to test 6. A byte-value did not get written into cache or main memory.
- **Error 13, Cache Failed To Flush Successfully**—Applicable to test 8. When checking cache after a flush command was executed, one or more locations still contained valid data (were detected as cache hits).
- **Error 14, Access with Force Bypass Did Not Cause Invalidate**—Applicable to test 9. The second access to an allocated location, with the force bypass bit (bit 9) set in the control register, did not result in a miss as expected.
- **Error 15, Tag Parity Error Did Not Set**—Applicable to test 10. The diagnostic could not set the tag parity error bit in the memory system error register when faced with an actual tag parity error.
- **Error 16, Abort on Cache Parity Error Did Not Occur**—Applicable to test 11. The cache logic did not abort the instruction under execution when a cache parity error was forced, and the abort bit (bit 7) was set in the control register.
- **Error 17, Unexpected Parity Trap During Abort Test**—Applicable to test 10. Although expected to, cache control bit 0 did not prevent the cache logic from taking a trap on bad parity. The address where the trap occurred is printed as optional information.
- **Error 20, Content of Memory System Error Register Incorrect**—Applicable to test 11. The error bits in the memory system error register (1777744) do not reflect the correct status for the operation under test. The expected and actual content are printed as optional lines.
- **Error 21, Return PC Wrong During Abort/Interrupt Test**—Applicable to test 11. The return PC on the stack is not equal to the value expected during an abort or interrupt operation caused by a cache parity error. The state sequencer gate array is most likely defective.
- **Error 22, Cache Data Parity Bit(s) Did Not Set**—Applicable to test 10. The diagnostic was unable to set the data parity error bit(s) in the memory system error register on a forced parity error. The parity logic may not be detecting parity errors or one of the bits in the memory system error register may be stuck low.

- **Error 23, Interrupt on Parity Error Did Not Occur**—Applicable to test 11. The cache did not interrupt through vector 114 on a forced parity error. The state sequencer or the parity detection logic may be faulty.
- **Error 24, Expected NXM Trap Did Not Occur**—Applicable to test 13. A NXM trap was not detected during an access to location 1777757776. The timeout logic that detects a NXM may be defective, or some problem may exist in the cache data path gate array that prevents it from acting on timeout.
- **Error 25, Parity Error Was Not Blocked By NXM**—Applicable to test 13. When accessing a location expected to result in a NXM, the parity error flag set instead, and a trap occurred through vector 114. The NXM signal may not have been detected by the cache data path gate array.
- **Error 26, Cache Data Miscompare on Word Operation**—Applicable to test 14. A word address in the cache array did not have the correct data when read. This may indicate address line faults or data path faults allowing the location to be rewritten after the test value was placed there. The expected/actual data values are printed as optional lines.
- **Error 27, Cache Data Miscompare on Byte Operation**—Applicable to tests 14 and 15. A location in the cache, when addressed in a byte fashion, did not have the expected data pattern. This may indicate address line faults or data path control faults which allowed overwriting the expected value.
- **Error 30, DMA Write to Memory Did Not Cause Cache To Invalidate**—Applicable to test 12. A DMA write by the RX33 controller to a test location, allocated to cache, still resulted in a hit status after the transfer. The cache has stale data.
- **Error 31, Instruction Still Completed During Abort Condition**—Applicable to test 11. With the abort bit set in the cache control register, an instruction set up to detect a parity error on an operand fetch still finished execution, modifying the destination of the instruction.
- **Error 32, Load Device Error During DMA Test**—Applicable to test 12. The load device subsystem did not respond correctly to the DMA test operation. There may be faults in the load device controller or the interrupt service logic. This message is information only.
- **Error 33, PDR Cache Bypass Failed**—Applicable to test 7. Setting the PDR bypass bit in the PAR/PDR pair under test did not bypass the cache. This points to a MMU or cache data path gate array problem. The PDR number and the CPU execution mode (kernel or user) are printed as optional lines in the error message.
- **Error 34, Tag Store Address Hit Failure**—Applicable to test 16. Changing the value of the tag bits (bits 16:22 of the physical address) still resulted in a hit condition (even though the address should not have compared) forcing a fetch to main memory. There may be a problem in the tag RAMs or the tag compare logic in the cache data path is not working.
- **Error 35, Tag Store Address Miss Failure**—Applicable to test 16. When going through the possible values for the tag bits (16:22 of the physical address), the cache failed to allocate for some combination of the bits. Possible problems are stuck bits in the address lines going to the cache array, bad RAMs in the cache array, or a fault in the tag compare logic.
- **Error 41, Processor Type Is Not J11**—Applicable to test 1. The processor type register does not show the correct value for a J11 chip set. Attempting to run this diagnostic on anything other than a J11 produces this error.

6.4.9 Test Troubleshooting

All of the logic under test is contained on the J11 (P.ioj) module with the exception of the memory used by the diagnostic. Main memory parity errors usually point to the memory module. Because much of the logic tested is buried within the two gate arrays on the module, troubleshooting is often limited to a best-guess replacement of one or both of these gate arrays.

Cache parity errors and data miscompare errors can usually be traced to specific RAMs if proper attention is paid to the data content and address.

For scope loops, the cache test is run with a large number of passes, and Ctrl/O is entered on the console to inhibit error message printout.

Constant hit/miss errors, or tag address hit problems, also may be caused by the tag compare logic, which is separate from the gate arrays and the data path.

6.5 OBIT—Offline Bus Interaction Test

The offline bus interaction test (OBIT) creates control and data bus contention among the requestors in the HSC controller subsystem. The contention is generated by simultaneously testing different portions of the same memory (control and/or data) from different requestors. In the process of testing the memories, the various requestors in the subsystem contend with each other for the use of the control and data buses.

In addition to the bus contention generated by the requestors, I/O control processor interaction can be selected with the program, control, and data memories, with the OCP, and/or with the load device. If I/O control processor interaction is selected, it occurs simultaneously with the bus contention generated by the requestors.

OBIT requires a minimum of two working requestors in order to operate and uses a maximum of nine requestors if they are available. The more requestors available for use by this test, the greater the amount of bus contention. A larger number of requestors makes it easier to isolate failures to a particular source. Also, the run time of this test increases linearly as the number of requestors is increased.

If the OBIT fails, it must first be determined if the failure was caused by an interaction problem. This is determined by running the offline K/P memory test (test memory by K). When the test prompts for parameters, specify the requestor number of the requestor that detected the failure in OBIT. Also specify the same starting and ending addresses displayed with the error report from the bus interaction test. If the requestor also fails the offline K/P memory test, the original problem was not an interaction problem. The problem is localized in the same manner as any ordinary memory failure.

6.5.1 System Requirements

Hardware required to run OBIT is shown in the following list:

- I/O control processor module with HSC boot ROMs
- Memory module
- Working control and data memories
- Load device with at least one working drive
- Terminal connected to I/O control processor console interface
- At least two working requestors (K.sdi, K.sti, or K.ci)

6.5.2 Offline Bus Interaction Test Prerequisites

Booting procedures and testing through successful loading of the offline diagnostics loader program are described in Section 6.1.2 and in Section 6.2.

Due to the sequence of tests that precede the memory test, OBIT assumes the I/O control processor module and the load device are tested and working. OBIT also assumes the control and data memories were previously tested with the offline memory test or the offline K/P memory test, and are working.

6.5.3 Operating Instructions

At the loader prompt ODL>, the operator types the TEST BUS command and OBIT is loaded and started. The test indicates it has been loaded properly by displaying the following:

```
HSC OFL Bus Interaction Test Version nnn
```

where: Version *nnn* is a three-digit version number.

The test then sizes the program, control, and data memories and determines the number of requestors available for testing.

6.5.4 Test Termination

OBIT can be terminated by entering Ctrl/C. OBIT may continue running for a few seconds after it is terminated.

6.5.5 Parameter Entry

After displaying the program name and version, the program, control, and data memories are sized. The bounds of each memory are displayed on the terminal.

NOTE
For any of the OBIT prompts, use the delete key to delete mistyped parameters. If an error in a parameter already terminated with is noted, enter Ctrl/C to return to the offline loader. Then enter START to restart the test from the beginning.

The test prompts for selection of the requestors used for the test, as follows:

```
Use requestor #001, K.ci (Y/N) [Y] ?
```

Answer with a Y if the K.ci should be used. Answer with N if the K.ci should not be used.

At least two working requestors must be used to run the bus contention test because one requestor cannot generate bus contention by itself. The program displays the following error message if less than two requestors remain after the requestors that should be used have been indicated:

```
Not Enough Working Ks for Test
```

Next, the program prompts for the type of I/O control processor interaction desired.

```
P.ioc Memory Interaction Desired (Y/N) [Y] ?
```

Answer the prompt by pressing Return or entering Y if I/O control processor interaction with memory is wanted. Answer with N if I/O Control Processor interaction with memory is not wanted. If the prompt is answered with an N, the following three prompts are skipped. If the prompt is answered with a Return, the following prompts are displayed:

```
Interact with Program memory (Y/N) [Y] ?
Interact with Control memory (Y/N) [Y] ?
Interact with Data memory (Y/N) [Y] ?
```

For each prompt, press Return if the I/O Control Processor is to interact with the specified memory while the requestors are generating contention on the control and data buses. Answer with N if the I/O control processor is not to interact with the specified memory. (If I/O control processor interaction is selected, the I/O control processor interacts with the memory at the same time the requestors are generating control and data bus contention.) The program next prompts for OCP interaction.

```
OCP Interaction Desired (Y/N) [Y] ?
```

If I/O control processor interaction with the OCP is wanted, press Return. If OCP interaction is not wanted, enter N. The test then prompts for load device interaction.

```
Interact with load device (Y/N) [Y] ?
```

If I/O control processor interaction with the load device is wanted, press Return. If such interaction is not wanted, enter N. The program then prompts:

```
# of passes to perform (D) [10000]?
```

Enter a decimal number between 1 and 2,147,483,647 (omitting commas) to specify the number of times the bus interaction test is repeated. Entering 0 causes 10,000 passes of the test. After the number of passes is entered, the bus contention test begins. The test can be aborted at any time by entering Ctrl/C. The test may continue running for a few seconds after Ctrl/C is entered.

After the specified number of passes is completed, the following prompt is displayed:

```
Reuse parameters (Y/N) [Y] ?
```

To repeat the last test specified using the parameters, answer this prompt by entering Y or pressing Return. To cause the test to prompt for new parameters, answer the prompt with N.

Use the delete key to delete mistyped parameters before terminating the entry by pressing Return. If an error in a parameter was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.5.6 Progress Reports

Each time the program completes one full set of bus contention tests, an end-of-pass report is displayed. A pass consists of completing a full set of contention tests, including: control bus tests, data bus tests, and combined control and data bus tests. The end-of-pass message is displayed as follows:

```
End of Pass nnnnnn, xxxxxx errors, yyyyyy total errors.
```

where:
nnnnnn is the decimal count of the number of passes completed.
xxxxxx is the decimal count of the number of errors detected on the current pass.
yyyyyy is the decimal count of the total number of errors detected since the test was initiated.

6.5.7 Test Summary

The moving inversions memory test (MOVI) is used to generate bus contention among the requestors. Each requestor in an HSC controller contains the moving inversions test as part of its microdiagnostic software set. The moving inversions RAM test is used to detect data and addressing problems in dynamic semiconductor memories.

The following are the steps in the moving inversions algorithm:

1. Write 000000 in each location being tested.
2. Read all locations in order from lowest to highest. After reading a location and checking for a 0, rewrite the same location with a 1 in the least significant bit. Then reread the location and verify the write worked correctly.
3. Again, read all locations in order from lowest to highest, checking to see each location contains the data previously written. Then rewrite the data found with a single additional 1 bit and reread to check that the write worked properly.
4. Repeat step 3 until the test pattern consists of a word containing all 1s (pattern 177777).
5. Repeat steps 1 through 4, but this time start at the highest memory address and work down to the lowest each time. However, instead of adding an additional 1, add an additional 0. This changes each memory location from all ones back to all zeros.
6. End of test. All memory is cleared to 000000.

6.5.8 Error Information

Error messages produced by this test conform to the HSC generic diagnostic error message format. Offline bus interaction test error messages are preceded by an OBIT> prompt.

Following is a typical OBIT error message.

```
OBIT>hh:mm T#aaa E#bbb U-000
Memory Test Error
Detected By K.sdi, requestor 006
MA-xxxxxxxx
EXP-yyyyyy
ACT-zzzzzz
< K-error-Summary-Info >
Memory Test Configuration:
K.ci , requestor 001, M.ctl 16000700 -- 16100274
K.sdi ,requestor 006, M.ctl 16100300 -- 16177674
```

where:

hr is the hours since Offline Loader was last booted.
mm is the minutes since Offline Loader was last booted.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-*000* is the unit number.
MA-*xxxxxxxx* is the address of location causing the error.
EXP-*yyyyyy* is the data pattern that was expected.
ACT-*zzzzzz* is the data pattern that was actually found.

Refer to Section 6.5.9 for information on the Requestor Error Summary, and to Section 6.5.10 for information on the Memory Test Configuration.

6.5.9 Requestor Error Summary

When the requestor reports a memory test failure to the I/O control processor, the following information is supplied:

- Address of the failing memory location
- Data expected and data actually found
- Error summary information

The error summary information is supplied as a 3-bit field, including:

- A bit indicating a parity error occurred while reading the location
- A bit indicating an NXM error occurred while accessing the location
- A bit indicating a control bus (CBUS) error occurred while accessing the location

When a memory error report is issued for an error detected by the requestor, the last line of the error report includes a list of the error summary bits that were set, if any.

A CBUS error indicates the requestor asserted an illegal combination of the three CCYCLE lines when accessing control memory. Because these lines were previously tested from the I/O control processor (in the OFL P.ioj/c test), a control bus error is probably caused by a problem with the requestor's drivers that assert the CCYCLE lines.

6.5.10 Memory Test Configuration

The memory test configuration lists each requestor being used for OBIT along with the section of memory each requestor was testing when the failure occurred. The configuration information consists of:

- Type of requestor (K.ci, K.sdi, K.sti, or K.si) and the requestor number
- Memory being tested by the requestor (M.ctl = control memory, M.data = data memory)
- First address of the chunk of memory being tested
- Last address of the chunk of memory being tested

6.5.11 Error Messages

The following list describes the nature of the failure indicated by each error number:

- **Error 000, Memory Test Error**—Indicates one of the requestors detected a memory error in the control or data memories. The following is a sample error report.

```
Memory Test Error
Detected by K.ci, requestor 001
MA -16010234
EXP-000177
ACT-000377
Parity error
Memory Test Configuration:
 K.ci ,requestor 001, M.ctl 16000700 -- 16100274
 K.sdi ,requestor 007, M.ctl 16100300 -- 16177674
```

where:
MA is the 22 bit address of the failing location.
EXP is the data pattern expected by the requestor.
ACT is the data pattern found by the requestor.
Memory Test Configuration: lists the other requestors that were enabled when failure occurred.

This sample error report indicates the K.sdi module detected a memory parity error while reading address 16010234 of control memory (M.ctl). The requestor expected to find the value 000177 in the location but instead found the value 000377. At the time the error occurred, the K.ci in requestor 1 was testing addresses 16000700 through 16100274 of control memory, and the K.sdi in requestor 7 was testing addresses 16100300 through 16177674 of the Control memory.

- **Error 001, K Timed Out During Init**—Displayed when a requestor fails to complete its Init sequence in time. This error usually indicates the specified requestor failed one of its internal microdiagnostics. A sample error report follows:

```
K Timed-out During Init
K.ci , requestor 001, Status = 104
Other Ks Enabled:
  K.sdi, requestor 6
  K.sdi, requestor 7
```

This sample error report indicates the K.ci in Requestor 1 did not finish its initialization diagnostics in the required time. The requestor status displayed with the error report indicates the requestor failed test 4 of its microdiagnostics (1xx in status = failed test xx). Two other requestors were enabled at the time the requestor K.ci timed out, and one of these requestors may be responsible for the timeout.

When the I/O control processor enables the requestor to perform the memory test, the requestor begins its initialization sequence, including execution of certain microdiagnostics. At the end of the requestor's Init sequence, the requestor indicates it found the K control area by complementing a pointer word in control memory. If the requestor fails to complement this pointer word within 50 milliseconds (4.2 seconds for the K.ci) after being enabled, error 001 is reported. The contents of the K status register are displayed with the error report.

- **Error 002, K Timed Out During Test**—Indicates the specified requestor failed to complete its memory test within the expected time. A sample error report follows:

```
K Timed-out During Test
K.sdi, requestor 007, Status = 002
Memory Test Configuration:
K.ci , requestor 1, M.ctl 16000700 -- 16100274
K.sdi, requestor 7, M.ctl 16100300 -- 16177674
```

The sample error report indicates the K.sdi module in Requestor 7 never completed the memory test it was assigned. (Ks are allowed up to 1 minute to complete a memory test.) The memory configuration displayed with the error report shows all Ks testing at the same time the K.ci timed out. In this example, the K.ci in requestor 1 was also testing at the time the K.sdi timed out.

Test timeout failures may be caused by a failure in the requestor that timed out. They may also be caused by a failure in one of the other requestors that was testing at the same time.

- **Error 003, Parity Trap**—Indicates the I/O control processor detected a parity error. The 22-bit address of the location causing the error is displayed as the MA data in the error report, where:

  - MA is the address causing the parity trap.
  - VPC is the virtual PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

The data is lost when a parity trap occurs so no expected or actual data can be displayed.

- **Error 004, NXM Trap**—Indicates the I/O control processor detected a nonexistent memory (NXM) error. An NXM error is caused when no memory responds to a particular address. The MA data in the error report indicates the address which produced the NXM trap. After the trap is reported, the program attempts to restart the test from the beginning. The MA and VPC fields have the same meanings as error 003.

  If this error occurs at a memory address that should be in the memory configuration, the memory in question is not supplying an ACK to the I/O control processor when the specified address is presented on the memory bus. The most probable point of failure is the logic on the memory module that compares addresses on the memory bus with the range of addresses to which the module is to respond. Also, the comparator itself could be faulty or the [C IN, C OUT], [D IN, D OUT], or [P IN, P OUT] lines on the backplane could be installed in error.

- **Error 005, Memory Test Error (P.ioj/c detected)**—Indicates the I/O control processor detected an error while testing program memory. This error can only occur if I/O control processor interaction with program memory is selected. This interaction consists of:

  - A series of PDP-11 instructions that perform read/modify/write (RMW) cycles to selected program memory locations
  - Quick-verify tests of the entire program memory (6 Kwords at a time)

  Error 005 can be caused by cross-talk between the program memory bus and either the control or data bus. It can also be caused by a failure in the program memory logic which inhibits refresh cycles in the middle of a RMW cycle.

- **Error 006, TU58 Synchronization Failure** – This is an HSC50-only error. The TU58 tape drive was unable to properly establish synchronization.

- **Error 007, General TU58 Error**— This is an HSC50-only error. Text is provided with the error message to indicate details about the TU58 tape drive failure.

- **Error 008, TU58 Checksum Error**— This is an HSC50-only error. The data checksum read from the TU58 tape drive did not match the one generated during the read operation.

- **Error 009, TU58 End Packet Error**— This is an HSC50-only error.

- **Error 010 (12 octal), Cache Parity Trap, VPC = xxxxxx**—Can happen during any test. The J11 trapped through the parity vector. The error was caused by the cache.

  NOTE
  Errors 011 through 017 can occur on an HSC controller when load device interaction is enabled.

- **Error 011, RX33 Drive Not Ready**—The drive selected for the operation was not ready. The door may be open or the diskette absent during a READ or POSITION command.

- **Error 012, RX33 CRC Error During Seek**— The RX33 disk drive detected a CRC error during a seek. The RX33 disk drive could not verify position when reading header information from the diskette.

- **Error 013, RX33 Track 0 Not Set on Recalibrate**—A recalibrate (seek to track 0) operation is performed before each block of read operations. The RX33 disk drive did not show correct status after the RECAL command.

- **Error 014, RX33 Seek Timeout**— The RX33 disk drive did not respond by interrupting during a seek.

- **Error 015, RX33 Seek Error**—Sets the seek error bit (bit 4 of the CSR). At the end of a seek operation, the RX33 disk drive was not where it thought it should be.

- **Error 016, RX33 Read Timeout**—Indicates the RX33 disk drive did not interrupt at the end of a READ command.
- **Error 17, RX33 CRC/RNF Error on Read Command**—Can be caused by a soft error or a bad spot(s) on the disk. For informational purposes, the following additional message prints out:

```
First LBN In Transfer = xxxx
```

Where *xxx* is the LBN of the first block in the transfer. The offline interaction bus test performs reads in blocks of four.

6.6 OKTS –Offline K Test Selector

The offline K test selector (OKTS) allows a K to perform an internal microdiagnostic self-test on command. OKTS executes from the P.ioj/c and uses the HSC K control area for instruction. Select the K for testing and the test number of the microdiagnostic test for execution.

6.6.1 System Requirements

The following hardware is required to run OKTS:

- P.ioj/c module with HSC boot ROMs
- Memory module
- A working section of control memory for use as a K control area
- One working load device drive
- A terminal connected to the P.ioj/c console interface

Due to the sequence of tests that precede this test, assume the P.ioj/c, program memory, and load device are working.

6.6.2 Operating Instructions

If the HSC controller is not booted and loaded, refer to Section 6.1.2 and Section 6.2. If the loader prompt ODL> is displayed, follow these steps to start the K test selector:

1. Enter TEST K. The load device drive-in-use LED lights as the test is loaded.
2. Test K indicates it has been loaded properly by displaying the following:

```
HSC OFL K Test Selector Version nnn
```

where: Version *nnn* is a three-digit version number.

3. The test next prompts for parameters.

6.6.3 Test Termination

OKTS can be terminated by entering Ctrl/C.

6.6.4 Parameter Entry

This section gives detailed information on how to enter the test parameters for the OKTS. Items in square brackets are the default value for each particular prompt. If no default is possible, the brackets are empty.

OKTS first prompts:

```
Requestor # of K (1 through 9) [] ?
```

Answer this question with a single digit (1 through 9) that specifies the requestor number of the K to be used. Terminate the response by pressing Return. After the requestor number is supplied, a K control area is located in control memory and tested. This area is required for communicating with the K that will run its microdiagnostics. The test then prompts:

```
Test # (1 through 17) (O) [] ?
```

Legal test numbers are octal numbers between 1 and 17, except for test 5. Test 5 is the K's control and data memory test, which is supported by the OFL K/P memory test. Terminate the test number entry by pressing Return.

OKTS then prompts:

```
# of passes to perform (D) [1] ?
```

Enter a decimal number between 1 and 2147483647 to specify the number of times the memory test should be repeated. (Entering 0, or just pressing Return, results in the performance of one pass.)

The P.ioj/c next instructs the K to perform the selected test, and allows up to 4.2 seconds for the K to complete its test. If the K completes the test within this time, the P.ioj/c displays an end-of-pass message. If the K fails to complete within 4.2 seconds, the P.ioj/c displays a K time-out error (error 009).

The K microdiagnostics are designed to hang when an error is detected, so all failures in the microdiagnostics are reported as time-out errors. The current test may be aborted at any time by entering Ctrl/C.

After the first test has been specified and completed, the following prompt is displayed:

```
Reuse parameters (Y/N) [Y] ?
```

To repeat the last test specified using the parameters, enter Y or press Return. To cause the test to prompt for new parameters, enter N.

Use the delete key to delete mistyped parameters before terminating the entry by pressing Return. If an error in a parameter was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.6.5 Progress Reports

Each time the K completes one full pass through the test specified, an end-of-pass report is displayed. A full pass is defined as:

- The K completes the test with no errors detected.
- The K fails its test, and the P.ioj/c times out.

The end-of-pass message is displayed as follows:

```
End of Pass nnnnnn, xxxxxx Errors, yyyyyy Total Errors
```

where:
nnnnnn is the number of passes.
xxxxxx is the number of errors detected during the current pass.
yyyyyy is the number of errors detected for all passes.

6.6.6 K.ci Path Status Information

Whenever a K.ci is enabled, it runs the CI link test as part of its microdiagnostics. The link test performs loop-back tests on CI paths A and B of the K.ci. To pass the link test, one of the paths must work (one failing path is not a fatal error). The microdiagnostics then return information in the K control area, which specifies which paths worked and how many retries were required. (The test retries 64 times before declaring a failure.)

The offline K test selector reports the CI path status each time the K.ci is initialized. If the link test is selected (K.ci test 11), the path status is reported only after the link test completes. (When the K.ci is enabled, it runs all of its microdiagnostics, including the link test. If the link test is selected, the K.ci runs that test once more.)

The CI path status display indicates which path failed the link test, if any. If both paths fail, the microdiagnostics fail in test 11, and no path status information is displayed. The status display also includes the number of retries required for paths that passed the link test.

6.6.7 Test Summaries

The following is a list of OKTS test summaries.

- **Test 000, Moving Inversions Test**—The moving inversions (MOVI) memory test is used by the P.ioj/c to test a K control area. The K control area is used to pass memory test parameters to the K and to return the results of memory tests to the P.ioj/c. The moving inversions RAM test is used to detect data and addressing problems in dynamic semiconductor memories.

  The following are the steps in the moving inversions algorithm:

  1. Write 000000 in each location being tested.
  2. Read all locations in order from lowest to highest. After reading a location and checking for a 0, rewrite the same location with a single 1 in the least significant bit. Then reread the location and verify the write worked correctly.
  3. Again, read all locations in order from lowest to highest. Check that each location contains the data previously written. Rewrite the data found with a single additional 1 bit. Reread it to verify the write operation worked properly.
  4. Repeat step 3 until the test pattern consists of a word containing all ones (pattern 177777).
  5. Repeat step 3, but this time substitute a single extra 0 each time, instead of a 1.
  6. Continue step 5 until the test pattern consists of a word of all zeros (pattern 000000).
  7. Repeat steps 1 through 6, but this time start at the highest memory address and work down to the lowest each time. This will work each memory location from all zeros to all ones, and back to all zeros.
  8. End of test. All memory is cleared to 000000.

- **Test 001 through test 020, K Microdiagnostics**—Refer to the following four lists for the names of each microdiagnostic. Included in each list is the type of K being used and the failing test number.

  1. K.ci microdiagnostics—The following list shows the test number and name of each of the K.ci microdiagnostics:

     Test 0 — Sequencer test
     Test 1 — ALU test
     Test 2 — Data bus test
     Test 3 — Control bus test
     Test 4 — PROM parity test
     Test 5 — Memory test (unavailable through K test selector)
     Test 6 — RAM test
     Test 7 — PLI interface test
     Test 10 — Packet buffer test
     Test 11 — Link test
     Test 12 — Scratch store test
     Test 13 — WCS moving inversion test
     Test 14 — Scratchpad interaction test
     Test 15 — WCS load
     Test 20 — Init packet search test (unavailable through K test selector.)

  2. K.sdi microdiagnostics—The following list shows the test number and name of each of the K.sdi microdiagnostics:

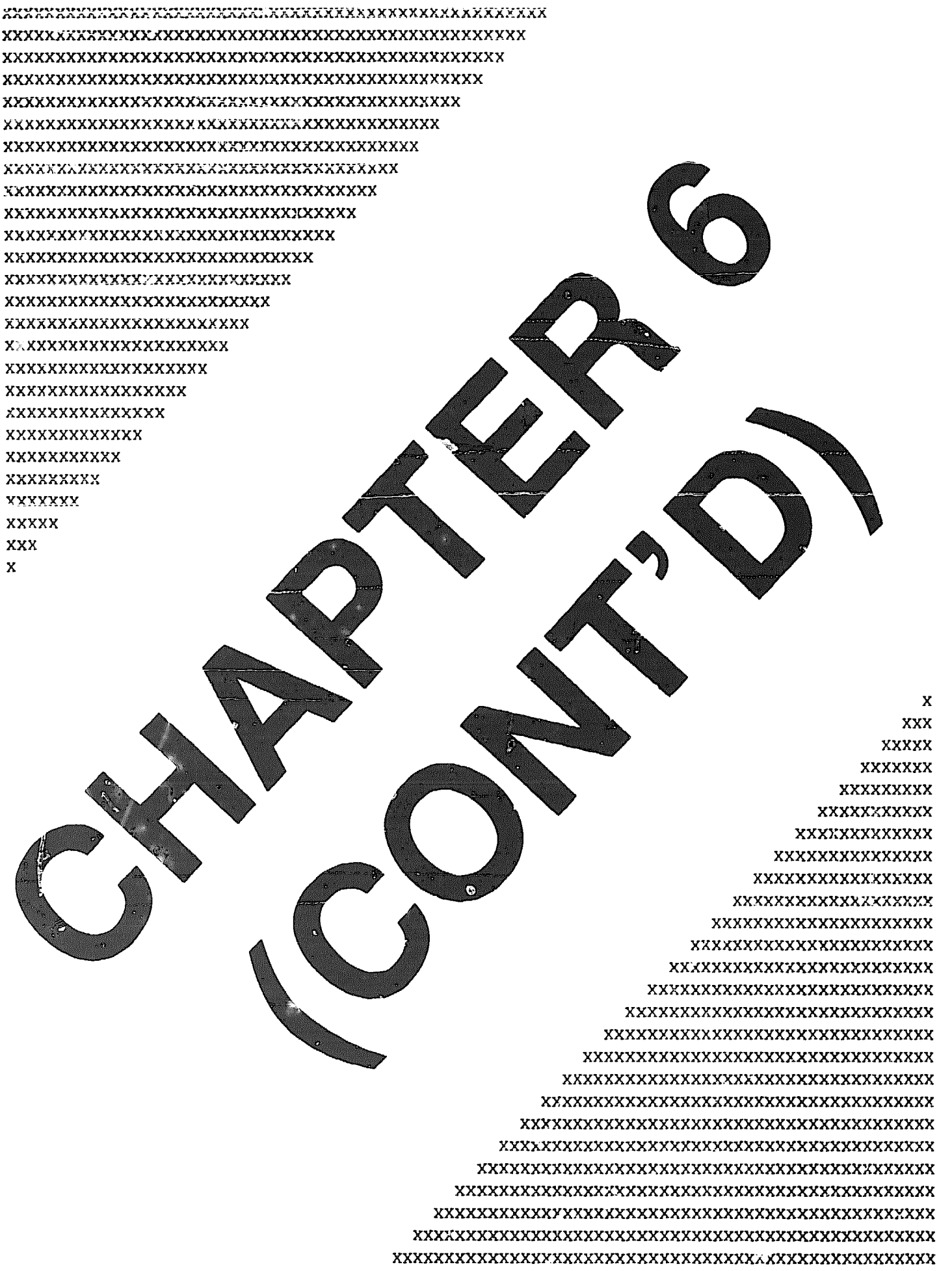
     Test 0 — Sequencer test
     Test 1 — ALU test
     Test 2 — Data bus test
     Test 3 — Control bus test
     Test 4 — PROM parity test
     Test 5 — Memory test (not available through K test selector)
     Test 6 — RAM test
     Test 7 — SERDES/RSGEN test
     Test 10 — Partial SDI interface test
     Test 11 — Control memory access test
     Test 12 — Lock test

  3. K.sti microdiagnostics—The following list shows the test number and name of each of the K.sti microdiagnostics:

     Test 0 — Sequencer test
     Test 1 — ALU test
     Test 2 — Data bus test
     Test 3 — Control bus test
     Test 4 — PROM parity test
     Test 5 — Memory test (not available through K test selector)
     Test 6 — RAM test
     Test 7 — SERDES test
     Test 10 — Partial STI interface test
     Test 11 — Control memory access test
     Test 12 — Lock test

  4. K.si microdiagnostics—The following list shows the test number and name of each of the K.si microdiagnostics:

     Test 0 — 2911 test
     Test 1 — ALU test


CHAPTER 6
(CONT'D)

Test 2 — ROM parity/traps test
Test 3 — Scratchpad test
Test 4 — Data bus test
Test 5 — MOVI for system test
Test 6 — Control bus test
Test 7 — RTS gate array test
Test 10 — SIECL test
Test 11 — Frame test (U ⇒ L)
Test 12 — Frame test (L ⇒ U)
Test 13 — Sector test (U ⇒ L)
Test 14 — Sector test (L ⇒ U)
Test 15 — WCS load/verify test
Test 16 — WCS MOVI test
Test 17 — WCS EDC check
Test 20 — Init packet search test (unavailable through K test selector.)

6.6.8 Error Information

Error messages produced by this test conform to the HSC generic diagnostic error message format. Offline K selector test error messages are preceded by an OKTS> prompt.

A typical OKTS error message format follows:

```
OKTS>hh:mm T#aaa E#bbb U-000
 < Text describing error >
 MA-xxxxxxxx
 EXP-yyyyyy
 ACT-zzzzzz
 < K-Error-Summary-Info >
```

where:
hh is the elapsed hours since last bootstrap.
mm is the elapsed minutes.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-*000* is the unit number.
MA-*xxxxxxxx* is the address of location causing the error.
EXP-*yyyyyy* is the data pattern that was expected.
ACT-*zzzzzz* is the data pattern that was actually found.

6.6.9 Error Messages

Errors detected by OKTS fall into one of three classes:

- Control memory errors occurring when the P.ioj/c is testing the portion of control memory used to communicate with the K. (The P.ioj/c does not test data memory.) Error numbers 000 through 007 are all control memory errors detected by the P.ioj/c. The difference between these errors is the exact step in the memory test where they are detected. The step where an error was detected can be a helpful clue to the cause of the error.
- Failures in a K microdiagnostic detected by a timeout. Error 008 indicates the K failed to initialize properly. Error 009 indicates the K failed the selected microdiagnostic.

- Unexpected traps detected by the Pioj/c (NXM and Parity). Errors 010 and 011 are unexpected trap errors detected by the Pioj/c. Error 010 signifies a parity trap occurred, and error 011 indicates an NXM trap. The reports for unexpected trap errors differ slightly from a data error report since they do not display expected and actual data. Error 012 indicates no working control memory could be found for a K control area. Error 13 is a cache parity trap.

The following list describes the nature of the failure indicated by each error number:

- **Error 000**—Occurs in the moving inversions test when the Pioj/c is testing the K control area at a memory location that did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem (the location was incorrectly addressed and written when some other location was written). At this step in the test, a dual-addressing problem is characterized by:
  - The actual data containing a single additional 1.
  - The additional 1 bit occurring immediately to the left of the left-most 1 in the expected data. For example:

```
EXP=000377, ACT=000777
EXP=077777, ACT=177777
EXP=000000, ACT=000001
```

  For the first example, the location in error was probably written with the pattern 000777 when a lower numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (000377), it contained the next pattern (000777).

  Data errors at this step of the test fall into one of the following classes:
  - The actual and expected data differ by more than one bit:

```
EXP=017777, ACT=017477
```

  - The actual data contains fewer ones than the expected data:

```
EXP=003777, ACT=001777
```

  - The bit in error is not in the bit position immediately to the left of the left-most 1 in the expected data:

```
EXP=000777, ACT=002777
```

- **Error 001**—Occurs in the moving inversions test when the Pioj/c is testing the K control area at a location written with a pattern. Immediately after the write, the location was read and found to contain an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written.
  - A bit was picked up or dropped when the location was read.

If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address is probably defective.

If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably faulty.

If the error occurs in more than one location but the addresses of the failing locations are similar, there could be crosstalk between the memory data and addressing lines. For instance, all failing addresses end with either 2 or 6.

- **Error 002**—Occurs in the moving inversions test when the Ploj/c is testing the K control area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem. (The location was incorrectly addressed and written when some other location was being written.) At this step in the test, a dual-addressing problem is characterized by:

  1. The actual data containing one more 0 than the expected data.
  2. The additional 0 occurring in the same bit position as the left-most bit in the expected data. For example:

     ```
     EXP=003777, ACT=001777
     EXP=000017, ACT=000007
     EXP=177777, ACT=077777
     ```

  In the first example, the location in error was probably written with the pattern 001777 when a lower numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (003777), it contained the next pattern (001777).

  data errors in this step of the moving inversions test fall into one of the following categories:

  - The actual and expected data differ by more than one bit:

    ```
    EXP=177777, ACT=174777
    ```

  - The actual data contains more ones than the expected data:

    ```
    EXP=037777, ACT=077777
    ```

  - The bit in error is not in the same bit position as the left-most bit in the expected data:

    ```
    EXP=001777, ACT=001377
    ```

- **Error 003**—Occurs in the moving inversions test when the Ploj/c is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read and found to contain an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

This error indicates a memory data problem. One of the following hardware failures is indicated:

- A bit was picked up or dropped when the location was written.
- A bit was picked up or dropped when the location was read.

If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address is probably defective.

If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing probably is faulty.

If the error occurs in more than one location but the addresses of the failing locations are similar, there could be crosstalk between the memory data and addressing lines. For instance, all failing addresses end with either 2 or 6.

- **Error 004**—Occurs in the moving inversions test when the P.io/c is testing the K control area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem (the location was incorrectly addressed and written when some other location was written). At this step in the test, a dual-addressing problem is characterized by:
  - The actual data containing a single additional 1.
  - The additional 1 bit occurring immediately to the left of the left-most bit in the expected data. For example:

    ```
    EXP=000377, ACT=000777
    EXP=077777, ACT=177777
    EXP=000000, ACT=000001
    ```

  In the first example, the location in error was probably written with the pattern 000777 when a higher numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (000377), it contained the next pattern (000777). Data errors at this step of the test fall into one of the following classes:
  - The actual and expected data differ by more than one bit:

    ```
    EXP=017777, ACT=017477
    ```

  - The actual data contains fewer ones than the expected data:

    ```
    EXP=003777, ACT=001777
    ```

  - The bit in error is not in the bit position immediately to the left of the left-most bit in the expected data:

    ```
    EXP=000777, ACT=002777
    ```

- **Error 005**—Occurs in the moving inversions test when the P.ioj/c is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read and found to contain an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address is probably defective. If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably faulty.

  If the error occurs in more than one location but the addresses of the failing locations are similar, there could be crosstalk between the memory data and addressing lines. For instance, all failing addresses end with either 2 or 6.
- **Error 006**—Occurs in the moving inversions test when the P.ioj/c is testing the K control area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem. (The location was incorrectly addressed and written when some other location was being written). At this step in the test, a dual-addressing problem is characterized by:
  - The actual data containing one more 0 than the expected data.
  - The additional 0 occurring in the same bit position as the left-most bit in the expected data. For example:

```
EXP=003777, ACT=001777
EXP=000017, ACT=000007
EXP=177777, ACT=077777
```

  In the first example, the location in error was probably written with the pattern 001777 when a higher numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (003777), it contained the next pattern (001777). Data errors in this step of the moving inversions test fall into one of the following categories:
  - The actual and expected data differ by more than one bit:

```
EXP=177777, ACT=174777
```

  - The actual data contains more ones than the expected data:

```
EXP=037777, ACT=077777
```

- The bit in error is not in the same bit position as the left-most bit in the expected data:

```
EXP=001777, ACT=001377
```

- **Error 007**—Occurs in the moving inversions test when the P.ioj/c is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read and found to contain an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written.
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address is probably defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations, and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably faulty.

  If the error occurs in more than one location but the addresses of the failing locations are similar, there could be crosstalk between the memory data and addressing lines. For example, all failing addresses end with either 2 or 6.

- **Error 008**—Indicates the selected K did not complete its Init sequence properly. When the P.ioj/c enables the K to perform a test, the K begins its Init sequence (which includes executing certain microdiagnostics). At the end of the K's Init sequence, the K indicates it found the K control area by complementing a pointer word in the control memory. If the K fails to complement this pointer word within 4.2 seconds of being enabled, error 008 is reported.

  The contents of the K status register are displayed with the error report.

  If this error occurs, make sure the requestor number parameter given matches the actual requestor number of the K.

- **Error 009**—Indicates the K failed the selected microdiagnostic test. This usually indicates a serious hardware problem in the K. The contents of the K status register are displayed with the error report.

- **Error 010**—Indicates the P.ioj/c detected a parity trap. The 22-bit address of the location that caused the trap is displayed as the MA data in the error report, where:
  - MA is the address causing the parity trap.
  - VPC is the virtual PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  Because the data is lost when a parity trap occurs, no expected or actual data is displayed. After the trap is reported, the program attempts to restart the test from the beginning.

- **Error 011**—Indicates the P.ioj/c detected a nonexistent memory trap. A NXM error is caused when no memory responds to a particular address. The MA data in the error report indicates the address which produced the NXM trap. After reporting the trap, the program attempts to restart the test from the beginning, where:
  - MA is the address causing the NXM trap.
  - VPC is the virtual PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  If this error occurs at a memory address that should be in your memory configuration, the memory in question is not supplying an ACK to the P.ioj/c when the specified address is presented on the memory bus. The most probable point of failure is the logic on the memory module that compares addresses on the memory bus to the range of addresses the module is to respond to. Also, the comparator itself could be faulty, or the [C IN, C OUT], [D IN, D OUT], or [P IN, P OUT] lines on the backplane could be in error.
- **Error 012**—Indicates no working Control memory could be found for a K control area. A K control area is required to communicate with a K. The control memory must be repaired before the K test selector can be used to test a K. Use the offline loader command TEST MEMORY to test control memory.
- **Error 013—Cache parity trap, VPC = xxxxxx**—This can happen during any test. The J11/F11 trapped through the parity vector. The error was caused by the cache.

  During the run of the diagnostic, the J11/F11 took a trap through the parity error vector. This is a cache error and the virtual PC at the time of the trap is printed.

6.7 OKPM—Offline K/P Memory Test

The offline K/P memory test (OKPM) tests the HSC control and data memories from a K.sdi, K.sti, K.si, or K.ci. OKPM executes from the I/O control processor and uses the HSC K control area to instruct one of the subsystem requestors to test either the control or data memories.

Select the K to be used, as well as the starting and ending addresses of the section of memory to be tested. The test algorithm used by the K stresses the memories detecting transient errors caused by bus and memory timing problems. Errors are displayed at the console terminal as they occur.

6.7.1 System Requirements

Hardware required by OKPM includes:

- I/O control processor module with HSC boot ROMs
- Memory module
- Load device and controller with at least one working drive
- Terminal connected to I/O control processor console interface
- At least one working K.sdi, K.sti, K.si, or K.ci
- Working control memory for a K control area

6.7.2 Operating Instructions

If the HSC controller is not booted and loaded, refer to Section 6.1.2 and Section 6.2. If these preceding steps are complete, the ODL> prompt is present. Follow these next steps to start OKPM.

1. Enter TEST MEMORY BY K in response to the loader prompt ODL>. The load device LED lights as the memory test is loaded.
2. OKPM indicates it has been loaded properly by displaying the following:

```
HSC OFL K/P Memory Test
```

6.7.3 Test Termination

OKPM can be terminated by entering Ctrl/C. The test may continue running for a few seconds after it is terminated.

6.7.4 Parameter Entry

This section describes the various parameters for OKPM.

NOTE
For any of the OKPM prompts, use the delete key to delete mistyped parameters before terminating the entry by pressing Return. If an error in a parameter entry was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

OKPM first prompts:

```
Requestor # of K (1 through 9) [] ?
```

Answer this question with the single digit (1 through 9) that specifies the requestor number to be used. Terminate the response by pressing Return. After the requestor number is supplied, a K control area is located in control memory and tested. This area is required for communicating with the requestor that performs tests of data and control memory. The test then prompts:

```
Control (0) or data (1) memory [0]?
```

Enter 0 to test control memory or enter 1 to test data memory. Press Return to terminate the response. (pressing just Return selects the control memory test.) The memory test next prompts for the first address to test.

```
First (min=XXXXXXXX) [min] ?
```

Enter the first address to be tested. Addresses are 8 octal digits long. The [min] address displayed is the lowest address that may be entered for the memory chosen. After entering the address, terminate the response by pressing Return. (Pressing just Return causes the first address to default to the [min] address.)

NOTE
Because requestors test control memory in 4-byte units, the lowest 2 bits of the starting address are ignored (treated as binary zeros). For example, if address 16000223 is entered as the first address, the requestor starts testing at address 16000200.

Because requestors test data memory in 64-byte units, the lower 6 bits of the starting address are ignored (treated as binary zeros). For example, if address 14012376 is entered as the first address, the K starts testing at address 14012300.

The test next prompts for the last address to test:

```
Last (max=XXXXXXXX) [] ?
```

Enter the last address to be tested. The max address displayed is the highest address still within the memory chosen. If the system being worked on does not have a fully populated memory, the last address that may be tested is less than the max address displayed. If a last address that exceeds the amount of memory in this system is chosen, the memory test displays a Nonexistent Memory (NXM) error when the test reaches the first address beyond the end of the memory. (Use the offline loader command SIZE to determine the actual last address in a given HSC controller.)

NOTE
Because requestors test control memory in 4-byte units, the lower 2 bits of the ending address are ignored (treated as binary ones). For instance, if address 16023400 is specified as the last address, the K will test up to and including address 16023403.

Because requestors test data memory in 64-byte units, the lower 6 bits of the ending address are ignored (treated as binary ones). If address 14005400 is specified as the last address, the requestor will test up to and including, address 14005477.

Finally, the memory test prompts:

```
# of passes to perform (D) [1] ?
```

Enter a decimal number between 1 and 2147483647 to specify the number of times the memory test is to be repeated. (If 0 or just Return is pressed, the test performs one pass.) The test can be aborted at any time by entering Ctrl/C.

After the first memory test completes, the following prompt is displayed:

```
Reuse parameters (Y/N) [Y] ?
```

To repeat the last test specified using the parameters, enter Y or press Return. To cause the test to prompt for new parameters, enter N.

Use the delete key to delete mistyped parameters before terminating the entry by pressing Return. If an error in a parameter is terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.7.5 Progress Reports

Each time the requestor completes one full pass through the memory specified, an end-of-pass report is displayed. A full pass is defined as:

1. A complete test of the memory specified with no errors detected.
2. Testing the memory specified until an error occurs.

The end-of-pass message is displayed as follows:

```
End of Pass nnnnnn, xxxxxx Errors, yyyyyy Total Errors
```

where:
nnnnnn is the number of passes.
xxxxxx is the number of errors detected during the current pass.
yyyyyy is the number of errors detected for all passes.

6.7.6 Parity Errors

When a parity error occurs, it is desirable to know whether the error was produced by the loss or gain of a data bit or by the loss or gain of a parity bit. When a parity trap occurs in the P.ioc module, the data that was read is discarded by the PDP–11. However, a feature of the P.ioc module allows parity traps to be disabled. Using this feature, a user can determine if a parity error is being caused by a data or parity bit as follows:

1. After a P.ioc module parity trap is reported, enter Ctrl/C to terminate the memory test.
2. Enter another Ctrl/C to return to the OFL diagnostic loader. The loader prompts ODL>.
3. Enter the address of the P.ioc module switch control and status register (SWCSR): Ex 17770042. The contents of this register is displayed as (I) 17770042 *nnnnnn*. Note the string *nnnnnn* for later use in the test.
4. Enter De * *nnnn4n*. The *nnnn4n* represents the previous contents of the register, including a 1 in bit 5. The P.ioc module parity traps are now disabled.
5. Return to the memory test by entering the START command.
6. Rerun the memory test with the original parameters. If the location that previously produced a parity trap then produces a data error, the original parity trap was caused by a data bit problem. The error report indicates the failing bit through the expected and actual data displayed.

   If the location that previously produced a parity trap does not fail again when the memory test is rerun, the original parity trap was caused by an error in one of the parity bits (high or low byte) for that word.

7 Enter Ctrl/C to return to the loader, and reenable parity errors by entering De 17770042 *nnnn0n*. The *nnnn0n* represents original contents of the I/O control processor SWCSR, before parity traps were disabled.

6.7.7 Test Summaries

The following is a summary of individual K/P memory tests.

- **Test 000, moving inversions test from P.ioj/c**—This is the moving inversions (MOVI) memory test used by the I/O control processor to test a requestor control area. The K control area is used to pass memory test parameters to the requestor and to return the results of memory tests to the I/O control processor. The moving inversions RAM test is used to detect data and addressing problems in dynamic semiconductor memories.

  The following are the steps in the moving inversions algorithm:

  1. Write 000000 in each location being tested.
  2. Read all locations in order from lowest to highest. After reading a location and checking for a 0, rewrite the same location with a single 1 in the least significant bit. Then reread the location and verify that the write worked correctly.
  3. Again read all locations in order from lowest to highest. Check each location for the data previously written. Rewrite the data found with a single additional 1 bit. Reread it to verify that the write operation worked properly.
  4. Repeat step 3 until the test pattern consists of a word containing all ones (pattern 177777).
  5. Repeat step 3, but this time substitute a single extra 0 each time instead of 1.
  6. Continue step 5 until the test pattern consists of a word of all zeros (pattern 000000).

7. Repeat steps 1 through 6, but this time start at the highest memory address each time and work down to the lowest. This changes each memory location from all zeros to all ones and back to all zeros.
8. End of test. All memory is cleared to 000000.

- **Test 001, moving inversions test from K**—This is the moving inversions test implemented in the K microcode. The algorithm is identical to that described in the previous test, except steps 5 and 6 are omitted to save time.

  When the requestor detects an error, the remainder of the test is aborted, and the information concerning the error is returned to the I/O control processor through the K control area. The I/O control processor is responsible for displaying the error report.

6.7.8 Error Information

Errors produced by OKPM can be caused by a memory error detected either by the I/O control processor or by the requestor being used to test memory. Errors detected by the I/O control processor occur when the I/O control processor is testing the portion of control memory used to communicate with the K. (The I/O control processor does not test data memory.)

A typical OKPM error message follows:

```
OKPM>hh:mm T#aaa E#bbb U-000
 < Text describing error >
 MA-xxxxxxxx
 EXP-yyyyyy
 ACT-zzzzzz
 < K-Error-Summary-Info >
```

where:
hh is the elapsed hours since last bootstrap.
mm is the elapsed minutes.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-*000* is the unit number.
MA-*xxxxxxxx* is the address of location causing the error.
EXP-*yyyyyy* is the data pattern that was expected.
ACT-*zzzzzz* is the data pattern that was actually found.

6.7.9 Requestor Error Summary

When the requestor reports a memory test failure to the I/O control processor, the following information is supplied:

- Address of the failing memory location
- Data expected and data actually found
- Error summary information

The error summary information is supplied as a 3-bit field, including the following:

- A bit indicating a parity error occurred while reading the location.
- A bit indicating an NXM error occurred while accessing the location.
- A bit indicating a CBUS error occurred while accessing the location.

When a memory error report is issued for an error detected by the K, the last line of the error report includes a list of the error summary bits that were set, if any.

A CBUS error indicates the requestor asserted an illegal combination of the three CCYCLE lines when accessing control memory. As these lines were previously tested from the I/O control processor (in the OFL P.ioj/c test), a control bus error is most likely caused by a problem with the requestor's drivers that assert the CCYCLE lines.

6.7.10 Error Messages

Error messages produced by OKPM can be caused by a memory error detected either by the I/O control processor or by the requestor being used to test memory. Errors detected by the I/O control processor occur when the I/O control processor is testing the portion of control memory used to communicate with the K. (The I/O control processor does not test data memory.)

To determine whether the I/O control processor or the requestor detected an error, examine the second line of the error message. The text begins either with a (P) or a (K). If the text begins with a (P), the I/O control processor detected the error. If the text begins with a (K), the requestor detected the error.

Error numbers 000 through 007 are all control memory errors detected by the I/O control processor. The difference between these errors is the exact step in the memory test where they are detected. The step where an error is detected can be a helpful clue to the cause of the error.

Error 008 indicates the requestor failed to initialize properly.

Error 009 indicates a control or data memory error detected by the K. In addition to the normal error information, the last line of the error report contains a K error summary.

Errors 010 and 011 are unexpected trap errors detected by the I/O control processor. Error 010 signifies a parity trap occurred. Error 011 indicates an NXM trap. The reports for unexpected trap errors differ slightly from a data error report because they do not display expected and actual data.

Error 012 indicates no working control memory could be found for a K Control area. Error 013 indicates a parity trap caused by cache.

The following list describes the nature of the failure indicated by each error number.

- **Error 000**—Occurs in the moving inversions test when the I/O control processor is testing the K Control Area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem (the location was incorrectly addressed and written when some other location was written). At this step in the test, a dual-addressing problem is characterized by:
  - The actual data contains a single additional 1 or,
  - The additional 1 bit occurs immediately to the left of the left-most bit in the expected data, such as:

```
EXP=000377, ACT=000777
EXP=077777, ACT=177777
EXP=000000, ACT=000001
```

  In the first example, the location in error was probably written with the pattern 000777 when a lower numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (000377), it contained the next pattern (000777).

  Data errors at this step of the test fall into one of the following classes:

- The actual and expected data differ by more than one bit:

```
EXP=017777, ACT=017477
```

- The actual data contains fewer ones than the expected data:

```
EXP=003777, ACT=001777
```

- The bit in error is not in the bit position immediately to the left of the left-most bit in the expected data:

```
EXP=000777, ACT=002777
```

- Error 001—Occurs in the moving inversions test when the I/O control processor is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read. It contained an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address probably is defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably the problem.

  If the error occurs in more than one location, but the addresses of the failing locations are similar, crosstalk between the memory data and addressing lines may be present. For example, all failing addresses end with either 2 or 6.

- Error 002—Occurs in the moving inversions test when the I/O control processor is testing the K control area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem. (The location was incorrectly addressed and written when some other location was being written.)

  At this step in the test, a dual-addressing problem is characterized by:
  - The actual data contains one more 0 than the expected data or,
  - The additional 0 occurs in the same bit position as the left-most bit in the expected data, such as:

```
EXP=003777, ACT=001777
EXP=000017, ACT=000007
EXP=177777, ACT=077777
```

In the first example, the location in error was probably written with the pattern 001777 when a lower numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (003777), it contained the next pattern (001777).

Data errors in this step of the moving inversions test fall into one of the following categories:

- The actual and expected data differ by more than one bit:

```
EXP=177777, ACT=174777
```

- The actual data contains more ones than the expected data:

```
EXP=037777, ACT=077777
```

- The bit in error is not in the same bit position as the left-most bit in the expected data:

```
EXP=0017777, ACT=00377
```

- **Error 003**—Occurs in the moving inversions test when the I/O control processor is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read. It contained an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address probably is defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably the problem.

  If the error occurs in more than one location but the addresses of the failing locations are similar, crosstalk between the memory data and addressing lines could be present. For example, all failing addresses end with either 2 or 6.

- **Error 004**—Occurs in the moving inversions test when the I/O control processor is testing the K control area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem (the location was incorrectly addressed and written when some other location was written). At this step in the test, a dual-addressing problem is characterized by:
  - The actual data contains a single additional 1 or,

- The additional 1 bit occurs immediately to the left of the left-most bit in the expected data, such as:

```
EXP=000377, ACT=000777
EXP=077777, ACT=177777
EXP=000000, ACT=000001
```

In the first example, the location in error was probably written with the pattern 000777 when a higher numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (000377), it contained the next pattern (000777).

Data errors at this step of the test fall into one of the following classes:

- The actual and expected data differ by more than one bit:

```
EXP=017777, ACT=017477
```

- The actual data contains fewer ones than the expected data:

```
EXP=003777, ACT=001777
```

- The bit in error is not in the bit position immediately to the left of the left-most bit in the expected data:

```
EXP=000777, ACT=002777
```

- **Error 005**—Occurs in the moving inversions test when the I/O control processor is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read. It contained an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address is probably defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably the problem.

  If the error occurs in more than one location but the addresses of the failing locations are similar, crosstalk between the memory data and addressing lines could be present. For example, all failing addresses end with either 2 or 6.

- **Error 006**—Occurs in the moving inversions test when the I/O control processor is testing the K control area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

This error can be caused by a data error in the address specified or it may indicate a dual-addressing problem. (The location was incorrectly addressed and written when some other location was being written.)

At this step in the test, a dual-addressing problem is characterized by:

- The actual data contains one more 0 than the expected data or,
- The additional 0 occurs in the same bit position as the left-most bit in the expected data, such as:

```
EXP=003777, ACT=001777
EXP=000017, ACT=000007
EXP=177777, ACT=077777
```

In the first example, the location in error was probably written with the pattern 001777 when a higher numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (003777), it contained the next pattern (001777).

Data errors in this step of the moving inversions test fall into one of the following categories:

- The actual and expected data differ by more than one bit:

```
EXP=177777, ACT=174777
```

- The actual data contains more ones than the expected data:

```
EXP=037777, ACT=077777
```

- The bit in error is not in the same bit position as the left-most bit in the expected data:

```
EXP=001777, ACT=001377
```

- **Error 007**—Occurs in the moving inversions test when the I/O control processor is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read. It contained an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address probably is defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably the problem.

  If the error occurs in more than one location but the addresses of the failing locations are similar, crosstalk between the memory data and addressing lines may be present. For example, all failing addresses end with either 2 or 6.

- **Error 008**—Indicates the selected requestor did not complete its Init sequence properly. When the I/O control processor enables the requestor to perform the memory test, the requestor begins its Init sequence (which includes executing certain microdiagnostics). At the end of the requestor's Init sequence, the requestor indicates it found the K control area by complementing a pointer word in control memory. If the requestor fails to complement this pointer word within 50 milliseconds (4.2 seconds for K.ci) of being enabled, error 008 is reported.

  The contents of the K status register are displayed with the error report. If this error occurs, make sure the requestor number parameter given matches the actual requestor number.

- **Error 009**—Indicates a control or data memory error detected by the K, where:
  - MA is the 22-bit address of the failing location.
  - EXP is the data pattern expected by the K.
  - ACT is the data pattern found by the K.

  In addition to the address and the expected/actual data, the K returns an error summary, displayed as the last line of the error report. The error summary information indicates whether the error was caused by a parity error, a NXM error, or a control bus (CBUS) error. If the error was not caused by any of the these, the error summary line does not appear in the error report. Refer to Section 6.7.9 for further information on the error summary.

- **Error 010**—Indicates the I/O control processor detected a parity trap. The 22-bit address of the location that caused the trap is displayed as the MA data in the error report, where:
  - MA is the address causing the parity trap.
  - VPC is the virtual PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  Because the data is lost when a parity trap occurs, no expected or actual data can be displayed. To further localize the problem, disable parity errors and rerun the test as described in Section 6.7.6. If the original failure was in a data bit position, the memory test detects and reports the error, displaying the expected and actual data. This helps to trace the error to a particular address and/or bit position. If no further errors are detected after disabling parity errors, the original failure was in one of the parity bits for the address displayed in the parity trap report.

- **Error 011**—Indicates the I/O control processor detected a NXM trap. A NXM error is caused when no memory responds to a particular address. The MA data in the error report indicates the address that produced the NXM trap. After the trap is reported, the program attempts to restart the test from the beginning, where:
  - MA is the address causing the NXM trap.
  - VPC is the virtual PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  If this error occurs at a memory address that should be in the memory configuration, the memory in question is not supplying an ACK message to the I/O control processor when the specified address is presented on the memory bus. The most probable point of failure is the compare logic on the memory module. This logic compares addresses on the memory bus with the range of addresses to which the module is to respond. The comparator itself could be faulty or the [C IN, C OUT], [D IN, D OUT], or [P IN, P OUT] lines on the backplane could be in error.

- **Error 012**—Indicates no working control memory could be found for a K control area. A K control area is required to communicate with a requestor. Control memory must be repaired before the K/P memory test can be used. Use the offline loader command TEST MEMORY to test the control memory.

- **Error 013, Cache Parity Trap, VPC = xxxxxx**—Indicates the J11 took a trap through the parity error vector during the run of the diagnostic. This is a cache error; the virtual PC at the time of the trap is printed.

6.8 OMEM—Offline Memory Test

The offline memory test (OMEM) exercises the HSC memories, including control, data, or program memory. The operator has the option to select a *quick verify* test or a *comprehensive* test.

The quick verify test writes a data pattern to the memory and reads it back, checking for errors. The test then writes the compliment of the data pattern and reads it back, again checking for errors. The quick verify algorithm detects stuck data and address bits.

The comprehensive test performs a more complete test of selected portions of the memory. This test contains two algorithms: a moving inversions test and a walking ones test. These tests stress the memory to detect transient errors caused by bus and memory timing problems.

In the quick verify and comprehensive tests, errors are reported at the console terminal as they occur. After reporting a data error, or a parity error from a location being tested, testing continues where it left off. If an NXM error occurs during the memory test, testing is restarted from the beginning.

This test also checks the single-bit error correction logic on the M.std4 module.

6.8.1 System Requirements

Following are the OMEM hardware requirements:

- I/O control processor module with HSC boot ROMs
- M.std, M.std2, or M.std4 memory module
- Load device with at least one working drive
- Terminal connected to I/O control processor console interface

An HSC50 offline diagnostic tape or RX33 offline diagnostic floppy is also required to perform this test.

6.8.2 Operating Instructions

If the HSC controller is not booted and loaded, refer to Section 6.1.2 and Section 6.2. If the HSC controller is booted and loaded, the terminal displays an ODL> prompt. At this point, follow these steps to start OMEM:

1. Enter TEST MEMORY in response to the loader prompt ODL>.

   The load device drive-in-use LED lights as OMEM is loaded. OMEM indicates it has been loaded properly by displaying the following:

   ```
   HSC OFL Memory Test, Version Vnnn-nn
   ```

2. OMEM is now ready to accept test parameters.

6.8.3 Test Termination

OMEM can be terminated by entering Ctrl/C.

6.8.4 Parameter Entry

This section describes OMEM parameter entry.

For all prompts, unless otherwise noted, press Return to terminate your entry. For any of the OMEM prompts, use the delete key to delete mistyped parameters before the pressing Return. If an error in a parameter is terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

The test first prompts:

```
Select the QUICK Verify test(0) or the COMPREHENSIVE test(1) (0) ?
```

Enter 0 to select the quick verify test, or 1 to select the comprehensive test. The default is the quick verify test.

If the quick verify test is selected, the next three prompts are skipped and the test displays the *number of passes* prompt.

```
Control(0), Data(1), or Program(2) Memory [0] ?
```

Enter 0 to test control memory. This is the default.

Enter 1 to test data memory.

Enter 2 to test program memory.

The memory test next prompts for the first address to test.

```
First (min=XXXXXXXX) [min] ?
```

Enter the first address to be tested. Addresses are 8 octal digits long. The default is the lowest address that may be entered for the memory chosen.

The test next prompts for the last address to test.

```
Last (max=XXXXXXXX) [] ?
```

Enter the last address to be tested. The max address displayed is the highest address in the memory chosen. If your system does not have a fully populated memory, the last address that may be tested will be less than the displayed max address. In this case, the memory test displays a NXM error when the test reaches the first address beyond the end of the installed memory. Use the offline diagnostic loader command SIZE to determine the actual last address in the installed memory.

The test then prompts:

```
# of passes to perform (D) [1] ?
```

Enter a decimal number between 1 and 2,147,483,647 (omitting commas) to specify the number of times the memory test should be repeated. Entering 0 , or selecting the default, results in one pass.

The OMEM now runs the selected test. After the memory test is completed for the specified number of passes, the following prompt is displayed:

```
Reuse parameters (Y/N) [Y] ?
```

To repeat the last test specified using the parameters, answer this prompt by entering Y or pressing Return. To cause the test to prompt for new parameters, answer the prompt with N.

6.8.5 Progress Reports

A complete pass through the quick verify test is signaled with the following sample output for an HSC controller with the M.std4 memory module installed:

```
M.std4 Logic Test Completed
Quick Verify Pass of CONTROL MEMORY Completed
Quick Verify Pass of DATA MEMORY Completed
Quick Verify Pass of PROGRAM MEMORY Completed
Quick Verify Pass Completed
```

If a comprehensive test of selected memory is chosen, the test consists of one pass through the moving inversions test, and one pass through the walking ones test. The following messages are displayed at the start of testing each 4 kilobyte chunk of memory:

```
MOVING INVERSION : Testing xxxxxxx -- xxxxxxx
WALKING ONEs     : Testing xxxxxxx -- xxxxxxx
```

The displayed range xxxxxxx—xxxxxxx is the octal address range that is tested. This display allows you to see that the test is being performed and allows you to estimate the test duration.

After each complete pass, an end-of-pass message is displayed as follows:

```
End of Pass nnnnnn, xxxxxx Errors, yyyyyy Total Errors
```

where:
nnnnnn is a decimal total of the complete passes made.
xxxxx is the number of errors detected on the current pass.
yyyyyy is number of errors detected during the passes completed so far.

NOTE
A complete pass through the memory test for program memory may take up to eight hours. Unless exhaustive memory testing is required, allow this test to run only until the quick verify pass complete message is displayed. This takes no more than ten minutes.

6.8.6 Parity Errors

When a parity error occurs, it is desirable to know whether the error was produced by the loss or gain of a data bit or by the loss or gain of a parity bit. When a parity trap occurs in the P.ioc module, the data that was read is discarded by the PDP–11. However, a feature of the P.ioc module allows parity traps to be disabled. Using this feature, a user can determine if a parity error is being caused by a data or parity bit as follows:

1. After a P.ioc module parity trap is reported, enter Ctrl/C to terminate the memory test.
2. Enter another Ctrl/C to return to the OFL diagnostic loader. The loader prompts ODL>.
3. Enter the address of the P.ioc module switch control and status register (SWCSR): Ex 17770042. The contents of this register is displayed as (I) 17770042 *nnnnnn*. Note the string nnnnnn for later use in the test.
4. Enter De * *nnnn4n*. The *nnnn4n* represents the previous contents of the register, including a 1 in bit 5. The P.ioc module parity traps are now disabled.
5. Return to the memory test by entering the START command.
6. Rerun the memory test with the original parameters. If the location that previously produced a parity trap then produces a data error, the original parity trap was caused by a data bit problem. The error report indicates the failing bit through the expected and actual data displayed.

If the location that previously produced a parity trap does not fail again when the memory test is rerun, the original parity trap was caused by an error in one of the parity bits (high or low byte) for that word.

7. Enter Ctrl/C to return to the loader, and reenable parity errors by entering De 17770042 *nnnn*0*n*. The *nnnn*0*n* represents original contents of the I/O control processor SWCSR, before parity traps were disabled.

6.8.7 Test Summaries

The following list describes the three algorithms used by OMEM.

- **Test 000, quick verify test**—Quickly detects stuck bits and dual-addressing problems. The algorithm used by the quick verify test is as follows:

```
Write 000000 to each location of the memory

FOR i = First to Last address

IF < location i does not contain 0 >
THEN < display error >

Write low 16 bits of address of location i into
  location i

IF < location i does not contain address i>
THEN < display error >

Write complement of address i to location i

IF < location i does not contain complement >
THEN < display error >

NEXT i
```

- **Test 001, moving inversions test**—Detects data and addressing problems in dynamic semiconductor memories.

  The moving inversions algorithm performs the following:

  1. Write 000000 in each location of the memory.
  2. Read all locations in order from lowest to highest. After reading a location and checking for a 0, rewrite the same location with a single 1 in the least significant bit. Reread the location and verify that the write worked correctly.
  3. Read all locations in order from lowest to highest, checking that each location contains the data previously written. Rewrite the data found with a single additional 1 bit. Reread the location to verify that the write operation worked properly.
  4. Repeat step 3 until the test pattern consists of a word containing all ones (pattern 177777).
  5. Repeat step 3 but this time substitute a single extra 0 each time instead of a 1.
  6. Continue step 5 until the test pattern consists of a word of all zeros (pattern 000000).
  7. Repeat steps 1 through 6, but this time start at the highest memory address each time and work down to the lowest. This test writes each memory location from all zeros to all ones and back to all zeros.
  8. Clear all memory to 000000.

- **Test 002, walking ones test**—An algorithm that stresses semiconductor memories and is effective in locating timing problems on the memory module or on the bus.

  The walking ones algorithm performs the following:

  1. Write all memory to zeros (pattern = 000000).
  2. Check all memory for zeros. Declare error 008 if not 0.
  3. Set TESTADDRESS to the first address to test.
  4. Write 177777 to TESTADDRESS.
  5. Check that all other locations are equal to 000000. Declare error 009 if not equal to 000000.
  6. Check that TESTADDRESS contains 177777. Declare error 010 if not equal to 177777.
  7. Write 000000 to contents of TESTADDRESS.
  8. IF [TESTADDRESS = last address to test] THEN [done testing] ELSE [add 2 to TESTADDRESS, GOTO step 4]

- **Test 003, M.std4 logic verification test** – The Logic Verification test is designed to test out the circuitry that will allow the correction of single bit errors with the M.Std4 memory board.

  The M.std4 logic verification algorithm is as follows:

```
Force single bit parity error
   1) On low nibble
   2) On high nibble

Force error counters to count and verify they
counted correctly.

Check all 3 megabytes of check RAM

Force error correction to use data from check RAM
to correct high nibble.
```

6.8.8 Error Information

OMEM displays the errors detected during execution on the console terminal. All error messages follow the diagnostics generic error message format preceded by an OMEM> prompt.

A typical OMEM error message format follows:

```
OMEM>hh:mm T#aaa E#bbb U-000
 < Text describing error >
 MA-xxxxxxxx
 EXP-yyyyyy
 ACT-zzzzzz
```

where:
hh is the elapsed hours since last bootstrap.
mm is the elapsed minutes
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-*000* is the unit number.
MA-*xxxxxxxx* is the address of location causing the error.
EXP-*yyyyyy* is the data pattern that was expected.
ACT-*zzzzzz* is the data pattern that was actually found.

Parity trap and NXM trap errors do not include expected and actual data.

6.8.9 Error Messages

Error messages produced by OMEM can be classified as either data errors or unexpected traps. Error numbers 000 through 010 are all memory data errors. The only difference between these errors is the exact step in the testing algorithm where they are detected. The step at which a data error occurs can be an important clue to the cause of the error. Errors 000 through 007 are declared in the moving inversions algorithm; errors 008 through 010 are declared in the walking ones algorithm.

Errors 011 and 012 are unexpected trap errors. Error 011 signifies a parity trap and error 012 indicates a nonexistent memory trap. The reports for unexpected trap errors differ slightly from a data error report because they do not display expected and actual data.

Errors 013 and 014 are memory errors discovered during the quick verify test. Error 013 signifies a possible dual-addressing problem, and error 014 signifies a possible data compare error.

Error 015 signifies that the user entered an address outside the memory bounds.

Error 016 signifies a P.ioj/c cache parity trap error.

Errors 020 through 031 are errors generated from M.std4 error-correction testing.

The following list describes the nature of the failure indicated by each error number.

- **Error 000**—Occurs in the moving inversions test, described in Section 6.8.7. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem. In the second case, the location was incorrectly addressed and written when some other location was written. At this step in the test, a dual-addressing problem is characterized by:
  - The actual data contains a single additional 1 or,
  - The additional 1 bit occurs immediately to the left of the left-most bit in the expected data, such as:

```
EXP=000377, ACT=000777
EXP=077777, ACT=177777
EXP=000000, ACT=000001
```

  In the first example, the location in error was probably written with the pattern 000777 when a lower numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (000377), it contained the next pattern (000777).

  Data errors at this step of the test fall into one of the following classes:
  - The actual and expected data differ by more than one bit:

```
EXP=017777, ACT=017477
```

  - The actual data contains fewer ones than the expected data:

```
EXP=003777, ACT=001777
```

- The bit in error is not in the bit position immediately to the left of the left-most 1 in the expected data:

```
EXP=000777, ACT=002777
```

- **Error 001**—Occurs in the moving inversions test (Section 6.8.7). A location was written with a pattern. Immediately after the write, the location was read and found to contain an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written.
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly, but only in a single location, the memory chip containing the failing bit for that address probably is defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing probably is the problem.

  If the error occurs in more than one location but the addresses of the failing locations are similar, crosstalk could exist between the memory data and addressing lines For example, if all failing addresses end with either 2 or 6.

- **Error 002**—Occurs in the moving inversions test (Section 6.8.7). A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem. (The location was incorrectly addressed and written when some other location was being written.)

  At this step in the test, a dual-addressing problem is characterized by:
  - The actual data contains one more 0 than the expected data or,
  - The additional 0 occurs in the same bit position as the left-most 1 in the expected data. For example:

```
EXP=003777, ACT=001777
EXP=000017, ACT=000007
EXP=177777, ACT=077777
```

  In the first example, the location in error was probably written with the pattern 001777 when a lower numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (003777), it contained the next pattern (001777).

  Data errors in this step of the moving inversions test fall into one of the following categories:

- The actual and expected data differ by more than one bit:

  ```
  EXP=177777, ACT=174777
  ```

- The actual data contains more ones than the expected data:

  ```
  EXP=037777, ACT=077777
  ```

- The bit in error is not in the same bit position as the left-most bit in the expected data:

  ```
  EXP=001777, ACT=001377
  ```

- **Error 003**—Occurs in the moving inversions test (Section 6.8.7). A location was written with a pattern. Immediately after the write, the location was read and found to contain an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem that could be caused by one of the following hardware failures:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address is probably defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably the problem.

  If the error occurs in more than one location but the addresses of the failing locations are similar, crosstalk could be present between the memory data and addressing lines. For example, all failing addresses end with either 2 or 6.

- **Error 004**—Occurs in the moving inversions test (Section 6.8.7) when the I/O control processor is testing the K control area. A memory location did not contain the expected pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem. In the latter case, the location was incorrectly addressed and written when some other location was written.

At this step in the test, a dual-addressing problem is characterized by:

- The actual data containing a single additional 1 or,
- The additional 1 bit occurring immediately to the left of the left-most 1 in the expected data. For instance:

```
EXP=000377, ACT=000777
EXP=077777, ACT=177777
EXP=000000, ACT=000001
```

In the first example, the location in error was probably written with the pattern 000777 when a higher numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (000377), it contained the next pattern (000777).

Data errors at this step of the test fall into one of the following classes:

- The actual and expected data differ by more than one bit:

```
EXP=017777, ACT=017477
```

- The actual data contains fewer ones than the expected data:

```
EXP=003777, ACT=001777
```

- The bit in error is not in the bit position immediately to the left of the left-most bit in the expected data:

```
EXP=000777, ACT=002777
```

- **Error 005**—Occurs in the moving inversions test (Section 6.8.7) when the I/O control processor is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read and it contained an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address probably is defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably the problem.

  If the error occurs in more than one location but the addresses of the failing locations are similar, crosstalk between the memory data and addressing lines could be present. For example, all failing addresses end with either 2 or 6.

- **Error 006**—Occurs in the moving inversions test (Section 6.8.7) when the I/O control processor is testing the K control area. A memory location did not contain the expected pattern, where:

- MA is the address of the failing location.
- EXP is the data pattern expected.
- ACT is the data pattern actually found.

This error can be caused by a data error in the address specified, or it may indicate a dual-addressing problem. That is, the location was incorrectly addressed and written when some other location was being written.

At this step in the test, a dual-addressing problem is characterized by:

- The actual data contains one more 0 than the expected data or,
- The additional 0 occurs in the same bit position as the left-most 1 in the expected data. For example:

```
EXP=003777, ACT=001777
EXP=000017, ACT=000007
EXP=177777, ACT=077777
```

In the first example, the location in error was probably written with the pattern 001777 when a higher numbered address was being written with the same pattern. When the location in error was subsequently checked to ensure it still contained the previous pattern (003777), it contained the next pattern (001777).

Data errors in this step of the moving inversions test fall into one of the following categories:

- The actual and expected data differ by more than one bit:

```
EXP=177777, ACT=174777
```

- The actual data contains more ones than the expected data:

```
EXP=037777, ACT=077777
```

- The bit in error is not in the same bit position as the left-most 1 in the expected data:

```
EXP=001777, ACT=001377
```

- **Error 007**—Occurs in the moving inversions test (Section 6.8.7) when the I/O control processor is testing the K control area. A location was written with a pattern. Immediately after the write, the location was read and found to contain an incorrect pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected.
  - ACT is the data pattern actually found.

  This error indicates a memory data problem. One of the following hardware failures is indicated:
  - A bit was picked up or dropped when the location was written or,
  - A bit was picked up or dropped when the location was read.

  If the error occurs repeatedly but only in a single location, the memory chip containing the failing bit for that address probably is defective.

  If the error occurs in many locations, but only occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is defective.

  If the error occurs in many locations and the bits in error are randomly spaced throughout the word, the memory or bus timing is probably the problem.

If the error occurs in more than one location but the addresses of the failing locations are similar, crosstalk may be present between the memory data and addressing lines. For example, all failing addresses end with either 2 or 6.

- **Error 008**—Occurs in the walking ones test (Section 6.8.7). All locations in the memory under test were written with the pattern 000000. Then all locations were read to check that they contained 000000. When the location specified in the error report was read, it did not contain 000000, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected (000000).
  - ACT is the data pattern actually found.

  Because all locations were cleared to 000000 before this error was detected, a dual-addressing problem is unlikely. More likely, a bit was picked up when the word was written or read.

  If the error occurs repeatedly but only in one location, the memory chip containing the bit in error for that address is probably marginal.

  If the error occurs in many locations, but always occurs in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is marginal.

  If errors occur in many locations and the bits in error are randomly spaced throughout the words, the memory or bus timing is probably marginal.

- **Error 009**—Occurs in the walking ones test (Section 6.8.7). One location in the memory under test was written with the pattern 177777 and all the other locations should contain the pattern 000000. While reading to check that all other locations are clear, a location was found containing something other than 000000, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected (000000).
  - ACT is the data pattern actually found.

  This error is either a data error or a dual-addressing error. That is, the location was incorrectly addressed and written when some other location was being written.

  At this step of the test a dual-addressing failure is possible if the actual data is 177777. During this part of the test, one location in the memory was written to 177777. When this write was performed, the failing location may also have been addressed and written with the same data. When the test was checking that all other locations were clear, it found the second location with the pattern 177777. If this is a true dual-addressing problem, the error is repeated on each pass of the test.

  At this step of the test, a data error is probable if the actual data is *not* 177777. Some clues to the possible causes of a data error follow.

  If the error occurs repeatedly but only in a particular bit in a single location, the memory chip that contains the failing bit for that location is defective.

  If errors occur in many locations, but only occur in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is marginal.

  If errors occur in many locations and the bits in error are randomly spaced throughout the words, the memory or bus timing is probably marginal.

- **Error 010**—Occurs in the walking ones test (Section 6.8.7). At this step of the test, one location in the memory under test was set to the pattern 177777 and all other locations were cleared to 000000. After checking that all other locations contain 000000, the location that should contain 177777 was read. It contained some other pattern, where:
  - MA is the address of the failing location.
  - EXP is the data pattern expected (177777).
  - ACT is the data pattern actually found.

  Because only read operations were performed after writing the 177777, a dual-addressing problem is highly improbable.

  If the error occurs repeatedly but only in a particular bit of a single location, the memory chip that holds that bit for the failing location is defective.

  If errors occur in many locations, but only occur in a particular nibble (4-bit field), one of the bus data transceivers for that nibble probably is marginal.

  If errors occur in many locations and the bits in error are randomly spaced throughout the words, the memory or bus timing is probably marginal.

  If errors occur in more than one location but the addresses of the failing locations are similar, crosstalk may be present between the memory data and addressing lines. For example, all failing addresses end in 2 or 4.

- **Error 011**—Indicates a parity trap occurred. The parity trap probably occurred in a location under test but may have been caused by program memory where the memory test itself resides. The MA data in the error report indicates the address of the location causing the parity trap. After reporting the parity trap, the memory test attempts to restart. The error location is reported, where:
  - MA is the address of the location causing the parity trap.
  - VPC is the virtual PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  Because the data is lost when a parity trap occurs, no expected or actual data is displayed. To further localize the problem, disable parity errors and rerun the test. (Refer to Section 6.7.6.)

  If the original failure was in a data bit position, the memory test detects and reports the error, displaying the expected and actual data. This helps trace the error to a particular address and/or bit position. If no further errors are detected after disabling parity errors, the original failure was in one of the parity bits for the address displayed in the parity trap report.

- **Error 012**—Indicates a nonexistent memory (NXM) trap occurred. An NXM error is caused when no memory responds to a particular address. The MA data in the error report identifies the address that produced the NXM trap. After reporting the error, the program attempts to restart testing from the beginning, where:
  - MA is the address being tested at the time the NXM trap occurred.
  - VPC is the PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  This error frequently occurs when trying to test beyond system memory addresses.

  If this error occurs at a memory address that should be within your memory configuration, the memory in question is not supplying an ACK to the I/O control processor when the specified address is presented on the memory bus. The most probable point of failure is the logic on the memory module that compares addresses on the Memory bus with the range of addresses to

which the module is to respond. The comparator itself could be faulty or the [C IN, C OUT], [D IN, D OUT], or [P IN, P OUT] lines on the backplane could be in error.

- **Error 013**—Occurs in the quick verify test. This error may indicate a dual-addressing problem. The quick verify test consists of clearing the entire memory, then writing two patterns to each location and checking that the writes worked properly. Before writing the first pattern to each location, the contents of the location is 0. Error 013 indicates a location contained something besides a 0 before the first pattern was written.

  If the actual data in the error report is 031463(8) or 146314(8), a dual-addressing problem probably is the cause of the error. Dual-addressing occurs when an address lower in memory was written with a test pattern, and the failing location also was written with the same pattern. Dual-addressing problems are normally caused by shorts between memory address bits.

  If the actual data is other than 031463(8) or 146314(8), the problem probably is caused by a memory bit or bits stuck in the 1 state. The first pattern written is 146314(8). The second pattern written is the ones complement of the first pattern, 031463(8).

- **Error 014**—Occurs in the quick verify test. The MA in the error report shows the failing address. The actual data shows the bit or bits that failed.

- **Error 015**—Occurs when an NXM trap occurs as the memory under test is initially being cleared. The last address to test (operator-supplied) exceeds the amount of memory actually installed in the HSC controller or part of the memory under test is not responding. If the NXM occurs at an address that should respond, enter Ctrl/C or Ctrl/Y to return to the offline loader. Use the loader's REPEAT EXAMINE (address that caused trap) to set up a scope loop for isolating the problem.

- **Error 016—Parity Trap, VPC = xxxxxx**—Indicates the J11 took a trap through the parity error vector during the run of the diagnostic, and the error was determined to be from the P.ioj/c module cache. The virtual PC at the time of the trap is printed, where:

  - MA is the address of the location causing the parity trap.
  - VPC is the PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  Because the data is lost when a parity trap occurs, no expected or actual data is displayed. To further localize the problem, disable parity errors and rerun the test. (Refer to Section 6.7.6.)

  If the original failure was in a data bit position, the memory test detects and reports the error, displaying the expected and actual data. This helps trace the error to a particular address and/or bit position. If no further errors are detected after disabling parity errors, the original failure was in one of the parity bits for the address displayed in the parity trap report.

- **Error 020** —Occurs in the M.std4 module logic test. This error indicates that read-modified-write test has failed. The purpose of this test is to ensure that the J–11 chip successfully executes one of the small subset of instructions where a read followed by a write is done as a result of executing one instruction. The J–11 chip has special hardware that ensures the successful execution of these instructions, and this test ensures that the hardware is working. The instruction that is used in this test is test destination and set low bit (TSTSET) instruction.

- **Error 021**—Occurs in the M.std4 module logic test. This error indicates that an any error bit was not set. The M.std4 module logic test attempts to force a single bit error on the low nibble, and the any error bit, which should signify that an error occurred, was not properly set. This indicates problems with the PAL error detection logic.

- **Error 022**—Occurs in the M.std4 module logic test. This error indicates that the correct bits were not set when trying to force a single bit error on the low nibble. The bits that should have been set are the single bit error, the nibble 2 bit error, and the nibble 0 bit error. The error message will display which bits were expected to be set, and which bits were actually set.
- **Error 023**—Occurs in the M.std4 module logic test. This error indicates that the low byte memory error counter is not keeping correct count of the errors that the test is forcing. This error indicates a possible problem with the counter logic.
- **Error 024**—Occurs in the M.std4 module logic test. This error indicates that the high byte memory error counter is not keeping correct count of the errors that the test is forcing. This error indicates a possible problem with the counter logic.
- **Error 025**—Occurs in the M.std4 module logic test. This error indicates that an any error bit was not set. This error occurs when the M.std4 module logic test tries to force a single bit error on the high nibble, and the any error bit, which should signify that an error occurred, is not set.
- **Error 026**—Occurs in the M.std4 module logic test. This error indicates that the correct bits were not set when trying to force a single bit error on the high nibble. The bits that should have been set are the single bit error, the nibble 3 bit error, and the nibble 1 bit error. The error message displays which bits were expected to be set,and which bits were actually set.
- **Error 027**—Occurs in the M.std4 module logic test. This error indicates that the single error and high parity error bits were expected to be set and were not set.
- **Error 028**—Occurs in the M.std4 module logic test. This error indicates that the single error and low parity error bits were expected to be set and were not.
- **Error 029**—Occurs in the M.std4 module logic test. This error indicates that an any error bit was not set. This error occurs when the M.std4 module logic test tries to force the error correction logic to correct a low parity error, and the any error bit, which should signify that an error has occurred, is not set.
- **Error 030**—Occurs in the M.std4 module logic test. This error indicates that the correct bits were not set when trying to force a single bit error on the high nibble. The bits that should have been set are the single bit error, the nibble 3 bit error, and the nibble 1 bit error. The error message displays which bits were expected to be set, and which bits were actually set.
- **Error 031**—Occurs in the M.std4 module logic test. This error indicates that the error correction was forced, but the data pattern was not corrected successfully.

6.9 OMCA—Offline Memory Cache Test

The Offline MCACHE test exercises the M.cache module and call out any problems encountered in the exercise. The operator has the ability to select several options that define the type of testing done on the M.cache module. This test is only run from a J–11 based processor.

OMCA writes a default data pattern of 5252 (octal) to M.cache module memory.

6.9.1 System Requirements

The following hardware is required to run OMCA:

- P.ioj–18 I/O control processor module
- M.std4 memory module
- M.cache module

- RX33 disk drive controller with at least 1 working drive
- Terminal connected to P.ioc's console interface

The following software is required to run OMCA:

- HSC70 offline diagnostic floppy disk

6.9.2 Operating Instructions

If the HSC controller is not booted and loaded, refer to Section 6.1.2 and Section 6.2. If the HSC controller is already booted and displaying the offline loader prompt ODL>, invoke OMCA by entering TEST MCACHE. This loads the OMCA from the media, and transfers control to the diagnostic. At the start, the diagnostic prints out the following string:

```
HSC OFL MCACHE Test Version Vnnn.nn
```

where: Version *nnn* is a three-digit version number.

The test now prompts for parameters.

6.9.3 Test Termination

This test may be aborted at any time by entering Ctrl/C.

6.9.4 Parameter Entry

The OMCA test first prompts:

```
MCACHE SELF-TEST number of passes to perform (D) [0] ?
```

Enter the number of times you want the MCACHE test to run. Each run of the test takes about 10 seconds.

The test then prompts:

```
# of times to check the CACHE Memory chips integrity (D) [0] ?
```

This prompt requests the number of passes to make through the complete M.cache module memory. Each pass consists of writing to selected portions of the memory, reading the data back to cache data memory, and performing data compares.

The test next prompts:

```
Number of passes to perform (D) [1] ?
```

Enter a decimal number between 1 and 2,147,483,647, omitting the commas, to specify the number of times the OMCA test is repeated. Entering 0, or pressing Return, results in 1 pass.

After the specified number of passes have completed, the test prompts:

```
Re-use parameters (Y/N) [Y] ?
```

Answering this prompt by entering Y or pressing Return results in repeating the last test, using the previous parameters. Answering by entering N causes the OMCA to prompt for new parameters.

6.9.5 Progress Reports

The following progress reports are issued by OMCA:

```
Starting MCache Self-Test
Starting Register Tests
Starting CACHE DATA REGISTER Loop Test
Starting CACHE MEMORY 8-Byte Test
Starting Check MCACHE Overwrite Test
Starting XFER Data & REFRESH Memory Test
Starting CACHE Queue Command Verify Test
```

After each complete pass, an end-of-pass message is displayed:

```
End of Pass nnnnnn, xxxxxx Errors, yyyyyy Total Errors
```

The pass count, *nnnnnn*, is a decimal count of the number of complete passes made. The error count, *xxxxxx*, indicates the number of errors detected on the current pass. The total error count, *yyyyyy*, is the running total of the number of errors detected on all passes of the test.

6.9.6 Test Summaries

The following tests are performed by OMCA:

- **Test 001, initial power-on self-test**—This test determines if communications can be established with the M.cache module. The test also checks if the module state machine starts up correctly. Test 001 is automatically invoked when OMCA is started.
- **Test 002, M.cache self test**—This test cycles the M.cache module self test to check out all of the cache and data memory on the M.cache module. The test is similar to Test 001 in that the self-test is invoked, but Test 002 allows multiple invocations of the module self test.
- **Test 003, read M.cache status register** – This test causes the M.cache module status register to be read and checked for a valid return value.
- **Test 004, read M.cache registers**—This test verifies that all M.cache module registers can be read properly.
- **Test 006, read/write loop test**—This test executes an 8-byte data transfer to and from the M.cache module data registers. The test allows the registers to be checked without writing data to the cache memory.
- **Test 006, read/write 8 bytes test**—This test transfers 8 bytes of data from data memory to cache memory. The data is then read back from cache memory to data memory and compared for errors. The 8 bytes used are the diagnostic cache memory blocks that occur once in every 32 kilobytes of cache memory. This test checks all such 8-byte memory blocks.
- **Test 007, data overwrite test**—This test writes one block (512 bytes) of data from data memory to cache memory, then reads the data back and compares for errors. The test also verifies that the M.cache module did not transfer more than 512 bytes of data.
- **Test 008, transfer data & refresh test**—This test writes 14 sectors from data memory to cache memory. It writes to each of the four memory banks, waits five seconds, then reads the data back and compares the data. This test verifies that the M.cache module is transferring data correctly and is performing successful refreshes of the on-board memory.
- **Test 009, queue command verify test**—This test verifies that the internal M.cache module hardware queue can handle and process 16 commands. This is the maximum number of commands allowed in the command queue. This test loads 16 commands, then performs 16 read data commands, verifying only the 16th command's data. This test verifies that the queue is operating properly.

6.9.7 Error Information

A generic message format for all offline diagnostic errors is found in Section 6.2.7. The following section contains information on specific errors associated with OMCA.

A typical OMCA error message follows:

```
OMCA>hh:mm T#aaa E#bbb U-000
 < Text describing error >
 EXP-yyyyyy
 ACT-zzzzzz
```

where:
hh is the elapsed hours since last bootstrap.
mm is the elapsed minutes.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-000 is the unit number.
yyyyyy is the data pattern that was expected. Currently, this data pattern is set at 5252 (octal).
zzzzzz is the data pattern that was actually found.

Parity trap and NXM trap errors do not include expected and actual data.

6.9.8 Error Messages

The following is a list of errors associated with test failures.

- **Error 001, Processor type is NOT a J11** – This error indicates that the test has been invoked on an HSC controller that does not contain a J–11 type processor.
- **Error 002, Time out occurred while reading the MCACHE Status Register**—This error occurs when trying to read the M.cache module status register, indicating that the state machine is in some indeterminate state and cannot synchronize with the command logic. Verify that the M.cache module is correctly seated in the backplane.
- **Error 003, Unexpected value in MCACHE Status Register**—This error occurs when the M.cache module status register is successfully read, but did not contain the expected value.

  This error message will display the expected and actual values for the status register, along with an interpretation of the actual status register data. The text can be any combination of the following:

```
Low Parity
High Parity
Summary
Multi ECC
Comparator
Single ECC
SYNDROME detected MORE than two symbol ECC errors
SYNDROME detected TWO symbol ECC errors
SYNDROME detected ERROR in CHECK BIT NUMBER xx
SYNDROME detected ERROR in DATA BIT NUMBER xx
```

  The following is an example of this error display:

```
OMCA00:10 T#005 E#003 U-000
Unexpected value in MCACHE Status Register
EXP-000377
ACT-012377
Errors Set: Summary Comparator
OMCA00:10
```

- **Error 004, M.cache module not present or not connected correctly**—This error occurs when OMCA is invoked on an HSC controller that does not have an M.cache module installed, or when the installation was performed incorrectly.

6.10 OFLRXE—RX33 Offline Exerciser

OFLRXE is a combined hardware diagnostic and exerciser for the HSC M.std2/M.std4 memory board resident RX33 controller subsystem. Diagnosis of the DMA hardware and diskette controller are provided, as well as a read/write exerciser to provide exercise for the actual drive portion of the subsystem.

OFLRXE is a standalone diagnostic running under the offline diagnostic loader. This loader provides terminal I/O service, time keeping, string conversions, and interrupt handling.

OFLRXE is an 8-Kword program of which approximately half is control code and half is mapped for data buffer transfers.

6.10.1 System Requirements

To run OFLRXE, the HSC controller must be booted from the offline diagnostic diskette. When the system is booted from this media, the ODL> prompt is displayed. Hardware and software requirements are:

- P.ioj module
- M.std2 or M.std4 memory module
- At least one RX33 drive
- One scratch diskette for each drive to be tested (maximum of two)
- Testing of the J11 chip set and cache is assumed if it is turned on
- Two tested 4-Kword partitions of memory

6.10.2 Operating Instructions

If the HSC controller is not booted and loaded, refer to Section 6.1.2 and Section 6.1.3. If the HSC controller is already booted and displaying the offline loader prompt ODL>, proceed as follows:

At the ODL> prompt, invoke OFLRXE by entering TEST RX. This loads the OFLRXE from the media, and transfers control to the diagnostic. At the start, the diagnostic prints out the following string:

```
HSC OFL RX33 Exerciser Version nnn
```

where: Version *nnn* is a three-digit version number.

NOTE
If unable to boot from drive 0, move the diskette to drive 1, try again, or use a backup copy of the offline diagnostics diskette.

6.10.3 Test Termination

OFLRXE can be terminated by entering Ctrl/C or Ctrl/Y. OFLRXE also terminates on expiration of the allotted time or on fatal errors.

6.10.4 Parameter Entry

Following are the OFLRXE modifiable parameters. Drive selection is prompted for by the program in the following manner:

```
Test drive n (Y/N) [Y] ?
```

where: *n* is the drive number (0 or 1)

The default is Y. The prompt repeats for each available diskette on the HSC. The test prompts if the initial write operation is to be performed:

```
Perform initial write on this drive (Y/N) [Y] ?
```

The default is Y. This lays down a background pattern on the entire disk in preparation for the random read/write exerciser. Selecting this option adds 10 minutes of test time per drive.

As soon as the previous prompts have been answered, the program directs placement of a scratch diskette in the selected drive:

```
Insert a scratch diskette in the drive, enter a carriage return to continue.
```

At this point, insert the scratch diskette. The random read/write exercise takes place over the entire surface of the diskette, so be sure the diskette is a scratch one only to be used for the exercise. Run time of the exerciser is user-selectable and is prompted for by the program as follows:

```
# of minutes to exercise (D) [30] ?
```

Enter a number between 1 and 32767. The default is 30 minutes. This 30 minutes starts after the initial patterning of the disk (if selected) so the total test time with two drives and initial patterning is amount of time selected plus 20 minutes. A value of 1440 minutes gives a 24-hour run time for burn-in purposes. The 30-minute default is sufficient for installation use and repair verification.

At the end of the amount of time allotted for the exerciser, the program prompts you by displaying:

```
Reuse parameters (Y/N) [Y] ?
```

To repeat the last test specified using the parameters, answer this prompt by entering Y or pressing Return. To cause the test to prompt for new parameters, answer the prompt with N.

Use the delete key to delete mistyped parameters before terminating the entry by pressing Return. If an error in a parameter was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.10.5 Progress Reports

OFLRXE does not run in a conventional sense. There are no pass-completed messages. Instead, informational messages are displayed indicating what the exerciser is doing. The program has a user-requested status available. If you enter Ctrl/T, the program responds:

```
Number of sectors transferred = xxxxxx, yyyyyy errors.
```

where:
xxxxxx is a 16-digit number of sectors successfully transferred.
yyyyyy is a 6-digit cumulative number of errors detected.

At the end of the initial write test (if selected), the exerciser displays:

```
Initial write completed on drive  000n
```

where: *n* is the drive number (0 or 1).

When the exerciser begins the random read/write phase of the testing, the following message is displayed:

```
Beginning random exercise.
```

The random exerciser is now in progress. It runs for the amount of time requested by you. When the requested time has expired, the program prints the following string:

```
Exerciser completed.
```

The program then returns to the parameter entry routine.

6.10.6 Test Summaries

The following is a summary of OFLRXE tests.

- **Test 1, RX33 controller registers**—Performs stuck-at testing on the RX33 controller registers at 17777400, 17777402, 17777404, and 17777406. A simple walking ones test is performed on each register, except for the CSR register at 177400, which only has the high byte tested.
- **Test 2, interrupt hardware**—Exercises the interrupt hardware on the memory module. The interrupts generated are also tested for the correct priority when they occur.
- **Test 3, DMA logic and counters**—Checks out all of the DMA handshake signals, the data path, and the address path. A special DMA test mode in the controller is used to perform one read or write to/from each memory location loaded in the DMA address registers. Correct incrementing action from the counters is checked. The actual data loaded to memory on a DMA write is checked as well.
- **Test 4, parity logic**—Also uses DMA test mode in addition to the force bad parity function (bit 11 of the CSR) to prove parity errors can be detected, and correct parity is written to memory by the DMA control logic. NXM action also is lumped into this test. Correct handling of NXM errors and correct reporting by the error bit in the CSR is checked.
- **Test 5, verify track counters and registers**—Uses the step function of the diskette controller chip to verify that all cases of the track counter bits internal to the diskette controller chip work as advertised. Step functions are performed for each power of two in the diskette track register (step four times, step eight times more, and so forth). The verify option is set on each step command so the diskette controller reads headers on each track to verify position.
- **Test 6, oscillating seek test**—Performs an oscillating seek test using the algorithm:

```
  oscillating seek test
   begin
incnt = 0
outcnt = 124
while incnt<> outcnt do
  begin
   seek outcnt;
   CHECK_STATUS;
   If outcnt <> rxtrk then error 11
   outcnt =outcnt-1;
   seek incnt;
   CHECK_STATUS;
     if incnt <> rxtrk then error 11
   incnt =incnt + 1;
  end;
  end { oscillating seek test. }
```

  In this manner, all seeks are performed in both directions with all seek counts between <0:77>. Verification is performed on each track to check the step logic.

- **Test 7, sequential read/write test**—Performs the basic patterning of the diskette with a background pattern. This test is user-selected. If selected, this test writes each LBN on the RX33 diskette in ascending order with a unique pattern consisting of the track, sector, and side of that LBN, and then an incrementing-byte pattern for the remainder of the 512-byte sector. Each LBN so written is then read back, and each word is compared to the data that was written. This test takes about 10 minutes per drive.
- **Test 8, random reads/writes**—Does random reads and writes to the selected drives. If both drives are selected for test, operations on each drive are performed in groups of five.

  This test runs until the allotted time for the exercise expires, or the user terminates the test by entering Ctrl/C. The mechanism of this test is as follows:

  A random number is generated. The value of this number determines if the operation is a read or a write, and which LBN is used.

  If the command is READ, the appropriate LBN is read from the disk. The header bytes (0:5) of the data read are then compared against the values expected. The pattern number bytes (6:7) are then compared against a list to see which pattern is to be used to compare the rest of the buffer (10:512).

  If the command is WRITE, other bits of the random number are used to select one of four different patterns to write to the disk. A buffer is then set up with the correct header bytes for the LBN to be written and the correct background data pattern. This buffer is then written out on the diskette.

  Descriptions of the data patterns used are found in the following section.

6.10.7 Data Patterns

Four unique data patterns were selected to give maximum delta of frequency with the modified frequency modulation (MFM) encoding used on the RX33. These patterns are as follows:

Pattern Number	Pattern Value
177400	Incrementing by bytes starting at 2404
11111	000101110001011 binary, 105613 octal
22222	0011001100110011 binary, 031463 octal
33333	0011000010010001 binary, 030221 octal
44444	0000101110001011 binary, 005613 octal

6.10.8 Error Information

A generic message format for all offline diagnostic errors is found in Section 6.2.7. The following section contains information on specific errors associated with OFLRXE.

A typical OFLRXE error message follows:

```
OFLRXE>52:22 T 008 E 010 D 001
 SEEK error detected during positioning operation
 LBN   = 004356
 Track = 000114
 Sector =000007
 Surface = 00000
```

Soft errors, such as seek errors, can build up to a point where a diagnostic defines them as fatal and terminates on a fatal error. The internal bias for soft errors is currently set to 20. When this number is exceeded, the exerciser determines the errors are fatal and terminates.

6.10.9 Error Messages

The following is a list of errors associated with test failures.

- **Error 00, Parity Trap, VPC = xxxxxx**—Applicable to all tests. Occurs at any time during execution of the diagnostic. The virtual PC on the stack is printed to help identify the program area where the error occurred. Both the content of the error address register and the virtual PC are displayed as optional lines. This error terminates the test. The diagnostic returns to the reuse parameters prompt.
- **Error 01, NXM Trap, VPC = xxxxxx**—Applicable to all tests. Causes the diagnostic to return to the reuse parameters prompt. Additional data, such as the virtual PC of the instruction which caused the trap, and the physical address contained in the error address register are printed as optional lines.
- **Error 02, Bit Stuck in Register**—Applicable to test 1. Indicates a stuck-at fault is present in one of the RX33 control registers. The register address and the expected and actual data are printed as optional lines in the error message. If the error is in the low byte, the problem is the diskette controller chip. If the error is in the high byte, the problem is with the MAR register at that address. If more than one register shows the same bit(s) in error, the problem is probably in the bus transceivers.
- **Error 03, Interrupt Occurred Without Enable Set**—Applicable to test 2. Indicates there is a stuck-at fault in the register, or the etch going into the DC003 interrupt control chip. The interrupt enable bit, <13> of the CSR, does not disable interrupts.
- **Error 04, RX33 Interrupt Occurred at Wrong Priority**—Applicable to test 2. Indicates the RX33 interrupt occurred with the priority at 5 or greater. The virtual PC where the interrupt occurred is printed out as an optional line. Using the listing of the program, the priority at the time of the interrupt can be determined.
- **Error 05, Unexpected Interrupt from RX33**—Applicable to all tests. Indicates an unexpected interrupt. An interrupt that occurs at any time when a command to the RX33 disk drive is not in progress is defined as unexpected. The virtual PC where the interrupt occurred is printed as an optional line.
- **Error 06, Track 0 Did Not Set after RECALIBRATE Command**—Applicable to test 5. Indicates the track 0 status bit (bit 2 of the CSR) did not set upon completion of a RECALIBRATE command. The drive may not be sending the signal or the cable to the drive may be faulty.
- **Error 07, RX33 Did Not Interrupt as expected**—Applicable to test 2. Indicates an expected interrupt never occurred. The interrupt control chip (DC003) may be at fault, or the diskette controller chip interrupt signal is stuck at 1. The J11 may be unable to recognize interrupts from the diskette controller or the backplane etches carrying interrupt control signals are open.
- **Error 10, Seek Error Detected during Positioning Operation**—Applicable to tests 5, 6, 7, and 8. Indicates a seek error status (bit 4 of the CSR) was set after a SEEK or RECALIBRATE command. The problem may be in the diskette controller chip or the diskette. If the errors are occurring mostly in test 5 starting with track 0, the problem probably is fundamental; the controller cannot read the diskette at all. If the errors occur in a random fashion, the problem is probably a faulty diskette.

- **Error 11, Current Track Register Incorrect**—Applicable to tests 5 and 6. Indicates the values in the track register of the diskette controller chip are not as expected after a given operation. This problem is probably in the diskette controller chip.
- **Error 12, CRC Error in Header Detected during Position verify**—Applicable to tests 5, 6, 7, and 8. Detects a CRC error when reading a header during a position verify. This error occurs when a valid header has been found and read, but the CRC at the end is incorrect. The problem is probably a faulty diskette. If the controller is able to detect the address and data marks that precede a header (so that it knows that a header is being read), the data separation logic is probably working.
- **Error 13, Processor Type Is Not J11**—Applicable to test 0. Does not contain the value which defines a J11. This error causes the diagnostic to terminate.
- **Error 14, Drive Under Test Is Not Ready**—Applicable to tests 5, 6, 7, and 8. Indicates the diskette drive is sending NOT READY status to the controller. The door may open on the drive, or no diskette is inserted. If these conditions are not the cause of the fault, the ready signal from the drive may be stuck.
- **Error 15, Last Command Did Not Complete**—Applicable to tests 5, 6, 7, and 8. Indicates the last command issued to the diskette controller never interrupted to show completion. This error points to the diskette chip since it occurs after the interrupt logic has already been tested.
- **Error 16, RX33 Header Does Not Compare**—Applicable to tests 7 and 8. The header information written in the data area of a sector is not what it should be for that sector and side, written as part of the data in that sector. This error happens when an undetected positioning error has occurred, either during the read or the write of the sector involved. The LBN, track, sector, and side are displayed as optional lines.
- **Error 17, Record Not Found during Read (Could Also Say Write)**—Applicable to tests 7 and 8. Indicates the controller was unable to find that sector on the current track when attempting to read or write a given sector. Either a misposition occurred, or that sector is unreadable. Because this error occurs after basic read capability has been tested, the most probable culprit is the diskette, with the diskette chip being the next most probable problem point. The LBN, track, sector, and side are displayed as optional lines.
- **Error 20, CRC Error in Data During Read (Could Also Say Write)**—Applicable to tests 7 and 8. Indicates the controller detected a CRC error when reading the desired sector. If the error occurs multiple times in a row for a given sector, the problem is most likely the diskette (or the drive it is installed in). Single errors, when an LBN has this error only once, are soft errors. The LBN, track, sector, and side information is printed as optional lines.
- **Error 21, Lost Data Detected During Read (Could Also Say Write)**—Applicable to tests 7 and 8. Indicates the DMA logic did not service an I/O request of the diskette controller chip in time. There are probably problems in the DMA logic, or stuck-at faults exist in the etch between the controller chip and the DMA logic.
- **Error 23, Invalid Pattern Code in Buffer**—Applicable to test 8. Indicates the data word, defined as the pattern code, that is read from the diskette does not match any of the possible patterns used. It is unlikely the data was read incorrectly from the diskette and not detected as a CRC error. Usually this error occurs when a diskette is not written with the initial data pattern. The LBN, track, sector, and side are displayed as optional lines.
- **Error 24, Drive Is Write-Protected**—Applicable to tests 7 and 8. Indicates the drive is sending write protect status. Either the interface is bad, or the drive is in error (assuming there is not a write-protected diskette in the drive). This error terminates the diagnostic, as a write-protected diskette cannot be written on.

- **Error 25, CRC Error in Header during Read (Could Also Say Write)**—Applicable to tests 7 and 8. Indicates the controller detected bad CRC in the header it was reading as part of a data transfer command. This probably is a diskette error. The LBN, track, sector, and side are displayed as optional lines.
- **Error 26, Data Incorrect after DMA TEST MODE Command**—Applicable to tests 3 and 4. Indicates the memory content after a DMA test mode command was not correct. There are either stuck-at faults in the DMA registers, or the transfer did not happen at all (that is, the memory is unchanged). This is a fundamental error in the diskette logic; the diagnostic terminates after detecting it.
- **Error 27, Data Compare Error**—Applicable to tests 7 and 8. Indicates a manual check of data read by the diskette turned up an error. Either the transfer did not complete, an intermittent error occurred in the data or address path, or what was written on the disk was written incorrectly. The LBN, track, sector, and side are displayed as optional lines.
- **Error 30, RX33 Detected Parity Error during Read (Could Also Say Write)**—Applicable to tests 7 and 8. Indicates the RX33 disk drive detected a parity error when doing a DMA read from memory. Either program memory is bad or the parity logic on the controller is in error.
- **Error 31, RX33 Detected NXM during Read (Could Also Say Write)**—Applicable to tests 7 and 8. Indicates the RX33 disk drive detected a NXM during a DMA operation. Either the DMA address was loaded wrong and pointed to a nonexistent location, or the handshake logic on the memory module is in error.
- **Error 32, RX33 MAR Value Incorrect after DMA Transfer**—Applicable to test 3. Indicates the value of the MAR address counters was in error after a DMA test operation. The problem is probably in the counters or the etch associated with them. The expected and actual data are printed out as optional lines.
- **Error 33, Parity Error Was Not Forced in Main Memory**—Applicable to test 4. Indicates a write to program memory with bad parity set (bit 11 of the CSR) did not result in bad parity in memory. There is either a stuck-at fault in the parity logic or the operation never wrote memory in the first place.
- **Error 34, Parity Error Did Not Set in CSR**—Applicable to test 4. Indicates a DMA read of a location with known bad parity did not set the parity error bit (bit 15 of the CSR). Either the data was never read or there is a stuck-at fault in the parity logic.
- **Error 35, NXM Did Not Set in CSR**—Applicable to test 4. Indicates a DMA read of a location expected to give a NXM did not set NXM in the CSR. Look for stuck-at faults in the NXM detection logic.
- **Error 36, Parity Error Set Along with NXM in CSR**—Applicable to test 4. Indicates both the parity error and the NXM error set simultaneously in the CSR. On a NXM error, the parity error should not set. Check for stuck-at faults in the NXM/parity error logic.
- **Error 37, Cache Parity Error, VPC = xxxxxx**—Applicable to all tests. Indicates the J11 took a trap through the parity error vector, a cache error during the run of the diagnostic. The virtual PC at the time of the trap is printed.

6.11 ORFT—Offline Refresh Test

The offline memory refresh test (ORFT) finds memory problems related to refresh. Patterns are written to memory and then checked after waiting 1 minute. Three separate patterns are used to test each memory bit (including parity bits) in both the 1 and 0 states. All three HSC memories are tested (program, Control, and data), although only the program and Control memories require refreshing. Tests of data memory are included because some static RAM failures resemble refresh problems.

ORFT can find problems in the memories not detected by the normal memory tests. ORFT is not intended to be run on memories that fail the normal memory tests.

6.11.1 System Requirements

The following hardware is required to run ORFT:

- I/O control processor module with HSC boot ROMs
- Memory module that passes the offline memory test and/or the offline K/P memory test
- HSC load device with at least one working drive
- Terminal connected to I/O control processor console interface

ORFT assumes the HSC memories pass both the offline memory test and the offline K/P memory test. In addition, ORFT assumes the memories are working except for the refresh circuitry.

6.11.2 Operating Instructions

If the HSC controller is not booted and loaded, refer to Section 6.1.2, and Section 6.2. If the HSC controller is already booted and displaying the offline loader prompt ODL>, enter **TEST REFRESH** in response to the prompt ODL>. ORFT indicates it is loaded properly by displaying the following:

```
HSC OFL Memory Refresh Test Version nnn
```

where: Version *nnn* is a three-digit version number.

The refresh test now prompts for parameters.

6.11.3 Test Termination

ORFT can be terminated by entering Ctrl/C.

6.11.4 Parameter Entry

This section describes the prompts for the ORFT parameters.

NOTE
For any of the ORFT prompts, use the delete key to delete mistyped parameters before pressing Return. If an error in a parameter already terminated with Return is noted, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

ORFT first prompts with:

```
# of passes to perform (D) [1] ?
```

Enter a decimal number between 1 and 2,147,483,647 (omitting commas) to specify the number of times the refresh test is to be repeated. Entering a 0 or pressing Return results in one pass. After selection of the number of passes the test begins. The test can be aborted at any time by entering Ctrl/C. Each pass of the test requires three minutes to complete.

After the refresh test completes, the following prompt is diplayed:

```
Reuse parameters (Y/N) [Y] ?
```

To repeat the last test specified using the parameters, answer this prompt by entering Y or pressing Return. To cause the test to prompt for new parameters, answer the prompt with N.

Use the delete key to delete mistyped parameters before terminating the entry by pressing Return. If an error in a parameter was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.11.5 Progress Reports

Each time the refresh test completes one full pass, an end-of-pass report is displayed. Each pass of the test requires three minutes to complete. The end-of-pass message is displayed as follows:

```
End of Pass nnnnnn, xxxxxx Errors, yyyyyy Total Errors
```

where:
nnnnnn is a decimal total of the complete passes made.
xxxxxx is the number of errors detected on the current pass.
yyyyyy is number of errors detected during the passes completed so far.

6.11.6 Test Summaries

The following are the ORFT test summaries.

- **Test 01, pattern 177777**—Fills the memories with the pattern 177777. This sets all data bits and also sets the upper and lower byte parity bits. The entire control and data memories are filled with the pattern. All of program memory not occupied by the refresh test and the offline loader is also filled with the pattern. After filling the memories, the program delays for one minute, then each memory location is read and checked for the pattern. Any errors detected are reported on the terminal.
- **Test 02, pattern 000000**—Fills the memories with the pattern 000000. This clears all data bits and sets the upper and lower byte parity bits. The entire control and data memories are filled with the pattern. All of program memory not occupied by the refresh test and the offline loader is also filled with the pattern. After filling the memories, the program delays for one minute, then each memory location is read and checked for the pattern. Any errors detected are reported on the terminal.
- **Test 03, pattern 100001**—Fills the memories with the pattern 100001. This sets data bits 0 and 15 and clears data bits 1 through 14. Both parity bits are also cleared. The entire control and data memories are filled with the pattern. All of program memory not occupied by the refresh test and the offline loader is also filled with the pattern. After filling the memories, the program delays for one minute, then each memory location is read and checked for the pattern. Any errors detected are reported on the terminal.

6.11.7 Error Information

All error messages produced by ORFT conform to the HSC diagnostic error message format (refer to Section 6.2.7). Following is a typical ORFT error message.

```
ORFT>hh:mm T#aaa E#bbb U-000
 < Text describing error >
 MA-xxxxxxxx
 EXP-yyyyyy
 ACT-zzzzzz
```

where:
hh is the elapsed hours since last bootstrap.
mm is the elapsed minutes.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.

U-*000* is the unit number.
MA-*xxxxxxx* is the address of location causing the error.
EXP-*yyyyyy* is the data pattern that was expected.
ACT-*zzzzzz* is the data pattern that was actually found.

6.11.8 Error Messages

The following list describes the nature of the failure indicated by each error number.

- **Error 01**—Indicates the test detected a parity error when reading the pattern from the indicated location. The expected and actual data are included in the error report. This error indicates a data bit or parity bit was not refreshed (assuming the memory in question passed the offline memory test). If the expected and actual data are the same, one of the parity bits was not refreshed.
- **Error 02**—Indicates the test detected a data compare error when reading the pattern from the indicated location. The expected and actual data are displayed in the error report. Note: a parity error did not occur so more than 1 bit must have failed to refresh.
- **Error 03**—Indicates the I/O control processor detected a parity error. The 22-bit address of the location that caused the trap is displayed as the MA data in the error report, where:
  - MA is the address causing the parity trap.
  - VPC is the virtual PC of the memory test at the time the trap occurred. Reference this address in the listing to locate the area of the test where the error occurred.

  Because the data is lost when a parity trap occurs, no expected or actual data can be displayed. The parity error occurred within the program itself, not within the memory being tested. After the trap is reported, the program attempts to restart the test from the beginning.
- **Error 04**—Indicates the I/O control processor detected a NXM trap. An NXM error is caused when no memory responds to a particular address. The MA data in the error report indicates the address that produced the NXM trap. After the trap is reported, the program attempts to restart the test from the beginning. (The MA and VPC fields have the same meanings as those in error 03.)

  If this error is at a memory address that should be in the memory configuration, the memory in question is not supplying an ACK to the I/O control processor when the specified address is presented on the Memory bus. The most probable point of failure is the logic on the memory module that compares addresses on the Memory bus with the range of addresses to which the module is to respond. The comparator itself could be faulty or the [C IN, C OUT], [D IN, D OUT], or [P IN, P OUT] lines on the backplane could be in error.
- **Error 05, Cache Parity Trap, VCP = xxxxxx**—Indicates the J11 took a trap through the parity error vector during the run of the diagnostic. This is a cache error. The virtual PC at the time of the trap is printed.

6.12 OOCP—Offline Operator Control Panel (OCP) Test

OOCP checks the operation of the HSC indicators and switches. Testing includes the five OCP indicators and switches, the State LED, the Secure/Enable switch, and the enable LED.

This section includes troubleshooting procedures for localizing faults detected by this test.

6.12.1 System Requirements

The following hardware is required to run OOCP:

- I/O control processor module with HSC boot ROMs
- Memory module
- HSC load device with at least one working drive
- Terminal connected to I/O control processor console interface
- OCP

Due to the sequence of tests that precede this test, it is safe to assume the I/O control processor module, program memory, and HSC load device are tested and working.

6.12.2 Operating Instructions

If the HSC controller is not booted and loaded, refer to Section 6.1.2, and Section 6.2. If the HSC controller is already booted and displaying the offline loader prompt ODL>, proceed as follows:

Enter TEST OCP in response to the ODL> prompt. The HSC load device in motion LED is ON.

The test indicates it is loaded properly by displaying the following message:

```
HSC OFL OCP Test Version nnn
```

where: Version *nnn* is a three-digit version number.

6.12.3 Test Termination

The test may be aborted at any time by entering Ctrl/C.

6.12.4 Parameter Entry

OOCP first checks the position of the Secure/Enable switch through a bit in the I/O control processor control and status register (address 17770040). If the switch is in the SECURE position, the following prompt is displayed. Otherwise, OOCP skips to the next prompt.

```
Put Secure/Enable switch into enable position
```

If the Secure/Enable switch is in the ENABLE position and the above prompt is displayed anyway, a problem is indicated with the bit in the I/O control processor CSR that monitors the Secure/Enable switch. Refer to the troubleshooting procedures in Section 6.12.8. The program waits until the Secure/Enable switch is changed to the ENABLE position and displays the following message:

```
(Enable LED is lit, State LED is blinking)
```

Check to verify the enable LED is lit and the OCP State LED is blinking. There are two State LEDs: one is to the left of the Init switch on the HSC OCP, and the other is located on the I/O control processor module (the fourth LED from the bottom of the rightmost module in the HSC card cage). If either LED is not blinking, refer to the troubleshooting procedures in Section 6.12.8. The test next prompts for a indicator test.

```
Press Fault (all OCP lamps should light) (Y/N) [Y] ?
```

Press the fault indicator and observe that all OCP indicators light. If none of the indicators light, a problem may be present in the indicator test logic on the OCP assembly. If all indicators light properly, enter a carriage return to continue the test. If the indicator test fails, replace the OCP.

Next, the program checks that all OCP switches are OFF (out position). If any switch bits in the I/O control processor switch/display register read as ones (ON), the program lights the indicators for those switches and prompts:

```
Put all lit switches in OFF (out) position (Y/N) [Y] ?
```

If the fault or Init indicators are lit (nonlocking switches), a problem exists with the wiring in those switches or with their respective bits in the switch/display register. Replace the OCP.

Otherwise, press all lit switches to release their locks and press return. If the message repeats and one or more indicators remain lit even though the switches are OFF (out position), refer to the troubleshooting procedures in Section 6.12.8.

The program then tests each of the OCP switches, one at a time. A switch lights and the following prompt is displayed:

```
Press and release the lit switch
```

Press the switch that is lit. The program allows about 1 second for the switch to be released after it is pressed and then continues to the next prompt. If the program fails to respond when a switch is pressed, refer to the troubleshooting procedures in Section 6.12.8. For those switches that lock in the ON position (Online switch and the two unmarked switches), the program prompts:

```
Press and release the lit switch again
```

Press the switch again to return it to the OFF (out) position. If the Online switch or either of the unmarked switches fails to lock in the ON position, the switch is defective, and the OCP should be replaced.

After the OCP switch tests are complete, several features of the Secure/Enable switch are tested. The program begins these tests by prompting:

```
Put Secure/Enable switch into secure position
```

The program waits until the Secure/Enable switch is in the proper position before continuing. If the program fails to respond when the switch is moved to the SECURE position, refer to the troubleshooting procedures in Section 6.12.8. When the program detects the switch is in the SECURE position, it prompts with:

```
(Enable LED should turn off)
```

Ensure the enable LED is off. If this LED fails to turn off when the switch is in the SECURE position, a short or wiring problem is probable.

Next, the program prompts:

```
Press Init (HSC should not re-boot) (Y/N) [Y] ?
```

Press the Init switch. When the Secure/Enable switch is in the secure position, pressing the Init switch has no effect. (Do not press any other switch or an error message results.) If the HSC controller starts to perform a bootstrap (Init indicator turns on and green LED on I/O control processor turns off), the Secure/Enable switch is not disabling the action of the Init switch. After pressing the Init switch, press Return to continue. The test responds with the following prompt:

```
Press terminal break key (HSC should not halt) (Y/N) [Y] ?
```

Press the break key as directed. When in secure mode, the break key does not cause the J11/F11 processor to halt (enter ODT). If the terminal displays the @ character when break is pressed, the Secure/Enable switch is not disabling the action of the break key. Refer to the troubleshooting procedures in Section 6.12.8.

NOTE
Newer I/O control processor modules do not use the break key to enter ODT. Use the SETSHO command SET ODT REBOOT and then enter Ctrl/P to get the ODT prompt. The prompt for these modules is an asterisk (*).

After pressing the break key, press Return to continue the test. The final prompt of the test is:

```
Put Secure/Enable switch into enable position.
```

The test waits until the Secure/Enable switch is returned to the ENABLE position. At that point the test terminates and returns to the offline loader.

To repeat the last test specified using the parameters, answer this prompt by entering Y or pressing Return. To cause the test to prompt for new parameters, answer the prompt with N.

Use the delete key to delete mistyped parameters before terminating the entry with Return. If an error in a parameter was terminated with Return, enter Ctrl/C to return to the initial prompt and re-enter all parameters.

6.12.5 Test Summaries

The following sections summarize test 000 through test 009.

- **Test 000, observe enable and State LEDs**—Performed by the operator, because the program cannot tell whether the enable or State LEDs are lit. If the enable LED is off, a wiring problem may be the cause (LED not connected to power/ground source) or the LED itself may be faulty.

  If the State LED on the OCP fails to blink, check the State LED on the I/O control processor module (fourth LED from the bottom of the rightmost module in the HSC card cage). If neither State LED is blinking, the problem probably is caused by the bit in the I/O Control Processor CSR register that controls the State LED (refer to Section 6.12.8.4). If one of the State LEDs is blinking but the other is not, the nonblinking LED probably is wired wrong or is faulty.

- **Test 001, lamp test through Fault switch**—Performs an automatic indicator test. When the Fault switch is pressed, all indicators light and remain lit until the switch is released.

  If none of the indicators light when the Fault switch is pressed, the problem is probably in the indicator test circuitry on the OCP assembly. It is possible all indicators are defective or they are not installed. Replace the OCP.

  If some indicators light when fault is pressed but others do not, replace the OCP.

- **Test 002, check all switches OFF**—Reads the I/O control processor switch/display register to see if any of the switch bits read as ON (switch bit is a 1). If the bit for any switch reads as ON, the corresponding indicator is lit and the program prompts to turn off any switch that is lit. The program will not proceed until all switch bits read as OFF.

  If a indicator remains ON, even though the corresponding switch is OFF (out position), the switch is either wired incorrectly or the bit in the I/O control processor switch/display register for that switch is faulty. Refer to Section 6.12.8.1 to localize the problem.

- **Test 003, Fault switch**—Directs pressing the lit Fault switch. The program then monitors the switch bits in the I/O control processor switch/display register and waits for the Fault switch bit to set. If any other switch bit sets, an error is reported and the program terminates.

  If pressing the Fault switch has no effect, one of the following could be the cause:

  - The Fault switch is broken.
  - The Fault switch is not properly wired.
  - The Fault switch bit in the I/O control processor CSR cannot be set.

Refer to the troubleshooting procedures in Section 6.12.8.

If pressing the Fault switch results in an error message, refer to Section 6.12.7.

- **Test 004, Online switch**—Directs pressing the lit Online switch. The program then monitors the switch bits in the I/O control processor switch/display register and waits for the Online switch bit to set. If any other switch bit sets, an error is reported and the program is terminated.

  If pressing the Online switch has no effect, one of the following could be the cause:

  - The Online switch is broken.
  - The Online switch is not properly wired.
  - The Online switch bit in the I/O control processor CSR cannot be set.

  Refer to the troubleshooting procedures in Section 6.12.8.

  If pressing the Online switch results in an error message, refer to Section 6.12.7.

- **Test 005, first unmarked switch**—Directs pressing the lit first unmarked switch. The program then monitors the switch bits in the I/O control processor switch/display register and waits for the first unmarked switch bit to set. If any other switch bit sets, an error is reported and the program is terminated.

  If pressing the first unmarked switch has no effect, one of the following could be the cause:

  - The first unmarked switch is broken.
  - The first unmarked switch is not properly wired.
  - The first unmarked switch bit in the I/O control processor CSR cannot be set.

  Refer to the troubleshooting procedures in Section 6.12.8.

  If pressing the first unmarked switch results in an error message, refer to Section 6.12.7.

- **Test 006, second unmarked switch**—Directs pressing the lit second unmarked switch. The program then monitors the switch bits in the I/O control processor switch/display register and waits for the second unmarked switch bit to set. If any other switch bit sets, an error is reported and the program terminates.

  If pressing the second unmarked switch has no effect, one of the following could be the cause:

  - The second unmarked switch is broken.
  - the second unmarked switch is not properly wired.
  - The second unmarked switch bit in the I/O control processor CSR cannot be set.

  Refer to the troubleshooting procedures in Section 6.12.8.

  If pressing the second unmarked switch results in an error message, refer to Section 6.12.7.

- **Test 007, enable LED off**—Begins with a prompt to put the Secure/Enable switch into the SECURE position. The program waits until bit 15 of the I/O control processor control and status register reads as a 0, indicating the switch is in the SECURE position. Then the program tells the operator to observe that the enable LED is OFF.

  If the enable LED fails to turn off when the switch is in the secure position, replace the OCP.

- **Test 008, Init switch in secure mode**—Checks that the Init switch has no effect when the Secure/Enable switch is in the SECURE position. The test prompts for the Init switch to be pressed while the program monitors the switch bits in the I/O control processor switch/display register. Monitoring ensures that pressing the Init switch does not cause any switch bits to set.

If pressing the Init switch causes the HSC controller to reboot, the secure position of the Secure/Enable switch is not disabling the Init switch. Replace the OCP.

If pressing the Init switch causes one of the switch bits in the switch/display register to set, an error message is displayed. Refer to Section 6.12.7 for further information.

- **Test 009, break key in secure mode**—Checks if the terminal break key has no effect when the Secure/Enable switch is in the SECURE position. (Normally the break key causes the I/O control processor J11/F11 CPU to halt and enter ODT.) The prompt is to press the break key and to observe if the HSC controller does not halt.

  If pressing the break key causes the terminal to print an @ symbol, the SECURE position of the Secure/Enable switch is not disabling break from halting the J11/F11 CPU.

  NOTE
  Newer I/O control processor modules do not use the break key to enter ODT. Use the SETSHO command SET ODT REBOOT and then enter Ctrl/P to get the ODT prompt. The prompt for these modules is an asterisk (*).

6.12.6 Error Information

All error messages produced by OOCP conform to the HSC diagnostic error message format (refer to Section 6.2.7). A typical OOCP error message follows:

```
OOCP>hh:mm T#aaa E#bbb U-000
 < Text describing error >
 MA-xxxxxxxx
 EXP-yyyyyy
 ACT-zzzzzz
```

where:
hh is the elapsed hours since last bootstrap.
mm is the elapsed minutes.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-*000* is the unit number.
MA-*xxxxxxxx* is the address of location causing the error.
EXP-*yyyyyy* is the data pattern that was expected.
ACT-*zzzzzz* is the data pattern that was actually found.

6.12.7 Error Messages

The following list describes the nature of the failure indicated by each error number.

- **Error 000, wrong bit set**—Occurs when the test detects a switch bit other than the switch bit being tested set in the I/O control processor switch/display register. This error can be caused by:
  - The operator pressing the wrong switch.
  - A short causing an additional switch bit to set along with the expected bit.
  - A wiring error causing the wrong bit to set when a switch is pressed.

  The media address (MA) field of the error report gives the address of the I/O control processor switch/display register. The expected and actual data in the error report show the switch bit the program expected to find set and the bit or bits that actually were set.

If the expected and actual data each consist of only one bit, the failure was caused by either the operator pressing the wrong switch or by a wiring error. If the actual data consists of two or more set bits, a short between switches is likely. Refer to the troubleshooting procedures in Section 6.12.8.

- **Error 001, bit set when Init is pressed** – Occurs when the Init switch is pressed while the HSC controller is in the secure mode (test 008). This error can be caused by one of the following:
  - Pressing some switch other than the Init switch.
  - Pressing the Init switch, causing a switch bit in the I/O control processor switch/display register to set.

  The media address (MA) field of the error report gives the address of the I/O control processor switch display register. The expected data is always 0 (no bit is expected to set). The actual data shows the bit or bits that read as a 1 when the Init switch was pressed. Refer to the troubleshooting procedures in Section 6.12.8.

6.12.8 Troubleshooting Registers and Displays through ODT

The following paragraphs and layouts are included to assist you with troubleshooting.

6.12.8.1 Switch Check through ODT

To check the operation of an HSC controller switch, follow this procedure:

1. With the Secure/Enable switch in the ENABLE position, press the terminal Break key. The I/O control processor J11/F11 CPU halts and displays an @ symbol.

   NOTE
   Newer I/O control processor modules do not use the break key to enter ODT. Use the SETSHO command SET ODT REBOOT and then enter Ctrl/P to get the ODT prompt. The prompt for these modules is an asterisk (*).

2. Enter: 17770042/ and press Return.

   The contents of address 17770042 (the I/O control processor switch display register) are displayed in octal. Refer to the layout of the switch display register in Figure 6–1 to locate the switch bits.

   Each bit is in the 1 state when the associated switch is ON (pressed in).

3. Press Return.
4. Enter a slash (/) to re-examine the switch display register.
5. To restart the offline loader (or the diagnostic that was interrupted), press Return, then enter a P.

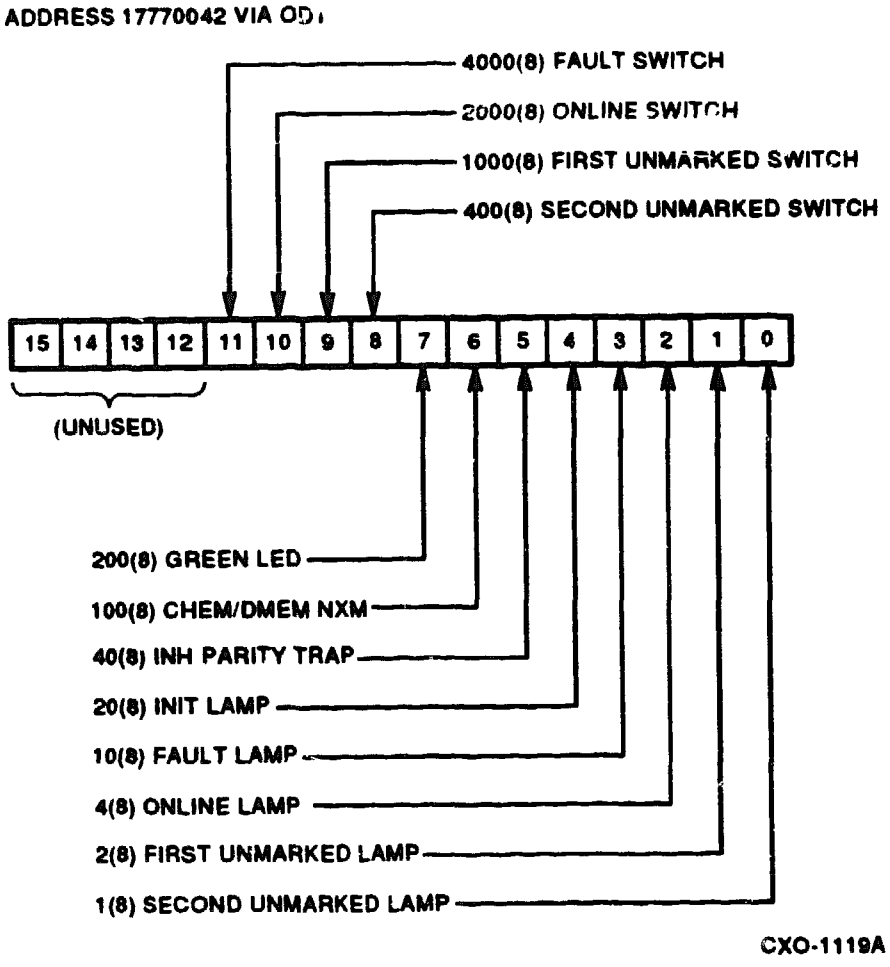


Figure 6–1 P.IoJ Switch Display Register Layout

Using this method, the switch bits of the switch/display register can be monitored when various switches are in the ON or OFF position.

6.12.8.2 Lamp Bit Check

To check the operation of the lamp control bits in the I/O control processor switch/display register, use the following method:

1. With the Secure/Enable switch in the ENABLE position, press the terminal Break key.

   The I/O control processor J11/F11 CPU halts and displays an @ symbol.

   NOTE
   Newer I/O control processor modules do not use the break key to enter ODT. Use the SETSHO command SET ODT REBOOT and then enter Ctrl/P to get the ODT prompt. The prompt for these modules is an asterisk (*).

2. Enter 17770042 and press Return.

   The contents of the switch/display register are displayed in octal.

3. Use Figure 6–1 to locate the bits controlling the OCP indicators.

   When a lamp bit is set, the corresponding indicator lights.

4. To light a indicator, enter the octal value that corresponds to the proper indicator, then press Return. The indicator lights.
5. Enter a slash (/) to re-examine the contents of the switch/display register.
6. Press Return to restart the offline loader (or the diagnostic that was interrupted), then enter a P.

Using this method, various indicators can be manually enabled or disabled.

6.12.8.3 Secure/Enable Switch Check

To manually check the operation of the secure/enable bit in the I/O control processor control and status register, use the following procedure. Using this method, the secure/enable bit in the I/O control processor CSR can be checked with the Secure/Enable switch in both positions.

1. With the Secure/Enable switch in the ENABLE position, press the terminal Break key. (If the HSC controller is stuck in the secure mode, this method cannot be used because break is disabled.) The I/O control processor J11/F11 CPU halts and displays an @ symbol.

   NOTE
   Newer I/O control processor modules do not use the break key to enter ODT. Use the SETSHO command SET ODT REBOOT and then enter Ctrl/P to get the ODT prompt. The prompt for these modules is an asterisk (*).

2. Enter 17770040 and press Return. The content of the I/O control processor control and status register is displayed in octal. Figure 6–2 identifies the various bits of this register.

   When the Secure/Enable switch is in the ENABLE position, the contents of the register is 1xxxxx. When in the secure position, the contents is 0xxxxx.

3. Press Return and then enter a slash (/) to re-examine the register.
4. Press Return, then enter a P to restart the offline loader (or the diagnostic that was interrupted).

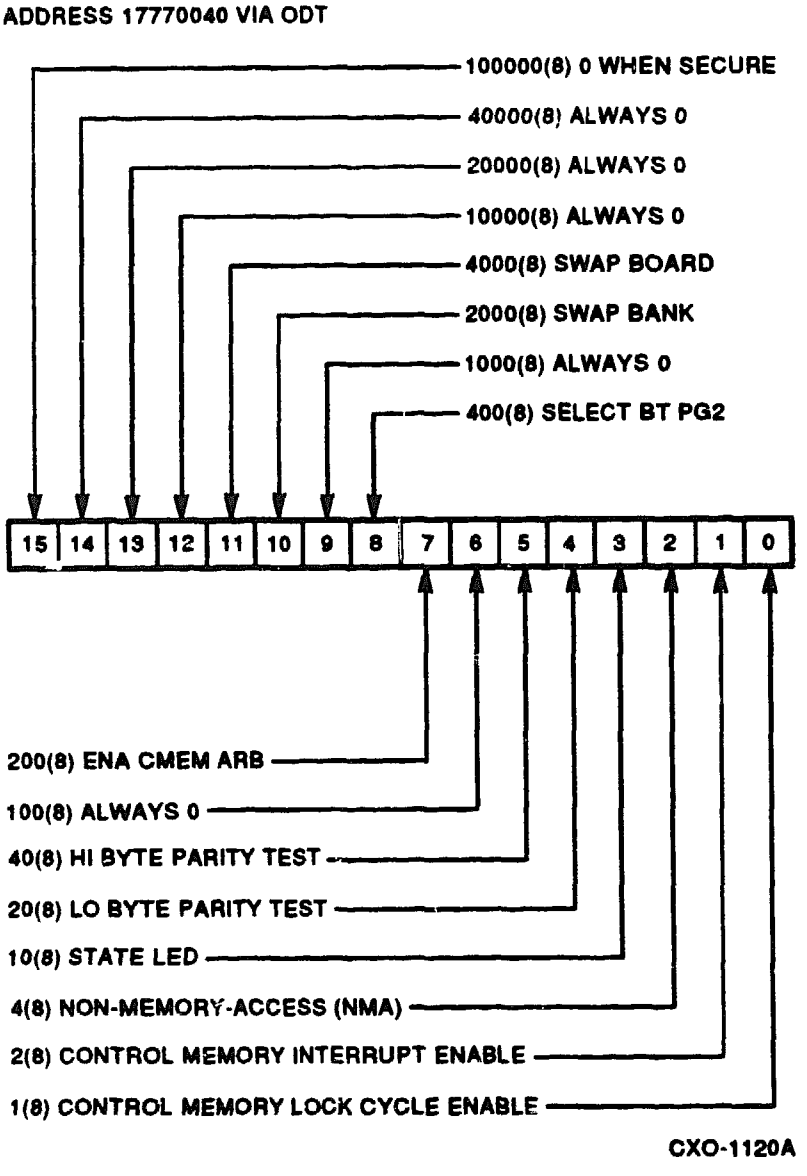


Figure 6–2 P.Ioj Control and Status Register Layout

6.12.8.4 State LED Check

There are two State LEDs in the HSC. One is on the OCP, far left. The other State LED is on the I/O control processor module (rightmost module in the HSC card cage, fourth LED from the bottom of the module). Both LEDs are controlled by a bit in the I/O control processor control and status register (refer to Figure 6–2 for a layout of this register). To manually control the State LED, use the following procedure:

1. With the Secure/Enable switch in the ENABLE position, press the terminal break key.

   The I/O control processor J11/F11 CPU halts and displays an @ symbol.

   NOTE
   Newer I/O control processor modules do not use the break key to enter ODT. Use the SETSHO command SET ODT REBOOT and then enter Ctrl/P to get the ODT prompt. The prompt for these modules is an asterisk (*).

2. Enter 17770040/ and press Return.

   The contents of the control and status register are then displayed in octal.

3. Use Figure 6–2 to find the octal value corresponding to the State LED.

4. To light the State LED, enter the octal value corresponding to the State LED, followed by Return. To extinguish the State LED, put a 0 in the same bit position and press Return.

   CAUTION
   Bit 7 of the I/O control processor CSR must be set to allow the HSC Ks to access control memory. The setting of other bits in the CSR can result in side effects. Be careful not to set any bits except the State LED bit and leave bit 7 set when done.

5. Enter a slash (/) to re-examine the contents of the I/O control processor CSR.

6. To restart the offline loader (or the diagnostic that was interrupted), press Return, then enter a P.

6.13 OCSL—Offline Control Store Loader

The offline K WCS control store loader (OCSL) allows the HSC controller to load any module with a loadable WCS control store area with program information from a .WCS file on the boot media. Modules that can be loaded with OCSL include the K.pli2 port processor module, and the 4- and 8-port K.si data channel modules. A 4-port K.si module can be configured as either a disk or tape data channel for this test.

The WCS command is used to load and execute OCSL.

6.13.1 System Requirements

The following system resources are required to run OOCP:

- P.ioj/c module with HSC boot ROMs
- Memory module
- Working control and data memories
- One working load device drive with .WCS file or files mounted
- Console terminal connected to P.ioj/c console interface
- One or more WCS-loadable modules installed in the HSC backplane

6.13.2 Operating Instructions

If the HSC controller is not booted and running the offline loader, necessary instructions are found in Section 6.1.2 and in Section 6.2. At the Diagnostic Loader prompt (ODL>), use the following procedure to start OCSL:

1. Enter the WCS command. The load device drive-in-use LED lights as OCSL is loaded.

2. When OCSL has successfully loaded it displays the following message:

```
HSC OFL Control Store Loader      Version V600
```

3. OCSL is now ready to accept test parameters.

6.13.3 Test Termination

The test may be aborted at any time by entering Ctrl/C. This returns you to the offline diagnostic loader prompt, ODL>.

6.13.4 Parameter Entry

This section describes the procedure for entering test parameters for OCSL. Parameters given enclosed in square brackets ([ ]) are the default value for each prompt. If no default is possible, the brackets are displayed empty.

The first prompt is for the requestors to test:

```
List of requestors to load (1,2,3,...,8,9 or *) []?
```

This prompt can be answered with a single requestor number, a series of requestor numbers delimited by commas, or with a single wildcard character (*).

If you enter multiple requestors delimited by commas, OCSL attempts to load all requestor numbers listed with the desired WCS code. If you answer with the wildcard character, OCSL attempts to load all requestors. Should a particular requestor not accept the load, due to module failure or inablility to load WCS code, and error message is displayed. OCSL then moves on to attempt loading any other requestors specified.

OCSL then prompts:

```
WCS files available: KSDISI.WCS KSTISI.WCS K8DISK.WCS KCIFC2.WCS
WCS file to use [KSDISI.WCS] ?
```

Answer this prompt with the filename of the WCS image to be loaded into the requestors listed in response to the first prompt. An error is displayed if the filename does not conform to the standard filename specification formats. The default is KSDISI.WCS, which is the code that configures the requestor as a 4-port K.si disk data channel. To configure the 4-port K.si as a tape data channel, enter KSTISI.WCS. The file K8DISK.WCS is used to configure the 8-port K.si disk data channel, and the file KCIFC2.WCS is used to configure the K.ci2 module. OCSL now loads the specified requestors. Requestors that do not accept the load because of either failure or inablility to load the WCS code are reported on the HSC console and the loader moves on to load the other specified requestors.

After all specified requestors are have been addressed, OCSL prompts:

```
Load other requestors (Y/N) [N] ?
```

Valid responses to this question are the single characters Y, N, or a default response, all followed by a Return. Entering N or pressing Return to select the default returns to the ODL> prompt. A Y response begins the test again with the "List of requestors to load" prompt.

6.13.5 Test Summaries

OCSL does not have any specific tests. The program reads the specified WCS file from the media into control and data memory, then loads the file to the selected requestor.

6.13.6 Error Information

All error messages produced by OCSL conform to the HSC diagnostic error message format (refer to Section 6.2.7). A typical OCSL error message follows:

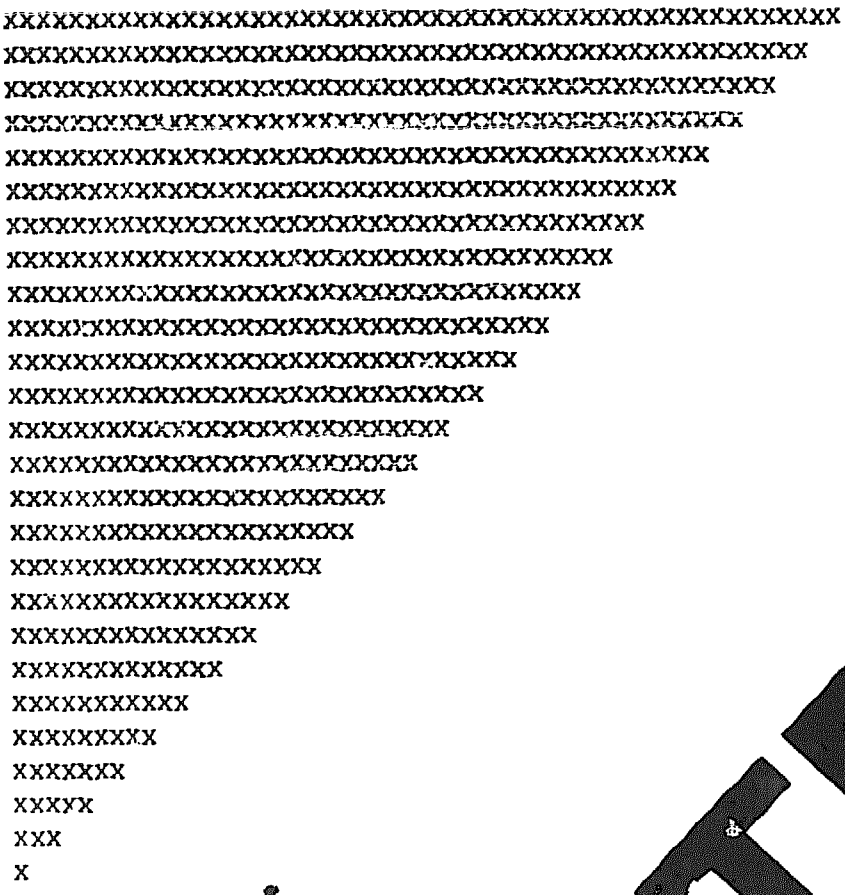
```
OBIT>hh:mm T#aaa E#bbb U-000
K failed during WCS load
```

where:
hh is the elapsed hours since last boot.
mm is the elapsed minutes.
aaa is the decimal number denoting test.
bbb is the decimal number denoting the error detected.
U-*000* is the unit number

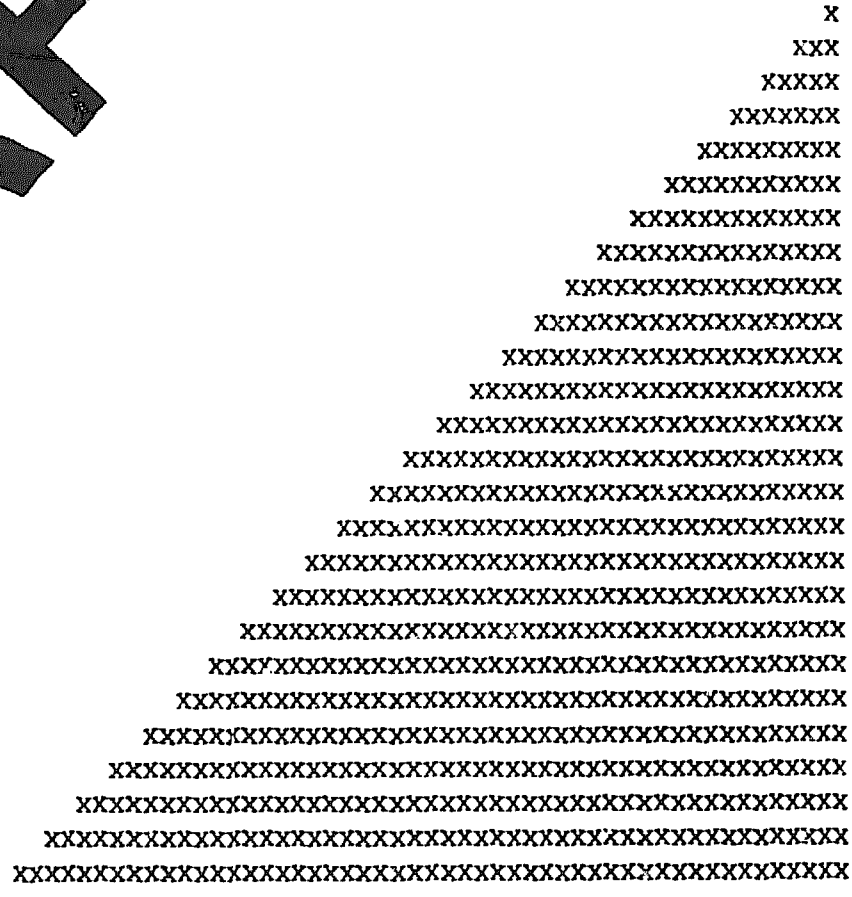
6.13.7 Error Messages

The following list describes the nature of the failure indicated by each error number.

- **Error 00, Parity trap, VPC = xxxxxx**—Applicable to all tests. Occurs at any time during execution of the diagnostic. The virtual PC on the stack is printed to help identify the program area where the error occurred. Both the content of the error address register and the virtual PC are displayed as optional lines. This error terminates the test. The diagnostic returns to the reuse parameters prompt.
- **Error 01, NXM trap, VPC = xxxxxx**—Applicable to all tests. Causes the diagnostic to return to the reuse parameters prompt. Additional data, such as the virtual PC of the instruction which caused the trap, and the physical address contained in the error address register are printed as optional lines.
- **Error 02, Cache parity error, VPC = xxxxxx** – Applicable to all tests. Indicates the J11 took a trap through the parity error vector, a cache error during the run of the diagnostic. The virtual PC at the time of the trap is printed.
- **Error 03, Requested file not found** –Occurs when the WCS file specified by the user cannot be found on the media. The user must be sure to input the full file name, with extension.
- **Error 05, K timed out during INIT** –Occurs when the K requestor timed out while running its initialization code.
- **Error 06, K does not support WCS**—Occurs when the requested K requestor does not support loading of WCS code. An example of this would be if a K.ci were selected for downline loading, instead of a K.ci2.
- **Error 07, K failed during WCS load**—An error on the K requestor has occurred while WCS code was being downloaded to it.



CHAPTER 7



7
Utilities

7.1 Introduction

This chapter contains the information required to run the following offline utilities:

- DKUTIL — Offline Disk Utility
- VERIFY — Offline Disk Verify Utility
- FORMAT — Offline Disk Formatter Utility
- PATCH — Offline Load Media Modification Utility

The HSC controller must be in the command mode before running the offline utilities. Enter Ctrl/Y to get the command prompt.

Topics covered in this chapter include initiating the utility, using commands, and interpreting error messages. These HSC utilities are interactive and therefore are prompt oriented. Note that prompt information displayed in square brackets is the default.

Refer to the *HSC Controller User Guide* for information on other HSC utilities that are not documented in this manual.

7.2 DKUTIL — Offline Disk Utility

DKUTIL is a general utility for displaying disk structures and disk data. Unlike some other utilities, DKUTIL is a command language interpreter. It is intended for use in debugging utilities, diagnostics, error recovery, and bad block replacement. DKUTIL has become a general utility for displaying disk structure and data.

Initially, the program goes into command mode. The user must then issue a GET command to obtain the unit to which other commands are to be applied. DKUTIL then returns to the command mode, prompting for a command, executing it, and prompting for another command. DKUTIL is terminated by entering Ctrl/C, Ctrl/Y, Ctrl/Z, or the EXIT command.

7.2.1 Starting DKUTIL

DKUTIL is started with the standard CRONIC command syntax RUN DKUTIL.UTL. It immediately enters the command mode. A drive must be acquired and brought online before any other commands can be executed. Enter GET D*nnn* at the DKUTIL prompt to acquire the drive and bring it online.

```
DKUTIL> GET Dnnn [Return]
```

The format for specifying the drive is a D followed by the unit number. If the drive parameter is omitted, DKUTIL defaults to D000 (unit 0).

After the disk drive is selected, DKUTIL reads the first block of the Format Control Table (FCT) if possible, and dumps it in a format similar to a VERIFY printout. The unit is then brought online with the ignore media format error modifier so drives improperly or not completely formatted can be examined. If the FCT cannot be read or the mode is invalid, the program prompts for the sector size.

```
DKUTIL-Q Enter sector size (512/576) [512]?
```

The program places the unit in diagnostic mode to access the DBN area. The program returns to the command mode and prompts for a command.

```
DKUTIL>
```

Comment lines can be entered by preceding them with an exclamation point (!). A null line is ignored. Entering Ctrl/Z terminates the program. Commands are executed immediately and take only the time necessary to display the results. Entering Ctrl/Y or Ctrl/C at any time aborts the program and releases the drive.

7.2.2 Command Syntax

The DKUTIL commands are:

- DEFAULT
- DISPLAY
- DUMP
- EXIT
- GET
- POP
- PUSH
- SET

Any initial substring recognizes commands, command options, and modifiers. For example, DUMP can be entered as DUM, DU, or D. In cases where the initial substring can indicate one of several commands, the match depends on an order based on history and expected frequency of usage. Thus, D specifies DUMP, DI specifies DISPLAY, and DE specifies DEFAULT. In the descriptions in this chapter, only the command (or part of the command) in **bold print** must be specified.

Some commands take optional parameters. If an option is not selected, DKUTIL takes a default.

7.2.3 Command Modifiers

Modifiers, specified only for commands that allow them, can occur anywhere after the command itself. They are preceded by a slash (one slash for each modifier). The following are equivalent:

```
DUMP /NOEDC RBN 0
DUMP RBN/NOEDC 0
DUMP RBN 0/NOEDC
DUMP RBN 0 /NOEDC
```

Modifiers are processed left to right and applied to the current default modifiers. The DUMP command is the exception. The default modifiers for DUMP can be changed through the DEFAULT command. The initial default modifiers for DUMP are /DATA, /EDC, and /IFERROR.

7.2.4 Command Descriptions

This section contains the DKUTIL command descriptions. Command options are shown by separate lines in the syntax specification. Parameters are indicated lowercase in the syntax by braces ({}). Options indicated by brackets ([ ]) can be omitted.

7.2.4.1 Command Summary

A summary of all DKUTIL commands follows:

- DEFAULT—Change default modifiers for the DUMP command.

  DEFAULT

- DISPLAY—Display disk characteristics, a disk block, disk error history, RCT, or FCT.

  DISPLAY ALL
  DISPLAY CHARACTERISTICS DBN {block}
  DISPLAY CHARACTERISTICS DISK
  DISPLAY CHARACTERISTICS LBN {block}
  DISPLAY CHARACTERISTICS PBN {block}
  DISPLAY CHARACTERISTICS RBN {block}
  DISPLAY CHARACTERISTICS XBN {block}
  DISPLAY ERRORS
  DISPLAY FCT
  DISPLAY RCT

- DUMP—Dump a given block or table of blocks.

  DUMP [BUFFER]
  DUMP DBN [{block}]
  DUMP FCT [BLOCK {number}] [COPY {copy}]
  DUMP LBN [{block}]
  DUMP RBN [{block}]
  DUMP RCT [BLOCK {number}] [COPY {copy}]
  DUMP XBN [{block}]

- EXIT—Terminate execution of the program.

  EXIT

- GET—Acquire or change the current drive.

  GET [{drive}]

- POP—Restore save buffer to current buffer.

  POP

- PUSH—Save current buffer in save buffer.

  PUSH

- SET—Change various program parameters.

  SET [SIZE {size}]

7.2.4.2 DEFAULT Command

The DEFAULT command is outlined as follows:

- Purpose: To change the default modifiers for the DUMP command.
- Syntax: DEFAULT
- Parameters: None.
- Modifiers: Shown in the following list.
  - /IFERROR (NOIFERROR) (defaults ON)—Dumps the error, header, and ECC fields in the buffer if an error occurs when reading the block. When this modifier is used in conjunction with the /RAW modifier, the error must occur on the read of the original LBN that has been revectored (see /RAW).
  - /ERRORS (NOERRORS) (defaults OFF)—Dumps the error fields in the buffer.
  - /EDC (NOEDC) (defaults ON)—Dumps the EDC and calculated EDC fields in the buffer.
  - /ECC (NOECC) (defaults OFF)—Dumps the ECC fields in the buffer.
  - /DATA (NODATA) (defaults ON)—Displays the data in the buffer unless the /NZ modifier is also specified.
  - /HEADERS (NOHEADERS) (defaults OFF)—Displays the header fields (4 copies of the header) in the buffer.
  - /ALL (NONE)—The same as /ERRORS/EDC/ECC/DATA/HEADERS. Requests all fields be displayed. Its opposite, /NONE, requests no fields be displayed. When using the /NONE qualifier, only the MSCP status line is displayed.
  - /RAW (NORAW)—Allows reading the original LBN that was revectored rather than the RBN that would be read without the /RAW qualifier. /RAW only affects revectored (primary or non-primary) LBNs. The /IFERROR modifier, if used, applies to the read of the original LBN.
  - /NZ (NONZ) (defaults OFF)—Prevents the data from being displayed if it is all zeros. Instead, a single line indicating that the data is zero is displayed. It has no effect if the /DATA modifier is not specified or is defaulted OFF.
  - /BBR (NOBBR) (defaults OFF)—Bad block replacement is usually inhibited by DKUTIL when a block is accessed. If this modifier is specified, bad block replacement can occur. It only occurs, however, if the error recovery code detects the block being accessed as bad, and the bad block is an LBN in the host area.
  - /ORIGINAL (NOORIGINAL) (defaults OFF)—Dumps the original data in a block read with an error. When a block is accessed for dumping, the data is seen twice by the program if an error occurs. It is seen first just after the K detects the error and sends it to error recovery. It is seen again after error recovery takes place and the data has been corrected or reread. Usually, the data saved for dumping is the data seen after error recovery has taken place. This modifier allows the data read prior to error recovery to be dumped.
- Usage: The modifiers specified are applied to the current default modifiers for the DUMP command. The result becomes the new default. Examples are:

```
DEFAULT/NONE
DEF/RAW/NODATA
DE/A/OR/NZ
```

7.2.4.3 DISPLAY Command

The DISPLAY command is outlined as follows:

- Purpose: To display the disk characteristics, the characteristics of a given block, the error history in the drive, the FCT, and/or the RCT.
- Syntax:
  - DISPLAY ALL
  - DISPLAY CHARACTERISTICS DBN (block)
  - DISPLAY CHARACTERISTICS DISK
  - DISPLAY CHARACTERISTICS LBN (block)
  - DISPLAY CHARACTERISTICS PBN (block)
  - DISPLAY CHARACTERISTICS RBN (block)
  - DISPLAY CHARACTERISTICS XBN (block)
  - DISPLAY ERRORS
  - DISPLAY FCT
  - DISPLAY RCT
- Parameters: Block is a number specifying the DBN, LBN, PBN, RBN, or XBN whose characteristics are displayed. The default radix is decimal, and can be changed to octal by prefixing the number with the letter O.
- Modifiers:
  - /FULL—Displays all defined fields in *x*CT block 0. /FULL applies only to the RCT and FCT command options. For the DISPLAY RCT command without the /full modifier, the bad block replacement fields in RCT block 0 are only displayed if certain RCT status flags are set to indicate that a BBR operation is in progress. This modifier forces all fields to be displayed regardless of the settings of the RCT status flags. For the DISPLAY FCT command, the number of bad PBNs field is normally displayed only if the FCT is valid. Also, the scratch area parameters, format version, and format flags are normally not displayed. This modifier forces all fields in FCT block 0 to be displayed.
  - /NOITEMS—Does not display the individual items in the FCT or RCT. /NOITEMS applies only to the FCT and RCT command options. If specified, only the block 0 information is displayed.
- Usage:
  - DISPLAY ALL—Displays FCT, RCT, disk characteristics, and error history. Because the error history in the drive is dumped by this option, it should not be used for RA60 disk drives, which do not maintain internal error logs.
  - DISPLAY CHARACTERISTICS DISK—Displays the drive type, media, cylinders, geometry, group offsets, number of LBNs, number of RBNs, number of XBNs, numbers of DBNs, number of PBNs, RCT parameters, FCT parameters, SDI version, transfer rate, SDI timeouts, SDI retry limit, SDI error recovery command levels, ECC threshold, revision levels, drive ID, drive type ID, DBN read/only groups, and preamble sizes.
  - DISPLAY CHARACTERISTICS xBN (block)—Displays the characteristics of the given block. For all block types except PBNs, the decimal block number is displayed, coupled with the associated octal header.

The geometry of the block—the cylinder, group, track, and position—are also displayed along with the PBN in decimal and octal formats. For an RBN, the RCT block number and offset are also displayed. For an LBN, the display includes the primary RBN number and its RCT block number and offset. PBNs are displayed in the format of the type of block: DBN, LBN, RBN, or XBN.

- DISPLAY ERRORS—Reads the error history in the drive. For RA8x series disk drives, only 16 bytes of the error log data is displayed (in hexadecimal). For all other series except RA60 disk drives, the error log header and all selected error log entries are displayed (in hexadecimal). RA60 disk drives do not support internal error logging.
- DISPLAY FCT—Displays the information in FCT block 0. Certain fields are not displayed unless the /FULL modifier is given. The list of bad PBNs is displayed unless the /NOITEMS modifier is given. For each item in the list, the header bits, PBN number, type (DBN, LBN, RBN, or XBN), and *x*BN number are displayed.
- DISPLAY RCT—Displays the information in RCT block 0. Certain fields are not displayed unless the /FULL modifier is given. The list of revectors and bad RBNs is displayed unless the /NOITEMS modifier is given. For bad RBNs, just the RBN number is displayed (in decimal). For revectors, the LBN number and RBN number to which it is revectored are displayed (in decimal). A primary revector is distinguished by the character sequence "->". A non-primary revector is distinguished by the character sequence "*->".
- The following examples show DKUTIL DISPLAY command usage:

```
DISPLAY/FULL ALL
DI/F A
DI C D
DIS CHAR LBN 1000
DI/NOI RCT
```

7.2.4.4 DUMP Command

The DUMP command is outlined as follows:

- Purpose: To dump the given block or table of blocks.
- Syntax:
  - DUMP [BUFFER]
  - DUMP DBN [{block}]
  - DUMP FCT [BLOCK {number}] [COPY {copy}]
  - DUMP LBN [{block}]
  - DUMP RBN [{block}]
  - DUMP RCT [BLOCK {number}] [COPY {copy}]
  - DUMP XBN [{block}]
- Parameters:
  - Block is a number specifying the DBN, LBN, RBN, or XBN to be dumped. The default radix is decimal. It can be changed to octal by prefixing the number with the letter "O".
  - Number is the relative block number in the FCT or RCT to be dumped. The default radix is decimal and can be changed to octal by prefixing the number with the letter "O". The value must be in the range 1 through the nonpad FCT or RCT size. That is, the first block is number 1 (not 0) and the block must lie in the nonpad area.

— Copy specifies which copy of the given block in the FCT or RCT is to be dumped. The first copy is number 1. The value must not exceed the number of copies.

- Modifiers:
  - — /IFERROR (NOIFERROR) (defaults ON)—Dumps the error, header, and ECC fields in the buffer when an error occurs while reading the block. When used in conjunction with the /RAW modifier, the error must occur on the read of the original LBN that has been revectored. See /RAW.
  - — /ERRORS (NOERRORS) (defaults OFF)—Dumps the error fields in the buffer.
  - — /EDC (NOEDC) (defaults ON)—Dumps the EDC and calculated EDC fields in the buffer.
  - — /ECC (NOECC) (defaults OFF)—Dumps the ECC fields in the buffer.
  - — /DATA (NODATA) (defaults ON)—Displays the data in the buffer unless the /NZ modifier is also specified.
  - — /HEADERS (NOHEADERS) (defaults OFF)—Displays the header fields (4 copies of the header) in the buffer.
  - — /ALL (NONE)—The same as /ERRORS/EDC/ECC/DATA/HEADERS. It requests display of all fields. Its opposite, /NONE, requests display of no fields. When using the /NONE qualifier, only the MSCP status line is displayed.
  - — /RAW (NORAW)—Allows a read of the original revectored LBN (rather than the RBN that would be read without the /RAW qualifier). /RAW only affects revectored (primary or non-primary) LBNs. If in effect, the /IFERROR modifier applies to the read of the original LBN.
  - — /NZ (NONZ)—Prevents data from being displayed when it is all zeros. Instead, a single line is displayed indicating the data is zeros. /NZ has no effect unless the /DATA modifier is specified. It also has no effect if /DATA is not specified (or is defaulted OFF).
  - — /BBR (NOBBR) (defaults OFF)—Permits bad block replacement. Normally, bad block replacement is inhibited when a block is accessed. BBR occurs if the block being accessed is detected as bad by the error recovery code and is an LBN in the host area.
  - — /ORIGINAL (NOORIGINAL) – Dumps the original data in a block read with an error. When a block is accessed for dumping, the data is seen twice by the program if an error occurs. It is seen first just after the K detects the error and sends it to error recovery. It is seen again after error recovery takes place and the data has been corrected or reread. Usually, the data saved for dumping is the data seen after error recovery has taken place. This modifier allows the data seen prior to error recovery to be dumped.
- Usage:
  - — DUMP xBN [{block}]—The specified DBN, LBN, RBN, or XBN is read in and dumped subject to the given modifiers. If the block number is not specified, it defaults to zero.
  - — DUMP xCT [BLOCK {number}] [COPY {copy}]—If a BLOCK number is given, that block in the FCT or RCT is read in and dumped. If none is specified, every block in the nonpad area of the FCT or RCT is read in and dumped. If a COPY is not specified, Copy 1 is used.
  - — DUMP [BUFFER]—The current buffer is dumped, subject to the given modifiers. If there is no current buffer, an error message is displayed.
  - — The following are examples of DKUTIL DUMP command usage:

```
DUMP RCT BLOCK 3 COPY 4
DU/NZ RCT C 2
```

```
DU LBN 1000
D F B 2
D X
D/DATA
```

7.2.4.5 EXIT Command

The EXIT command is outlined as follows:

- Purpose: To terminate execution of the program.
- Syntax: EXIT.
- Parameters: None.
- Modifiers: None.
- Usage: The current drive is released, all resources are returned, and the program exits. The following are examples of DKUTIL EXIT command usage:

```
EXIT
E
```

7.2.4.6 GET Command

The GET command is outlined as follows:

- Purpose: To obtain a drive or change the current drive.
- Syntax: GET [(drive)].
- Parameters: Drive is a valid drive unit specification of the form Dnnn. If this parameter is omitted, GET defaults to D000 (unit 0).
- Modifiers:
  - /NOIMF—Allows the reading of FCT block 0 to determine the mode and the reading and writing of RCT block 0 to verify the RCT is valid. If this modifier is specified, the IMF MSCP modifier is not used when the drive is brought online, and these actions take place. By default, a new drive is brought online with the IMF (MD.IMF) MSCP modifier.
  - /WP—Brings the drive online in software or volume write protected mode.
  - /NOWP—Brings the drive online without the software or volume write protect indicators set. If the drive was previously write protected, it will remain so.
  - NOONLINE—The drive is acquired but not brought online with the MSCP ONLINE command. Only the DISPLAY CHARACTERISTICS, DISPLAY ERRORS, and the SET SIZE commands can be executed on a drive in this state.
- Usage: The current drive, if acquired, is released. The new drive is acquired and then brought online with the requested modifiers and unit flags. If the drive is nonexistent, in use, or inoperative, the user is put back in command mode. If the mode word in FCT block 0 is invalid or all copies of FCT block 0 are bad, the program prompts for the sector size to use. The following are examples of DKUTIL GET command usage:

```
GET D133
G/WP D64
G
```

7.2.4.7 POP Command

The POP command is outlined as follows:

- Purpose: To restore the data in the current buffer from the save buffer.
- Syntax: POP.
- Parameters: None.
- Modifiers: None.
- Usage: The data in the save buffer is restored to the current buffer. The data in the current buffer is lost. The following are examples of DKUTIL POP command usage:

```
POP
P
```

7.2.4.8 PUSH Command

The PUSH command is outlined as follows:

- Purpose: To save the data from the current buffer into the save buffer.
- Syntax: PUSH.
- Parameters: None.
- Modifiers: None.
- Usage: The data in the current buffer is placed in the save buffer. The data in the save buffer is lost. The following are examples of DKUTIL PUSH command usage:

```
PUSH
PU
```

7.2.4.9 SET Command

The SET command is outlined as follows:

- Purpose: To change various program parameters.
- Syntax: SET [SIZE (size)
- Parameters: The size parameter specifies the new sector size to be used for the current drive. It must be either 512 or 576 bytes.
- Modifier: None.
- Usage: SET SIZE (size).

  The sector size is changed to the given value and the disk parameters are recomputed. This new sector size is used when doing I/O to the LBN area and is also reflected in the parameters displayed by the DISPLAY CHARACTERISTICS DISK command. The following are examples of DKUTIL EXIT command usage:

```
SET SIZE 576
S S 512
```

7.2.5 Sample Session

The following is a sample session using DKUTIL. User input is indicated in bold print. Enter Ctrl/Y to get the HSC> command prompt.

```
Ctrl/Y
HSC> RUN DKUTIL Return

DKUTIL> GET D133 Return
 Serial Number:        0000000004
 Mode:                 512
 First Formatted:      17-Nov-1858 00:35:47.48
 Date Formatted:       04-Apr-1984 00:05:09.20
 Format Instance:      6
 FCT:                  VALID

DKUTIL> DIS/F FCT Return

         Factory Control Table for D133 (RA80)

 Serial Number:        0000000004
 Mode:                 512
 First Formatted:      17-Nov-1858 00:35:47.48
 Date Formatted:       04-Apr-1984 00:05:09.20
 Format Instance:      6
 FCT:                  VALID

 Bad PBNs in FCT:      1 (512), 0 (576)

 Scratch Area Offset:  63
 Size (Not Last):      417
 Size (Last):          289

 Flags:                000000
 Format Version:       0

              PBNs in 512 Byte Subtable

(04) 244865 (LBN 237213),

DKUTIL> DIS/F RCT Return

         Revector Control Table for D133 (RA80)

 Serial Number:        0000000004
 Flags:                000000

 LBN Being Replaced:   1000 (000000 001750)
 Replacement RBN:      33 (060000 000041)
 Bad RBN:              32 (060000 000040)

 Cache ID:             0000000000
 Cache Incarnation:    0
 Incarnation Date:     17-Nov-1858 00:00:00.00

Bad RBN:      32,   1000 *->    33,  25512 -->   822,
139512 -->  4500,

 RCT Statistics:          1 Bad RBNs,
                          3 Bad LBNs,
                          2 Primary Revectors,
                          1 Non-Primary Revectors,
                          0 Probationary RBNs.

DKUTIL> DEF/NODATA Return
DKUTIL> DUMP LBN 1000 Return

 ****** Buffer for LBN 1000 (000000 001750), MSCP Status: 000000

 Error Summary = header compare
```

```
 Original Error Bits  = 004000     BN = 1000 (000000 001750)
 Error Recovery Flags = 000        ECC Symbols Corrected = 0,0
 Error Retry Counts   = 0,1,0      Error Recovery Command = 000

  Header = 001750 030000 001750 030000 001750 030000 001750 030000

      EDC = 000105    Calculated EDC Difference = 000000

      ECC = 000000 000000 000000 000000 000000 000000
            000000 000000 000000 000003 000000 000000

DKUTIL> DIS CHAR LBN 1000 Return

      Characteristics for LBN 1000 (000000 001750)

 Cylinder 1, Group 0, Track 4, Position 8

 PBN 1032 (000000 002010)

 Primary RBN 32 (060000 000040) in RCT Block 3 at Offset 128

DKUTIL> DIS CHAR DISK Return

      Drive Characteristics for D133

 Type:           RA80 (576 byte mode allowed)

 Media:          FIXED

 Cylinders:      275 LBN, 2 XBN, 2 DBN

 Geometry:       14 tracks/group, 2 groups/cylinder, 28 tracks/cylinder
                 31 LBNs/track, 1 RBNs/track, 32 sectors/track,
                 32 XBNs/track, 896 XBNs/cylinder, 868
                 LBNs/cylinder, 28 RBNs/cylinder

 Group Offset:   16 (LBN), 16 (XBN)

 LBNs:           237212 (host), 238700 (total)

 RBNs:           7700

 XBNs:           1792

 DBNs:           1344 (read/write), 448 (read only)

 PBNs:           249984

 RCT:            465 (size), 63 (non-pad), 4 (copies)

 FCT:            480 (size), 63 (non-pad), 4 (copies)

 SDI Version:    3

 Transfer Rate: 97

 Timeouts:       3 (short), 7 (long)

 Retry Limit:    5

 Error Recover: 0 command levels

 ECC Threshold: 2 symbols

 Revision:       10 (microcode), 0 (hardware)

 Drive ID:       0A7A00000000

 Drive Type ID: 1

 DBN RO Groups: 1

 Preamble Size: 11 (data), 4 (header)

DKUTIL> DEF/DATA Return

DKUTIL> DUMP RCT BLOCK 3 Return

        ****** RCT Block 3, Copy 1 ******
```

```
****** Buffer for LBN 237214 (000003 117236), MSCP Status: 000000

Data = 000000 000000 000000 000000 000000 000000 000000 000000
  +16  000000 000000 000000 000000 000000 000000 000000 000000
  +32  000000 000000 000000 000000 000000 000000 000000 000000
  +48  000000 000000 000000 000000 000000 000000 000000 000000
  +64  000000 000000 000000 000000 000000 000000 000000 000000
  +80  000000 000000 000000 000000 000000 000000 000000 000000
  +96  000000 000000 000000 000000 000000 000000 000000 000000
 +112  000000 000000 000000 000000 000000 000000 000000 000000
 +128  000000 040000 001750 030000 000000 000000 000000 000000
 +144  000000 000000 000000 000000 000000 000000 000000 000000
 +160  000000 000000 000000 000000 000000 000000 000000 000000
 +176  000000 000000 000000 000000 000000 000000 000000 000000
 +192  000000 000000 000000 000000 000000 000000 000000 000000
 +208  000000 000000 000000 000000 000000 000000 000000 000000
 +224  000000 000000 000000 000000 000000 000000 000000 000000
 +240  000000 000000 000000 000000 000000 000000 000000 000000
 +256  000000 000000 000000 000000 000000 000000 000000 000000
 +272  000000 000000 000000 000000 000000 000000 000000 000000
 +288  000000 000000 000000 000000 000000 000000 000000 000000
 +304  000000 000000 000000 000000 000000 000000 000000 000000
 +320  000000 000000 000000 000000 000000 000000 000000 000000
 +336  000000 000000 000000 000000 000000 000000 000000 000000
 +352  000000 000000 000000 000000 000000 000000 000000 000000
 +368  000000 000000 000000 000000 000000 000000 000000 000000
 +384  000000 000000 000000 000000 000000 000000 000000 000000
 +400  000000 000000 000000 000000 000000 000000 000000 000000
 +416  000000 000000 000000 000000 000000 000000 000000 000000
 +432  000000 000000 000000 000000 000000 000000 000000 000000
 +448  000000 000000 000000 000000 000000 000000 000000 000000
 +464  000000 000000 000000 000000 000000 000000 000000 000000
 +480  000000 000000 000000 000000 000000 000000 000000 000000
 +496  000000 000000 000000 000000 000000 000000 000000 000000

 EDC = 023277    Calculated EDC Difference = 000000

DKUTIL> EXIT Return
DKUTIL--I Exiting.
```

7.2.6 Error and Information Messages

DKUTIL error messages conform to the HSC utility error message format.

7.2.6.1 Error Message Variables

Variable output in the error and information messages is shown in *italic* print. These fields are formed as follows:

n = A decimal number
par = BLOCK or COPY
parameter = The part of the command in error (modifier, and so forth)
status = MSCP status (an octal number)
text = The actual text in error
xBN = DBN, LBN, and so forth
xCT = FCT or RCT

7.2.6.2 Error Message Severity Levels

Each DKUTIL error message contains the utility name at the start of the message followed by a letter indicating the severity level of the message. These are defined as:

E = Error
F = Fatal
I = Informational

7.2.6.3 Fatal Error Messages

The following is a list of the DKUTIL fatal error messages:

- **DKUTIL-F Insufficient resources to run.**—This message is displayed if DKUTIL cannot acquire the necessary resources to run or if the disk functional code is not loaded. The program terminates after this message is displayed.
- **DKUTIL-F I/O request was rejected.** – This message is displayed if the diagnostic interface (DDUSUB) rejects a request to start an I/O operation. It indicates a bug in DKUTIL or an inability to obtain the necessary resources to perform the transfer. This error should be reported to Digital Customer Services. The program terminates after this message is displayed.

7.2.6.4 Error Messages

The following is a list of the DKUTIL error messages.

- **DKUTIL-E All copies of xCT Block *n* are bad.**—Displayed when all copies of an FCT or RCT block are bad. It occurs when the FCT or RCT is being read just after a drive has been selected or when the DISPLAY FCT or DISPLAY RCT command is being used.
- **DKUTIL-E Cannot ONLINE unit.**—Indicates that the requested unit is available, but the ONLINE command failed. The unit is released, and DKUTIL then goes into command mode. The user must then issue a GET or EXIT command at the DKUTIL> prompt.
- **DKUTIL-E Copy *n* of xCT Block *n* (xBN *n*) is bad.**—Displayed when an FCT or RCT block cannot be read correctly with error recovery. This error occurs when the FCT or RCT is read just after a drive is selected or when the FCT or RCT is read using the DISPLAY FCT or DISPLAY RCT command.
- **DKUTIL-E Drive must be acquired to execute this command.**—Displayed if the requested command requires that a drive must first be acquired before the command can be executed. A drive can be acquired and not brought online by using the /NOONLINE modifier with the GET command.
- **DKUTIL-E Drive must be online to execute this command.**—Displayed if the requested command requires that a drive first be acquired and brought online before the command can be executed.
- **DKUTIL-E Drive went AVAILABLE**—Displayed if the unit selected goes available while DKUTIL is running. DKUTIL then goes into command mode and the user must issue a GET or EXIT command at the DKUTIL> prompt.
- **DKUTIL-E Drive went OFFLINE**—Displayed if the selected unit goes offline while DKUTIL is running. DKUTIL then goes into command mode and the user must issue a GET or EXIT command at the DKUTIL> prompt.
- **DKUTIL-E Error log corrupted, cannot display entries.**—Indicates that the DISPLAY ERRORS command is unable to read a valid entry from region FFFB.
- **DKUTIL-E Error log corrupted, cannot display header.**—Displayed when the DISPLAY ERRORS command reads a header that does not begin with the standard FFFB code.

- **DKUTIL–E Error log not implemented in drive.**—Displayed when the DISPLAY ERRORS command is executed on an RA60.
- **DKUTIL–E Illegal response.**—Displayed if an invalid response to a start-up question or prompt is entered. The program reprompts the user for input.
- **DKUTIL–E Invalid ASCII byte count from drive, cannot display error log.**—Displayed if the drive returns an invalid ASCII byte count when DISPLAY ERRORS command processing asks the drive for its error log size.
- **DKUTIL–E Invalid block number for *x*BN space.**—Displayed if the block number specified for a DISPLAY CHARACTERISTICS *x*BN command is out-of-range for the given space.
- **DKUTIL–E Invalid decimal number.** – Displayed if an invalid decimal number is entered in a command line.
- **DKUTIL–E Invalid octal number.**—Displayed if the user entered an invalid octal number in a command line.
- **DKUTIL–E Invalid sector size; only 512 and 576 are legal.**—Displayed if the sector size entered for the SET SIZE command is other than 512 or 576 bytes.
- **DKUTIL–E Missing modifier (only "/" was specified).**—Displayed if a command line is entered with a slash (/) followed by a blank or is entered at the end of the line. A modifier is expected, but is missing.
- **DKUTIL–E Missing parameter.**—Displayed if a command line is entered with a required parameter missing.
- **DKUTIL–E *n* is an invalid *par* number; maximum is *n*.** – Displayed if an out-of-range number is entered for a BLOCK or COPY value for the DUMP command.
- **DKUTIL–E Nonexistent unit number.** – Displayed if the unit number entered does not correspond to any known unit attached to the HSC controller. DKUTIL then goes into command mode and the user must enter a GET or EXIT command at the DKUTIL> prompt.
- **DKUTIL–E SDI command was unsuccessful.** – Displayed when an SDI command is rejected by the drive.
- **DKUTIL–E *text* is an invalid *parameter*.**—Displayed when an invalid command, invalid command option, invalid modifier, invalid block type, or invalid SET option is specified in a command line.
- **DKUTIL–E There is no buffer to dump.**—Displayed if the DUMP BUFFER command is entered, and there is no current buffer. This can only happen if a drive has just been selected.
- **DKUTIL–E There is no buffer to PUSH.** – Displayed if the user entered a PUSH command but no data has been dumped into the local buffer.
- **DKUTIL–E There is no PUSHED buffer to POP.** – Displayed if the user entered a POP command, but there is no data PUSHed into the save buffer.
- **DKUTIL–E Unable to read error log.**—Indicates that the DISPLAY ERRORS command is unable to execute the SDI READ MEMORY command.
- **DKUTIL–E Unit is not available.** – Displayed if the unit requested is unavailable. The unit may be in use by a host or another diagnostic or it may be inoperative. DKUTIL then goes into command mode and the user must enter a GET or EXIT command at the DKUTIL> prompt.

7.2.6.5 Information Messages

DKUTIL has the following information messages:

- **DKUTIL–I Ctrl/Y or Ctrl/C Abort.**—Termination message that is displayed if DKUTIL is aborted by entering Ctrl/Y or Ctrl/C.
- **DKUTIL–I Exiting.**—Displayed when DKUTIL exits through the EXIT command, or in the event of a DKUTIL abort.

7.3 VERIFY — Offline Disk Verifier Utility

The VERIFY utility checks the integrity of the disk architectural structure. This utility checks a disk to ensure it conforms to the Digital Standard Disk Format.

VERIFY displays many messages while performing disk structure verification. Although many of these messages offer some visibility into the functional integrity of a drive, the main purpose of VERIFY is to check that the architectural structure of a drive is intact. In addition to messages reporting various drive or media errors, other messages are designed to report architectural inconsistencies.

At the completion of a VERIFY run, a message reports a drive as OK if no structural or permanent unrecoverable errors have been detected. If a structural or permanent unrecoverable error has been encountered, VERIFY displays a message indicating the number of inconsistencies detected.

NOTE
The VERIFY utility only reads the disk. It does not destroy user data and does not perform bad block replacement.

The following steps describe the process by which this utility verifies a disk:

1. The first block of the Format Control Table (FCT) is read to determine how the disk is formatted. The serial number, format mode, date first formatted, date last formatted, format instance, state of the FCT, number of bad PBNs, scratch area parameters (offset, size of not last, and size of last), flags, and format version are displayed.
2. The first block of the Replacement Control Table (RCT) is then read. The information in it is displayed, including the serial number, flags, bad block replacement variables (LBN being replaced, replacement RBN, and bad RBN), and cache variables (ID, incarnation, and incarnation date).
3. All copies of the first two blocks in the RCT (used by bad block replacement) are read and compared. Discrepancies or bad blocks are reported.
4. All copies of the rest of the RCT are read and compared. Any discrepancies or bad blocks are reported. The information about revectors and bad RBNs is dumped. A summary of the number of bad blocks and revectors is shown.
5. All copies of FCT block 0 are read and compared, and bad blocks or discrepancies are reported.
6. All copies of the appropriate FCT subtable are read (if not null), and bad blocks or discrepancies are reported.
7. The list of bad PBNs is displayed. Each entry is displayed with the header bits, PBN number, and xBN number (in parentheses) as separate fields. If a bad PBN is found which should be in the RCT but is not, the xBN number is displayed in brackets instead of parentheses. If any such PBNs are found, an error message indicating the total number is displayed following the bad PBN list.

8. After reading and dumping the FCT, a quick scan of the DBN space is done. Every block is accessed only once. A summary is displayed at the end of the scan, listing the counts of various detected errors. If more than nine positioner errors are detected, a message is displayed suggesting that the DBN space be reformatted. If more than nine EDC errors are detected, a message is displayed suggesting the INITIAL WRITE option should be used when running ILEXER.
9. All LBN space up to the RCT and all RBNs are scanned. Any block with an error is reread five more times to determine the type of error. Information about bad blocks and revectors collected in this phase is compared with information collected from reading the RCT. During the scan, errors are classified into four categories:

   Structure errors
   Permanent recoverable errors
   Permanent unrecoverable errors
   Transient errors

   Structure and permanent unrecoverable errors are considered inconsistencies and are always reported. Permanent recoverable errors, usually ECC errors, are reported if requested by the user. During the five rereads of a block with an error, a block read at least once with no detected error is considered to have a transient error. Transient errors are reported if requested by the user.
10. At the end of the scan, certain other errors are reported. Some errors can only be determined at that time by examining information collected during the scan.
11. Finally, a summary, by type, of the errors detected and certain other information is displayed. If no inconsistencies were discovered, a message displays saying the drive is OK. Otherwise, the message indicates the number of inconsistencies.

7.3.1 Running VERIFY

Start VERIFY by entering the following command at the HSC> prompt:

```
HSC>RUN VERIFY Return
```

The following prompt asks for the unit number of the disk to verify:

```
VERIFY-Q Enter unit number to verify (U) [D0]?
```

Enter the letter D followed by the disk unit number, or press Return to use the default disk unit number of zero.

Verify then prompts to determine if the unit was recently formatted:

```
VERIFY-Q Was this unit just FORMATted (Y/N) [Y]?
```

Enter Y or press Return if the disk has not been accessed by a host or HSC diagnostic since it was formatted.

This question is asked because certain errors are classed as inconsistencies only when the disk has not undergone bad block replacement since the disk was last formatted. The next prompt determines whether errors that are not considered inconsistencies should be reported:

```
VERIFY-Q Print informational (non-warning) messages (Y/N) [N]?
```

Enter N or press Return if you want VERIFY to only report inconsistencies . Enter Y if you want informational messages as well as inconsistencies to be reported.

If you answered Y to the "Print informational messages" prompt, VERIFY next prompts:

```
VERIFY-Q Report transient errors by block (Y/N) [N]?
```

If you enter Y, VERIFY displays a message for each block that contains a transient error. If you enter N or press Return, you will not get this report.

Regardless of the response to this question, the number of transient errors is displayed in the final summary. The response to this question determines whether or not individual blocks with transient errors should be reported.

Ctrl/Z can be entered at any prompt to cause the default to be taken for the remainder of the responses. Also, the responses to subsequent questions can be supplied at any question by typing them separated with commas. For example, if unit D133, which was just formatted, is to be verified with all options selected, the user could enter D133,,Y,Y at the first prompt.

If the unit does not exist or cannot be accessed, notification and reprompt for another unit number are received. If the unit can be accessed, it is acquired and brought online. VERIFY runs to completion, unless aborted by Ctrl/Y or Ctrl/C.

7.3.2 Sample Session

The following is a sample session using VERIFY. User input is in bold print.

```
Ctrl/Y
HSC> RUN VERIFY Return

VERIFY-Q Enter unit number to verify (U) [D0]? D133 Return
VERIFY-Q Was this unit just FORMATted (Y/N) [Y]? Return
VERIFY-Q Print informational (non-warning) messages (Y/N) [N]? Y Return
VERIFY-Q Report transient errors by block (Y/N) [N]? Y Return

   ***    FCT Block 0 Information

   Serial Number:       0000000004
   Mode:                512
   First Formatted:     17-Nov-1858 00:35:47.48
   Date Formatted:      10-Apr-1984 00:05:09.20
   Format Instance:     6
   FCT:                 VALID
   Bad PBNs in FCT:     1 (512), 0 (576)

   Scratch Area Offset: 63
   Size (Not Last):     417
   Size (Last):         289

   Flags:               000000
   Format Version:      0

   ***    RCT Block 0 Information

   Serial Number:       0000000004
   Flags:               000000

   LBN Being Replaced:  0 (000000 000000)
   Replacement RBN:     0 (060000 000000)
   Bad RBN:             0 (060000 000000)

   Cache ID:            0000000000
   Cache Incarnation:   0
   Incarnation Date:    17-Nov-1858 00:00:00.00

   ***     Revector Control Table for D133

VERIFY-I Copy 1 of RCT Block 2 (LBN 237213.) is bad.
  25512 -->   622, 139512 -->  4500,

   RCT Statistics:          0 Bad RBNs,
                            2 Bad LBNs,
                            2 Primary Revectors,
                            0 Non-Primary Revectors,
                            0 Probationary RBNs,
                            1 Bad RCT Blocks,
                            1 Bad First Copy RCT Blocks.

   ***                     Factory Control Table for D133

                             PBNs in 512 Byte Subtable

  (04) 244865 (LBN 237213),

   ***             Quick Scan of DBN Area
```

```
  Statistics:
                    0 total blocks with any error.

   ***                Scan of LBN Area

VERIFY-I LBN 26003. has a 1 symbol correctable ECC error.
VERIFY-I PBN 2471. has a 1 symbol correctable ECC error.
VERIFY-I LBN 139961. has a 1 symbol correctable ECC error.

  Statistics:
                    3 total ECC symbols corrected,
                    3 blocks with 1 symbol ECC errors,
                    2 revectors verified,
                    5 total blocks with any error.

VERIFY-I Drive is OK.
VERIFY-I Exiting
```

The preceding example is the output of an actual session for an RA80 disk drive with one bad PBN in the FCT. Notice this PBN corresponds to copy 1 of RCT block 2. RCT block 2 is used to store the copy of the user data during bad block replacement. In its scan of the RCT, VERIFY noticed this block was bad and displayed an informational message to indicate this condition. If information messages had been suppressed by responding with N to the "Print informational messages" prompt, this information would show only in the summary of the RCT dump.

In the example, VERIFY also displayed informational messages for the three blocks it found with solid one-symbol correctable ECC errors. If informational messages had been suppressed, these messages would not have been displayed. However, the number of such blocks would still show up in the summary statistics.

No transient errors were detected; therefore, no count is reported in the summary statistics. Also note that although no messages were displayed, the two revectors in the RCT were verified (as indicated in the summary statistics). Note the odd date in the First Formatted field. This default date is supplied when no date is provided by a host or a human during manufacturing format. If structural inconsistencies had been found, some of the following VERIFY error messages would have been displayed.

7.3.3 Error and Information Messages

This section describes error and information messages that may be displayed by VERIFY. Error messages are arranged alphabetically according to the actual message.

7.3.3.1 Variable Output Error Fields

Error message fields with variable output are in *italic* print. Definitions for these variable fields are:

xCT = FCT or RCT
n = A decimal number
n. = A decimal LBN, RBN, or XBN
xBN = LBN, RBN, or XBN
o = An octal number
t = Type code: I or W
error-type = Error: ECC, EDC, and so forth

7.3.3.2 Error Message Severity Levels

VERIFY error messages conform to the HSC utility error message format. In each case, the utility name at the start of the message is followed by a letter indicating severity level. These are:

F = Fatal
I = Information
t = Type: either W or I, depending on the error
W = Warning

7.3.3.3 Fatal Error Messages

Following is a list of the error messages fatal to the VERIFY utility. The program terminates after displaying one of these messages.

- **VERIFY–F All copies of *x*CT block *n* are bad.**—Displayed if all copies of some block in either the RCT or the FCT are bad. The program cannot continue to run because vital information is missing. The unit has been verified as bad.
- **VERIFY–F Current system sector size is 512.**—Displayed if the mode field in FCT block 0 indicates the unit is formatted in 576-byte mode, but the system sector size is set to 512. In this case, VERIFY cannot run because it cannot read sectors 576 bytes long.
- **VERIFY–F Drive went OFFLINE.**—Displayed if the unit selected goes offline while VERIFY is running.
- **VERIFY–F Insufficient resources to run.**—Displayed if VERIFY cannot acquire the necessary resources to run or the disk functional code is not loaded.
- **VERIFY–F I/O request was rejected.** – Displayed if the diagnostic interface (DDUSUB) rejects a request to start an I/O operation. This message could be an indication of a problem in the VERIFY utility, but it is more likely that DDUSUB could not obtain resources to complete the I/O request.
- **VERIFY–F Mode is bad or format is in progress on this unit.**—Displayed if the mode field in FCT block 0 of the selected unit is not valid.
- **VERIFY–F Too many bad blocks.**—Displayed if VERIFY detected more bad blocks than it can fit into its internal buffers. This may not mean that the disk is bad, but you should not run VERIFY on this disk.

7.3.3.4 Warning Messages

The following messages are warning messages. In many cases, they are true warnings; in other cases, they simply precede a reprompt.

- **VERIFY–W Cannot ONLINE unit.**—Displayed if the unit requested is available but the ONLINE command failed. The unit is released and the user is reprompted for another unit.
- **VERIFY–W Cannot read track with starting *x*BN *n*.**—Displayed if VERIFY fails to access a track containing the given LBN or RBN. This error may be caused by a hardware problem.
- **VERIFY–W Copy *n* of *x*CT Block *n* (*x*BN *n*.) does not compare.**—Displayed if VERIFY finds an FCT (XBN) or RCT (LBN) block that does not compare to the first good copy it read.
- **VERIFY–W Illegal response to start-up question.**—Displayed if an invalid response is entered for a start-up question. The program reprompts with the same question.
- **VERIFY–W LBN *n*., a non-primary revector, is improper.**—Indicates that an LBN is not a non-primary revector but is recorded in the RCT as such. The LBN headers did not indicate that the block is non-primary revectored; however, the LBN is listed in the RCT as a non-primary revector.
- **VERIFY–W LBN *n*., a primary revector, is improper.**—Indicates that an LBN is not a primary revector but is recorded in the RCT as such. The LBN headers did not indicate that the block is primary revectored; however, the LBN is listed in the RCT as a primary revector.
- **VERIFY–W LBN *n* has corrupted data (forced error).**—Displayed if a bad block replacement in which the data could not be recovered produces a revectored LBN with forced error set, indicating the data is probably bad. No such LBNs should exist after FORMAT has been run.

If you answered YES to the Was Unit Formatted prompt, this message is displayed with a severity of W (warning). If the disk has undergone bad block replacement since the last format operation, this message is displayed with a severity of I (informational).

- **VERIFY-W LBN *n*. marked primary in RCT, not revectored to its primary.**—Displayed if the specified LBN number that is marked primary in the RCT is not revectored to its primary RBN.
- **VERIFY-W LBN *n*. revectors to RBN *n*. which is bad.**—Displayed if, after scanning the collected RCT information, VERIFY determines that LBN n is revectored to a bad RBN.
- **VERIFY-W *n* bad PBNs (in brackets above) not in the RCT.**—Displayed to show the number of bad PBNs that are not in the RCT. VERIFY searches the RCT for LBNs or RBNs that correspond to known bad PBNs and keeps track of the number of these bad PBNs that are not found in the RCT.
- **VERIFY-W Nonexistent unit number.** – Displayed if the unit number entered does not correspond to any known unit. The program reprompts for the unit number.
- **VERIFY-W RBN *n*. is good but not used for a revector.**—Displayed if VERIFY finds a valid RBN (with valid EDC) in the verification pass, but it is not recorded in the RCT as being used. This record should not exist just after FORMAT has been run. Unused RBNs are written with an invalid EDC.

  If you answered YES to the Was Unit Formatted prompt, this message is displayed with a severity of W (warning). If the disk has undergone bad block replacement since the last format operation, this message is displayed with a severity of I (informational).--If the drive was just formatted, do another reformat operation. If the drive was not recently formatted, no action is necessary.
- **VERIFY-W RBN *n*. marked bad in the RCT was not bad.**—Displayed if VERIFY finds an RBN marked as bad in the RCT that is not bad. This condition should not exist just after FORMAT has been run.

  If you answered YES to the Was Unit Formatted prompt, this message is displayed with a severity of W (warning). If the disk has undergone bad block replacement since the last format operation, this message is displayed with a severity of I (informational).
- **VERIFY-W *x*BN *n*. has a hard EDC error.**—Displayed for LBNs and RBNs found to have a bad EDC (neither correct nor forced error). This error is classed as an inconsistency. Only a software error can result in a record with a bad EDC.
- **VERIFY-W *x*BN *n*. has an uncorrectable ECC error.**— Displayed if VERIFY detects an LBN with an uncorrectable ECC error or an RBN with an uncorrectable ECC error that is not marked bad in the RCT. An LBN with an uncorrectable ECC error should be revectored by FORMAT or bad block replacement; an RBN with an uncorrectable ECC error should be marked bad in the RCT. Both of these errors are classed as inconsistencies.

  NOTE
  If VERIFY detects an RBN with an uncorrectable ECC error and this RBN is marked bad in the RCT, this message is displayed as an informational message.
- **VERIFY-W *x*BN *n*. I/O error in access (MSCP Code: *o*).**—Indicates that an inconsistency was found in the drive or data channel module. VERIFY provides its own error processing for records read where the K detects errors. This message is displayed under two conditions:
  - If requests do not return with a SUCCESS code, indicating a problem in the drive or disk data channel.

- If the return from an I/O operation is not successful after VERIFY reads the record in error one more time with error recovery enabled, and the error is not a forced error, EDC error, or an uncorrectable ECC error.

- **VERIFY-W *x*BN *n*. is bad but not in the RCT.**—Displayed if a bad LBN or RBN is not in the RCT. VERIFY detected an error each time it accessed an LBN or RBN. All of the detected areas were header errors, which implies that the LBN/RBN is revectored; however, the LBN or RBN is not recorded as revectored in the RCT.
- **VERIFY-W Unit is not available.** – Displayed if the unit requested is unavailable. It may be in use by a host or another HSC diagnostic, or it may be inoperative. The program reprompts for another unit.

7.3.3.5 Information Messages

Following are descriptions of the information messages displayed by VERIFY. Some of these messages require that informational message reporting be enabled. Other messages are reported regardless of whether or not informational message reporting is enabled.

- **VERIFY-I Copy *n* of *x*CT Block *n* (*x*BN *n*.) is bad.**—Displayed if VERIFY could not correctly read, using error recovery, the indicated RCT (LBN) or FCT (XBN) block. This message is displayed only if informational error message reporting is enabled.
- **VERIFY-I CTRL/Y or CTRL/C Abort.** – Displayed if the user aborts VERIFY by entering a Ctrl/Y or Ctrl/C.
- **VERIFY-I DBN area should probably be reformatted.**—Displayed whether or not information messages are enabled. If more than nine DBNs are detected with positioner errors during the DBN scan, this message is displayed.
- **VERIFY-I Drive is OK.**—Displayed at the end of VERIFY if no inconsistencies have been discovered.
- **VERIFY-I INITIAL WRITE should be specified for ILEXER.**—Displayed whether or not informational messages are enabled. If more than nine DBNs are detected with EDC errors during the DBN scan, this message is displayed.
- **VERIFY-I LBN *n*., a primary, has a bad header (is non-primary).**—Displayed if informational messages are enabled. An LBN is recorded in the RCT as a primary revector, but has a bad header. Either the header is garbled or the LBN header indicates a non-primary revector. Such a condition is abnormal but not an error.
- **VERIFY-I RBN *n*. is good but not used for a revector.**—Displayed if VERIFY finds a valid RBN (with valid EDC) in the verification pass, but it is not recorded in the RCT as being used. Unused RBNs are written with an invalid EDC. This message is displayed as informational instead of warning if the FORMAT utility was not run on the drive immediately preceding the VERIFY run.
- **VERIFY-I RBN *n*. marked bad in the RCT was not bad.**—Displayed if VERIFY finds an RBN marked bad in the RCT that is not bad. This message is displayed as informational instead of warning if the FORMAT utility was not run on the drive immediately preceding the VERIFY run.
- **VERIFY-I There were *n* inconsistencies found for this drive.**—Displayed at the end of VERIFY if inconsistencies have been discovered. An inconsistency is a structural or permanent unrecoverable error.
- **VERIFY-I *x*BN *n*. has a *n* symbol correctable ECC error.**—Displayed if informational message reporting is enabled. This message indicates the highest number of ECC symbols corrected on the seventh access of an LBN or RBN with a solid ECC error.

- **VERIFY–I *x*BN *n*. has a transient (*n* out of 6) *error_type* error.** – Displayed if both informational and transient error reporting are enabled. This message indicates the number (*n*) of times out of six that VERIFY detected the indicated error, *error_type*.
- **VERIFY–I *x*BN *n*. has an uncorrectable ECC error.** — Displayed if VERIFY detects an RBN with an uncorrectable ECC error that is marked bad in the RCT. If VERIFY detects an RBN with an uncorrectable ECC error and it is NOT marked bad in the RCT, this message is displayed with a severity of W (Warning).
- **VERIFY–I *x*BN *n*. has corrupted data (forced error).**—Displayed if a bad block replacement in which the data could not be recovered produced a revectored LBN with forced error set, indicating the data is probably bad. This message is displayed as informational instead of warning if the FORMAT utility was not run on the drive immediately preceding the VERIFY run.
- **VERIFY–I *x*BN *n*. has solid errors: *error_type*—**Displayed for LBNs or RBNs with errors on all six accesses when informational message reporting is enabled. The errors include those other than ECC or EDC. The record is read a seventh time with error recovery enabled to determine if the error is correctable. If it is not, a warning message is displayed.
- **VERIFY–I Exiting**—Displayed to indicate that VERIFY has completed its run and is exiting, or that the user has aborted VERIFY by entering Ctrl/C or Ctrl/Y.

NOTE
The following VERIFY messages are statistical messages displayed at the end of a verify run. These messages are informational, but are not displayed with the VERIFY–I header.

- ***n* bad DBNs,**—Indicates the number of bad DBNs VERIFY encountered.
- ***n* bad RBNs verified,** – Indicates the number of bad RBNs that were also recorded as bad in the RCT.
- ***n* blocks with EDC errors,**—Indicates the number of blocks in which EDC errors were detected.
- ***n* blocks with hard EDC errors,**—Indicates the number of blocks with hard EDC errors.
- ***n* blocks with header compare errors,**—Indicates the number of blocks in which header compare errors were detected.
- ***n* blocks with *n* symbol ECC errors,**—Indicates the number of blocks in which a specified number of ECC symbols were corrected.
- ***n* blocks with non–header, non–EDC errors,**—Indicates the number of blocks in which non–header, non–EDC errors were detected.
- ***n* blocks with positioner errors,**—Indicates the number of blocks in which positioner errors were detected.
- ***n* blocks with solid (non–ECC) errors,**—Indicates the number of blocks with solid (not ECC, header, or EDC) errors.
- ***n* blocks with transient errors,**—Indicates the number of blocks in which transient errors were detected.
- ***n* blocks with uncorrectable ECC errors,**—Indicates the number of blocks in which uncorrectable ECC errors were detected.
- ***n* good RBNs marked bad in the RCT,**—Indicates the number of RBNs marked bad in the RCT that are actually good.

- ***n* LBNs with corrupted data,**—Indicates the number of revectored LBNs with forced error set. This indicates that the data is probably bad.
- ***n* revectors verified,** – Indicates the number of revectors that were correctly verified. Correct verification requires that all blocks that are primary or non-primary revectors are recorded as such in the RCT.
- ***n* total blocks with any error.**—Indicates the total number of blocks that contained an error(s) of any kind.
- ***n* total ECC symbols corrected,**—Indicates the total number of ECC symbols corrected during the VERIFY operation.
- ***n* unused RBNs with good EDC,**—Indicates the number of RBNs with valid EDCs that are recorded in the RCT as being used (unused RBNs have invalid EDCs).
- **NOTE: Table is null or empty (no bad PBNs).** – Displayed whether or not informational message reporting is enabled. The FCT on the drive is null or empty.

7.4 FORMAT — Offline Disk Formatter Utility

The HSC utility FORMAT is used to format disks. It can be used to format only the read-only DBN space or to format both the LBN area and the read-only DBN space.

CAUTION
The FORMAT utility destroys user data if used by persons not familiar with DSA.

The DBN area is always formatted. If the user requests it, the LBN area also is formatted. When the LBN area is formatted, there are two modes of operation: the reformat and the best guess modes.

In reformat mode, the existing FCT on the disk is used to obtain bad block information. If, in reformat mode, the FCT is found to be null or corrupt, a best guess mode is used.

The main difference between best guess mode and reformat mode is that each track is reread at least three times during the check pass in best guess mode, instead of once in reformat mode. If any error is detected, the track is reread 20 times in best guess mode instead of 3 times in reformat mode.

CAUTION
Be careful when using Ctrl/C or Ctrl/Y to abort the FORMAT utility after formatting operations begin. Doing this may destroy the contents of the RCT. The FORMAT utility should only be aborted under fatal-unrecoverable disk failure conditions.

7.4.1 Running FORMAT

FORMAT is started with the standard CRONIC command syntax RUN DX0:FORMAT.UTL. The last field in the following prompts (shown in square brackets) indicates the default for that prompt.

The program prompts for the unit number of the disk to format with the following question:

```
FORMAT-Q Enter unit number to format (U) [D0]?
```

Enter the letter D followed by the disk unit number, or press Return to use the default disk unit number of zero.

The next prompt determines whether the LBN (user data) area should be formatted or whether only the read-only DBN (diagnostic) area should be formatted. If this prompt is answered with a Y, user data is destroyed.

```
FORMAT-Q Format user data area (Y/N) [N]?
```

If replied with an N or Return only (to obtain the default), the program starts executing and formatting only the DBN area. If a Y is entered, the program prompts for the sector size to use when formatting the disk.

```
FORMAT-Q Enter sector size to be used (512/576) [512]?
```

Although this prompt gives the option of formatting with 576-byte sectors, the HSC controller no longer supports 576-byte operations. As a result, enter 512 or press Return to accept the 512-byte default.

```
FORMAT-Q Continue if bad block information is inaccessible (Y/N) [N]?
```

If an N is entered, reformat mode is used if the FCT is valid. If it is not valid, the program aborts with an appropriate error message. If Y is entered, reformat mode is used if the FCT is valid, or best guess mode is used if the FCT is null or corrupt.

If the response to the preceding prompt is Y, the program prompts for a serial number:

```
FORMAT-Q Enter a non-zero serial number (D)?
```

This serial number is used if all copies of FCT block 0 are unreadable (in best guess mode). FORMAT allows a number of special options, not only for debugging purposes but also to increase data reliability. To determine if any of these options are desired, the program prompts with the following:

```
FORMAT-Q Do you want special options (Y/N) [N]?
```

If the response is N or Return (the default of N), FORMAT starts processing.

If the response is Y, the following three special option prompts appear. The first prompt option is:

```
FORMAT-Q Revector blocks with 1 symbol ECC errors (Y/N) [N]?
```

Normally, blocks discovered with one-symbol ECC errors during the format check pass are not replaced. The program assumes this level of error is tolerable. If the response to this prompt is Y, all blocks with solid (nontransient) ECC errors are replaced. However, in all cases, blocks with two-symbol (or more) ECC errors are always replaced, regardless of the drive's ECC symbol threshold.

The second special option prompt is:

```
FORMAT-Q Revector blocks with transient errors (Y/N) [N]?
```

After a track is formatted, it is read either once (reformat) or three times (best guess). If an error is detected, and the mode is reformat, the track is read twice more. If any block not previously replaced shows an error twice, it is replaced and the track is reformatted with this check pass done again. If no block had errors twice, the track is read 3 more times (reformat) or 20 more times (best guess). Blocks that show an error only once during all of these reads are normally not replaced. Such errors are considered tolerable transient errors. If the response to this prompt is Y, blocks that show any error are replaced.

The third and final special option prompt is:

```
FORMAT-Q Report position of bad blocks (Y/N) [N]?
```

Blocks replaced during the format process are reported with a single line printout. The type, block number, and cause for replacement are displayed. If the response to this prompt is Y, the PBN number, cylinder, track, group, and position are also displayed on a subsequent line.

The user can enter Ctrl/Z at any prompt to use the default for the remainder of the responses. Also, the responses to subsequent questions can be supplied at any question by typing the responses separated by commas. For example, if unit D133 has an FCT and is to be formatted in 512-byte mode with no special options, the user could enter D133,Y,,,, at the first prompt.

7.4.2 Sample Session

The following is a sample session using FORMAT. User input is in **bold print**.

```
Ctrl/Y
HSC> RUN DX0:FORMAT Return
FORMAT-Q Enter unit number to format (U) [D0]? D133 Return
FORMAT-Q Format user data area (Y/N) [N]? Y Return
FORMAT-Q Enter sector size to be used (512/576) [512]?
FORMAT-Q Continue if bad block information is inaccessible (Y/N) [N]?
FORMAT-Q Do you want special options (Y/N) [N]? Y Return
FORMAT-Q Revector blocks with 1 symbol ECC errors (Y/N) [N]?
FORMAT-Q Revector blocks with transient errors (Y/N) [N]?
FORMAT-Q Report position of bad blocks (Y/N) [N]?
FORMAT-S Format begun.
FORMAT-I    2 cylinders left in DBN space at 00:05:34.60.
FORMAT-I  275 cylinders left in LBN space at 00:05:39.60.
FORMAT-I Bad LBN 237213 (FCT), in the RCT area.
FORMAT-I  265 cylinders left in LBN space at 00:06:05.60.
FORMAT-I  255 cylinders left in LBN space at 00:06:31.40.
   .
   .
   .
   .
FORMAT-I Bad LBN 139512 (check), a primary revector to RBN 4500.
   .
   .
   .
FORMAT-I Bad LBN 25512 (check), a primary revector to RBN 822.
FORMAT-I   25 cylinders left in LBN space at 00:16:36.20.
FORMAT-I   15 cylinders left in LBN space at 00:17:02.00.
FORMAT-I    5 cylinders left in LBN space at 00:07:28.40.
FORMAT-S Format completed.
FORMAT-I Stats:    0 Bad RBNs,
                   2 Revectored LBNs,
                   2 Primary Revectored LBNs,
                   0 Non-Primary Revectored LBNs,
                   1 Bad Blocks in RCT Area,
                   0 Bad Blocks in DBN Area,
                   0 Bad Blocks in XBN Area,
                   9 Blocks Retried on Check Pass.
FORMAT-I FCT was used successfully.

   ****************************************************************
   *                                                              *
   *   VERIFY must be RUN to complete FORMAT verification!        *
   *                                                              *
   ****************************************************************
FORMAT-I Exiting
```

CAUTION
The boxed message at the end of the FORMAT run indicates that VERIFY must be run to complete verification. This is an essential step and should not be skipped.

The preceding example is the output for an actual session for an RA80 disk with one bad PBN in the FCT. Notice the message that indicates that the bad PBN is in the RCT area. Note the information message that is displayed every 10 cylinders. This confirms that progress is actually being made and gives some insight into the rate of progress. Also, note the two LBNs that were retired because they had two-symbol ECC errors; they became primary revectors.

The final statistics of the sample session indicate that two LBNs were revectored and one bad LBN was found in the RCT area. The nine "Blocks Retried on Check Pass" include the two bad LBNs plus seven other blocks with transient errors that were not retired. The bad block in the RCT was not retried in the check pass because it was known to be bad from the FCT. This would be true for any blocks found in the FCT. The final message indicates an FCT was found and was successfully used.

7.4.3 Error and Information Messages

This section describes the error and information messages displayed by FORMAT. Error messages are arranged alphabetically according to the actual message.

7.4.3.1 Error Message Variables

Variable output in the error and information messages is shown in *italic* print. These fields are formed as follows:

n = A decimal number
x = The way a block was found bad: FCT or check
*x*BN = A space: DBN, XBN, or LBN
hh = Hours
mm = Minutes
ss = Seconds
xx = Hundredths of a second

7.4.3.2 Message Severity Levels

FORMAT error messages conform to the HSC utility error message format. In each case, the utility name at the start of the message is followed by a letter indicating severity level. These are defined as:

F = Fatal
I = Informational
E = Error
S = Success
W = Warning

7.4.3.3 Fatal Error Messages

This section describes the fatal error messages displayed by FORMAT. The FORMAT program terminates after one of these messages is displayed.

- **FORMAT-F Cannot FORMAT this drive type.** – Displayed if FORMAT is run on a drive that does not support formatting operations.
- **FORMAT-F Cannot position to DBN area.**—Displayed if FORMAT cannot verify positioning to the DBN area. FORMAT attempts to verify that it has positioned the heads to the DBN area before it formats the disk unless FORMAT is running in best guess mode. FORMAT does this by reading the first sector of every track in the DBN read/write area until a sector is read without a header error. This fatal error message is displayed if no such sector can be found.

- **FORMAT-F Current maximum sector size is 512.**—Displayed if the user requests a 576-byte sector size but the system sector size is set to 512. In this case, FORMAT cannot run because I/O cannot be done with sectors that are 576 bytes long. The HSC controller no longer supports the 576-byte sector size; therefore, this message will always be seen if 576-byte mode is requested.
- **FORMAT-F DBN format error (drive FORMAT command Failed).**—Displayed if a FORMAT command fails five times when formatting the DBN area.
- **FORMAT-F Drive does not support 576 mode on this media.**—Displayed if the user requests a 576-byte sector size for a drive that does not support it.
- **FORMAT-F Drive is write-protected.**—Displayed if the requested drive is hardware write protected and therefore cannot be formatted.
- **FORMAT-F FCT does not have enough good copies of each block.**—Displayed if there are not two good copies of each FCT block.
- **FORMAT-F FCT is improper.**—Displayed if one or more PBNs remain to be processed when FORMAT completes. When FORMAT finishes formatting the LBN area, it checks to see if all PBNs in the FCT have been processed. If one or more PBNs remain to be processed, this message is displayed. This condition usually indicates an FCT in which some PBNs are out of order.
- **FORMAT-F FCT nonexistent.**—Displayed if the user has instructed the program not to continue when the FCT is found to be null or clobbered.
- **FORMAT-F FCT read error**—Displayed if all copies of some block of the FCT cannot be successfully read.
- **FORMAT-F FCT write error**—Displayed if all copies of some block of the FCT cannot be successfully written.
- **FORMAT-F Formatter initialization error.**—Displayed if FORMAT cannot acquire enough resources to start formatting or if the disk functional code is not loaded.
- **FORMAT-F GET STATUS failure.**—Displayed if the unit requested is not available or cannot be brought online.
- **FORMAT-F LBN format error (drive FORMAT command failed).**—Displayed if a FORMAT command fails five times when formatting the LBN area.
- **FORMAT-F Nonexistent unit number.** – Displayed if the requested unit does not exist.
- **FORMAT-F RCT does not have enough good copies of each block**—Displayed if there are not two good copies of each RCT block.
- **FORMAT-F RCT is full.**—Displayed if the RCT is overflowed with too many bad blocks.
- **FORMAT-F RCT read error**—Displayed if all copies of some block of the RCT cannot be successfully read.
- **FORMAT-F RCT write error**—Displayed if all copies of some block of the RCT cannot be successfully written.
- **FORMAT-F SDI receive error.**—Displayed if a track cannot be read at all after it has been formatted.
- **FORMAT-F Too many bad RBNs found before RCT was formatted.**—Displayed if more RBNs than can be recorded in memory are encountered before the RCT area has been formatted.

- **FORMAT-F Unsuccessful SDI command.**—Displayed if the drive fails to respond to an SDI command. FORMAT issues SEEK, RECALIBRATE, and DRIVE CLEAR SDI commands.

7.4.3.4 Warning Message

The FORMAT utility displays only one warning message.

- **FORMAT-W WARNING: Possible head addressing problem; run diagnostics.**—Displayed if no sector could be successfully read from one or more tracks in the XBN area. Note that all cylinders are checked. This is a simple check for a bad head.

7.4.3.5 Information Messages

Following are the information messages displayed by FORMAT.

- **FORMAT-I Bad LBN *n (x)*, a non-primary revector.**—Displayed for LBNs retired by being revectored to some RBN other than the primary RBN; they are marked in the RCT as nonprimary revectors. They are formatted with a header code of "non primary" or with a header code of "bad" if their header area is bad. The variable *x* indicates whether the RBN was found bad in the "FCT" or was determined to be bad in the "check" pass.
- **FORMAT-I Bad LBN *n (x)*, a primary revector to RBN *n*.**—Displayed for LBNs retired by being revectored to the first RBN on the same track; they are marked in the RCT as primary revectors. They are formatted with a header code of "primary". The variable *x* indicates whether the RBN was found bad in the "FCT" or was determined to be bad in the "check" pass.
- **FORMAT-I Bad LBN *n (x)*, in the RCT area.**—Displayed for retired LBNs in the RCT area. They are formatted with a header code of "bad". The variable *x* indicates whether the RBN was found bad in the "FCT" or was determined to be bad in the "check" pass.
- **FORMAT-I Bad RBN *n (x)*.**—Displayed for retired RBNs. They are marked bad in the RCT and are formatted with a header code of "bad". The variable *x* indicates whether the RBN was found bad in the "FCT" or was determined to be bad in the "check" pass.
- **FORMAT-I CTRL/Y or CTRL/C abort.** – Displayed if the user aborts FORMAT by entering a Ctrl/Y or Ctrl/C. Note that this probably leaves the disk in an unusable state if the format has begun.
- **Cylinder *n*, Group *n*, Track *n*, Position *n*, PBN *n*.** – Displayed following any of the four "FORMAT-I– Bad LBN/RBN..." messages if the user requested the special option to display the position of bad blocks.
- **FORMAT-I FCT was not used.**—Displayed if the FCT on the disk was found to be null or clobbered. In this case, FORMAT used the best guess mode to format the disk.
- **FORMAT-I FCT was used successfully.**—Displayed if a valid FCT was found on the disk and was used to obtain bad block information.
- **FORMAT-I *n* cylinders left in *x*BN space at *hh:mm:ss.xx*.**—Displayed after every 10 cylinders are formatted in order to record the progress of the FORMAT program.
- **FORMAT-I Only DBN area formatted (*n* bad DBNs.)**—Displayed if the user requested formatting of the DBN area only. It displays after the format of the DBN area is completed. After this message displays, the program terminates.

7.4.3.6 Error Messages

Following are the error messages displayed by FORMAT.

- **FORMAT-E Illegal response to start-up question.**—Displayed if an invalid input is supplied for a start-up question. The program reprompts with the same question.
- **FORMAT-E Nondefaultable parameter.**—Displayed if the user enters only Return, requesting the default for the only nondefaultable parameter (the serial number). FORMAT reprompts for the serial number.

7.4.3.7 Success Messages

Following are the FORMAT success messages.

- **FORMAT-S Format begun.**—Displayed when FORMAT actually begins formatting the disk.
- **FORMAT-S Format completed.**—Displayed after the format process is done and all verification tests are complete.

7.5 PATCH — Offline Load Media Modification Utility

The PATCH utility is designed to modify files on the HSC controller load media. You can also use it to examine locations within a file without modifying the file.

After you make changes to the load medium, the system version number is incremented on both the system and utility software. Because the version number is included in the checksum, make sure you install patches in the exact order supplied. All previously shipped patches must be installed before you make a new patch. Make sure you supply a checksum to verify the patch has been properly installed.

7.5.1 PATCH Commands

Table 7–1 lists the PATCH commands to enter in response to the PATCH prompts. All commands, except control characters (such as Ctrl/C or Ctrl/Y), must be terminated by pressing Return. In all instances, the current location refers to the file location of the address (Base + Offset) and the contents displayed under the *Old* column.

Table 7–1 PATCH Commands

Command	Function
Return	Closes the current location without modifying it, and opens and displays the next consecutive location.
n	Sets the current location to a value of n, closes it, and opens and displays the next location.
^	Closes the current location without modifying it and opens and displays the previous location.
n^	Sets the current location to n, closes it, and opens and displays the previous location.
;B	Backs up to the previous prompt. If requesting new value, backs up to Offset. If at Offset, backs up to Base. If at Base, prompts for the checksum.
;C	Restores the value originally in the open location. Used when an incorrect location is modified.
;E	Exits to the checksum prompt. If entered at the checksum question, causes PATCH to exit without making any modifications to the file.
;Q!n ;Q!n^	Performs a logical inclusive OR of the contents of the open location with n, and opens and displays the contents of the next (or previous) location.

Table 7–1 (Cont.) PATCH Commands

Command	Function
;Q&n ;Q&n^	Performs a logical AND of the contents of the open location with n, and opens and displays the contents of the next (or previous) location.
;V	Displays all changes made to the file during the current session.
Ctrl/C Ctrl/Y	Exits PATCH without modifying the file.

7.5.2 Running PATCH

The following section describes the steps in the PATCH operation. Each PATCH prompt is described, as well as the input you must supply.

Before running PATCH, take all disks and tapes offline that are attached the HSC controller to be patched. Take the HSC controller offline, or fail over to an alternate HSC controller in the cluster.

To initiate PATCH, enter the following command at the HSC> prompt:

```
HSC>RUN PATCH [Return]
PATCH-I Patches made:
      No patches recorded.
```

The "Patches made" message refers to the number of patches currently installed in the software. When the session is first started, no number is given.

PATCH prompts for the device and name of the file to be patched.

```
HSC>PATCH-Q RX33 Unit and filename (dev:file.ext) [SY:]?
```

Enter the file and device name. To use the default system drive, specify only the filename. Refer to the following table for special considerations.

If	Then
The file being modified with PATCH is on the device containing the system or utility software.	Install system and utility software of the same revision level.
The system version numbers do not match.	PATCH displays an error message, releases all acquired resources, and terminates.
The file or device name is invalid.	PATCH displays an error message and prompts for another file and device name.
The filename extension is .SAV.	The load device unit is acquired for exclusive access and all changes by other programs are locked out.
The filename extension is not .SAV.	The SYSCOM.INI file on the system medium and the 2NDTAP.VER on the utility medium are accessed to compare the system version numbers.

PATCH now locates the file and checks the version numbers. Next, PATCH prompts for the base address of the patch.

```
Base    (O) [000034]?
```

If the base address is odd, PATCH displays all values as bytes, rather than word values, unless no file was specified.

PATCH next prompts for the offset address of the patch.

```
Offset (O) [000000]? (100)
```

The default offset address is zero. If the offset address is odd, PATCH displays all values as bytes, rather an word values, unless no file was specified.

PATCH prompts for the new contents of the file location.

```
Base     Offset    Old      New?
aaaaaa   bbbbbb    cccccc   ?
```

Enter the new contents of the file location in the *New* field. Each field in the prompt is described in the following table:

Field	Meaning
aaaaaa	Base address as supplied
bbbbbb	Current offset
cccccc	Current contents of file location (sum of base and offset)
?	New contents of the file location, as supplied in the patch documentation

Press Return after entering in the new location contents. PATCH automatically increments the offset to the next address, displays the current contents of that location, and prompts for a new location contents. Use ;B to enter new address/offset values as directed by the patch documentation, and continue installing the patch data until completed.

Enter ;V to list the patch locations for verification. Check the changes carefully, and when you are satisfied that all data has been entered correctly, exit the data entry prompt by entering ;E. If you discover a mistake, enter Ctrl/C to abort the program without the patch, and start over.

After entering ;E, PATCH next prompts for the checksum.

```
Enter checksum?
```

Enter the checksum given in the patch documentation. If you enter the wrong value, patch gives you an error message and reprompts for the checksum. PATCH does not make any changes to the file until you have entered the checksum.

Next, PATCH prompts for an identification string:

```
Enter patch id?
```

Enter the *patch_id* supplied with the patch. PATCH now asks for verification of the ID:

```
Is this the correct id (Y or [N])?
```

PATCH then proceeds with the patch operation and displays a message indicating whether the patch was successful and what patches were made.

After a patch has been installed using the PATCH utility, many SETSHO parameters cannot be SET until the HSC controller has been rebooted. The affected parameters are those which require the System Configuration Table (SCT) to be updated. If you try to SET these parameters before rebooting the HSC controller, the following message is displayed:

```
SETSHO-Q MEDIA VERSION MISMATCH.  Correct media problem.
       Press RETURN to continue, CTRL/Y to abort:
```

You can use any of the SETSHO SHOW commands to display the previously set commands before rebooting.

After installing the patch, reboot the HSC controller and verify that the system version number is incremented on both the system and utility software. COPY the patched media to any backup media as required and return the system to service.

7.5.3 Sample Session

Example 7–1 is a sample PATCH session. The checksum shown is an arbitrary value. *This example is for display only.*

```
HSC>RUN PATCH Return
 PATCH-I Patches made:
     No patches recorded.
PATCH-Q Unit and filename (dev:file.ext) [SY:]?PATCH.UTL
Base (O)    [000034]?)12000
Offset (O)  [000000]?) Return
   Base     Offset     Old      New?
  012000    000000    004767    ?137
  012000    000002    010524    ?15000
  012000    000004    012700    ?;E
Offset (O)  [000004]?;E
Base (O)    [012000]?15000
Offset (O)  [000004]?0
   Base     Offset     Old      New?
  015000    000000    000000    ?12701
  015000    000002    000000    ?177560
  015000    000004    000000    ?137
  015000    000006    000000    ?1004
  015000    000010    000000    ?;E
Enter checksum?)12345
Enter patch id:PATCH_06789

Is this the correct id (Y or [N]?Y
PATCH-S Wait...
PATCH-S 6 changes made
```

Example 7–1 Example Patch of a File

1. Base is *12000*
2. Offset is *0* (default)
3. Replace *4767* with *137*
4. Replace *10524* with *15000*
5. Back up to new Offset
6. Back up to new Base
7. New Base of *15000*
8. New Offset of *0*
9. Insert new values...
10. Exit command
11. Enter checksum of *12345*
12. Enter the ID supplied with the patch
13. Verify ID, if you answer *N* PATCH reprompts you for another ID

7.5.4 Error and Information Messages

This section describes the messages that may be displayed during a PATCH operation. The most common causes of the errors and the correct actions are included.

7.5.4.1 Fatal Error Messages

The following fatal error messages are issued by PATCH:

- **PATCH–F Cannot access PATCH data file** – PATCH cannot access the file you specified to be patched.
- **PATCH–F Cannot Access Version On Off-line Diagnostic medium**—PATCH could not access the file OFLLDR.SAV on the offline diagnostic utility medium.
- **PATCH–F Cannot Access Version On System medium** – PATCH could not access the file SYSCOM.INI on the system medium. If this message displays after the *Wait ...* message is displayed, a serious bug or problem exists with the load medium. If the message displays just after the filename has been entered, the system medium is probably not mounted.
- **PATCH–F Cannot Access Version On Utility medium**—PATCH could not access the file 2NDTAP.VER on the utility medium. If this message displays after the *Wait ...* message is displayed, a serious bug or problem exists with the load device. If this message displays just after the filename has been entered, the utility medium is probably not mounted.
- **PATCH–F File Not Found**—The user specified a nonexistent file. PATCH exits cleanly.
- **PATCH–F Insufficient Resources To Run**—The program could not acquire the resources to run. Sufficient common pool memory is not available to allocate the necessary structures.
- **PATCH–F Read Failure: *block-number***—When PATCH attempted to read the specified block of the file, a media error occurred that cannot be recovered. PATCH exits cleanly.
- **PATCH–F You cannot PATCH this file**—The filename you specified cannot be patched.
- **PATCH–F Unit(s) write-protected: update was not done**—The disk unit on which the load medium to be patched resides is write protected.
- **PATCH–F Version On System Medium Does Not Match Utility Medium**— The version numbers on the system and utility media do not match, indicating media from two different revision levels are being used.
- **PATCH–F Write Failure: *block-number***—When PATCH attempted to update the file with the requested changes, a media error that cannot be recovered occurred in the specified file block. This is the most serious of errors because both file and medium integrity are questionable. The usual recovery is to restore the medium with the backup copy made before starting the patch.
- **PATCH–F Write failure during write check, status: *block number***—PATCH verifies that a file can be written before it actually writes to the file. You will get this message if the the file cannot be written for some reason other than the file being write protected or a recoverable software error.

7.5.4.2 PATCH Error Messages

The following error messages are issued by PATCH:

- **PATCH–E Incorrect Checksum**—You entered a checksum different from the checksum PATCH calculated. PATCH repeats the checksum question.
- **PATCH–E Invalid Command**—You entered information out of context.

- **PATCH–E Invalid Device Name Or Switch**—You entered an invalid device name (not the load medium) or the syntax of the filename is incorrect.

7.5.4.3 Warning Messages

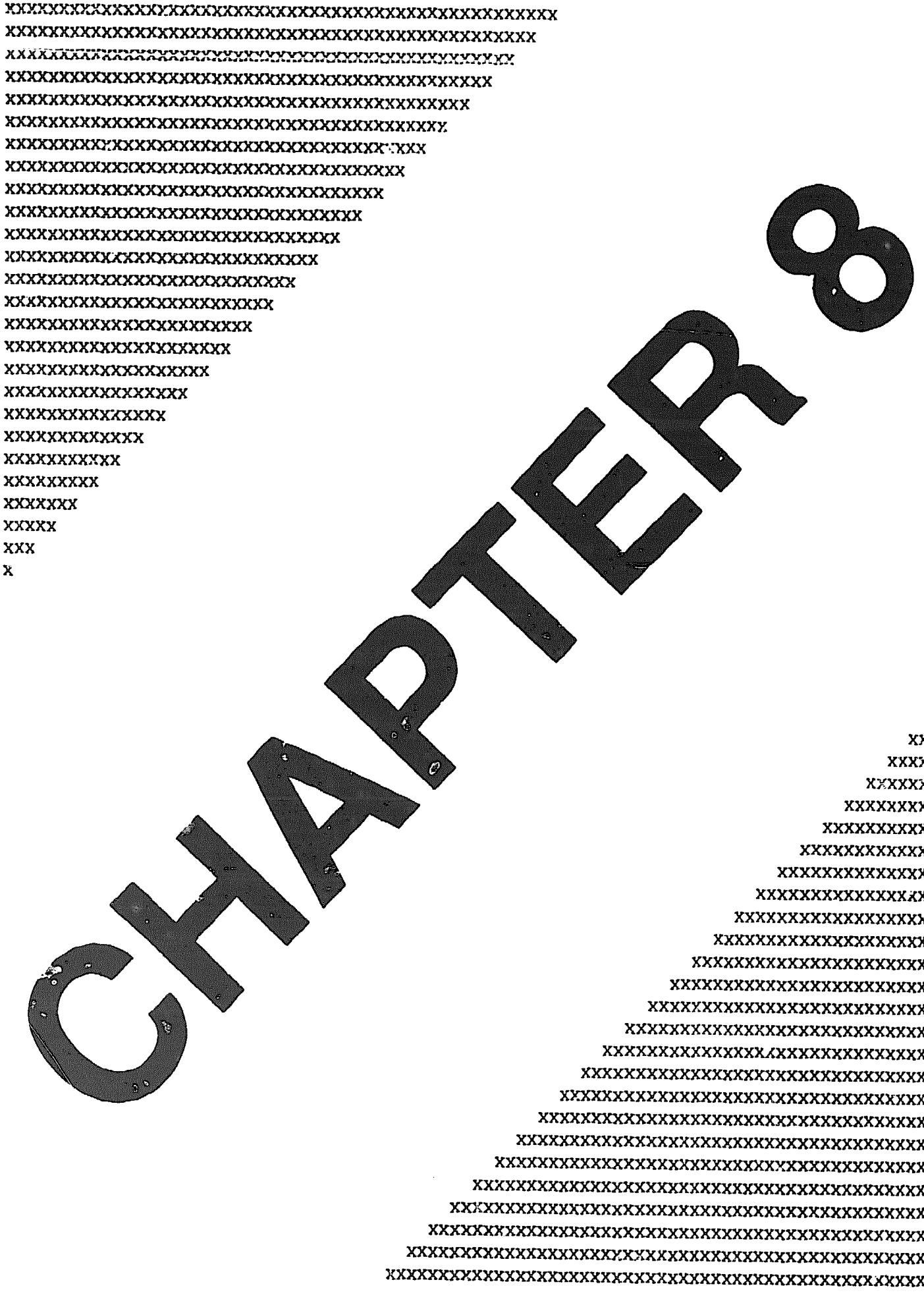
- **PATCH–W Buffer Space Exhausted**—You entered a patch when the internal buffers were full.
- **PATCH–W Nonfile Structured Mode Assumed** – You entered a null filename. This message is a reminder that all patches will now be applied to the load medium as a whole instead of to a specific file.

7.5.4.4 Informational Messages

- **PATCH–I Checksum = *octal–checksum* (O)**—You entered the **;X** command, requesting that a checksum prompt not be displayed.
- **PATCH–I CTRL/Y Or CTRL/C Abort**—You entered a Ctrl/Y or Ctrl/C. No changes are made to the file unless the abort occurs during the update, after the *Wait...* message has been displayed.
- **PATCH–I No patches recorded**—In a normal session, PATCH informs you of how many patches have been made. You will get this message if PATCH records no patches in the file PATCH.DAT, the file used to keep track of the patches made.
- **PATCH–I Patches made:**—PATCH completes and displays the patches made following the colon (:).

7.5.4.5 Success Messages

- **PATCH–S *patch–count* Changes Made**—You exited PATCH. The value of *patch–count* is the number of changes made to the file. Note that if you modify and then restore a location, it is not considered a change. The file is only rewritten when *patch–count* is not a zero.
- **PATCH–S Wait...**—PATCH has started writing changes to the file.


CHAPTER 8

8
Troubleshooting Techniques

8.1 Introduction

This chapter describes the types of errors that may occur during HSC controller boot and operation. The major divisions are initialization errors and system-type errors. Initialization errors occur while the HSC controller is trying to boot. System-type errors occur while the HSC controller is running functional code. System-type errors may be reported to a host node and possibly the HSC console device. Some system errors may result in the HSC controller crashing and rebooting. System errors include MSCP, TMSCP, BBR, and out-of-band errors.

8.2 How To Use This Chapter

Initialization error indications are displayed by the operator control panel (OCP) fault codes and the module LEDs. In addition, the bootstrap diagnostics may produce error messages displayed on the console. Read Section 8.3 for an understanding of initialization errors that do not produce a message. All errors displayed as English messages on the console are listed in alphabetical order in Section 8.5 and are also listed in this manual's index. Section 8.3 divides initialization errors into three types:

- OCP fault codes
- Module LEDs
- Boot diagnostic messages

HSC console error message descriptions for system-type errors are described in this chapter and are organized into the following sections:

- MSCP/TMSCP errors, Section 8.4.2
  - — Controller errors, Section 8.4.2.1
  - — MSCP SDI errors, Section 8.4.2.2
  - — Disk transfer errors, Section 8.4.2.3
- BBR errors, Section 8.4.2.4
- TMSCP errors, Section 8.4.3
  - — STI communication or command errors, Section 8.4.3.1
  - — STI formatter error log, Section 8.4.3.2
  - — STI drive error log, Section 8.4.3.3
- Out-of-band errors, Section 8.4.4

8.3 Initialization Error Indications

Initialization errors are indicated by:

- OCP fault code displays
- Module LEDs
- Boot diagnostic messages

8.3.1 OCP Fault Code Displays

OCP fault codes are divided into two categories: hard fault codes and soft fault codes. Soft fault codes are also called nonfatal fault codes. Soft faults impede HSC controller operation, but the fault does not hinder the boot process. Hard fault codes are fatal to the HSC controller and prevent further operation of the HSC subsystem until the condition is remedied.

Figure 8–1 shows possible displays on the OCP in the event of errors during initialization or operation.

DESCRIPTION	HEX	OCT	BINARY	OCP INDICATORS				
				INIT	FAULT	ON. INE		
K.PLI/K.PLI2 ERROR	01	01	00001	OFF	OFF	OFF	OFF	
K.SDI/K.SI INCORRECT VERSION OF MICROCODE	02	02	00010	OFF	OFF	OFF		OFF
K.STI/K.Si INCORRECT VERSION OF MICROCODE	03	03	00011	OFF	OFF	OFF		
P.IOJ CACHE FAILURE[1]	08	10	01000	OFF		OFF	OFF	OFF
K.CI FAILURE[1]	09	11	01001	OFF		OFF	OFF	
DATA CHANNEL MODULE ERROR[1]	0A	12	01010	OFF		OFF		OFF
P.IOJ/C MODULE FAILURE	11	21	10001		OFF	OFF	OFF	
M.STD2/M.STD4 MODULE FAILURE[4]	12	22	10010		OFF	OFF		OFF
BOOT DEVICE FAILURE[2]	13	23	10011		OFF	OFF		
PORT LINK NODE ADDRESS SWITCHES OUT OF RANGE	15	25	10101		OFF		OFF	
MISSING FILES REQUIRED[3]	16	26	10110		OFF			OFF
NO WORKING K.CI, K.SDI, K.STI, OR K.SI IN SUBSYSTEM	18	30	11000			OFF	OFF	OFF
INITIALIZATION FAILURE	19	31	11001			OFF	OFF	
SOFTWARE INCONSISTENCY	1A	32	11010			OFF		OFF
ILLEGAL CONFIGURATION[5]	1B	33	11011			OFF		

1. THESE ARE TERMED SOFT OR NONFATAL ERRORS.
2. POSSIBLE MEMORY MODULE/CONTROLLER (EXCEPT ON THE HSC50 CONTROLLER).
3. THIS FAULT CODE WILL ALSO BE DISPLAYED IF THE P.IOC MODULE IS NOT AT THE MINIMUM REVISION LEVEL.
4. SWAP MEMORY MODULE FIRST. IF PROBLEM PERSISTS, TRY REPLACING THE P.IOJ/C MODULE.
5. REFER TO TABLE 1-1 AND CHECK PROPER MODULE CONFIGURATION.

CXO-3133A

Figure 8–1 Operator Control Panel Fault Codes

8.3.1.1 Fault Code Interpretation

All failures occurring during the Init P.io test are reported on the OCP LEDs. When the Fault indicator is lit, pressing the Fault switch results in the display of a failure code in the OCP LEDs. This code indicates which HSC module is the most probable cause of the detected failure. The failure code blinks on and off at 1-second intervals until the HSC controller is rebooted if the fault code represents a fatal fault. A soft fault code is cleared in the OCP by pressing the Fault switch

a second time. To restart the boot procedure, press the Init switch. To identify the probable failing module, refer to Figure 8–1.

The following paragraphs describe specific fault codes displayed in the OCP indicators. All fault codes are indicated with octal values.

- **Fault Code 1, Port processor error**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
01	01	00001	OFF	OFF	OFF	OFF	ON

CXO-2666A

Figure 8–2 OCP Fault Code 1

Fault code 1 indicates the CIMGR initialization routine discovered bad requestor status from a previously tested good requestor module in requestor slot 1. The expected requestor status should be 001. The FRU is the port processor module.

During CIMGR initialization, the K.ci is directed to set the HSC controller node address into its own control structure. If the K.ci failed to modify this node address field one-half second after K.ci requestor initialization, fault code 1 is displayed. In addition, the port processor microcode version is checked to ensure it is compatible with this functional version. If compatibility checks fail, this fault code is displayed.

Run offline diagnostics to test the K.ci requestor. Replace the port processor module on failure. If the fault code persists, refer to the HSC revision control document to verify all HSC controller components are at the current revision.

- **Fault Code 2, K.sdi/K.si incorrect version of microcode**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
02	02	00010	OFF	OFF	OFF	ON	OFF

CXO-2667A

Figure 8–3 OCP Fault Code 2

All disk data channel modules are initialized during the disk server functional code initialization. If a disk data channel module passes initialization, the disk server initialization code checks the disk data channel module microcode version number to ensure it is compatible with this version of functional code. If code versions are not compatible, fault code 2 is displayed. The FRU is the disk data channel module.

- **Fault Code 3, K.sti/K.si incorrect version of microcode**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
03	03	00011	OFF	OFF	OFF	ON	ON

CXO-2668A

Figure 8–4 OCP Fault Code 3

Fault code 3 indicates tape data channel module microcode is incompatible.

- **Fault Codes 10, 11, and 12, Soft errors**

Faults codes 10, 11, and 12 are the soft or nonfatal errors related to the disk/tape data channels, the K.ci host interface, and the I/O control processor cache. None of these errors causes the HSC controller functional operation to suspend when the fault is reported. Once displayed, soft error indicators cannot be recalled. The HSC controller may buffer up to eight soft fault codes. Subsequent toggling of the Fault switch displays all remaining soft fault codes until the buffer is empty.

— **Fault Code 10, Pioj cache failure**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
08	10	01000	OFF	ON	OFF	OFF	OFF

CXO-2669A

Figure 8–5 OCP Fault Code 10

Fault code 10 is displayed for any failure detected in the J–11 instruction cache during HSC subsystem initialization. This fault results in disabling the cache while the HSC controller continues operation. Replace the I/O control processor module and reboot.

— **Fault Code 11, K.ci failure**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
09	11	01001	OFF	ON	OFF	OFF	ON

CXO-2670A

Figure 8–6 OCP Fault Code 11

Fault code 11 indicates one or more modules of the K.ci set is not present or has failed its initialization tests. This fault is displayed while the HSC controller continues to operate. The most probable FRU is the port link module.

— **Fault Code 12, Data channel module failure**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
0A	12	01010	OFF	ON	OFF	ON	OFF

CXO-2671A

Figure 8–7 OCP Fault Code 12

Fault code 12 reports an unknown requestor type was found in a requestor slot other than 0 or 1. Expected valid requestor types for requestor slots 2 through 8 are either 002 for a disk data channel module, or 203 for a tape data channel module.

The 4-Port data channel module will answer with 205 if it is initiated as a disk data channel or with 206 if it is initiated as a tape data channel. The 8-Port data channel module can only be initialized as a disk data channel and answers with an 007. The failing module is identified by being the data channel module with a lit red LED indicator.

- **Fault Code 21, I/O control processor module failure**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
11	21	10001	ON	OFF	OFF	OFF	ON

CXO-2672A

Figure 8–8 OCP Fault Code 21

Fault code 21 indicates the I/O control processor module is the most probable cause of the failure detected by the Init P.io test. If possible, run the offline P.io test for a more definitive report on the error. Otherwise, replace the I/O control processor module and run the Init P.io test again. If the test still fails, run the offline P.io test to help further isolate the failure.

- **Fault Code 22, Memory module failure**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
12	22	10010	ON	OFF	OFF	ON	OFF

CXO-2673A

Figure 8–9 OCP Fault Code 22

Fault code 22 indicates the memory module is the most probable cause of this bootstrap failure. Possible causes include:

— The failure of the memory test of the first 1 Kword (vector area) of program memory as well as the use of the Swap Banks bit in the I/O control processor in trying to correct the problem (test 2).

— A contiguous 8-Kword partition not found in program memory below address 00160000 (test 3).

— A hard fault detected in the RX33 controller logic (test 4).

Determine the error that occurred by examining physical location 17772340, which contains the number of the failing boot ROM test. In each of these cases, replace the memory module, and run the initialization tests again. If the module still fails, run the offline P.io test. Refer to Section 6.12.8 for information on troubleshooting registers and displays using ODT.

Enter the SETSHO utility and execute the SHO MEM command. If any memory locations appear in the suspect or disabled memory locations list, set the Secure/Enable switch to ENABLE and execute the SET MEM ENABLE ALL command.

- **Fault Code 23, Boot device failure**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
13	23	10011	ON	OFF	OFF	ON	ON

CXO-2674A

Figure 8–10 OCP Fault Code 23

Fault code 23 indicates a problem with an HSC boot device, the system media, the boot device controller, or the read/write logic on the memory module. This fault can be any of the following, in order of least likely cause to most likely cause:

— A failure in the I/O control processor.

— A failure in the read/write logic of the memory module.

— A faulty boot device controller/drive interface cable. Replace the cable.

— Diskettes or tapes not installed in the drives.

— Doors left open on the RX33 drives.

— Tape improperly inserted in the TU58 tape drive.

— No bootable image in the system device media.

Ensure a known good HSC bootable media is properly loaded in the system boot device. If checking the obvious (doors, diskettes, or tapes) does not remedy the situation, refer to Chapter 6 for more information before beginning repair. Running the offline P.io and offline RX33 or TU58 tests (if possible) is strongly recommended before modules are replaced. These tests may help further isolate or define the problem.

- **Fault Code 25, port link node address switches out of range**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
15	25	10101	ON	OFF	ON	OFF	ON

CXO-2675A

Figure 8–11 OCP Fault Code 25

Fault code 25 indicates the port link module node address switches are set to a value outside the currently suggested range of 32 decimal (HSC software V3.90).

- **Fault Code 26, missing files required**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
16	26	10110	ON	OFF	ON	ON	OFF

CXO-2676A

Figure 8–12 OCP Fault Code 26

Fault code 26 indicates the system diskette does not contain one of the files necessary for operation of the HSC control program. This failure should occur only if one of the required files is inadvertently deleted from the HSC system media.

Note that the condition of the State indicator must be observed prior to the fault occurrence. The State indicator is always steady (either ON or OFF) when the Fault indicator is lit during boot faults.

If the State indicator is steady (ON), it can mean:

— SYSCOM.INI is not present on the load device.

— EXEC.INI is not present on the load device.

— A version mismatch exists between either EXEC, SUBLIB, or SYSCOM and OLBVSN (Object Library Version Number).

If the State indicator was blinking before the fault, it can mean:

— Any of the the normally loaded programs (SINI, CERF, DEMON, etc.) are not present on the load device.

— A version mismatch exists on any one of the normally-loaded programs.

Replace the system media with a backup copy.

- **Fault Code 30, No working K.ci, K.sdi, K.sti, or K.si in subsystem**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
18	30	11000	ON	ON	OFF	OFF	OFF

CXO-2677A

Figure 8–13 OCP Fault Code 30

Fault code 30 indicates the HSC controller does not contain any working K.ci, or disk/tape data channel modules. Either no modules are installed in the HSC controller, or all of those installed failed their initialization diagnostics. Also, if the disk server code is loaded and no working disk data channel module is found, this fault code is displayed.

Insert the HSC Offline Diagnostic media into the appropriate system drive and reboot the HSC controller. When the offline loader prompts with ODL>, enter SIZE. The SIZE command displays the status of all the Ks. This status indicates whether the modules are missing or are failing initialization diagnostics.

If all else fails, replace the I/O control processor module and check subsystem power for proper operation.

- **OCP error code of 31, Initialization failure**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
19	31	11001	ON	ON	OFF	OFF	ON

CXO-2678A

Figure 8–14 OCP Fault Code 31

Fault code 31 indicates a crash occurred while the HSC controller was attempting to load and initialize its control program.

Use microODT to diagnose these initialization crashes, as follows:

1. For HSC50 controllers only, press the break key on the local console terminal.
2. Enter 17 777 656/.

   This is the address of the UPAR7 register. The code that indicates the reason for the reboot is stored in UPAR7 bits 8 to 11 when OCP code 31 has been detected. The other UPAR registers store useful information for some of the errors related to an OCP fault code of 31. Refer to the fault code 31 reasons in the following paragraphs for UPAR content usage. Table 8–1 shows the addresses of the UPAR registers.

Table 8–1 UPAR Register Addresses

Register	Address
UPAR0	17 777 640
UPAR1	17 777 642
UPAR2	17 777 644
UPAR3	17 777 646
UPAR4	17 777 650
UPAR5	17 777 652
UPAR6	17 777 654
UPAR7	17 777 656

3. Analyze bits 8 to 11 of the 16-bit message displayed by examining UPAR7. Table 8–2 shows the bit/error relationship.

Table 8–2 Control Program Bits

16 Bit Message	Meaning	FRUs
X XXX XXX 1XX XXX XXX	NXM	I/O control processor module Memory module Software
X XXX XX1 0XX XXX XXX	Illegal inst.	I/O control processor module Memory module Software
X XXX XX1 1XX XXX XXX	Parity trap	Memory module I/O control processor module
X XXX X10 0XX XXX XXX	Level 7 interrupt	Data channel module port processor
X XXX X10 1XX XXX XXX	MMU trap	I/O control processor module Software
X XXX X11 0XX XXX XXX	Software crash	Software
X XXX X11 1XX XXX XXX	K.ci host reset	Memory module
X XXX 100 0XX XXX XXX	User requested reboot	N/A

4. If this error occurs repeatedly, it indicates an intermittent hardware error or degraded diskette media. The boot-in-progress flag is indicated by KPDR7 bit 3 set. The KPDR7 register address is 17 772 316. Use microODT to examine bit 3 (it can be reset).

The following list describes actions to be taken for each type of error related to OCP fault code 31 as pointed out by examining UPAR7:

— **NXM trap**: Examine UPAR1 to find the lower 16 bits of the failing memory address by typing 17 777 642/. Examine UPAR2's lower byte for the high 6 bits of the failing memory address by typing 17 777 644/.

— **Illegal inst**: Replace the I/O control processor module.

— **Parity trap**: Use the same method for parity traps as for NXM traps to determine the failing address.

— **Level 7 interrupt**: Determine which K UPAR4. Refer to Table 8–1 for the address of each UPAR register. Each byte of each register contains module status for each requestor (K) in the HSC controller. Refer to Appendix C to determine a failing status code. Table 8–3 shows the designation of requestors to UPAR registers for a Level 7 interrupt.

Table 8–3 Status of Requestors for Level 7 Interrupt

Register	High Byte	Low Byte
UPAR0	REQ 2	REQ 1
UPAR1	REQ 4	REQ 3
UPAR2	REQ 6	REQ 5
UPAR3	REQ 8	REQ 7
UPAR4	N/A	REQ 9

— **Memory management unit (MMU) trap**: Examine UPAR1, UPAR2, and UPAR3 to determine the status of the MMU at the time of the OCP fault code 31. When an MMU trap occurs, status of the MMU is found in these registers.

— **Software crash**: Try using another copy of the boot media. If the problem is not corrected, replace the I/O control processor module. If the problem still persists, replace the memory module.

— **Kci host reset**: Press the break key again and at the @ symbol enter 17 770 000/ when a host reset is known as the reason for an OCP fault code of 31. This is the address of control memory window 0. When the / is pressed, the contents of control window 0 are displayed. Enter a 0 into this location followed by a Return. Then enter 17 760 002/. This is the second location in control memory. The number displayed as the contents of 17 760 002 is the number of the host that issued the HOST RESET command.

- **OCP error code 32, Software inconsistency**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
1A	32	11010	ON	ON	OFF	ON	OFF

CXO-2679A

Figure 8–15 OCP Fault Code 32

Fault code 32 indicates an inconsistency in the software. Reboot the HSC controller. If this failure persists, use a backup copy of the system media. If the failure still persists, use the Offline diagnostics to help isolate any hardware failures in the subsystem. Also, try using an earlier version of the HSC operating software.

- **OCP error code 33, Illegal configuration**

CODE VALUE			OCP INDICATORS				
HEX	OCT	BINARY	INIT	FAULT	ONLINE		
1B	33	11011	ON	ON	OFF	ON	ON

CXO-2906A

Figure 8–16 OCP Fault Code 33

Fault code 33 indicates that you have installed an illegal configuration of modules in the HSC backplane. Table 8–4 lists the elements that the HSC software checks to verify that a legal configuration exists in the HSC controller. Note that the following modules are not checked for proper configuration: Link (L0118–YA) and Buffer (L0109–00, L0109–YA, or L0125–AA).

In HSC software V6.0 and higher, fault code 33 is accompanied by a console message listing the illegal modules in the HSC controller backplane.

Table 8–4 Required Configuration Checks for HSC Controllers

HSC Model	Configuration Check
HSC40	15 MHz IO Processor module (L0111–YA) installed K.pli2 Port Processor module (L0124–AA) not installed No 8-port K.si modules (L0119–YB) installed in any requestors No modules installed in requestors 5 through 9 No M.Cache module (L0121–AA) installed
HSC70	15 MHz IO Processor module (L0111–00) installed K.pli2 Port Processor module (L0124–AA) not installed No 8-port K.si modules (L0119–YB) installed in any requestors No M.Cache module (L0121–AA) installed
HSC60	18 MHz IO Processor module (L0111–YD) installed M.std4 Memory module (L0123–AA) installed K.pli Port Processor module (L0107–YA) not installed No 8-port K.si module (L0119–YB) installed in requestor 2 No modules installed in requestors 5 through 9
HSC90	18 MHz IO Processor module (L0111–YC) installed M.std4 Memory module (L0123–AA) installed K.pli Port Processor module (L0107–YA) not installed No 8-port K.si modules (L0119–YB) installed in requestors 2, 7, 8, or 9

8.3.2 Module LEDs

HSC controller modules contain LEDs used as State indicators for each module. Refer to Chapter 2 for a summary of the function and location of all module LEDs. This section contains additional information on the indicators to be used in troubleshooting the HSC controller.

8.3.2.1 I/O Control Processor LEDs

Table 8–5 shows the I/O control processor LEDs and their functions.

Table 8–5 I/O Control Processor LEDs

LED	Color	Meaning
D1	Yellow	MicroODT—Used during J–11 power-up microdiagnostics. Lit when J–11 is executing microODT.
D2	Yellow	Terminal Port OK—Used during J–11 power-up microdiagnostics. Serial line unit (SLU) output of UART.
D3	Yellow	Memory OK—Used during J–11 power-up microdiagnostics. Turned off as J–11 successfully accesses program memory.
D4	Yellow	Sequencing indicator—Used during J–11 power-up microdiagnostics. Turned off as J–11 verifies proper functioning of its sequencers for control store.
D5	Yellow	State indicator—Mirrors the OCP State indicator (under software control).
D6	Yellow	Run indicator—Pulses at the on-board microprocessor run rate. Blinks once for every PDP–11 instruction fetched (J–11 run LED).
D7	Red	Board status—Indicates an inoperable module except during initialization when it is lit during module testing.
D8	Green	Board status—Indicates the module has passed all applicable diagnostics.

8.3.2.2 Power-up Sequence of I/O Control Processor LEDs

This section defines the power-up sequence of the LEDs shown in Table 8–5. First, LED numbers D8 and D7 are used to indicate whether the I/O control processor module has successfully completed all of its initialization diagnostics. The module powers up with the red (D7) LED lit and the green (D8) LED off. D1 through D4 (yellow) are initially lit. As soon as the J–11 starts operating, D1 (microODT LED) turns off.

Several microcode steps later, D4 (sequence LED) is turned off, indicating the J–11 is sequencing and has succeeded in reaching this point in its microcode. The J–11 performs several program memory operations and, if successful, turns off D3 (memory OK LED). Finally, the J–11 accesses the console terminal port of the UART (universal asynchronous receiver/transmitter) and turns off D2 (SLU LED).

Upon successful completion of the boot time initialization diagnostics, D8 (module OK LED) is lit, and D7 (module failure LED) turns off. The J–11 then proceeds to the software initialization programs.

In addition to being initially ON, the D1 (microODT run LED) is lit any time the J–11 is executing microODT. D6 (the fetch LED, sometimes referred to as the run LED) blinks once for every PDP–11 instruction fetch cycle. When the J–11 is running, D6 is illuminated at half-brilliance compared to the other yellow LEDs.

8.3.2.3 Memory Module LEDs

Table 8–6 shows the memory module LEDs and their functions. These LEDs are controlled by a bit in the system boot device FDC MAR02 register. The green LED is lit by the I/O control processor boot/ROM self-test diagnostics after the system boot device has passed its self-tests, and program memory has found 8-Kwords to load INIPIO/OFLPIO.

Table 8–6 Memory Module LEDs

LED	Color	Meaning
	Red[1]	Board status—Indicates an inoperable module except during initialization, when it comes on for testing.
	Amber[1]	Memory status—Lit during every memory cycle.
	Green[1]	Board status—Indicates the operating software is running and has successfully tested this module.
M.std4	Amber	Cache present—Indicates that an M.cache module is properly installed and cache memory is enabled
LED pack (M.std4 module only)	Amber (8 LEDs)	D1–Single bit error D2–Multiple bit error D3– High-byte parity error D4–Low-byte parity error D5 thru D8 -NIB3 thru NIB0 error

[1]All three of these LEDs are contained in a single package.

8.3.2.4 Data Channel Module LEDs

Table 8–7 shows the data channel module LEDs and their functions with the system software.

Table 8–7 Data Channel Module LEDs

LED	Color	Meaning
	Red	Module failure—Indicates a module microdiagnostic failed to successfully complete, or this module is still under initialization by the subsystem.
	Green	Module OK—Lit by the Init/Func Flag signal in the K functional microcode. The green LED is lit after successful initialization or while the data channel module is running functional microcode.
LED pack (K.si module only)	Amber (8 LEDs)	D1—Off for PROM load, lit for RAM load. D2 through D8—Upper register #2 contents. The LEDs reflect the implemented bits of the upper error register #2. When a microinstruction parity error is detected, the module clocks are inhibited, stopping the module. The bit content of the upper error register #2 is displayed on the LEDs.

8.3.2.5 M.cache Module LEDs

Table 8–8 shows the M.cache LEDs and their functions.

Table 8–8 M.cache Module LEDs

LED	Color	Meaning
	Green	Board status—Indicates the operating software is running and has successfully tested this module.
	Amber	Board status—Indicates module testing is in progress.
	Red	Board status—Indicates an inoperable module except during initialization, when it comes on during module testing.
D1	Amber	Single-bit ECC error—Lit when there is a single-bit ECC error.
D2	Amber	Multiple-bit ECC error—Lit when there is a multiple-bit ECC error.
D3	Amber	Hi-byte data memory parity error—Lit when there is a hi-byte data memory parity error.
D4	Amber	Lo-byte data memory parity error—Lit when there is a lo-byte data memory parity error.
D5	Amber	Functional state machine activity—Indicates the cache memory is being tested. The LED is lit for 4 to 5 seconds.
D6	Amber	Diagnostics state machine activity—Indicates the diagnostics are running. The LED will blink every 250-msec and will be hard to see unless you are watching closely for the blink.
D7	Amber	M.cache waiting to be enabled—Lit at the end of module testing. This LED will be lit regardless of the module pass/fail status and will stay lit until the I/O control processor module turns the M.cache module on after software initialization.
D8	Amber	Pattern compare failure—Lit when an error is found during pattern compare.

8.3.2.6 Host Interface LEDs

Table 8–9 lists the three modules in the K.ci host interface module set, their LEDs, and the functions of the LEDs with the system software.

Table 8–9 Host Interface Module Set LEDs

Module	LED	Color	Meaning
Port processor	D2	Red	Lit when the port processor module has booted or rebooted, but has not yet passed its self-test.
Port processor	D1	Green	Lit when the port processor module has passed its self-test.
Port buffer	D2	Red	Lit when the port buffer module has not yet passed the test performed by the port processor.
Port buffer	D1	Green	Lit when the port buffer module has passed the test performed by the port processor. This LED is controlled by the port processor.
Port buffer	D3	Yellow	Not found on all module revisions. lit when port processor is asserting Init. When Init is true, both the red and the green port buffer LEDs are forced off.
Port link	D998	Green	Lit when local activity is present on the port link module. Whenever the port link module detects a message directed to its node or when it detects an outgoing message.
Port link	D999	Red	Lit during the CI maintenance loop test.

8.3.3 Communication Errors

It is possible for the HSC controller to complete its initialization and not report the fact on the local console terminal. This is an indication of a failure in the serial communication path between the UART chip on the I/O control processor and the local console terminal.

As a method of testing this serial path, the HSC controller echoes the characters displayed on the local console terminal as if the terminal were in local mode. Use the following procedure to test the serial path:

1. Place the Secure/Enable switch in the ENABLE position.
2. With power on, push in and hold the OCP Init switch.
3. Enter a series of characters on the terminal keyboard.
4. Check to see that the series of characters is echoed correctly on the terminal.

NOTE
When the Init switch is released, the HSC controller reboots.

If this procedure fails to echo characters typed at the keyboard, the failure is either a terminal to I/O control processor baud-rate mismatch (default is 9600), a I/O control processor module failure, or a problem within the terminal-cabling subsystem. Ensure the terminal setup parameters are correct. Refer to the *HSC Controller Installation Manual* for the proper terminal configuration, the *VTxxx Owner's Manual* for problem-solving techniques related to the VTxxx, and the *DECwriter Correspondent Technical Manual* for solving problems related to the LA12.

8.3.4 Requestor Status Codes

When a requestor successfully completes all internal microdiagnostics, the requestor status (Status=) contains a code to define the module type. When a module fails internal microdiagnostics or its functional code, the status byte reflects the failure.

Refer to Appendix D for a complete list of host interface and disk/tape data channel module status codes.

8.3.5 HSC Boot Flow and Troubleshooting Chart

The HSC controller boot flow and troubleshooting chart calls out useful milestones that aid in troubleshooting problems which can occur during initialization. Figure 8–17 is a flowchart of the entire HSC controller boot sequence.

The flowchart has three main divisions:

- Information on activity common to both the system and offline diskettes is contained in boxes A through O
- Information on activity specific to the system diskette is contained in boxes SA through SJ
- Information on activity specific to the offline diskette is contained in boxes OA through OG

The flowchart begins when one of the following occurs:

- The Init button is pushed.
- Powerup has started.
- Other software caused reboot.

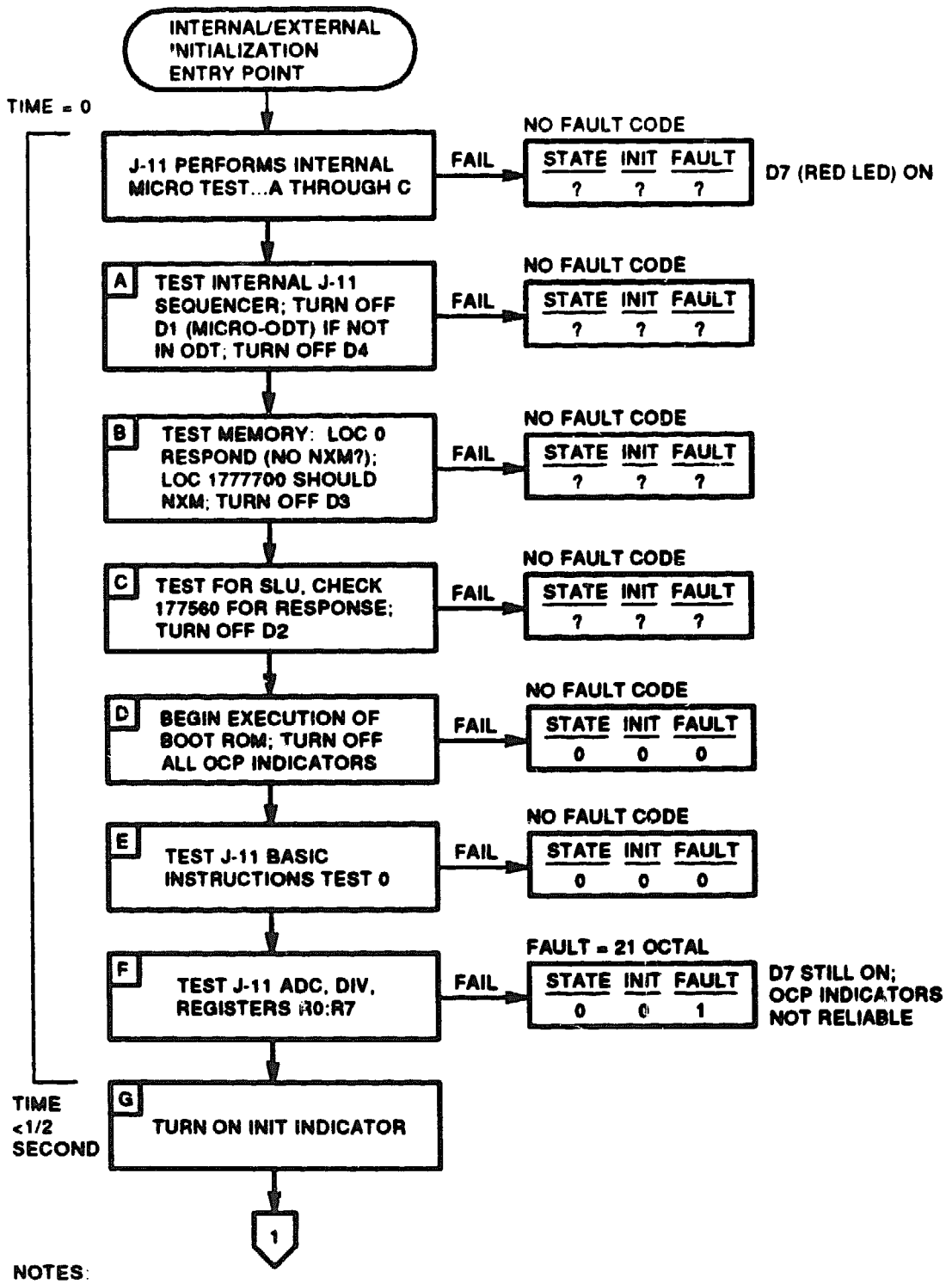
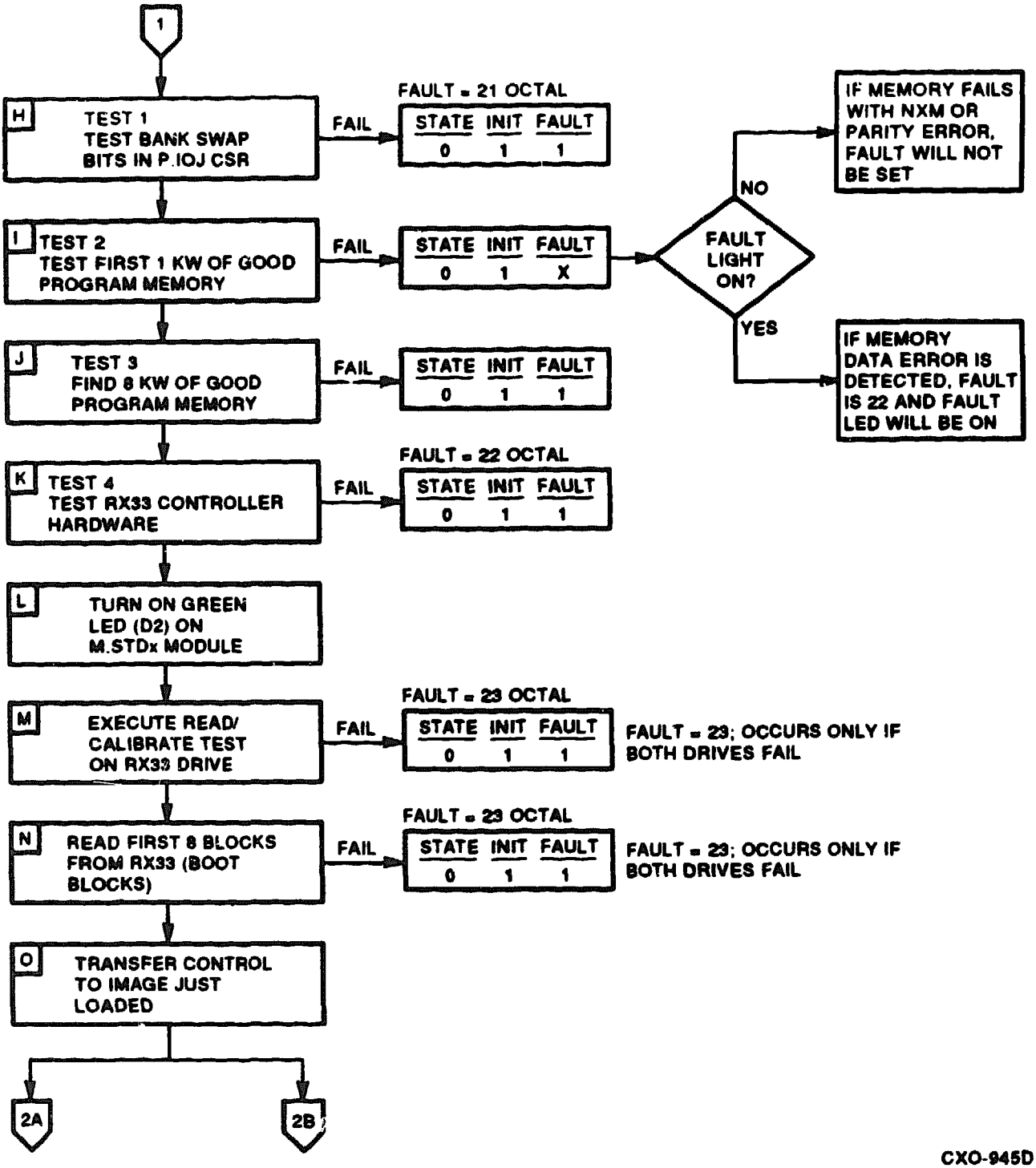


Figure 8–17 (Cont.) HSC Boot Flow and Troubleshooting Chart



CXO-945D
Sheet 2 of 5

Figure 8–17 (Cont.) HSC Boot Flow and Troubleshooting Chart

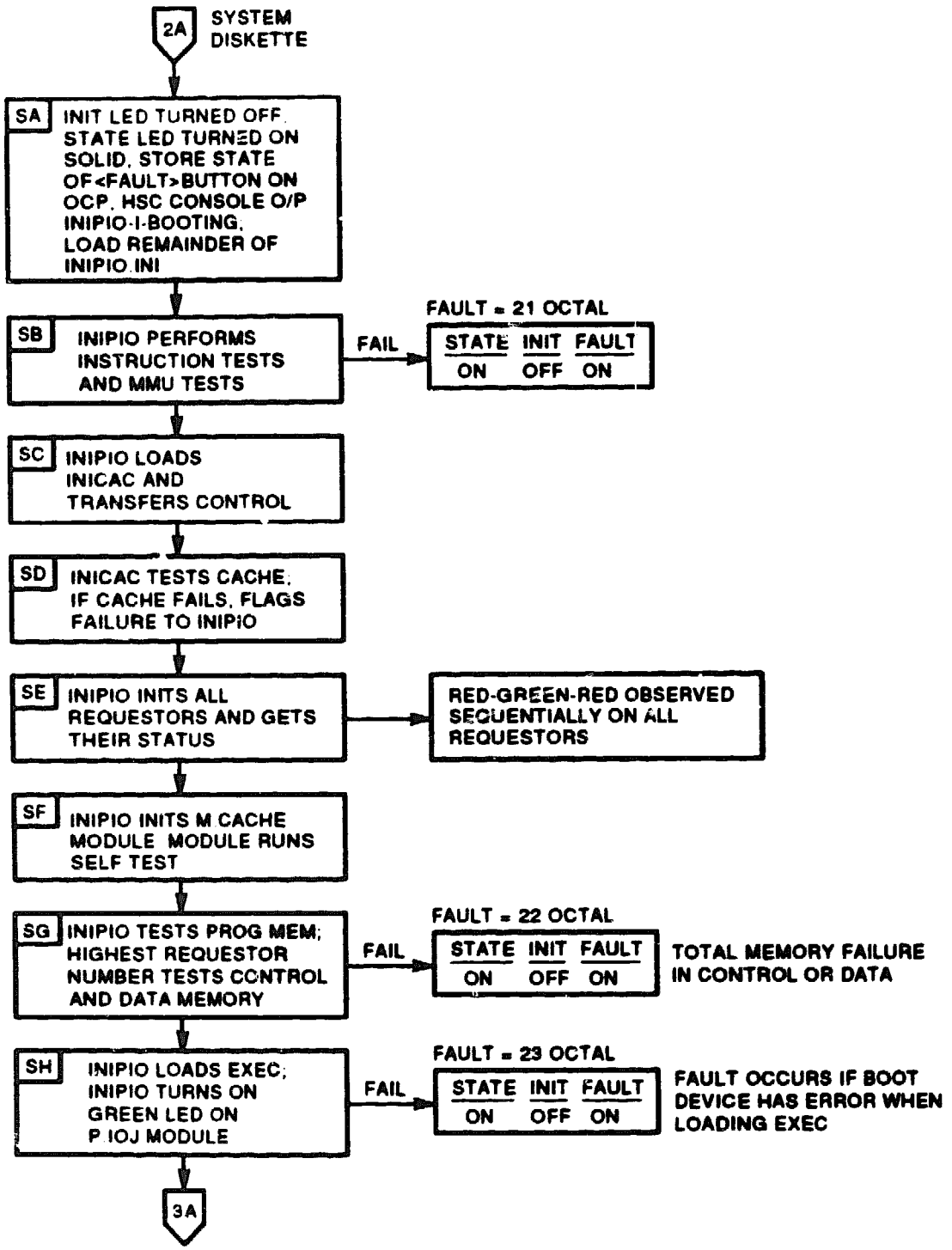
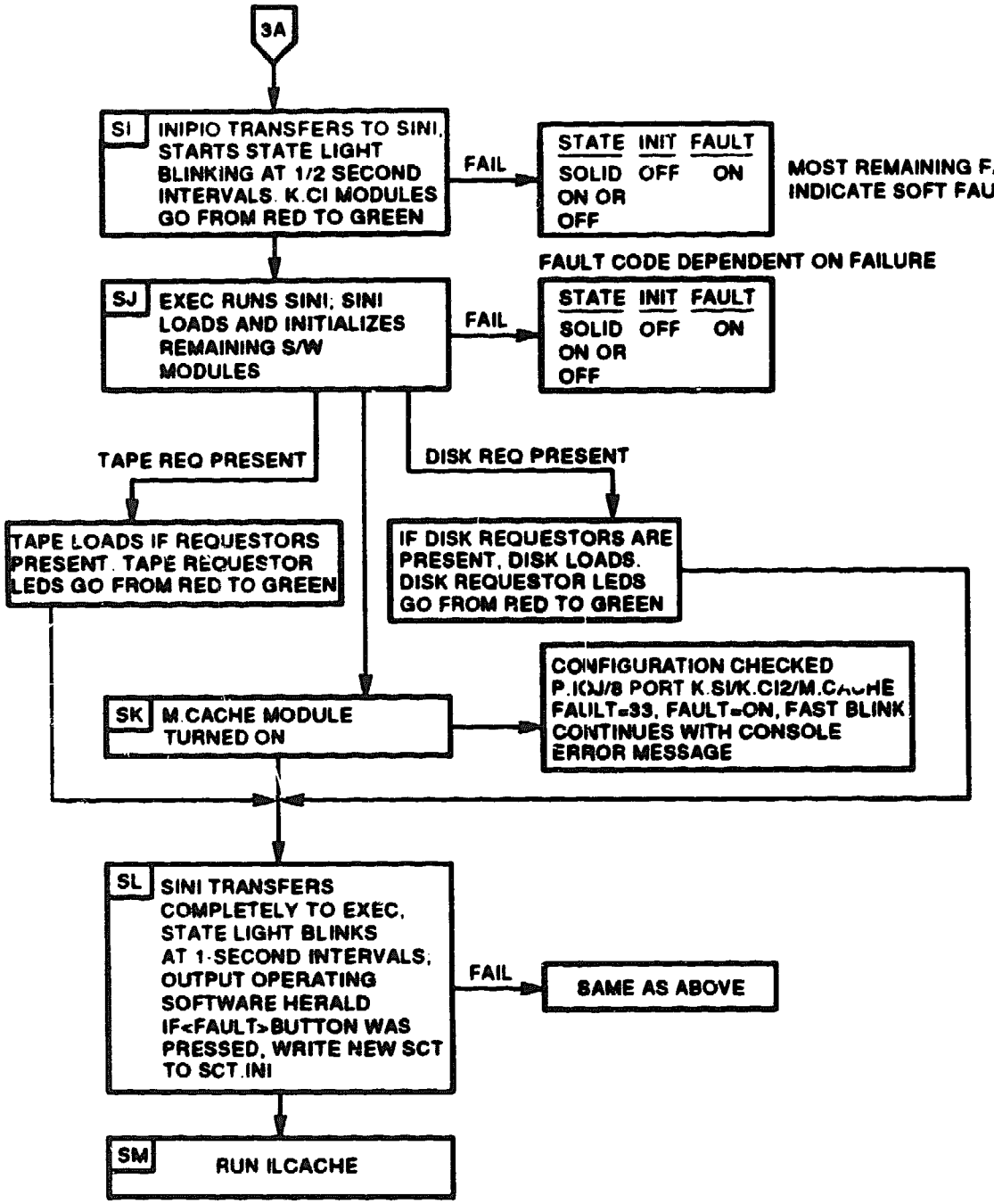


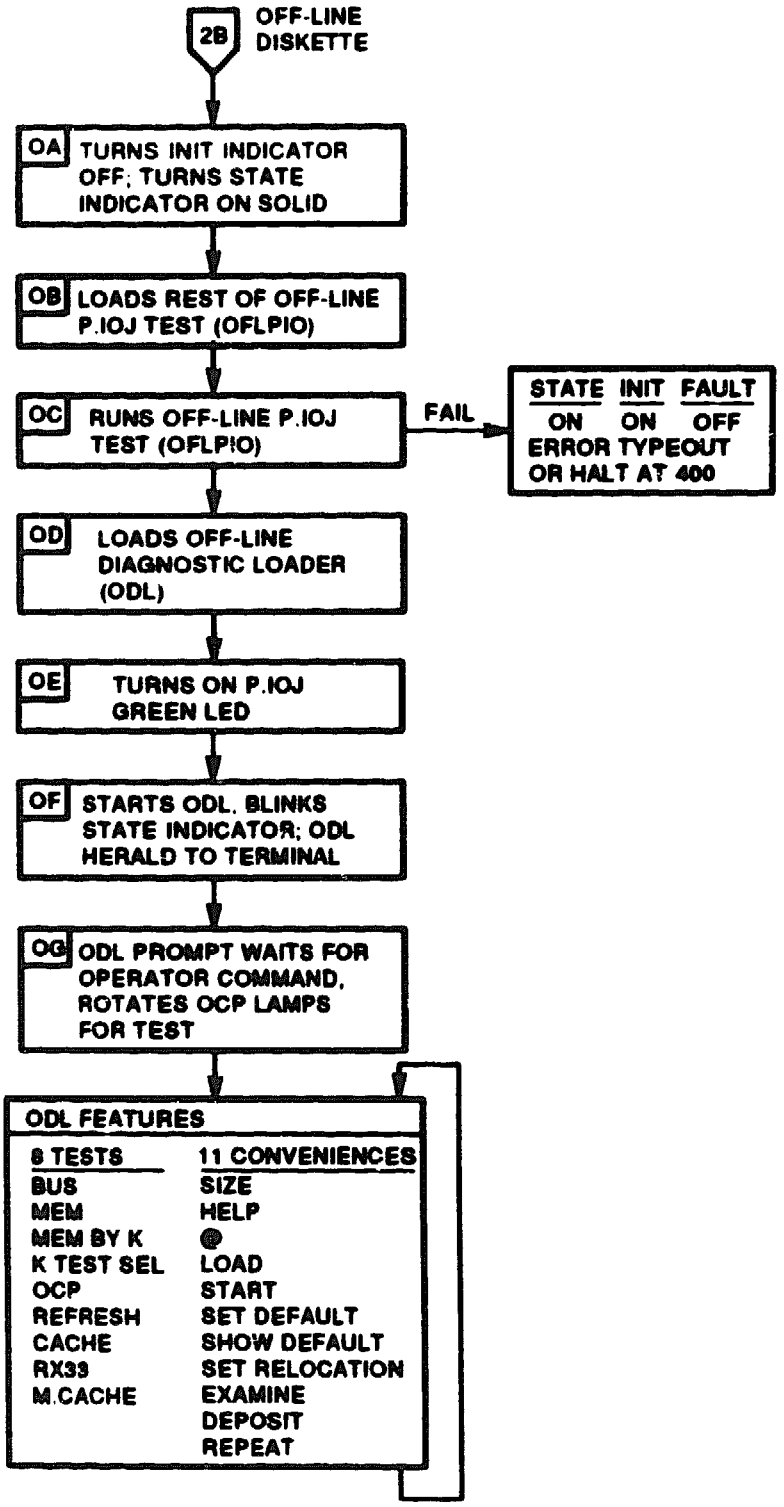
Figure 8–17 (Cont.) HSC Boot Flow and Troubleshooting Chart



NOTE: AFTER THE OPERATING SOFTWARE HERALD, OTHER INITIALIZATION MESSAGES MAY BE REPORTED.

CXO-945D
Sheet 4 of 5

Figure 8–17 (Cont.) HSC Boot Flow and Troubleshooting Chart



NOTE: FIRST PORTION OF THE OFLPIO TESTS WAS LOADED WITH THE PREVIOUS LOAD OF EIGHT BOOT BLOCKS.

CXO-945D
Sheet 5 of 5

Figure 8–17 HSC Boot Flow and Troubleshooting Chart

8.3.6 HSC50 controller Flow and Troubleshooting Chart

The HSC50 controller boot flow and troubleshooting chart calls out useful visual milestones that aid in troubleshooting the problems which can occur during initialization.

The flowchart has three main divisions:

- Information on activity common to both the system and offline media.
- Information on activity specific to the system media.
- Information on activity specific to the offline media.

The flowchart begins when one of the following occurs:

- The Init button is pushed.
- Powerup has started.
- Other software caused reboot.

Figure 8–18 maps the entire HSC50 controller boot sequence.

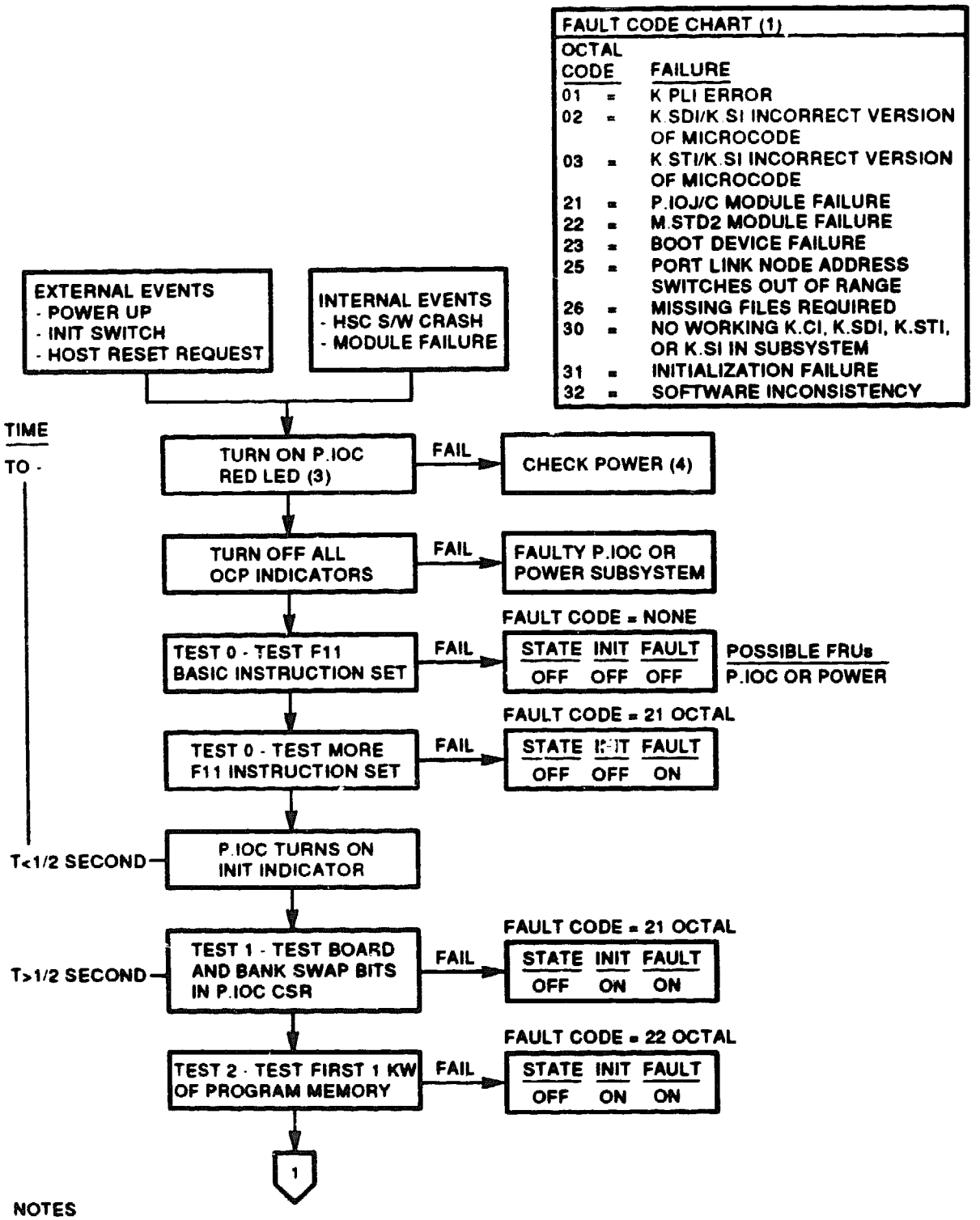
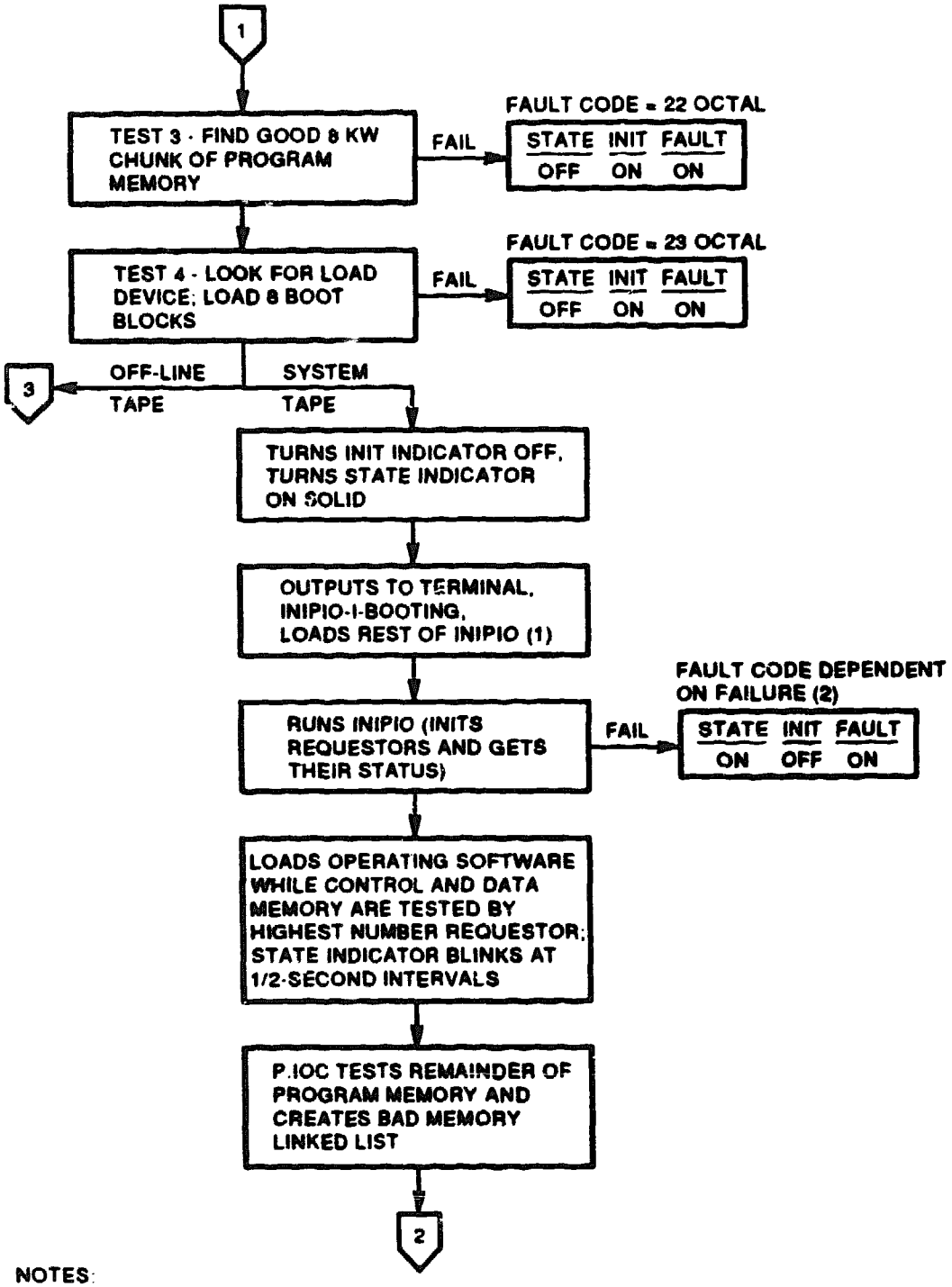


Figure 8–18 (Cont.) HSC50 Boot Flow and Troubleshooting Chart

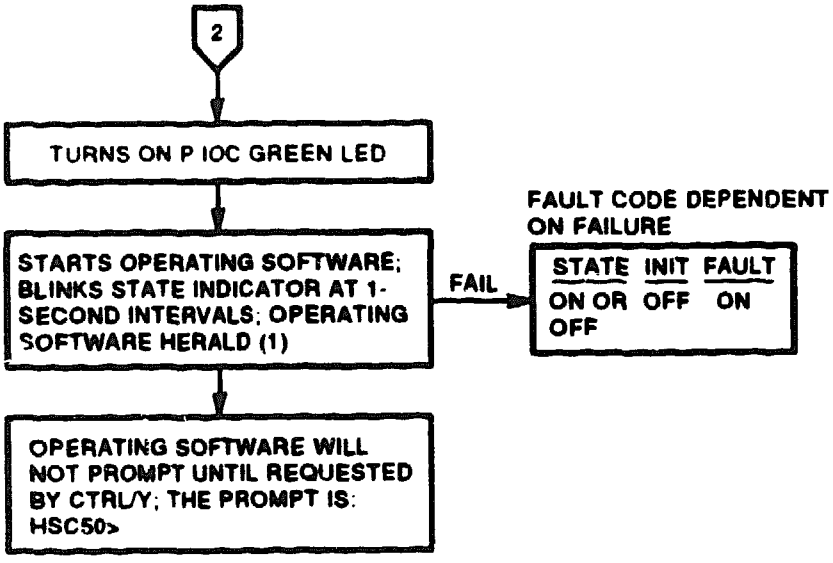


NOTES:

1. FIRST PORTION OF INIT P.IOC TESTS (INIPIO) WAS LOADED WITH PREVIOUS LOAD OF EIGHT BOOT BLOCKS.
2. FOR DETAILED INFORMATION ON INIPIO TESTS AND ERROR REPORTS, REFER TO HSC50 IN-LINE DIAGNOSTICS USER DOCUMENTATION.

CXO-052C
Sheet 2 of 4

Figure 8–18 (Cont.) HSC50 Boot Flow and Troubleshooting Chart



NOTE: AFTER THE OPERATING SOFTWARE HERALD, ONE OF SEVERAL NONFATAL INITIALIZATION FAILURE MESSAGES MAY BE PRINTED:

- REQUESTOR n FAILED TO INIT STATUS = XXX

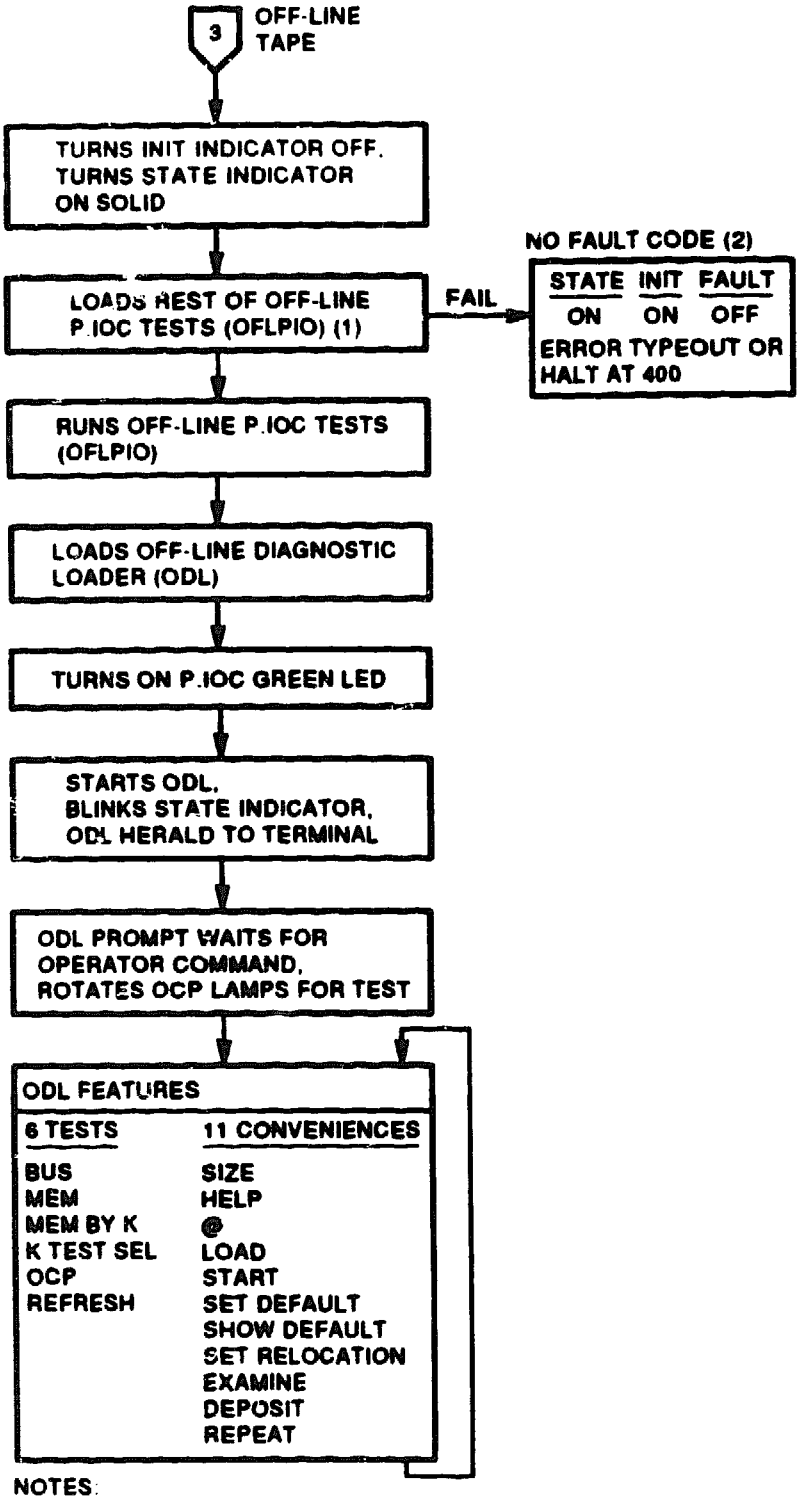
  THIS MESSAGE INDICATES SPECIFIED REQUESTOR FAILED ITS INTERNAL INITIALIZATION SELF-TEST OR COULD NOT BE LOADED WITH MICROCODE (K.SI).

- SWAP BANK BIT SET

  THIS MESSAGE INDICATES THAT A GOOD CONTIGUOUS SECTION OF 8 KW PROGRAM MEMORY COULD NOT BE FOUND WITHOUT USING THE SWAP BANK BIT IN THE P.IOC CSR. THE MEMORY MODULE IS SUSPECT.

CXO-052C
Sheet 3 of 4

Figure 8–18 (Cont.) HSC50 Boot Flow and Troubleshooting Chart



NOTES:

1. FIRST PORTION OF THE OFLPIO TESTS WAS LOADED WITH PREVIOUS LOAD OF EIGHT BOOT BLOCKS.
2. REFER TO FAULT CODE CHART. FOR DETAILED INFORMATION ON INITPIOC TESTS, REFER TO THE HSC50 IN-LINE DIAGNOSTICS USER DOCUMENTATION.

CXO-052C
Sheet 4 of 4

Figure 8–18 HSC50 Boot Flow and Troubleshooting Chart

8.3.7 Boot Diagnostic Indications

The HSC controller can pass boot diagnostics with a failing requestor. Although the HSC controller passed the boot, the failure associated with the requestor is considered an initialization error.

Following is an example of an error message displayed when a requestor fails on initialization of the operating software. The HSC controller has passed most of the initialization/boot diagnostics, but a requestor has failed.

```
SINI-E ERROR SEQUENCE 2. AT 20-SEPT-1985 00:00:02.80
    REQUESTOR 2 FAILED INIT DIAGS, STATUS = 107
```

The requestor with the red LED lit is the failing requestor. In this case, the diagnostic identifies Requestor 2 as failing its internal self-test number 7. Additionally, the Fault indicator is lit, and a soft fault code of octal 12 is displayed on the OCP after the Fault switch is pressed. Refer to Appendix C for a listing of STATUS = nnn codes.

See Section 8.3.1 for more information on errors indicated by the OCP.

8.4 Software Error Messages

HSC software error messages are classified into three categories:

- MSCP errors
- TMSCP errors
- Out-of-band errors

This section explains the different error types in each category, and shows examples of console error formats for each type in a category.

8.4.1 MSCP/TMSCP Error Format, Description, and Flags

Error formats, descriptions of the fields within the error format, and error flags are nearly identical for MSCP and TMSCP errors. Differences are noted where they exist. See Section 8.5 for listings and explanations of HSC software error messages.

8.4.1.1 Error Format

Example 8–1 shows the generic error format for all MSCP/TMSCP errors. Optional lines may be used with some errors to display additional information.

```
ERROR-x Text of message at (date) (time)
        Command Ref #    xxxxxxxx
        Err Seq #        x.
        Format Type      xx
        Error Flags      xx
        Event            xxxx
        (Optional line)
        (Optional line)
        (Optional line)
ERROR-x End of error.
```

Example 8–1 MSCP/TMSCP Error Message Format

8.4.1.2 Error Message Fields

Table 8–10 describes the various fields found in an MSCP/TMSCP error message. These are common fields to all MSCP/TMSCP error messages.

Table 8–10 MSCP/TMSCP Error Message Field Descriptions

Field	Description
ERROR-x	The x is a code indicating the severity level of an error. The codes are: E for error, Q for inquiry, I for informational, F for fatal, W for warning, and S for success. **NOTE** **Only severity levels E and Q require user action.** Information following the severity level code is a textual version of the error message describing the event code, followed by the date and time.
Command Ref #	This number (in hexadecimal) is the MSCP/TMSCP command number which caused the reported error. It is zero if the error does not correspond to a specific outstanding command. This number is normally assigned by the issuing host CPU.
Err Seq #	This number (in decimal) is a sequential number which counts error log messages since the MSCP/TMSCP server established a connection with the host. It is zero if the MSCP/TMSCP server does not implement error log sequence numbers.
Format Type	This number (in hexadecimal) is the byte that describes the detailed format of the error log message. Table 8–11 defines the format type codes. Format Type xx basically defines the type of error packet.
Error Flags	This number (in hexadecimal) indicates bit flags, collectively called error log message flags, used to report various attributes of the error. Refer to Table 8–12.
Event	This number (in hexadecimal) identifies the specific error or event being reported by this error log message. This code consists of a 5-bit major event code and an 11-bit subcode. The event codes and their meanings are listed in Appendix C.

8.4.1.3 Format Type Codes

Table 8–11 defines the format type code numbers. The format type code numbers are in hexadecimal.

Table 8–11 MSCP/TMSCP Error Message Format Type Code Numbers

Number	Definition
00	Controller errors
01	Host memory access errors with memory address
02	Disk transfer errors
03	SDI errors
04	Small disk errors
05	Tape transfer errors
06	STI errors
07	STI drive error log
08	STI formatter error log
09	Bad block replacement attempt
OA	Media loader error

Table 8–11 (Cont.) MSCP/TMSCP Error Message Format Type Code Numbers

Number	Definition
OB	Host error log media format

8.4.1.4 Error Flags

Table 8–12 defines the MSCP/TMSCP error flags.

Table 8–12 MSCP/TMSCP Error Flags

Bit Number	Bit Mask Hex	Format Description
7	80	If set, the operation causing this error log message has successfully completed. The error log message summarizes the retry sequence necessary to successfully complete the operation.
6	40	If set, the retry sequence for this operation continues. This error log message reports the unsuccessful completion of one or more retries.
5	20	This is MSCP-specific. If set, the identified logical block number (LBN) needs replacement.
4	10	This is MSCP-specific. If set, the reported error occurred during a disk access initiated by the controller bad block replacement process.
1	2	If set, the data contained in this error log message is informational only. The information is not necessarily related to any single command or event and does not signify the occurrence of an error.
0	1	If set, the error log sequence number has been reset by the MSCP server since the last error log message was sent to the receiving class driver.

8.4.2 MSCP Errors

MSCP (Mass Storage Control Protocol) errors are displayed on the console terminal and reported to a host. The errors are printed according to one of the following formats:

- Controller errors
- SDI errors
- Disk transfer errors
- Bad block replacement (BBR) errors

8.4.2.1 MSCP/TMSCP Controller Errors

Example 8–2 is a example of a typical MSCP/TMSCP controller error.

```
ERROR-E Data Memory Error (NXM or Parity) at 5-Mar-1985 12:52:14.43
        Command Ref #   1C430008
        Err Seq #       1.
        Error Flags     41
        Format Type     00
        Event           012A
        Buffer Addr     143611
        Source Req.     0.
        Detecting Req.  3.
ERROR-I End of error.
```

Example 8–2 Controller Error Message Example

The direction of data transfer may be deduced from the types of requestors identified in the Source Requestor and Detecting Requestor fields of the error message. These fields correspond to the requestor slot in the HSC controller backplane. In this example, the source requestor number shows it to be a I/O control processor, which filled the buffer. The detecting requestor number is 3, which is reading the buffer.

This section lists controller and compare errors together because their format and fields are the same. These errors contain three optional fields in addition to those described in Table 8–10. The controller/compare specific fields are shown in Table 8–13.

Table 8–13 MSCP/TMSCP Controller Error Message Field Descriptions

Field	Description
Buffer Addr	This number (in octal) is the starting address of the HSC data buffer where the error occurred.
Source Req.	This is the number (in decimal) of the requestor that originally filled the buffer with data.
Detecting Req.	This is the number (in decimal) of the requestor that detected the error.

8.4.2.2 MSCP SDI Errors

Example 8–3 shows a typical SDI error message. Table 8–14 describes the fields specific to SDI errors. Tables 8–15 through 8–18 further define the fields in Table 8–14. For the remaining fields, refer to Table 8–10. For listings and explanations of SDI type errors, see Section 8.5.

```
ERROR-E Drive Detected Error at 5-Mar-1985 12:52:14.43
        Command Ref #    00000000
        RA81 unit #      124.
        Err Seq #        4.
        Error Flags      40
        Format Type      03
        Event            00EB
        Request          1B
        Mode             00
        Error            80
        Controller       00
        Retry/Fail       00
        Extended Status  88
                         00
                         03
                         00
                         07
                         4B
                         1A
        Requestor #      6.
        Drive port #     2.
ERROR-I End of error.
```

Example 8–3 MSCP SDI Error Example

Table 8–14 describes the SDI error example fields.

Table 8–14 MSCP SDI Error Field Descriptions

Field	Description
RA81 unit #	This is the number of the unit that is related to the error log message. The number 4095 is given if the unit number is unknown. In this example, the message indicates the drive is an RA81 with a unit number of 124.
Request	This number (in hexadecimal) is a byte describing various requests from the drive for controller action and information about the state of the drive. Figure 8–19 shows the bits of this byte field, and Table 8–15 describes the bits. In this example, the 1B indicates: • RUN/STOP switch in • Port switch in • Useful log information in extended area • Spindle ready
Mode	This number (in hexadecimal) is a byte describing various unit modes. Some of these modes can be altered by the controller. Figure 8–20 shows the bits of this byte field, and Table 8–16 describes the bits. In this example, the 00 indicates: • No subunits are write protected. • The disk is in 512-byte sector format.

Table 8–14 (Cont.) MSCP SDI Error Field Descriptions

Field	Description
Error	This number (in hexadecimal) is a byte describing the the current drive error conditions that prevent normal drive operations. Figure 8–21 shows the bits of this byte field, and Table 8–17 describes the bits. In this example, the 80 indicates a drive error has occurred, and the drive Fault indicator may be on.
Controller	This number (in hexadecimal) is a byte containing information related to which subunits have attention available messages suppressed in the controller and a status code indicating various states of drive operation. Figure 8–22 shows the bits of this byte field, and Table 8–18 describes the bits. In this example, the 00 indicates: • No subunits with attention available message suppressed in the controller. • Drive normal operation.
Retry/Fail	This number (in hexadecimal) is a byte containing one of two types of information depending upon the status of the DF bit in the error field. The DF bit describes the drive initialization process. The DF bit is a zero if the drive initialization was successful. (In this case, the Retry/Fail field contains the retry count from the previous operation.) The DF bit set indicates the drive initialization failed, and therefore, the Retry/Fail contains a specific drive error code. This error code is defined in the appropriate drive service manual. In this example, 00 indicates no retry count exists for the previous operation. (The DF bit is zero in the Error field.)
Extended status	These bytes (in hexadecimal) contain the extended status of the particular drive. (In this example it is an RA81.) Refer to the appropriate drive service manual for the meaning of these bytes. In this example, the extended status is: • 88—Controller command functional code last executed by the drive. (In this case, a GET SUBUNIT CHARACTERISTICS command.) • 00—Interface error status bits which are all reset. • 03—Low-order cylinder address bits of the last seek operation. • 00—High-order cylinder address bits of the last seek operation. • 07—The present group address. • 4B—Error code (index pulse error) displayed by the drive LEDs during the execution of a drive-resident diagnostic. • 1A—Error code (servo fine positioning error) displayed on the OCP of the RA81 disk drive.
Requestor #	This number (in decimal) is the number of the requestor to which the drive is connected.
Drive port #	This number (in decimal) is the number of the specific port on the requestor to which the drive is connected. The ports are numbered 0 through 3 on a 4-port disk data channel, and 0 through 7 on an 8-port disk data channel.

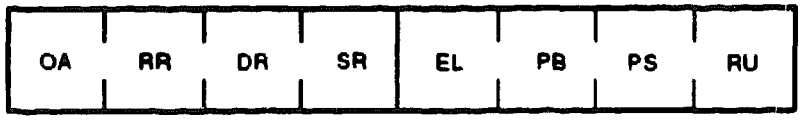


Figure 8–19 Request Byte Field

Table 8–15 Request Byte Field Descriptions

Bit	Description
OA	A logical 1 in this position indicates the drive is unavailable to the controller. A logical 0 indicates the drive is available or online to the controller.
RR	A logical 1 in this position indicates the drive requires an internal readjustment. Some drives do not use this bit.
DR	A logical 1 in this position indicates a request is outstanding to load a diagnostic in the drive microprocessor memory. A logical 0 indicates no diagnostic load is being requested.
SR	A logical 1 in this position indicates the drive spindle is up to speed. A logical 0 indicates the drive spindle is not up to speed.
EL	A logical 1 in this position indicates usable information in the extended status area. A logical 0 indicates no information is available in the extended status area.
PB	A logical 1 in this bit position indicates the drive is connected to the controller through Port B. A logical 0 indicates the drive is connected through Port A.
PS	A logical 1 in this bit position indicates the drive port select switch for this controller is pushed in (selected). A logical 0 indicates the switch is out. The unit number is not valid unless PS=1.
RU	A logical 1 in this position indicates the RUN/STOP switch is pushed in (RUN). A logical 0 indicates the switch is out (STOP).

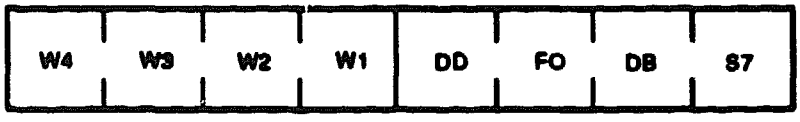


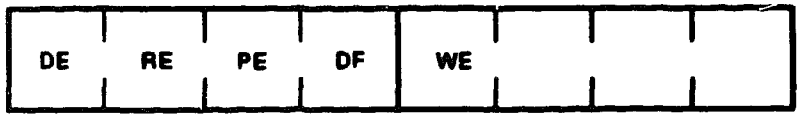
Figure 8–20 Mode Byte Field

Table 8–16 Mode Byte Field Descriptions

Bit	Description
W4-W1	A logical 1 in any of these four bit positions represents the hardware write-protect status for the subunit. A sub-unit is hardware write protected if the WRITE PROTECT switch is in for the sub-unit. For example, a 0001 indicates subunit 0 within the selected drive is write protected. Since the HSC controller does not implement subunits, W1 corresponds to the unit in question.

Table 8–16 (Cont.) Mode Byte Field Descriptions

Bit	Description
DD	A logical 1 in this position indicates the drive was disabled by a controller error routine or diagnostic. The Fault indicator is on when this bit is set. A logical 0 indicates the drive is enabled for communication with a controller.
FO	A logical 1 in this position indicates the drive can be formatted.
DB	A logical 1 in this position indicates the diagnostic cylinders on the drive can be accessed.
S7	A logical 1 in this position indicates the 576-byte sector format is selected. A logical 0 indicates that the 512-byte sector format is selected.

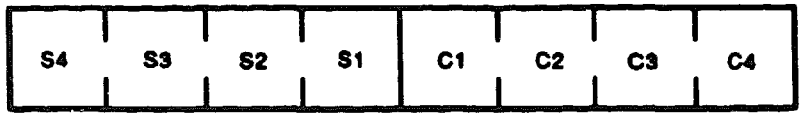


CXO-1123A

Figure 8–21 Error Byte Field

Table 8–17 Error Byte Field Descriptions

Bit	Description
DE	A logical 1 in this position indicates a drive error has occurred and the drive Fault indicator may be on.
RE	A logical 1 in this position indicates an error occurred in the transmission of a command between the drive and the controller. The error could be a checksum error or an incorrectly formatted command string.
PE	A logical 1 in this position indicates improper command codes or parameters were issued to the drive.
DF	A logical 1 in this position indicates a failure in the initialization routine of the drive.
WE	A logical 1 in this position indicates a write-lock error has occurred. This means that the drive received a command requiring a write operation when the drive was write protected.



CXO-1124A

Figure 8–22 Controller Byte Field

Table 8–18 Controller Byte Field Descriptions

Bit	Description
S4-S1	This is a 4-bit representation of the subunits with attention available messages suppressed in the controller. The right-most bit (S1) represents subunit 0. The left-most bit (S4) represents subunit 3. If one of the bits is set, it indicates the controller is not to interrupt the host CPU with an attention available message when the specified subunit raises its available real-time drive status line to the controller. The S4 through S1 bits reflect the results of the SDI command CHANGE CONTROLLER FLAGS in which attention available messages are not desired for certain subunits.
C4-C1	This is a 4-bit drive status code indicating various states of drive operation.

NOTE

When the HSC controller marks the drive as inoperative, it places the drive in the MSCP state of Unit-Offline with a substate of Unit-Inoperative relative to this HSC controller.

8.4.2.3 MSCP Disk Transfer Errors

Disk transfer errors are either data or media format type errors. Example 8–4 shows a disk transfer error example, and Table 8–19 describes the various fields of the example. See Section 8.5 for listings and explanations of various disk transfer errors.

```
ERROR-E Seven Symbol ECC Error at 27-Mar-1985 12:15:15.00
        Command Ref #       50400015
        RA81 unit #         120.
        Err Seq #           9.
        Format Type         02
        Error Flags         E0
        Event               01C8
        Recovery level      0.
        Recovery count      0.
        LBN                 426978
        Orig err flags      100020
        Recovery Flags      000003
        Lvl A retry cnt     0.
        Lvl B retry cnt     0.
        Buffer addrs        143022
        Source Req.         5.
        Detecting Req.      5.
Error-I End of error.
```

Example 8–4 Disk Transfer Error Example

Table 8–19 describes the fields in the disk transfer error message example not described in Table 8–10. Unless otherwise specified, all fields in this table are shown in decimal numbers. These fields are specific to an RA81 disk drive and may not be the same for other RAxx type drives.

Table 8–19 Disk Transfer Error Field Descriptions

Field	Description
RA81 unit #	This is the number of the unit that is related to the error log message. The number 4095 is given if the unit number is unknown. In this example, the message indicates the drive is an RA81 with a unit number of 120.
Recovery level	This number indicates the SDI drive error recovery command level used for the most recent transfer attempt by the unit. In this example, the 0 indicates that no SDI error recovery commands were used.
Recovery count	This number indicates the number of times the SDI ERROR RECOVERY command was tried at the specified level. In this example, the 0 indicates that no retries were done.
LBN	This number indicates the logical block number. In this example, the LBN is 426978.
Original error flags	This number (octal) indicates the original errors associated with this error. Table 8–20 describes the bits associated with this field. In this example, the 100020 indicates: • ECC error • EDC error
Recovery flags	This number (octal) indicates the error recovery flags that were set during error processing. These flags specify certain additional actions that should be instigated by error recovery processing. Table 8–21 describes the bits associated with this field. In this example, the 000003 indicates: • An LBN should be replaced. • The current error should be logged on the console and to the host if a connection is present.
Level A retry count	This number indicates the number of times the HSC controller attempted the Level A recovery routines. These routines are those not requiring any SI exchanges as part of the recovery sequence. In this example, no Level A recovery was done because the error was corrected by the ECC correcting code.
Level B retry count	This number indicates the number of times the HSC controller attempted the Level B recovery routines. These routines require extensive SDI exchanges as part of the recovery sequence. In this example, the 0 indicates no Level B error recovery was attempted.
Buffer address	This number (octal) is the address of the HSC controller internal data buffer associated with this error. In this example, the buffer address is 143022.
Source Requestor	This number is the requestor that filled the buffer with data. In this example, the 5 indicates the source requestor was requestor number 5. A requestor of 1 in this field would indicate a disk write operation because data would be supplied by the K.ci host interface. All other values would indicate a disk read operation.
Detecting Requestor	This number is the requestor that detected the error. In this example, the 5 indicates requestor number 5 detected the ECC error.

Table 8–20 shows definitions of the original error flags and Table 8–21 defines the recovery flags.

Table 8–20 Original Error Flags Field Descriptions

Bit	Mask (Octal)	Definition
15	100000	ECC error
14	040000	SERDES overrun error
13	020000	SDI Response/Data line pulse error
12 and 11	014000	Suspected position error—low header mismatch
12	010000	Header sync error
11	004000	Header compare error—compare-64 performed (high header mismatch)
10	002000	Data sync timeout
09	001000	Drive clock timeout
08	000400	SDI State line pulse or parity error
07	000200	Data bus overrun
06	000100	Data memory parity error
05	000040	Data memory NXM error
04	000020	EDC error
03 and 02	000014	Read/Write Ready down at end of sector
03	000010	Lost Read/Write Ready before transfer began
02	000004	Lost Receiver Ready before transfer began
01	000002	Forced error (EDC = Ones complement of correct EDC)
00	000001	Drive inoperative

Table 8–21 Recovery Flags Field Definitions

Bit	Mask (Octal)	Definition
07	000200	Indicates a revector was done for this LBN.
06	000100	Indicates a positioner error was detected on this block.
05	000040	Indicates the error count reported by the ILEXER should be updated.
04	000020	Indicates an error log message has already been generated for the current error.
03	000010	Indicates an RCT entry for the desired logical block number was found.
02	000004	Indicates revectoring and replacement should be suppressed for this block.
01	000002	Indicates the current error should be logged on the console and to the host if a connection is present.
00	000001	Indicates the logical block should be replaced.

8.4.2.4 Bad Block Replacement Errors (BBR)

Another type of MSCP error displayed on the console terminal is for a bad block replacement request. The bad block replacement request is a result of the one of the following errors:

- Any error that persists after all levels of SDI error recovery are exhausted
- ECC symbol error above the drive threshold
- Header compare error
- Header sync error
- Loss of Read/Write Ready at end of read from disk (SERDES read)
- Uncorrectable ECC error

Example 8–5 shows a bad block replacement message. This message reports completion, successful or unsuccessful, of a bad block replacement attempt. A message is generated regardless of the success or failure of the replacement attempt. See Section 8.5 for listings and explanations of BBR errors.

```
ERROR-W Bad Block Replacement (Success) at 18-Dec-1985 18:05:37.1
        Command Ref #    B8590012
        RA60 Unit #      251.
        Err Seq #        2.
        Format Type      09
        Error Flags      80
        Event            0014
        Replace Flags    8000
        LBN              205.
        Old RBN          0.
        New RBN          5.
        Cause Event      00E8
ERROR-I End of error
```

Example 8–5 Bad Block Replacement Error Example

Table 8–22 defines BBR error fields not previously described in Table 8–10.

See Table 8–23 for definitions of the replace flags field bits.

Table 8–22 Bad Block Replacement Error Field Definitions

Field	Description
Replace Flags	This number (in hexadecimal) indicates bit flags used to report in detail the outcome of the bad block replacement attempt. In this example, the 8000 indicates the block was verified as bad.
LBN	This number (in decimal) is the logical block number that is the target of the replacement. In this example, the LBN is 205.
Old RBN	This number (in decimal) indicates the RBN with which the bad LBN was formerly replaced. This number is set to zero if it was not formerly replaced. In this example, the 0 indicates it was not formerly replaced.
New RBN	This number (in decimal) indicates the RBN with which the bad LBN was replaced. This number is set to zero if no actual replacement was attempted. In this example the new RBN is 5.

Table 8–22 (Cont.) Bad Block Replacement Error Field Definitions

Field	Description
Cause Event	This number (in hexadecimal) is the event code from the original error that caused the replacement to be attempted. The number is zero if that event code is not available. Refer to Appendix C for a listing of generic error log fields. In this example, the 00E8 indicates an uncorrectable ECC error caused the bad block replacement.

Table 8–23 Replace Flags Field Bit Descriptions

Bit Number	Bit Mask (Hex)	Flag Bit Definition
15	8000	Replacement attempted—This bit is set if the suspect bad block indeed tested bad during the initial stages of the replacement process. If not set, the suspect block was not verified as bad and no replacement was completed.
14	4000	Forced error—The data from the suspected bad block could not be corrected or obtained without error. The Forced Error indicator will be written to the replacement block along with the bad data from the block that was replaced. The Forced Error indicator basically indicates that the data in the block may not be good. The user data from the bad block is read with a forced error when accessed. If this condition occurs frequently on a specific drive, a closer analysis of the drive is recommended to look for possible problems.
13	2000	Nonprimary revector—This bit is set if the replacement process was accomplished and required putting the bad block data into a replacement block that is not the primary RBN for the bad block.
12	1000	Reformat error—This bit is set during the replacement process if the status coming back from the execution of the replacement operation is a "REPLACE failure." This means that the HSC controller was not able to reformat the headers of the bad block to indicate it is a replaced block. If this occurs, the drive should not be used until it is reformatted.
11	800	RCT inconsistent—This bit is set if the Replacement Control Tables are not usable. The drive should not be used until it can be reformatted.
10	400	Bad replacement block—This bit is set if the bad block reported is a replacement block. The replacement block can be replaced just like any other LBN.

8.4.3 TMSCP Errors

The TMSCP (Tape Mass Storage Control Protocol) error messages displayed on the console terminal are in one of the following formats:

- Controller errors (Section 8.4.2.1)
- STI communication or command errors
- STI formatter error log errors
- STI drive error log errors
- Tape transfer errors

See Section 8.5 for listings and explanations of tape errors.

8.4.3.1 STI Communication or Command Errors

Example 8–6 is a sample console printout of an STI communication or command error. Table 8–24 explains the fields not previously defined in Table 8–10.

```
ERROR-E Drive detected error at  6-Mar-1985 09:51:11.88
        Command Ref #   864E0004
        TA78 unit #     0
        Err Seq #       12
        Error Flags     40
        Event           00EB
        Position        13026
        GSS Text        02 00 00 00
                        05 00 00 00 00 00 00 00
Error-I End of error
```

Example 8–6 STI Communication or Command Error Example

Table 8–24 explains the error fields.

Table 8–24 STI Communication or Command Error Printout Field Descriptions

Field	Description
Event	The number (in hexadecimal) identifies the specific error or event reported by this error log message. The event codes and their meanings are shown in Appendix C. In this example, the 00EB means drive-detected error.
Position	This is the last known tape position the formatter received. This is given in gap counts from BOT. In this example, the number 13026 means 13026 gaps from BOT.
GSS Text	The GSS Text field is the response received by the HSC controller from the formatter when the HSC controller issues the GET SUMMARY STATUS (GSS) and TOPOLOGY commands. The GSS text in this example is 02 00 00 00 05 00 00 00 00 00 00 00. This means Level 2 protocol error, Speed Management Enabled, and Zero Threshold. See Section 8.4.3.5 for details on field definitions and bit decoding.

8.4.3.2 STI Formatter Error Log

The following is an example of the console display of an STI formatter error log. Example 8–7 shows the example, and Table 8–25 explains the fields not previously defined in Table 8–10.

Table 8–25 explains the error log fields.

```
ERROR-E Tape Formatter Requested Error Log at 30-Jan-1986 11:20:09.31
        Command Ref #   43900012
        TA81 unit #     95
        Err Seq #       47
        Format Type     08
        Error Flags     40
        Event           FF6C
        Position        1057
        Formatter E Log 40 00 00 81 00 00 00
                        01 98 72 00 00 00 00
                        C4 48 00 00
ERROR-I End of error.
```

Example 8–7 STI Formatter Error Log Example

Table 8–25 STI Formatter Error Log Field Descriptions

Field	Description
Position	The last known tape position the formatter received. This is given in gap counts from BOT. In this example, the number 1057 means 1057 gaps from BOT.
STI Formatter Error Log	See Table 8–26.

Table 8–26 STI Formatter E Log

Byte No.	Byte Data	Description
1	40	Formatter error
2	00	Not set for this example
3	00	Not set for this example
4	81	Data pulse parity error during data transfer
		The information contained in these fields is product specific. Refer to the appropriate drive manual for a description of the remainder of the bytes.

8.4.3.3 STI Drive Error Log

The following is an example of a console display of an STI drive error log. Example 8–8 shows the example. Table 8–28 describes GEDS Text field, and Table 8–29 describes the Drive Error Log field.

Table 8–27 explains the error log fields.

```
ERROR-E Tape Drive Requested Error Log at 5-Mar-1985 14:43:31.15
        Command Ref #   D6300023
        TA78 unit #     528
        Err Seq #       210
        Error Flags     40
        Event           FF6B
        Position        1
        GEDS Text       7D 04 5000 01000000
        Drive Error Log 00 00 00 00 50 3B 04 0D
                        46 FF 07 FF 00 00 00 00
                        81 00 00 00 FF 22 04 C4
                        00 00 80 FF 17 94 00 08
                        00 00 D9 FF FF FF FF FF
                        FF 47 E6 E0 00 16 25 97
                        A2 00 00
ERROR-I End of error
```

Example 8–8 STI Drive Error Log Example

Table 8–27 STI Drive Error Log Field Descriptions

Field	Description
Position	The last known tape position where the HSC believes the tape drive is, upon successful completion of all outstanding commands. This is given in gap counts from BOT. In this example the number 1 means 1 gap from BOT.
GEDS Text	See Table 8–28.

Table 8–27 (Cont.) STI Drive Error Log Field Descriptions

Field	Description
Drive Error Log	See Table 8–29.

Refer also to Section 8.4.3.4 for field definitions and bit decoding.

Table 8–28 GEDS Text

Byte No.	Byte Data	Description
1	7D	125 ips tape drive
2	04	6250 bpi GCR encoding
3 4	50 00	MSCP unit number=80
5 6 7 8	01 00 00 00	Gap count=1

The information shown in Table 8–29 is product specific to the TA78 tape drive. See the *TA78 Service Manual* for details.

Table 8–29 STI Drive Error Log (TA78 Drive Product Specific)

Byte No.	Byte Data	Description
1, 2	00	No soft error
3	00	
4	00	
5	50	Set byte count
6, 7	3B, 04	Operational error Error ID = 59 CRC error ACRC error Pointer mismatch Uncorrectable or two-track error set in ECCSTA register Unknown fault number
8	0D	RMC write fail bits
9	46	Statistics select clock stopped STATUS VALID
10	FF	Non-BOT command status is OK
11	07	Last cmd sent to M8953 through RCMD = normal NON-BOT read
12	FF	Read channel AMTIE status (CH 7:0)
13	00	
14	00	Read channel illegal status (CH 7:0)

Table 8–29 (Cont.) STI Drive Error Log (TA78 Drive Product Specific)

Byte No.	Byte Data	Description
15	00	
16	00	End mark for read channels 7:0
17	81	Weak amplitude on parity bit ECC corrected output (parity bit)
18	00	Read channel PE postamble detect
19	00	Data from read channels to ECC
20	00	CRC checker output bits
21	FF	Corrected data (ECC to CRC)
22	22	Two-track ECC performed on data AMTIE during data of record
23	04	Channel 0 tie bus 2 Amplitude track in error AMTIE
24	C4	Channel 3 tie bus 3
25	00	
26	00	
27	80	Tie bus = 0F(X)
28	FF	Tape unit bus line AMTIE 7:0
29	17	AMTIE parity READ parity WCS parity Tape unit present
30	94	TU bus line read data 7:0
31	00	STI bus error byte
32	08	CRC to WMC DR bus
33, 34	00	Tape unit selected = 0
35	D9	Read/Write Data, intermediate DRD bus
36, 37	FF	Byte count = 65535
38, 39	FF	PAD counter = 65535
40, 41	FF	Unknown error code
42	47	DR MBD parity error
43	E6	PE write parity error POWER OK
44	E0	Tape unit ready and on line
45	00	
46	16	125 ips tape drive
47, 48	25, 97	Tape unit serial #2597
49	A2	AMTIE threshold field = 2 READ ENABLE Write BIT 4

Table 8–29 (Cont.) STI Drive Error Log (TA78 Drive Product Specific)

Byte No.	Byte Data	Description
50	00	
51	00	

8.4.3.4 Breakdown of GEDS Text Field

Example 8–9 is an example of a tape drive-related error message displayed on the HSC terminal.

```
ERROR-W Tape Drive Requested Error Log at 15-Aug-1984 18:43:05.80
        Command Ref #    00001D8E
        TA78 unit #      20.
        Err Seq #        1.
        Error Flags      40
        Event            FF6B
        Position         2.
        GEDS Text        7D 02 0014 00000002
        Drive Error Log  00 00 00 00 C5 38 04 04
                         46 FF 07 FF 00 00 00 00
                         81 00 00 21 FF B0 00 04
                         00 00 80 FF 17 DE 00 08
                         00 00 21 FF FF 00 00 99
                         99 47 F4 E8 00 56 85 19
                         A2 0A 80 FF 17 DE
```

Example 8–9 Tape Drive Related Error Message

Both the GEDS Text and Drive Error Log portions of this message result from a GET EXTENDED DRIVE STATUS command to the drive from the HSC controller. The Drive Error Log portion can be interpreted by referencing the service manual for the appropriate tape drive. (The preceding example is for a TA78 tape drive.)

Following is a breakdown of the information contained in the GEDS Text field. The left-most byte is referenced as the first byte and the right-most byte as the eighth byte.

Bytes in the GEDS Text field are described in the following list:

- **First byte = Speed**—Currently set speed of the drive; drive speed is defined as an integer value (in hex) in inches per second (ips) rounded down to the nearest integer. For a totally variable speed drive, the speed returned is the lower bound on the range of permissible speeds. In the example shown, this field contains a value of 7D, which corresponds to 125 ips.
- **Second byte = Density**—The current operating density of the tape unit. Only one bit is set to indicate the current operating density.

  04 =6250 bpi
  02 = 1600 bpi
  01 = 800 bpi

- **Third and fourth bytes = Unit number** – Contain the drive unit number (in hex).
- **Fifth through eighth bytes = Gap count** – The formatter's gap count is from the beginning of the tape to where the tape drive is. The contents of this field may differ from the Position field in this error message. The HSC's gap count is contained in the Position field at the end of successful completion of all outstanding commands.

8.4.3.5 Breakdown of GSS Text Field

Example 8–10 is another example of a tape drive-related error message displayed at the HSC console:

```
ERROR-E Drive detected error at 18-Aug-1984 12:05:34.82
        Command Ref #    0346003
        TA78 unit #      3.
        Err Seq #        7.
        Error Flags      40
        Event            00EB
        Position         0.
        GSS Text         02 20 00 00
                         28 00 00 00 00 00 14 00
ERROR-I End of error.
```

Example 8–10 Additional Tape Drive-Related Error Message

The HSC controller receives the GSS Text field form of this error message from the tape formatter when the HSC controller issues the GET SUMMARY STATUS (GSS) and TOPOLOGY commands. The field is also the unsuccessful response for all Level 2 commands. Figure 8–23 is a breakdown of this response.

AF	A3	A2	A1	A0	OA	PS	DR	SUMMARY MODE BYTE 1
FE	TE	PE	DF	CE				SUMMARY ERROR BYTE
		AC	PB	EL	RP	RT	FD	SUMMARY MODE BYTE 2
C1	C2	C3	C4	C5	C6	C7	C8	CONTROLLER BYTE
TM	EOT	BOT	WL	OL	AV	MR	EL	DRIVE 0 MODE BYTE
DE	LP	PL	EX	DTE	SME	DI	ZT	DRIVE 0 ERROR BYTE
TM	EOT	BOT	WL	OL	AV	MR	EL	DRIVE 1 MODE BYTE
DE	LP	PL	EX	DTE	SME	DI	ZT	DRIVE 1 ERROR BYTE
TM	EOT	BOT	WL	OL	AV	MR	EL	DRIVE 2 MODE BYTE
DE	LP	PL	EX	DTE	SME	DI	ZT	DRIVE 2 ERROR BYTE
TM	EOT	BOT	WL	OL	AV	MR	EL	DRIVE 3 MODE BYTE
DE	LP	PL	EX	DTE	SME	DI	ZT	DRIVE 3 ERROR BYTE

CXO-2116A

Figure 8–23 GSS Text Field Bits Summary Breakdown

8.4.3.6 GSS Text Field Bit Interpretation

An interpretation of the GSS text field bits follows:

- **AC: Cache attention**
- **AF: Formatter attention asserted**
- **A3: Drive 3 attention asserted**
- **A2: Drive 2 attention asserted**
- **A1: Drive 1 attention asserted**

- **A0: Drive 0 attention asserted**
- **ASM: Automatic speed management**
- **AV: Drive available to formatter**
- **BM: Block mode**
- **BOT: Beginning of tape**
- **CB: Cache busy**
- **CC: Cache capable**
- **CDL: Cache data lost**
- **CE: Cache error**
- **CF: Cache full**
- **CMT: Cache empty**
- **Cn: Controller flags (C0 - C8)—The following combinations are implemented. All other combinations are reserved.**

  C0: Normal operation
  C1: Formatter off line—Formatter is off line to hosts due to being under diagnostic control.

- **DE: Drive error—Asserted when any drive error not covered by other status bits is detected.**
- **DF: Formatter diagnostic failed**
- **DI: Diagnostic mode—When set, instructs the formatter to use special internal algorithms to report imperfect performance.**
- **DIR: Direction—When clear, indicates the tape will be positioned in the forward direction.**
- **DR: Diagnostic requested—Asserted when the formatter is requesting permission to execute a diagnostic.**
- **DTE: Data transfer error—Asserted when any error occurs which prevents a data transfer from completing successfully.**
- **EL: Error logging request—Asserted by either the drive or formatter when error logging information is available.**
- **EOT: End of tape—Asserted when the tape is positioned at or past the end of tape marker.**
- **ER: Erase—When set, indicates that a rewind operation will erase the tape from the current position forward to EOT before rewinding the tape.**
- **EX: Exception condition—Asserted whenever the formatter encounters TM, BOT, or EOT during a data transfer operation.**
- **FD: Retry Bit, failure/direction – Asserted during error recovery to indicate the direction of a retry or to indicate a failing operation. If RP = 0 and RT = 1, then FD = direction to transfer. FD = 0 means transfer in the same direction as original operation; FD = 1 means transfer in the opposite direction of original operation. If RP = 1 and RT = 0, then FD indicates success or failure of operation. FD = 0 means the retry sequence succeeded; FD = 1 means the retry sequence failed.**
- **FE: Formatter error—Asserted on formatter errors not covered by the TE, PE, or DF bits.**
- **LP: Lengthy operation in progress—Asserted when a rewind or position operation (including the optional data security erase portion of a rewind) is in progress.**

- **LS: Long/short success time**—When a formatter rejects a command with cache busy and cache full, it also appropriately sets the LS bit. If the formatter thinks the rejected command can be accepted if immediately issued, LS is clear. If not, LS is set. LS is clear if CB is cleared, and therefore if CB is clear, LS must be clear.
- **MR: Maintenance mode request**—Asserted when the drive is put into maintenance mode. On the TA78, this is accomplished through a thumbwheel switch on the operator panel.
- **NR: No read-ahead**—Set if read-ahead caching is disabled on this unit.
- **OA: Formatter on line or available (for the TOPOLOGY command)**
- **OL: Drive on line to formatter**
- **PB: Active port button**—PB = 0 if the formatter is connected to the controller through port A; PB = 1 if the formatter is connected to the controller through port B.
- **PE: Level 2 protocol error**—Asserted when a protocol error is detected while processing a Level 2 command.
- **PL: Position lost**—Asserted when the formatter is not certain of the current tape position.
- **PR: Position for retry**
- **PS: Port switch**—Asserted when the port switch is enabled.
- **PT: Position for termination**—Positions the tape to where it would have been had there been no error and exits the error recovery state.
- **RP: Request position**—Used by the formatter along with RT to inform the controller of the next step in the error recovery sequence.
  - Retryable RP = 1, RT = 1
  - Transfer RP = 0, RT = 1
  - Done RP = 1, RT = 0
  - No Error RP = 0, RT = 0
- **RR: Read reverse is supported**
- **RT: Request transfer**—Refer to the explanation for RP.
- **RWC: Rewrite capable**—This bit must not be set if CC is not set.
- **RWE: Rewrite error recovery**—Can only be set if CC is set.
- **SG: Space gaps**—Indicates a location where the tape operation will position the tape. This is determined by the number of gaps specified in the gap field.
- **SM: Speed mask**—SM = 0, supports up to four fixed speeds. SM = 1, supports totally variable speeds.
- **SME: Speed management enabled**—Asserted whenever the formatter may change the current operating speed of a particular drive at any time (provided the changing of the drive operating speed is transparent to the controller).
- **SR: Space records**—Positions the tape according to the number of records in the count field.
- **TE: Transmission error**—Used by the formatter to report Level 0 and Level 1 STI errors. The formatter only reports Level 0 real-time state parity errors and Write/Cmd Data Line pulse errors when a transfer is in progress. Level 1 errors are framing errors, checksum errors, inappropriate value in data field of real-time command, or a real-time command occurring in an invalid context.

- **TM: Tape mark**
- **U0: Low order drive number bit**—The drive to which a command applies.
- **U1: High order drive number bit**—The drive to which a command applies.
- **UN: Unload**—Unloads a tape after rewind.
- **WB: Write back**—Set if write back caching is enabled on this unit. CC also must be set.
- **WL: Write locked**
- **WP: Write protect**—Set when the controller desires to illuminate the write protect indicator on the selected unit.
- **ZT: Zero threshold**—Instructs the formatter to change all error thresholds from their default values to zero.

NOTE
Always verify proper dc voltage levels if the indicated possible FRUs do not rectify failure.

8.4.3.7 Tape Transfer Error Log

Example 8–11 is an example of a console display of a tape transfer error log.

```
ERROR-E Tape Transfer Error - Offline, No Media Mounted at 10-DEC-1990 21:50
        Command Ref #   FCA60034
        TA78 unit #     70.
        Err Seq #       170.
        Format Type     05
        Error Flags     00
        Event           0023
        Position        1081.
        Retry Level     0.
ERROR-I End of error.
```

Example 8–11 Tape Transfer Error Log Example

Table 8–30 Tape Transfer Error Log Field Descriptions

Field	Description
Command Ref #	This number (in hexadecimal) is the TMSCP command number which caused the reported error. It is zero if the error does not correspond to a specific outstanding command. This number is normally assigned by the issuing host CPU.
Err Seq #	This number (in decimal) is a sequential number which counts error log messages since the TMSCP server established a connection with the host. It is zero if the TMSCP server does not implement error log sequence numbers.
Format Type	This number (in hexadecimal) is the byte that describes the detailed format of the error log message. In this example, format type 05 indicates a tape transfer error.
Error Flags	This number (in hexadecimal) indicates bit flags, collectively called error log message flags, used to report various attributes of the error.
Event	This number (in hexadecimal) identifies the specific error or event being reported by this error log message. This code consists of a 5-bit major event code and an 11-bit subcode.
Position	This is the position that the tape would be at if the tape transfer in error had completed successfully.
Retry Level	This is the number of times the HSC controller has retried the transfer.

8.4.4 Out-of-Band Errors

The out-of-band errors are those not conforming to a specific template format, as the MSCP and TMSCP errors do. The method of reporting differs for each of these errors.

The HSC operating software allows the setting of different levels of error reporting for out-of-band type errors using the SETSHO utility. These message error levels are Informational, Warning, Fatal, Error, and Success. The identifiers for the out-of-band errors are followed by an I, W, F, E, or S, depending on the SETSHO value. The x in the following list represents the message error level.

Out-of-band errors are classified into the five categories listed below:

- **CI errors**—Identified by HOST-x identifier printed prior to message
- **Load device errors**—Identified by SYSDEV-x identifier prior to message
- **Disk functional errors**—Identified by DISK-x identifier prior to message
- **Tape functional errors**—Identified by TAPE-x identifier prior to message
- **Miscellaneous (software inconsistencies)**—Identified by SINI-x identifier prior to message

See Section 8.5 for listings and explanations of the above categories of out-of-band errors.

NOTE
Some out-of-band errors report microcode-detected error status codes within the printout. Refer to Appendix D for a full list of all K.ci, and disk/tape data channel module, and microcode-detected errors.

NOTE
When replacing indicated FRUs, always verify correct dc voltage levels before and after replacing a module.

8.4.4.1 RX33 Errors

Detected errors from the RX33 load device are classified in the out-of-band error category. The following is an example printout of a detected RX33 error:

```
SYSDEV-S Seq 104. at  6-JAN-1986 10:12:00.76
        DX1: LBN 1488. (49,0,02), Status 001
        Seek 000, 000000
        Tran 003, 021404
        T.O. 000
        87 3 1485 -7680 1 49 1 4
```

The -S following the SYSDEV prompt and before the Seq. number indicates the severity level. The RX33 has three severity levels:

- **Success (S):** Two or less errors during a command/retry.
- **Informational (I):** More than two errors.
- **Error (E):** Unrecoverable error.

The status field is most important and is a direct indication of the error. Following is a list of the RX33 status codes:

- **000:** Success.
- **001:** Success with retries.
- **002:** Software version mismatch (driver versus operating code).
- **200:** Command aborted through a Ctrl/Y or exception operation.
- **201:** Illegal file name.

- **202:** File not found.
- **203:** File is not in a loadable image format.
- **204:** Insufficient memory to load image.
- **205:** No free partition to load image into.
- **206:** Unit is software-disabled.
- **365:** Unit is write protected.
- **367:** No media mounted.
- **375:** EOF detected during read or write.
- **376:** Hard disk error, other than the following:
  - **370:** Bad unit number.
  - **357:** Data check error.
  - **343:** Motor broken (would not spin up).
  - **340:** Uncorrectable seek error (desired cylinder not found).
  - **311:** Bad record (LBN) number (not on media).
  - **272:** Parity error in controller on the memory module.

In the preceding example, the failing diskette drive is indicated by DX1:. The logical block number where the failure occurred is displayed by LBN 1488. The three numbers in parentheses, separated by commas after the logical block number indicate in order the cylinder, the media surface, and the drive sector.

The Seek entry's first group of zeros shows the retry count for seek/recal errors or the number of times the command was issued but not completed. The second group of zeros shows an inclusive OR of the control and status registers CSR bits set during seek error retries. The important bit in a seek error is bit 4.

The Tran (transfers) entry's first group of zeros shows the retry count for read, write, and format errors, or the number of times the command was issued and not completed. The second group of zeros shows an inclusive OR of the CSR bits set during read, write, and format error retries. A breakdown of the upper CSR bits is shown in Figure 8–24.

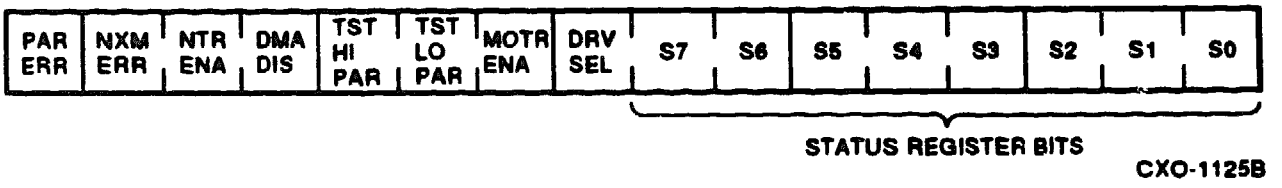


Figure 8–24 RX33 Floppy Controller CSR Breakdown

Table 8–31 shows the status of the lower CSR bits S7 through S0.

Table 8–31 Status Register Summary

Bit	All Type I Commands	Read Address	Read Sector	Read Track	Write Sector	Write Track
S7	Not Ready	Not Ready	Not Ready	Not Ready	Not Ready	Not Ready
S6	Write Protect	0	0	0	Write Protect	Write Protect
S5	Head Loaded	0	Record Type	0	0	0
S4	Seek Error	RNF	RNF	0	RNF	0
S3	CRC Error	CRC Error	CRC Error	0	CRC Error	0
S2	Track 0	Lost Data	Lost Data	Lost Data	Lost Data	Lost Data
S1	Index Pulse	DRQ	DRQ	DRQ	DRQ	DRQ
S0	Busy	Busy	Busy	Busy	Busy	Busy

The T.O. entry line is a timeout recording for each command type. This counter reflects the total number of timeouts for the command in error. All RX33 commands (READ, WRITE, RECAL, SPINUP, and FORMAT TRACK) time out in one second.

The last line in the error message is more complicated to break down. Figure 8–25 shows the breakdown of the last line of the example RX33 error message.

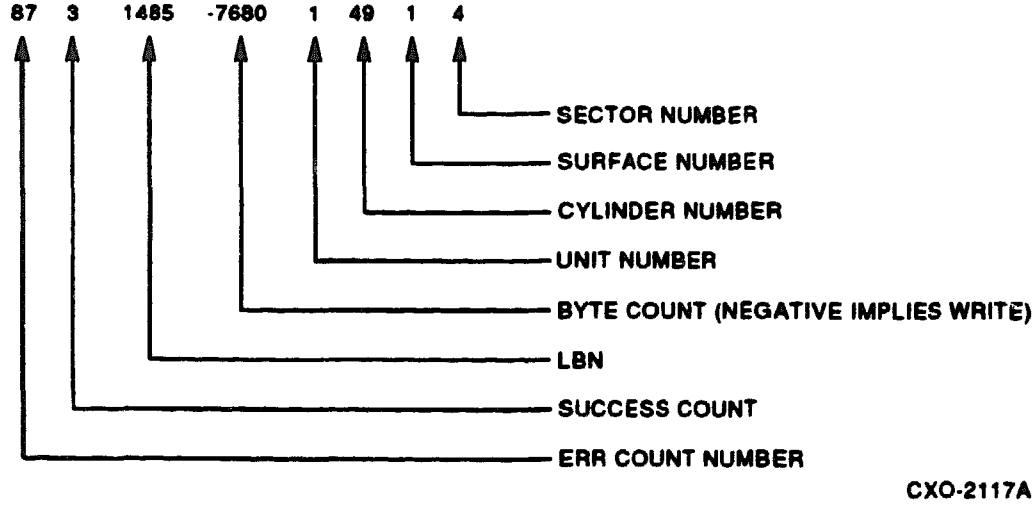


Figure 8–25 RX33 Error Message Last Line Breakdown

Most information in the error printout is reiterated in the last line. Starting from the right, sector, surface, cylinder number, and unit number are displayed as in the main body of the error message. The byte count has an indicator for write and read commands; the negative indicates a write operation. The LBN in this field is the starting LBN for this transfer. The LBN in the main message body is the failing LBN. The success count and error count are for informational purposes.

8.4.4.2 Disk Functional Errors

Although most disk drive-related errors are MSCP errors, several disk functional errors fall into the out-of-band error category. They are identified by the DISK-E identifier displayed on the console terminal prior to the error.

The message, message description, action, and probable FRUs for the disk functional out-of-band errors are listed in Section 8.5.

8.4.4.3 Tape Functional Errors

Although most tape errors are covered under TMSCP errors, certain tape functional errors are classified in the out-of-band error category. They are identified by the TAPE-E identifier printed prior to the error display on the local console terminal. See Section 8.5 for listings and explanations of out-of-band tape functional errors.

8.4.4.4 Miscellaneous Errors

Miscellaneous errors are identified by the SINI-E identifier displayed on the local console terminal. Many of these messages consist of one or two lines, but some have several lines of informational text that result from subsystem exceptions. Subsystem exceptions detect inconsistencies in the operating software. Listings and explanations of SINI errors are located in Section 8.5.

The SINI error messages are a result of the operating software performing a consistency check which failed. When consistency checks fail, the HSC controller performs a soft initialization causing it to crash and reboot. This is known as a subsystem exception. Upon successful completion of the reboot, the subsystem exception printout displays the contents of several HSC controller registers as well as the status of all requestors. As a result of the subsystem exception, the SINI error message is printed. This message tells why the last soft Init happened.

The actual sequence of events for a SINI-E out-of-band error printout is as follows:

1. When the HSC controller detects an unrecoverable problem, a soft Init or crash occurs. A system dump is performed under the heading SUBSYSTEM EXCEPTION. The HSC controller then reboots.
2. When the HSC controller reboots, a message indicating it has rebooted, followed by the multiline SINI message which gives the reason for the last soft Init (crash).
3. The same message is written on the system diskette and can be examined with the SHO EXCEPTION command. A host error message log is also filed in host memory as an HSC controller datagram, storing the out-of-band error SINI message.

8.4.5 Traps

The four traps described in the following sections (Trap through 4, Trap through 10, Trap through 114, and Trap through 134) are the same as are found in the 11/70 CPU.

8.4.5.1 NXM (Trap through 4)

If the error registers in the nonexistent memory (NXM) printout equal 170024 000077, the error is not an NXM error. Instead, it is a stack overflow or some illegal instruction. When the error register is any number other than 170024 000077, the number represents the unresponsive address. The NXM trap produces a subsystem exception printout similar to the example in Section 8.4.5.6.

If the error register equals 16xxxx, the window bus register equals the control memory address causing the NXM error. If the failing address is in control memory and shows an NXM error, it is definitely a hardware problem. Otherwise, it can be either a software or a hardware problem.

8.4.5.2 Reserved Instruction (Trap through 10)

The subsystem exception message for this trap indicates the vector number is 10 and identifies the trap as ILOP (an illegal Opcode). Refer to the (PC-6) to (PC): field in the Level 7K interrupt example of Section 8.4.5.6.

With a Trap through 10, the third word from the left is the instruction causing the trap. If this is a valid PDP–11 instruction, it is definitely a hardware problem. Otherwise, the program may not be executing in the right place, indicating the problem could be either hardware or software.

8.4.5.3 Parity Error (Trap through 114)

This error, caused by hardware, does not crash the HSC controller but causes a reboot and SINI error message. The error message shows the last reboot caused by the Trap through 114 and the address that caused the trap.

Determine if the error occurred in memory or in P.ioj instruction cache memory by reading the contents of the low error address given in the error display. If the content is the address of the low error address register (170024), the error is in cache memory. Any other address indicates the error is in memory.

In the following example, note the low error address and the high error address fields. When these fields contain the exact addresses as shown in this example, the error is from the I/O control processor cache.

```
SINI-E  Seq 1. at 17-Nov-1858 00:00:01.60
        Parity Error (Trap through 114)
        Process PSCHED
        PC  111022
        PSW 140000
        Lo err adr 170024
        Hi err adr 000077
        WBUSR 020633
```

8.4.5.4 Level 7 K Interrupt (Trap through 134)

A Level 7 K interrupt, detected by hardware or microcode, occurs when one or more requestors detect a fatal error condition while executing functional code. The microcode-detected errors causing Level 7 K interrupts result from a microcode consistency check failure in the disk/tape data channel module microcode. Requestor hardware-detected errors are the result of errors detected on the control bus, scratchpad RAM parity errors/data bus parity errors, or host clears, or control bus NXMs (not related to data transfers). The requestor, upon detecting the error, generates a Level 7 interrupt to the I/O control processor. The I/O control processor traps through location 134, causing a reboot.

8.4.5.5 Control Bus Error Conditions (Hardware-Detected)

The hardware detected control bus errors causing Level 7 K interrupts are:

- Control bus error—The requestor was in the process of executing a control bus cycle and received CERR L (control bus error low) from the I/O control processor. The I/O control processor had detected an illegal control bus cycle type.
- Control bus parity error—The requestor detected bad parity on the data it read off the control bus.
- Control bus NXM—The requestor tried to reference control memory and did not receive an acknowledgment (CACK L) from the memory module within the timeout period.

8.4.5.6 Level 7 K Interrupt Example

An example of a detected Level 7 K interrupt follows.

```
   SUBSYSTEM EXCEPTION *-        V# 250          HSC  LONDON
       at 25 Oct 1985  00:08:46.64           0 23:23:21.40

User    PC:  110574 caused by  (134  ) Kint
PSW: 140011

PSCHED active  PCB addr = 054536

R0-R5:
000000  000024  000000  000000  000000  000000

Kernel SP: 000774

Kernel Stack

005046  000004  052744  045412  001012  000000  045644  000000
052136  000000  047260  000000  051300  000000  054742  000000

User SP: 000774

User Stack:
150042  147502  147516  000000  102146  000000  000000  000000
000000  000000  000000  000000  000000  000000  000000  000000

KPAR(0-7):
000440  000640  001040  1577770  001440  001240  000240  177600

KPDR(0-7):
077506  077506  077506  077406  077506  077406  077506  077506

UPAR(0-7):
000000  000000  000000  000000  002204  001240  000240  177600

UPDR(0-7):
077406  077406  077406  077406  063406  077406  077406  000116

MMSR(0-2): 000017  000000  037260

Window Index Reg: 000026

Window Bus Reg: 001431

WADR(0-7):

160004  161004  162004  163004  164004  165004  166004  167004

Translated WADR(0-7):
001401  001401  001401  001401  001401  001401  001401  001401

Error Regs: 170024  000077

Status of Requestors(1-9):
000001  000377  000377  000377  000377  000175  000377  000377  000377

(PC-6) to (PC):
013737  141020  110560  013701
Control area for slot #000006
Control area address: 017660:
Register area contents:
```

```
000000
000000
000011
021154
102557
000770
000000
000000
017650
000000
057502
005317
002224
001000
000000
000671
000000
143444
107001
001000
005317
002212
000671
001000
000000
000000
000000
040506
000010
000374
043520
005400
001000

Booting
INIPIO-I Booting
```

Requestor 6 failed with a status of 175. Refer to Appendix D to determine if the failure was a control bus error.

At this time the HSC controller reboots. A message is displayed on the local console terminal stating the HSC controller has rebooted.

```
    HSC Version 200 29-Sept-1985 23:17:28   System LONDON
```

The actual SINI error message is displayed on the local console terminal after the HSC controller has rebooted.

```
SINI-E  Error sequence 1. at 17-Nov-1858 00:00:03.00
        Last soft Init caused by Level 7 K interrupt
        From process PSCHED
        PC  110574
        Status: 001 377 377 377 377 175 377 377 377
```

The resulting 134 trap information is displayed on the local console terminal. The PSCHED statement indicates PSCHED was the active process when the error occurred. The status statement shows Requestor 6 failed with a status of 175. Also, three lines after the status line is a message line indicating the control area for slot six and slot six control address. This indicates Requestor 6 is the failing requestor. The INIPIO-I Booting statement indicates the HSC controller is attempting to reboot.

When the HSC controller completes the initialization, the last soft init caused by Level 7 K interrupt failure is displayed on the local console terminal identified by SINI-E. The active process at time of failure is identified. In this case, the active process was PSCHED. If the failure is a hard failure, the following message may also be displayed on the local console terminal.

```
SINI-E ERROR SEQUENCE 1. AT 25-OCT-1858 00:00:02.80
    REQUESTOR 6 FAILED INIT DIAGS, STATUS 107
```

This message is also considered an out-of-band error.

8.4.5.7 MMU (Trap through 250)

Following is an sample printout of a detected MMU failure:

```
** JBSYSTEM EXCEPTION**    V# Y10B          HSC LAYER
      at 12-DEC-1985 13:43:40.05    up   2 19:24:07.40

User PC:  004747  caused by (250 ) MMU
PSW: 140000

SETSHO active, PCB addr = 104116

R0-R5:
000320  000001  100000  100212  000266  000002

Kernel SP: 000774

Kernel Stack:
005046  000004  053314  045762  001012  000000  046214  000000
047022  000000  047426  000000  052052  000000  051042  000000

User SP: 000226

User Stack:
040314  021356  033552  021356  021246  000040  017440  017440
020040  020037  020037  000330  101000  027113  000144  060542

KPAR(0-7):
000440  000640  001040  001440  002040  001240  000240  177600

KPDR(0-7):
077506  077506  077506  077506  077506  077506  077506  077506

UPAR(0-7):
007074  007274  006410  000000  002240  001240  000240  177600

UPDR(0-7):
077506  077406  013406  077406  077406  077506  077506  000116

MMSR(0-2): 040145  000000  004743

Window index reg: 000002

Window bus reg: 001407

WADR(0-7):

160000  161004  162440  163000  164004  165004  166220  167034

Translated WADR(0-7):
000000  001401  067510  040000  001401  001401  010444  001407

Error regs: 170024  000077

Status of requestors(1-9):
000001  000002  000002  000002  000203  000203  000203  000377  000377

(PC-6) to (PC):
027441  067516  051040  071545
```

Because the trap is a MMU trap, look first at the register contents of MMSR0 (memory management status register 0). Refer to Figure 8–26 for a breakdown of the bits in MMSR0.

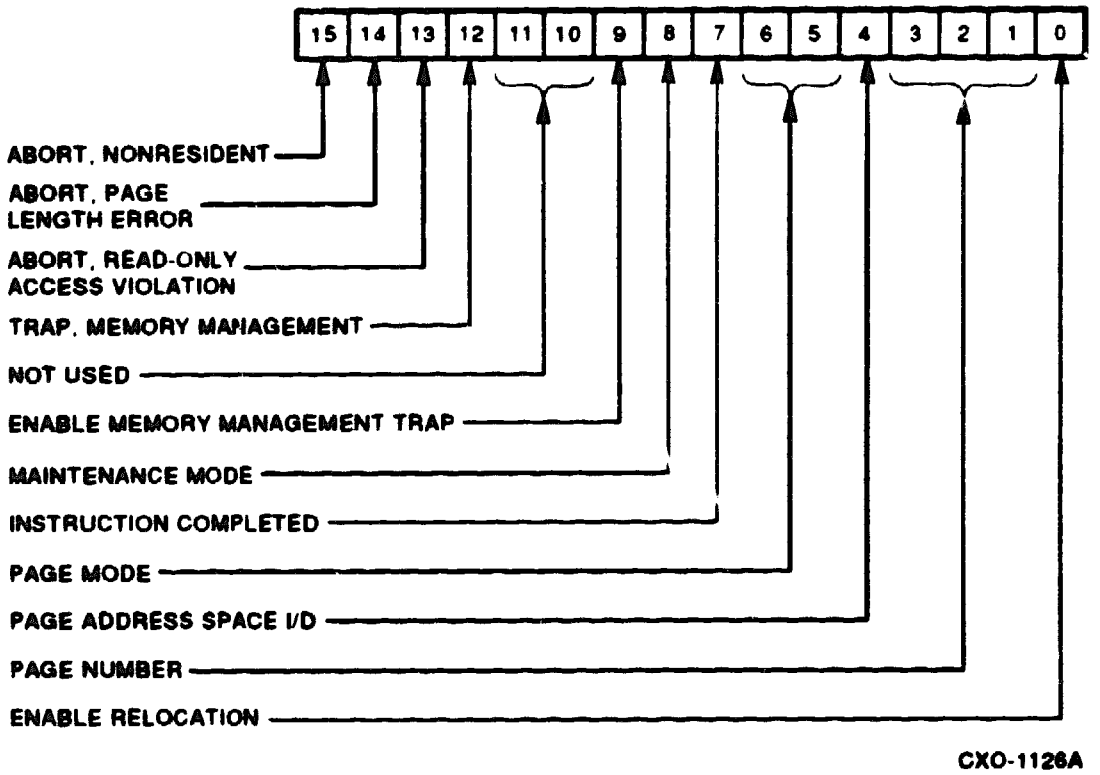


Figure 8–26 MMSR0 Bit Breakdown

Look at the printout lines for MMSR (0-2). Compare the bits set in MMSR0 to the bit breakdown in Figure 8–26. The example indicates a page length violation on page 2. The page length error bit is set, and the page number 2 bit is set.

Next, check the PSW line and determine the mode in which the HSC controller reported this error. A 14xxxx in the PSW means User mode, a 00xxxx in the PSW means Kernel mode. Also, above the PSW line the word User or Kernel appears to identify the mode. Our example shows User mode is active. Therefore, the next register contents of any value are the UPAR and UPDR. If the active mode had been Kernel, the important registers would have been the KPDR and KPAR registers.

The first group of numbers under the UPAR(0-7) line is for page zero, the second for page one, the third for page two, and so forth. The third group of numbers in the example are for page two, the violated page. Note the difference in UPDR contents on page two versus the UPDR contents on other pages. The UPDR contents on other pages all start with 077 designating a full page of memory to be allocated for that page. The UPDR contents on page two starts with a 013., indicating a short page.

Two possible problems cause this error:

- MMU on the I/O control processor
- Software

Software inconsistency (Trap through 20) is reported similar to an MMU trap. A subsystem exception is dumped on the local console terminal with the trap vector reported being a Trap through 20 (AT). An example printout and explanation are found in Appendix B.

The subsystem exception is followed by the HSC controller reboot. Upon successful reboot, the following message is displayed:

```
HSC Version Y10B   16-Jan-1986  15:30:20.20  System MASTER
```

Then the SINI error resulting from the detected subsystem exception is printed.

```
SINI-E Sequence 1. at 16-Jan-1986  00:00:11.20
 Last soft Init caused by software
inconsistency
 From process HOST
 PC  007044
 PSW 140001
 Stack dump: 000016  006401  015476
```

8.5 Alphabetical Listing of Software Error Messages

Each message description includes the following:

- **Actual error message**—The error message text as displayed in English at the HSC console terminal.
- **Error type**—The type of error detected by the HSC controller. Error types include MSCP, TMSCP, disk out-of-band, and tape out-of-band. The out-of-band message number (in octal) or MSCP/TMSCP event code (in hexadecimal) is included for most messages and can be used for reference with VAXsimPLUS or host error logs. In addition, more information on specific MSCP/TMSCP event codes is given in Appendix C.
- **Error message severity level**—The error message severity level included in the error message.
- **Message description**—A review of what the error is about.
- **Action**—Remedies or troubleshooting paths that the Customer Service representative can take to correct the problem.
- **Possible FRUs**—Suggested components that are likely suspects causing the malfunction, listed in order of probability.

Aborting Error Recovery Due to Excessive RECALs
Disk Unit xxx.
Requestor xx
Port xx

Error Type: Disk functional out-of-band (001204)

Severity: Error

Description: For each group in a transfer, a count of the number of RECALS issued to the drive is kept. If the count exceeds a hard-coded value, this message is displayed. Recovery from an error is not possible because of excessive RECALS, and the drive is declared inoperative.

Action: Refer to the drive service manual and any other logged errors to determine reasons for persistent positioning failures.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Aborting Error Recovery Due to Excessive Timeouts
Disk Unit xxx.

Error Type: Disk functional out-of-band (001244)

Severity: Error

Description: This message is displayed when the HSC detects several transfer timeouts on a disk drive. A timeout occurs because the HSC disk server could not complete a subset of a transfer operation within an expected amount of time. All error recovery attempts are aborted and the drive is declared inoperative.

Action: May need to replace the following FRUs. Further testing may be necessary.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module

Acknowledge Not Asserted at Start of Transfer

Error Type: Tape controller error (TMSCP event code FD6A)

Severity: Error

Description: The HSC controller is ready to start a transfer by sending the formatter a Level 1 command and the formatter does not have ACKNOWLEDGE asserted.

Action: Check the formatter. This error may indicate a formatter STI communications error, or if preceded by tape transport errors, may be a result of a transport failure.

Possible FRUs:

- Formatter
- Tape data channel module
- STI cable set

Bad Block Replacement (Block OK)

Error Type: BBR error (MSCP event code 0034)

Severity: Warning

Description: A block submitted for bad block replacement tested OK and was not replaced.

Action: Monitor drive for the frequency of these reports. If frequency increases, troubleshoot the error that triggers BBR. This error is identified in the cause event error message field.

Possible FRUs: Refer to the Cause Event error message field in Table 8–22.

Bad Block Replacement (Drive Inoperative)

Error Type: BBR error (MSCP event code 0094)

Severity: Warning

Description: Replacement failure due to a drive access failure. One or more transfers specified by the replacement algorithm failed because the drive is in an inoperative state. If necessary and possible, write protect the drive and perform a volume backup immediately.

Action: Drive should be tested further. Look for other HSC console messages indicating why the drive might have been declared inoperative by the HSC controller. Move the drive to

another disk data channel module (or to just another disk data channel port) if available. If the problem persists, failure is probably in the drive.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Bad Block Replacement (RCT Inconsistent)

Error Type: BBR error (MSCP event code 0074)

Severity: Warning

Description: Replacement failure due to an inconsistent RCT. This error generally occurs due to a failure to successfully read or write any copy of an RCT block.

Action: Drive media should not be used until replaced or verified as good. If necessary, write-protect this drive and have the customer perform a volume backup immediately. Further testing of the drive may be necessary.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Bad Block Replacement (Recursion Failure)

Error Type: BBR error (MSCP event code 00D4)

Severity: Warning

Description: Replacement failure due to a recursion failure. During a BBR operation, the HSC controller found two successive RBNs to be bad.

Action: Monitor drive for the frequency of these reports. If frequency increases, troubleshoot the error triggering BBR.

Possible FRUs: Refer to the Cause Event error message field in Table 8–22. Also, inspect the drive for possible problems. You may need to replace drive modules.

Bad Block Replacement (REPLACE Failed)

Error Type: BBR error (MSCP event code 0054)

Severity: Warning

Description: Replacement failure due to a failure to complete a replacement operation. This indicates that the HSC controller was unable to format the headers of the bad block to indicate it is replaced.

Action: Drive media should not be used until it is replaced or verified as good. If necessary, write protect this drive and have the customer perform a volume backup immediately. Further testing of the drive may be necessary.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Bad Block Replacement (Success)

Error Type: BBR error (MSCP event code 0014)

Severity: Warning

Description: A bad block was successfully replaced.

Action: Monitor drive for the frequency of these reports. If frequency increases, troubleshoot the error triggering BBR.

Possible FRUs: Refer to the Cause Event error message field in Table 8–22.

Bad Dispatch State in CB...

Error Type: CI-detected out-of-band (001001)

Severity: Warning

Description: The CI Manager attempts to send an SCS control message and finds an invalid dispatch state in the control block. The CI Manager then uses the dispatch state to determine where to send the proper control message. If this is the only known problem, a software problem could exist within the HSC controller. Otherwise, the problem could be caused by a control bus addressing problem with the port processor, memory module, or I/O control processor modules.

Action: Replace the following FRUs.

Possible FRUs:

- Port processor module
- Memory module
- I/O control processor module

Buffer EDC Error

Error Type: Tape controller error (TMSCP event code FF8A)

Severity: Error

Description: The tape data channel module detected an EDC error on the data buffer it read from memory on a write operation.

Action: Test the data path from the tape data channel module to HSC data memory and the K.ci. Also, check for memory parity errors.

Possible FRUs:

- Formatter/tape drive
- Memory module
- Tape data channel module
- K.ci module

Cache functionality requested but M.cache hardware not present.

Error Type: SINI out-of-band (001702)

Severity: Error

Description: Cache server functionality has been previously requested using the SETSHO command **SET SERVER DISK/CACHE**, but there is no M.cache module present in the HSC controller. If an M.cache module is correctly installed, a possible cause of this error is a hardware failure in the M.cache module.

Action: If no M.cache module is installed in the HSC controller, use the SETSHO command **SET SERVER DISK/NOCACHE** to disable caching. If an M.cache module is installed, run the diagnostic ILCACH to verify proper M.cache module operation. If ILCACH cannot be invoked, replace the M.cache module.

Possible FRUs: M.cache module

Cannot reopen VC to node x. I/O rundown not yet complete.
Open connections: y

Error Type: CI-detected out-of-band (001101)

Severity: Error

Description: The CIMGR requires that all I/O initiated during the previous incarnation of a virtual circuit be run down and that the connections established be closed before it can remake the virtual circuit. This message is issued within 15 seconds after a virtual circuit closure if the I/O has not been run down and the connections are closed. If this condition exists for more than 10 minutes, the CIMGR issues exception code 7024.

Action: This message may occur under heavy load conditions on the HSC controller, when it may take a significant amount of time to run down all I/O. Under these conditions, the message is a warning. If 7024 exceptions occur repeatedly, indicating excessively long I/O rundown times, the HSC controller should be tested for possible hardware faults. If no hardware faults are encountered, submit an SPR and include the HSC console log and system error log.

Clock dropout from ONLINE disk unit xx.

Error Type: Disk functional out-of-band (000644)

Severity: Error

Description: The online disk has lost its real-time state clock.

Action: Check the path between the disk data channel module and the disk drive that was reported. Determine if the problem is in the HSC controller or the disk drive. Other disk error reports may precede this message and provide more detail about this error condition.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- SDI cable
- Disk data channel module

Compare Error

Error Type: Controller error (MSCP event code 0007)

Severity: Error

Description: A compare error occurred during a read-compare or a write-compare operation. For the read-compare operation, the HSC controller again obtains the data from the unit or shadow set and compares it with data obtained from host memory. If the data is not the same, a compare error results. For the write-compare operation, the controller obtains data previously written to the drive and compares it with data again obtained from host memory. If the data is not the same, a compare error results.

Action: Isolate the FRU by moving the disk or tape drive to another data channel module and retrying the exact failing operation. Also, check the HSC data memory buffer address for repetition. If failure occurs on multiple physical units across multiple data channels, *and* HSC data memory buffer address is not repetitive, investigate a possible K.ci problem.

Possible FRUs:

- Isolated disk (or tape) unit
- Data channel module
- Memory module

- K.ci module set
- Host CI/memory

Control microprocessor running with memory bank or board swap enabled

Error Type: SINI out-of-band (001002)

Severity: Error

Description: Upon initialization, an error was detected in the low address space of private memory. The I/O control processor asserted the Swap Bank signal, and the second bank of private memory was enabled. The I/O control processor and memory combination can still function under limited capabilities.

Action: Replace the memory module. The HSC controller still functions with limited capabilities.

Possible FRUs: Replace memory module

Controller Detected Position Lost

Error Type: Tape error (TMSCP event code FFF1)

Severity: Error

Description: Position information contained in the response from the formatter after an STI POSITION command was executed does not match the expected tape drive position.

Action: Check the formatter. If the error persists, run the ILTAPE diagnostic to help isolate to the FRU.

Possible FRUs: Formatter

Controller Transfer Retry Limit Exceeded

Error Type: Tape error (TMSCP event code FF88)

Severity: Error

Description: The controller failed to perform the transfer within the limit of allowable retries.

Action: Check the formatter and the drive.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Formatter

Controller Detected Transmission or Timeout Error

Error Type: SDI error (MSCP event code 4B)

Severity: Error

Description: The controller detected an invalid framing code or a checksum error in a Level 2 response from the SDI drive.

Action: Determine if this error is occurring on more than one drive, which may indicate a disk data channel problem. However, if it is occurring only on one drive, the SDI cable or the drive may be at fault. Refer to the appropriate drive service manual for assistance with drive FRUs.

Possible FRUs:

- SDI cable
- Drive SDI interface module
- Disk data channel module
- SDI transition bulkheads

Could Not Complete On-line Sequence

Error Type: Tape error (TMSCP event code FECB)

Severity: Error

Description: Could not complete online sequence due to a condition in the drive. One of the following STI commands in the online sequence failed: REWIND, SET BYTE COUNT, SET UNIT EXECUTION MODE, or SET UNIT CHARACTERISTICS.

Action: Check the formatter and the drive.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Formatter

Could Not Get Extended Drive Status

Error Type: Tape error (TMSCP event code FDEC)

Severity: Error

Description: Issued the GET EXTENDED DRIVE STATUS command and the drive did not respond with the extended drive status.

Action: Check the formatter.

Possible FRUs: Formatter

Could Not Get Formatter Summary Status During Transfer Error Recovery

Error Type: Tape error (TMSCP event code FFEC)

Severity: Error

Description: Issued the command and the formatter did not respond with the formatter summary.

Action: Check the formatter.

Possible FRUs: Formatter

Could Not Get Formatter Summary Status While Trying to Restore Tape Position

Error Type: Tape error (TMSCP event code FEDC)

Severity: Error

Description: Issued the command and the formatter did not respond with the formatter summary status.

Action: Check the formatter.

Possible FRUs: Formatter

Could Not Position for Formatter Retry

Error Type: Tape error (TMSCP event code FFCB)

Severity: Error

Description: The HSC controller issued a data error recovery command to position for retry, and the drive could not complete the command.

Action: Check the media, drive, and formatter.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Media
- Formatter

Could Not Set Byte Count

Error Type: Tape error (TMSCP event code FE2B)

Severity: Error

Description: Issued command to set byte count and could not complete command.

Action: Check the formatter.

Possible FRUs: Formatter

Could Not Set Unit Characteristics

Error Type: Tape error (TMSCP event FE6B)

Severity: Error

Description: Issued command to set unit characteristics and could not complete command.

Action: Check the formatter.

Possible FRUs: Formatter

Data Bus Overrun

Error Type: Controller error (MSCP/TMSCP event code 010A)

Severity: Error

Description: The HSC controller attempted to perform too many concurrent transfers, causing one or more of them to fail due to a data overrun or underrun. For example, data is sent to a bus by a data producer and then removed from the bus by a data consumer. If the producer sends data to the bus more quickly than the consumer can remove it, a data overrun occurs. If the consumer removes data more quickly than the producer can send it, a data underrun occurs.

Action: This error is not to be considered serious unless large numbers of these errors are occurring. If this is the case, determine which module is the data producer and which module is the consumer for a given error. Use the requestor number for assistance.

If the problem persists after replacing the suspect module(s), an HSC software problem should be investigated.

Possible FRUs:

- Source requestor module
- SDI/STI cable
- Tape formatter
- Disk or tape drive

Data Error Flagged in Backup Record
Disk Unit xx, LBN xx
Tape Unit xx

Error Type: Tape functional out-of-band (001045)

Severity: Warning

Description: During a backup, a data error was encountered. During BBR, the record was written with a forced error bit set.

Action: Check BBR history on source drive.

Possible FRUs:

- Disk unit
- Media

Data Memory Error (NXM or Parity)

Error Type: Controller error (MSCP/TMSCP event code 012A)

Severity: Error

Description: The HSC controller detected an error in internal data memory. The error was either a parity error, detected through a parity generator/checker (data only—not address) on the requestor module, or a nonresponding address (the requestor did not receive a DACK from the memory module).

Action: Determine if this error is repetitive; if so, the problem is probably the memory module. However, it may be a data bus problem caused by a number of things, such as failing bus drivers/receivers on the indicated requestor modules.

NOTE
If an M.cache module is installed, the data memory being used is located on the M.cache module, not the M.std4 memory module.

Possible FRUs: Memory module or a possible data bus problem.

Data Ready Timeout

Error Type: Tape error (TMSCP event code FD2A)

Severity: Error

Description: The controller did not detect data ready from the formatter within the timeout interval after sending it a Level 1 command.

Action: Check the STI path.

Possible FRUs:

- Formatter

Data Sync Not Found

Error Type: Disk transfer error (MSCP event code 0068)

Severity: Error

Description: This error occurs when the SERDES 16 does not detect the SYNC character immediately preceding read data from the disk drive. The disk data channel module has already read a valid header and is awaiting the data SYNC character.

Action: Determine if additional errors occur from this drive to indicate a drive or media error. If not, the problem is probably the disk data channel module.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module
- SDI interface

Date/Time Set By Node nn

Error Type: CI-detected out-of-band error (000201)

Severity: Informational

Description: The HSC controller received either a START or STACK (start acknowledge) message over the CI, and the date and time was not set.

Action: None. This is a normal message as part of establishing a VC between a host and an HSC controller.

Possible FRUs: None

Disk unit xx cannot be brought available. HSC is currently set up to support a maximum of yy sectors per track, but disk unit xx has zz sectors per track. Use SET SERVER DISK/MAX_SECTORS_PER_TRACK=n to change set up.

Error Type: Disk functional out-of-band (001644)

Severity: Error

Description: The user has attached a drive to the HSC controller that has more sectors per track than the HSC controller is currently set up to support. The HSC controller is set up to support a maximum of yy sectors, but the attached drive has zz sectors per track.

Action: Use the SETSHO command SET SERVER DISK/MAX_SECTORS_PER_TRACK=zz to set the HSC controller to support this drive. This SETSHO command requires an immediate reboot on exit to reallocate structures that are based on this new value. The default value of sectors-per-track is 74.

Possible FRUs: None.

Disk unit xx. (Requestor xx., Port xx.) being INITialized.
DCB addr: xxxxxx

Error Type: Disk functional out-of-band (001004)

Severity: Informational

Description: A disk is being initialized. The initialization sequence is used by the controller to re-establish communication with the drive.

Action: None

Possible FRUs: None

Disk unit xx. ready to transfer.
Retrieval failure or subsystem deadlock probable.

Error Type: Disk functional out-of-band (000244)

Severity: Informational

Description: A disk transfer did not complete within an allowable timeout period. The HSC software cannot detect any problems to account for the failure. Possible problems include:

- No available buffers
- Drive problems
- Disk data channel problems
- Very busy system

Action: Check data transfer path. This error may indicate too many utilities or inline diagnostics running simultaneously. The problem might also be an HSC software problem.

Possible FRUs:

- Disk data channel module
- K.ci host interface module set

Disk unit xxx. (Requestor xx., Port xx.) declared inoperative.
Intervention required.

Error Type: Disk functional out-of-band (000504)

Severity: Error

Description: The HSC controller disk path process has concluded that the drive is no longer usable but has no evidence that the drive is broken. Any pending I/O is cleaned up, and the drive is placed in the offline state. The HSC controller ignores the disk until it detects some intervention.

Action: Examine previous error reports to help resolve failure. Toggle port switch on drive.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- SDI cable
- Disk data channel module

DRAT/SEEK timeout, disk unit xxx.

Error Type: Disk functional out-of-band (000144)

Severity: Informational

Description: A stimulus resulting in error recovery code action is the expiration of the DRAT/SEEK timer for the drive. A DRAT represents data transfer action with the drive, whereas the SEEK represents position requests to the drive.

Each drive has a timer allocated on its behalf at subsystem initialization time. This timer, called the DRAT/SEEK timer, is active whenever data transfer activity to the drive is outstanding. If the timer expires with transfer or seek activity in progress, this message is printed, if informational messages are enabled.

A timer may expire for several reasons:

- The drive has detected a drive error and has lowered the Read/Write Ready line.
- The drive has lowered the Receiver Ready line.
- The drive has stopped sending clock signals.
- A SEEK has timed out.
- Another element in the subsystem has not supplied resources to the disk transfer operation in a reasonable time, or the disk transfer is stalled somewhere in the subsystem.

Action: Check the drive. Also, make sure that there are no CI problems preventing data from reaching the HSC controller.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- K.ci host interface
- Disk data channel module

Drive Clock Dropout

Error Type: SDI or disk transfer error (MSCP event code 00AB)

Severity: Error

Description: Either data or state clock was missing when it should have been present. This is detected by the requestors connected to this SDI drive, usually by means of a timeout.

Action: Determine if this error is occurring on more than one drive, which may indicate a disk data channel problem. However, if it is occurring on only one drive, the SDI cable or the drive may be at fault. If other errors surround or precede this one, those errors may have sequentially triggered this error. Refer to the appropriate drive service manual for assistance with drive FRUs.

Possible FRUs:

- SDI cables
- Drive SDI interface module
- Disk data channel module
- SDI transition bulkheads

Drive Detected Error

Error Type: SDI error (MSCP event code 00EB)

Severity: Error

Description: The controller received an SDI GET STATUS response or other unsuccessful SDI response with the EL bit set, or the controller received a response with the DR flag set and does not support automatic diagnosis for that SDI drive type.

Action: Determine if the drive has a hard fault (Fault indicator on and an error code in the drive microprocessor LEDs). Refer to the drive service manual for assistance with drive internal diagnostics and LED error codes. Decode remaining error message bytes for more detailed error information. If error message decoding does not clearly indicate a drive error, move the drive to another requestor (or requestor port) to help isolate failure between HSC controller and drive.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- SDI cables
- SDI bulkheads

Drive Inoperative

Error Type: SDI error (MSCP event code 0043)

Severity: Error

Description: The HSC controller has marked the drive inoperative due to an unrecoverable error in the previous Level 2 exchange, the drive's C1 flag is set, or the drive has a duplicate unit identifier. Once the HSC controller reports the drive as inoperative, the drive state clocks must transition to return the drive to an operational state. This is accomplished by toggling the port button on the drive.

Action: Refer to the drive service manual. Run ILDISK to help isolate failure between HSC controller and drive.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module
- SDI cables

Duplicate Disk Unit xx

Error Type: Disk functional out-of-band (001544)

Severity: Informational

Description: Disk unit numbers are duplicated within the system.

Action: Locate the duplicate disks and change the unit number on one.

Possible FRUs: Drive modules. It is possible that the unit number sensing on the drive may be at fault. (Refer to the drive service manual.)

EDC Error

Error Type: Controller error (MSCP event code 004A)

Severity: Error

Description: The sector was read with correct or correctable ECC and invalid EDC. A fault probably exists in the logic of either this controller or the controller that last wrote the sector. Look at the source and detecting requestor fields in the error message to determine which requestor detected the error and the direction of the transfer (read or write).

NOTE
If an M.cache module is installed, note if the requestor ID indicates that the M.cache module supplied the data.

Action: Determine if other errors indicate a problem with the data path circuitry on the indicated requestor modules.

Possible FRUs:

- Disk data channel module
- Memory module, if an address parity error on data memory occurs, as this is checked by the EDC field.
- M.cache module, if installed.

ERASE Command Failed

Error Type: Tape error (TMSCP event code FF0B)

Severity: Error

Description: Issued ERASE command and the command failed.

Action: Check the formatter.

Possible FRUs: Formatter

ERASE GAP Command Failed

Error Type: Tape error (TMSCP event code FEEB)

Severity: Error

Description: Issued ERASE GAP command and the command failed.

Action: Check the formatter.

Possible FRUs: Formatter

Forced Error

Error Type: Disk transfer error (MSCP event code 0008)

Severity: Error

Description: The sector was written with a Force Error modifier indicating this is a replaced image and the original data could not be read correctly using retries and the ECC algorithms.

Action: Restore the media from a previous backup. A VMS RESTORE of the current media will clear the forced error condition but will leave the sector corrupt.

Possible FRUs: None

Formatter Detected Position Lost

Error Type: Tape error (TMSCP event code FF71)

Severity: Error

Description: The formatter lost track of tape position.

Action: Check the media, drive, and formatter.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Formatter
- Media

Formatter and HSC Disagree On Tape Position

Error Type: Tape error (TMSCP event code FFD1)

Severity: Error

Description: The formatter and the HSC controller disagree on position of the tape.

Action: Check the formatter.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Formatter
- Tape data channel module

Formatter Requested Error Log

Error Type: Tape error (TMSCP event code FFC6)

Severity: Error

Description: The formatter detected an error and set the EL bit to request an error log be taken.

Action: Check the formatter.

Possible FRUs: Formatter

Formatter Retry Sequence Exhausted

Error Type: Tape error (TMSCP event code FF68)

Severity: Error

Description: HSC software issued a data error recovery command with position for termination to the formatter, and it failed.

Action: Check the media, drive, and formatter.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Formatter
- Media

Hard transfer error loading (file) xx

Error Type: SINI out-of-band (000142)

Severity: Error

Description: The I/O control processor detected a hard error while loading a file from the system media into program memory. The particular files that can produce this error are DUP and MIRROR. The xx field is the error status value from the device driver.

Action: Load the file from the other system load device; load the back-up media.

Possible FRUs:

- System media
- System load device

Hard transfer error writing SCT xx

Error Type: SINI out-of-band error (000202)

Severity: Error

Description: The HSC controller detected an error while attempting to write the SCT on the console load media. The xx designates the octal byte that is the error status value returned from the device driver.

Action: Make sure the media is not write protected; try the back-up media; try the other system load device.

Possible FRUs:

- System media
- System load device

Header Error

Error Type: Disk transfer error (MSCP event code 0048)

Severity: Error

Description: The subsystem read an inconsistent or invalid header for the requested sector. For recoverable errors, this code implies that a retry of the transfer read a valid header. For unrecoverable errors, this code implies the subsystem attempted nonprimary revectoring and determined the requested sector is not revectored. Causes of an invalid header include header mis-sync, header sync timeout, and an unreadable header.

Action: Determine if this error is repetitive on this unit indicating a deteriorating media.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

HMLSER set—HM$ERR = nn

Error Type: CI-detected out-of-band (000141)

Severity: Warning

Description: A host memory block (HMB) operation resulted in an error. A breakdown of HMB error word (HM$ERR) bits follow.

- 000002 HME$BM—Insufficient BMBs to receive message.
- 000004 HME$NC—Sequenced message received over a connection with 0 in credit field.

- 000010 HME$NC—Sequenced message received over a connection with credit field > 1. Excess has been added to CB$EM.
- 000020 HME$OV—Oversize message received (>1096. bytes).
- 000040 HME$DN—Data memory NXM during BMB operation.
- 000100 HME$DP—Data memory parity error in BMB operation.
- 000200 HME$DO—Data memory overrun during BMB operation.
- 000400 HME$FP—Reception buffer parity error in packet header. Message not receivable.
- 001000 HME$PL—Reception buffer parity error in body of message.
- 002000 HME$CN—Transmission not attempted because connection not valid.
- 004000 HME$VC—Transmission not attempted because VC closed or connection invalid.
- 010000 HME$TE—Transmission attempted but failed (no ACK).
- 020000 HME$TP—Transmission failed due to transmission buffer parity error.
- 040000 HME$HC—Packet inconsistent with K.ci context received from host.
- 100000 HME$IC—Illegal control function opcode.

Action: Compare the displayed code to the previous list and determine where the problem lies. For example, a code of 000040 indicates a failure in the memory module, and a code of 002000 indicates a problem in the K.ci module set.

Possible FRUs:

- Port buffer module
- Port processor module
- Memory module
- M.cache module

Host clear from CI node xx

Error Type: SINI out-of-band (000642)

Severity: Error

Description: The host reset the HSC controller for some reason, such as a non-response from the HSC controller within a certain amount of time. This message is generally printed when the HSC controller reboots following the host reset operation.

Action: Check the HSC console messages and the error logs of the systems connected to the HSC controller. Analyze the HSC console crash dump, if available, for more information.

Possible FRUs:

- CI cable
- HSC/CI interface
- Host/CI interface
- HSC software
- System software

Host interface (K.ci) failed INIT diags, status = xxx

Error Type: SINI out-of-band (000302)

Severity: Error

Description: The failing status indicates which module in the K.ci set has failed. A soft fault code is generated and may be examined by pressing the fault button on the OCP.

Action: Determine which is the failing module by comparing the failing status value to the values in Appendix D. This comparison points more directly to the failing module.

Possible FRUs:

- Port link module
- Port buffer module
- Port processor module

Host interface (K.ci) is required but not present

Error Type: SINI out-of-band (000242)

Severity: Error

Description: A K.ci module set is absent, or the failure in the K.ci module set was so severe upon initialization that the initialization diagnostics did not run. This error can occur when the K.ci module set is not connected to a star coupler, or when a loopback connector is not installed during testing.

Action: Check for the presence of a K.ci module set. If missing, install the K.ci module set. If K.ci module set is present, determine which module is failing by running offline diagnostics. This error generates a soft fault and is examined by pressing the fault button on the OCP.

Possible FRUs: See list below and error message Last Soft Init resulted from unknown cause.

- Port processor module
- K.ci module set (any one of the three modules in the set)

Host Requested Retry Suppression On A Formatter Detected Error

Error Type: Tape error (TMSCP event code FFE8)

Severity: Error

Description: The formatter detected an error on a command that had the suppress error recovery modifier set.

Action: Check the formatter.

Possible FRUs: Formatter

Host Requested Retry Suppression On A K.sti/K.si Detected Error

Error Type: Tape error (TMSCP event code FFA8)

Severity: Error

Description: An error was detected in the tape data channel on a command that had the suppress error recovery modifier set.

Action: Check the tape data channel module.

Possible FRUs: Tape data channel module

Illegal bit change in status from disk unit xxx.
EL bit forced on so status logged.

Error Type: Disk functional out-of-band (000344)

Severity: Error

Description: An unsupported bit was received in status returned from the disk unit.

Action: Check the drive and the version of software in HSC controller.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Version of software

Insufficient Control Memory for K.sti in Requestor xx

Error Type: Tape functional out-of-band (000105)

Severity: Error

Description: Not enough control memory left in the pool to allocate a control block. A certain amount of control memory is needed to set up control blocks. Enough memory was not found to set up control blocks for turning on the K.sti/K.si tape data channel module functional code.

Action: Use the HSC SETSHO utility to show available HSC memory (control, data, and program). If less than 87.5 percent of available control memory is usable, replace the memory module. Run offline TEST MEM by K diagnostic and test control memory.

Possible FRUs:

- Memory module
- I/O control processor module
- Software

Internal Consistency Error

Error Type: Controller error (MSCP/TMSCP event code 006A)

Severity: Error

Description: A high-level check detected an inconsistent data structure. For example, a reserved field contained a nonzero value, or the value in a field was outside its valid range. This error is probably caused by the requestor microcode or hardware.

Action: If the error is repetitive, check for consistent requestor numbers in detecting requestor field of error. Determine if any other surrounding error reports indicate a possible internal memory error.

Possible FRUs:

- FRU noted in the detecting requestor field
- Memory module

Invalid module configuration

Error Type: SINI out-of-band (001542)

Severity: Error

Description: You have an illegal configuration of modules in your HSC controller backplane.

Action: Refer to the Section 8.3 for OCP Fault Code 33 and verify the configuration of modules in the HSC backplane.

Possible FRUs: None applicable.

J11 cache disabled due to failure.

Error Type: SINI out-of-band (001242)

Severity: Error

Description: SINI looks back at the J11 cache diagnostic and senses the cache is disabled due to cache failure or manually disabled in the diagnostic. This error also shows as a soft fault code on the OCP.

Action: Load the offline J11 cache diagnostic and answer the prompt asking to disable or enable Cache with an enable. Reboot the system diskette and check if the original message is displayed again.

Possible FRUs:

- I/O control processor module
- Memory module

K.ci exception detected, code = nnn

Error Type: CI-detected out-of-band (000101)

Severity: Warning

Description: The code is composed of the contents of KH$FLG (the second word in the K.ci Control Area). Below is a breakdown of the bits contained in this word.

000001 KHF$PD—Path(s) disabled by K.ci due to a transmit error or VC breakage due to other K.ci-detected errors.
000002 KHF$EQ—Item(s) placed on error queue (KH$EQ).
000004 KHF$BL—Data memory error during BMB list operation.
000010 KHF$UP—Unreceivable packet. K.ci stopped (causes a crash).
000100 KHF$NH—Sequenced message received while reserved-to-receive queue was empty.
040000 KHF$PD—Set by diagnostics to disable interrupts.

Action: Compare the code from the printout to the previous list, and determine whether the error code points to an HSC controller module or to the host.

Possible FRUs:

- Status 1: Port processor module
- Status 4: Memory module
- Status 10: Port buffer module, host K.ci set
- Status 100: Host K.ci set

K.ci loopback microcode loaded

Error Type: CI-detected out-of-band (000601)

Severity: Error

Description: The CIMGR detected K.ci loopback microcode was loaded during initialization. When this message occurs, a problem with the port processor module probably exists.

Action: Replace the following FRU.

Possible FRUs: Port processor module

K.sdi in slot xx. failed init DIT, status = xxx

Error Type: Disk functional out-of-band (001104)

Severity: Error

Description: A K.sdi/K.si requestor failed during boot. The displayed disk data channel module has failed with the displayed status. This message is displayed only at the end of the boot procedure.

Action: Record the status for module repair purposes.

Possible FRUs: The disk data channel module displayed.

K.sti in Requestor xx has microcode incompatible with this TMSCP Server

Error Type: Tape functional out-of-band (000305)

Severity: Error

Description: The data structure version within the microcode version residing on the K.sti/K.si tape data channel module is a lower version than the TMSCP Server can support.

Action: Use the SET REQUESTOR command to ensure the version of microcode on the tape data channel module is up to current revision. If not, replace the microcode or replace the tape data channel module with a tape data channel module of the current revision.

Possible FRUs: Tape data channel module

Last soft init resulted from unknown cause

Error Type: SINI out-of-band (000742)

Severity: Error

Description: The software has a list of known reasons for reboot (Trap through 134, Trap through 250, IOT, SETSHO, etc.). If no reason for reboot is apparent, the software may have failed to detect the source of the error.

Action: Check the HSC console error messages and the system error logs on all the systems connected to the HSC controller.

Possible FRUs: Dependent upon the information obtained from the error logs.

LBN xx. repaired for shadow member unit xx.

Error Type: Disk functional out-of-band (001404)

Severity: Informational

Description: A shadow repair operation was done in which good data was read from one member of a shadow set and written to a bad LBN on a different shadow set member.

Action: An uncorrectable error occurred on an LBN on the subject drive and was successfully rewritten with good data. If the problem persists, check for other errors that would give information on what the uncorrectable error was.

Possible FRUs: Drive modules or media. (Refer to the drive service manual.)

LBN Restored with Forced Error in RESTOR operation
Disk Unit xx, LBN xx.
Tape Unit xx.

Error Type: Disk functional out-of-band (001144)

Severity: Warning

Description: The HSC utility BACKUP detected a hard error in the LBN and wrote the LBN with a forced error indicator. RESTOR has read this LBN and noted the forced error condition. A forced error results from a hard, unrecoverable error, and the LBN data may be suspect.

Action: Restore data from a previous backup operation. Use the VMS command ANALYZE/DISK_STRUCTURE/READ_CHECK to determine which file contains the forced error.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Less than 87.5% of Control memory is available

Error Type: SINI out-of-band (001102)

Severity: Error

Description: This message is a result of the I/O control processor polling control memory on initialization and finding an insufficient amount of working memory. This message may appear in combination with the out-of-band error messages 001142 or 001042.

Action: The error printout lists control memory as failing.

Possible FRUs: Memory module

Less than 87.5% of Data memory is available

Error Type: SINI out-of-band (001142)

Severity: Error

Description: This message is a result of the I/O control processor polling data memory on initialization and finding an insufficient amount of working memory. This message may appear in combination with the out-of-band error messages 001102 or 001042.

Action: The error printout lists data memory as failing.

Possible FRUs:

- Memory module
- M.cache module, if installed.

Less than 87.5% of Program memory is available

Error Type: SINI out-of-band (001042)

Severity: Error

Description: This message is a result of the I/O control processor polling program memory on initialization and finding an insufficient amount of working memory. This message may appear in combination with the out-of-band error messages 001102 or 001142.

Action: The error printout lists program memory as failing.

Possible FRUs: Memory module

Level 7 K interrupt (Trap thru 134)
Process xxxxxx
Status: xxx xxx xxx xxx xxx xxx xxx xxx xxx

Error Type: SINI out-of-band, subsystem exception (000502)

Severity: Error

Description: A Level 7 K interrupt occurs when any requestor detects a fatal error condition while executing functional code. The requestor, upon detecting the error, generates a Level 7 K interrupt to the I/O control processor. The I/O control processor traps through location 134, causing a reboot. The status values of each requestor, including the failing requestor, are displayed on the last line of the error printout.

Action: In some cases, the error printout shows a failing requestor when the real problem is in the memory module. This error can also be caused by software problems.

Wait for two or more failures of this type to determine if the real problem is the memory module. If the memory module is at fault, the same requestor is not displayed twice as the failing requestor. Refer to Appendix D for failing status values and their meanings. Check the status line message to determine the failing requestor status. Change the requestor exhibiting the failing status if the same requestor is displayed more than once.

Possible FRUs:

- Requestor displaying a continuous failing status value
- Memory module

Lost Read/Write Ready

Error Type: SDI or disk transfer error (MSCP event code 008B)

Severity: Error

Description: The Read/Write Ready line dropped when the controller attempted to initiate a transfer or at the completion of a transfer, and Read/Write Ready had previously been asserted. This usually results from a drive-detected transfer error, where additional error log messages containing the drive-detected error subcode may be generated.

Action: Look for surrounding drive-detected errors and/or associated disk transfer error log. Move suspect drive to another port or data channel module to help isolate failure, as this error may be caused by any of several communication components.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module

- SDI cables
- SDI transition bulkheads

Lost Receiver Ready

Error Type: Disk transfer error (MSCP event code 00CB)

Severity: Error

Description: The Receiver Ready signal was negated when the controller attempted to initiate an SDI disk transfer or did not assert at the completion of a transfer. This includes all cases of the controller's timeout expiring for a transfer operation (Level 1 real-time command).

Action: Look for a probable drive error or a possible SDI cable problem. Move suspect drive to another port or data channel module to help isolate failure, as this error may be caused by any of several communication components.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module
- SDI cables
- SDI transition bulkheads

Lower Processor Error

Error Type: Tape error (TMSCP event code FF6A)

Severity: Error

Description: A bit was set in the lower processor error register. Bits included in the lower processor error register are data bus NXM, data SERDES overrun, data bus overrun, data bus parity error, data pulse missing, and sync real-time parity error.

Action: Check the tape data channel module and the tape formatter.

Possible FRUs:

- Tape data channel module
- Tape formatter

Lower Processor timeout

Error Type: Tape error (TMSCP event code FE8A)

Severity: Error

Description: The upper processor in the tape data channel module detected the lower processor had stopped and restarted it.

Action: Check the tape data channel module and tape formatter.

Possible FRUs:

- Tape data channel module
- Tape formatter

M.cache Comparator Error

Error Type: SINI out-of-band (001402)

Severity: Error

Description: Automatic diagnostics found a data compare error.

Action: Replace the M.cache module.

Possible FRUs: M.cache module

M.cache Disabled Due to Excessive Errors.

Error Type: SINI out-of-band (001502)

Severity: Error

Description: The M.cache module was disabled due to an excessive amount of single bit or double bit errors.

Action: Replace the M.cache module.

Possible FRUs: M.cache module

M.cache Single Bit ECC Error.

Error Type: SINI out-of-band (001442)

Severity: Error

Description: The number of correctable ECC M.cache module errors exceeded an internal threshold.

Action: HSC software maps around small areas of bad memory. Replace the M.cache module if the errors persist or a message is displayed saying that 25% to 50% of memory has been disabled.

Possible FRUs: M.cache module

M.cache Multiple Bit ECC Error.

Error Type: SINI out-of-band (001342)

Severity: Error

Description: An M.cache module double bit uncorrectable ECC error occurred.

Action: If problem persists, replace the M.cache module.

Possible FRUs: M.cache module

MMU (Trap thru 250)

Error Type: SINI out-of-band, subsystem exception (000542)

Severity: Error

Description: A failure was detected in the memory management unit (MMU) on the I/O control processor. The active process is displayed for this error message, as well as the bit assignments for the memory management status registers, the program counter (PC), and the processor status word (PSW).

Action: Examine the MMSR registers to determine the failure in the MMU.

Possible FRUs:

- I/O control processor module
- Software error

nnn Symbol ECC Error

Error Type: Disk transfer error (see MSCP event code below)

Severity: Error

Description: If a drive has more symbols in error than a drive-defined threshold, the HSC controller will print one of the following error messages, even though the error might have been corrected.

One Symbol ECC Error (MSCP event code 0108)
Two Symbol ECC Error (MSCP event code 0128)
Three Symbol ECC Error (MSCP event code 0148)
Four Symbol ECC Error (MSCP event code 0168)
Five Symbol ECC Error (MSCP event code 0188)
Six Symbol ECC Error (MSCP event code 01A8)
Seven Symbol ECC Error (MSCP event code 01C8)
Eight Symbol ECC Error (MSCP event code 01E8)

The following description covers all of the correctable ECC error types that are printed.

ECC errors occur when the data read from the disk does not agree with the data written. When data is written to the disk, an ECC is calculated (by the R-S GEN) and appended to the end of the sector. When the data is subsequently read from the sector, the ECC is revalidated. This message is printed when the data error falls within the ECC error correction capability (less than nine 10-bit symbols in error), and data correction is performed. In this case, depending on the drive type, no data errors are shown.

Action: Although an occasional correctable ECC error is not a serious problem, a large number of correctable or uncorrectable ECC errors can indicate a drive media problem or a failure in the drive read path. Further analysis of the block in error, such as location of block on the disk, should be performed if possible.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module

No control block available to satisfy HMB request.

Error Type: CI-detected out-of-band (000541)

Severity: Warning

Description: The CIMGR tried to allocate an host memory block (HMB) from the free control block queue when none were available. If a significant amount of control memory was removed from use due to errors detected during boot, this message occurs. Otherwise, it may indicate an internal HSC software problem where control blocks in HSC memory are taken by some service and never returned to the list of free control blocks.

Action: Enter the SHOW MEMORY command to determine how much control memory is being used. Compare the amount of control memory shown on the SHOW MEMORY printout to the amount contained in the HSC controller. If more than 12.5% has been disabled from use, replace the memory module.

Possible FRUs:

- Memory module
- Software

No Tape Drive Structures available for Requestor xx Port xx.
Unit xx.
Increase structures via SET MAX_TAPES cmd

Error Type: Tape functional out-of-band (000645)

Severity: Error

Description: An additional tape drive has been added to an existing tape formatter, but the tape structures set up in initialization have been exceeded.

Action: Use the SETSHO utility to increase to the number of tape structures with the SET MAX_TAPES command.

Possible FRUs: None

No Tape Formatter Structures available for Requestor xx Port xx
Increase structures via SET MAX_FORMATTERS cmd

Error Type: Tape functional out-of-band (000605)

Severity: Error

Description: An additional tape formatter above the max formatter limit has been added to the HSC. Since tape formatter structures are set up during initialization, not enough structure space was reserved for this additional tape formatter.

Action: Use the SETSHO utility to set the structure level higher to compensate for the additional tape formatter with the SET MAX_FORMATTERS command.

Possible FRUs: None

No usable K.sti boards were found by the TMSCP Server

Error Type: Tape functional out-of-band (000145)

Severity: Error

Description: The TMSCP server polled the HSC controller and found no working K.sti/K.si tape data channel modules. This message does not appear frequently because the TMSCP server software is not usually loaded if there are no tape data channel modules.

Action: Check for a failed initialization diagnostic error message prior to this message. This prior message displays the failed requestor slot and failing status.

Possible FRUs: The tape data channel module displaying the failing status.

Node nn Cables have gone from crossed to uncrossed

Error Type: CI-detected out-of-band (000701)

Severity: Error

Description: This message occurs only when check for a crossed path finds a previously crossed path no longer crossed. More detail is covered in the description of the error message "Node nn Cables have gone from uncrossed to crossed."

Action: Note, if both the "uncrossed to crossed" and "crossed to uncrossed" messages are occurring, it is probably an indication of failing hardware, not a cable problem. See the Action

in the next message for more detail.

Possible FRUs:

- CI cables, if a single message is displayed
- K.ci module set, if both messages are displayed

Node nn cables have gone from uncrossed to crossed

Error Type: CI-detected out-of-band (000641)

Severity: Warning

Description: This message occurs when an IDRSP (ID response) packet is received by an HSC controller in response to an IDREQ (ID request) message. Upon receiving an IDRSP packet, the HSC controller checks two bits in the IDRSP message that indicate which path was used by the sending node. If these two bits do not indicate the same path the HSC controller received the message on, this error occurs.

Action: Determine if the problem is broken hardware in the HSC CI interface, broken hardware in the host CI interface, or if the CI cables are crossed. Before replacing any modules or cables, determine if the HSC controller is encountering crossed paths to multiple nodes in the cluster or only to a particular node. If the HSC controller is encountering crossed paths to all nodes, the problem is probably in the HSC controller or the cables. If it is encountering crossed paths to only one node, it is likely a problem with that host node's CI module set or the cables running from the host to the star coupler.

Possible FRUs:

- Cables physically connected wrong at HSC, star coupler, or host CI
- Any of the three K.ci modules in the HSC: port link, port buffer, and port processor
- CI interface hardware in the host
- Duplicate node address settings

Node xx Path (A or B) has gone from bad to good

Error Type: CI-detected out-of-band (000741)

Severity: Warning

Description: A disconnected CI cable has been reconnected, or an intermittent hardware or cable problem is indicated. More detail is found in the description of the error message "Node nn Path (A or B) has gone from good to bad."

This message also occurs if an open VC node path was previously found to be bad. During this polling cycle the node sends out ID_REQ (ID request) packets to all nodes and receives successful ID_RSP (ID response) messages.

Action: If the cable is connected, there is no further action. Otherwise, replace the possible FRUs.

Possible FRUs:

- CI cable
- Host
- CI interface hardware in the host

Node nn path (A or B) has gone from good to bad

Error Type: CI-detected out-of-band (000041)

Severity: Warning

Description: K.ci microcode detects a hard (unrecoverable) transmission error on a previously good path. Examples of hard transmission errors are:

Transmit Buffer Parity Error
Unrecoverable NACK
Unrecoverable NO_RSP
Transmitter Attention Timeout

Determining the reason for failure using the error message is not possible.

Action: Before replacing any FRU, determine if the message is occurring because of problems with one host or problems with multiple hosts. If the problem involves one host, it is probably in the star coupler's host side. If the problem involves multiple hosts, it is probably on the star coupler's HSC controller side. Also, if the message occurs on both paths to a host, that host may have been powered down, stopped, or may have crashed. Examine the host console log and the error log to determine if something did happen to the host. Note that heavy traffic on the CI can also cause the symptoms of one or more paths going bad.

Determining which error caused the bad path is not possible except with the transmit buffer parity error (XBUF PE) which prints as an MSCP-type message.

Possible FRUs:

- CI cable
- HSC/CI interface
- Host/CI interface

NXM (Trap thru 4)

Error Type: SINI out-of-band, subsystem exception (000342)

Severity: Error

Description:

a. A memory location did not respond within the specified timeout period.

b. A stack overflow occurred.

c. An odd address access was attempted, for example, a word access instead of a byte.

d. A halt was executed in User mode.

Action: Determine which memory is failing by examining the low and high error address registers for module repair.

Possible FRUs:

- Memory module
- I/O control processor module

Parameter change
Process yyy
PC xxx
PSW xxx
Reason xxx

Error Type: SINI out-of-band (000702)

Severity: Error

Description: A parameter has been changed through the SETSHO utility.

Action: None

Possible FRUs: None

Parity Error (Trap thru 114)

Error Type: SINI out-of-band, subsystem exception (000442)

Severity: Error

Description: This message covers parity errors in memory and in instruction cache. In the case of a memory parity error, the address of the failing memory is latched into the low error address register. In the case of a cache parity error, the address is not latched into the low error address register. Instead, the address of the low error address register is displayed in the error printout.

Action: Determine if the error occurred in memory or in cache memory by reading the contents of the low error address given in the error printout. If the contents is the address of the low error address register (170024), the error is in cache memory. If the error is in cache, the probable FRU is the I/O control processor module.

Possible FRUs:

- I/O control processor module
- Memory module

PLI Buffer Parity Error

Error Type: Controller error (MSCP event code 18A)

Severity: Error

Description: One of two conditions has occurred:

- When the data from the packet in a r ·ive buffer on the port buffer module was transferred to the port processor module, a parit ·ror was detected on the bus. In this case, parity is generated by the port link module . ıd checked by the port processor module. The port buffer module stores the data witho t :hecking or generating parity.
- When data was being transferred from the port processor to the port buffer transmit buffer, a parity error was detected on the bus. In this case, parity is generated by the port processor module and checked by the port link module. The port buffer module stores the data without checking or generating parity.

Action: If failure is persistent and is accompanied by K.ci Level 7 K interrupt HSC crashes, analyze K.ci module status code for more detailed information. Run Offline Test K diagnostic to test the K.ci. Any error report should more clearly indicate the specific K.ci module failure. For very intermittent failures follow the sequence of possible FRUs.

Possible FRUs:

- Port buffer module

- Port processor module
- Port link module

Position or Unintelligible Header Error

Error Type: Disk transfer error (MSCP event code 006B)

Severity: Error

Description: The drive reported a seek operation was successful by returning successful status in response to the INITIATE SEEK SDI command and asserting the Read/Write Ready signal when on the desired cylinder. However, the controller determined the drive had positioned itself to an incorrect cylinder. The header read from the drive is consistent (three out of four header copies are identical) but does not match the desired target header value. The transfer will be retried several times, and the error is considered recoverable if the data can be read successfully.

Action: The drive servo system or media is probably at fault in this case. If one is available, move the drive to a different requestor. A drive failure is indicated if the failure persists on the new requestor.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module

Positioner error on disk unit xxx. DRAT addr: xxx
Desired hdr (lo,hi):xxx, xxx
Actual hdr (lo,hi):xxx, xxx

Error Type: Disk functional out-of-band (000404)

Severity: Informational

Description: The drive positioned the heads in the wrong place or the HSC software is processing transfers out-of-order. This message is displayed only if certain debugging features are enabled, and is always accompanied by an MSCP error log.

Action: Check drive modules and the disk data channel module.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module

Premature LP flag in RTNDAT sequence from host node xx

Error Type: Disk functional out-of-band (000304)

Severity: Error

Description: A violation of packet protocol; the last packet flag was set before all data was received from a host.

Action: If the problem is transient, monitor error for repetitive node numbers as this may indicate a host CI problem. If the problem is persistent across all cluster nodes, test the K.ci.

Possible FRUs:

- K.ci modules
- CI cables

Program Memory Single Bit ECC Error.

Error Type: SINI out-of-band (001302)

Severity: Error

Description: Correctable single bit errors in program memory exceeded an internal threshold.

Action: Run M.std4 module diagnostics.

Possible FRUs: M.std4 module

Pulse or Parity Error

Error Type: Disk transfer error (MSCP event code 010B)

Severity: Error

Description: The controller detected a pulse error on either the SDI drive state or data line, or the controller detected a parity error in a drive state frame. The HSC controller does an SDI GET STATUS command, reports any errors from it, and then clears those errors, if possible. After this, the HSC controller retries the original command up to two more times before considering the error unrecoverable.

Action: If the error is reported on more than one drive, a disk data channel module problem is indicated. If the error is reported on only one drive, an SDI cable or drive problem is indicated.

Possible FRUs:

- SDI cable
- Drive modules. (Refer to the drive service manual.)
- SDI transition bulkhead
- Disk data channel module

RCT Corrupted Error

Error Type: Disk transfer error (MSCP event code 0105)

Severity: Error

Description: The RCT search algorithm encountered an invalid RCT entry. The subcode may be returned under the following conditions:

- During replacement of a block
- During nonprimary revectoring of a block
- When bringing a unit online

Action: Determine if this error is repetitive for this unit possibly indicating a defective media or drive read path failure. Run the HSC VERIFY utility on the drive.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Receiver ready not asserted at start of transfer

Error Type: Tape error (TMSCP event code FCEA)

Severity: Error

Description: The HSC controller is ready to start a transfer by sending the formatter a Level 1 command and the formatter does not have the Receiver Ready line asserted.

Action: Check the formatter, cable, and tape data channel module.

Possible FRUs:

- Formatter
- Cable
- Tape data channel module

Record EDC error

Error Type: Tape error (TMSCP event code FE2A)

Severity: Error

Description: On a read from tape operation, the EDC calculated by the tape data channel module did not match the EDC generated by the tape formatter.

Action: Check the formatter, cable, and tape data channel module.

Possible FRUs:

- Formatter
- Cable
- Tape data channel module

Requestor xx failed INIT DIT, status = xxx

Error Type: SINI out-of-band (000042)

Severity: Error

Description: The data channel module in the displayed requestor has failed initialization diagnostics with the displayed status.

Action: Determine which data channel module is in the displayed requestor slot. Make note of the status value for module repair. Replace the failing data channel module.

Possible FRUs: The disk/tape data channel module exhibiting the failing status.

Requestor xx failed INIT DIT with status = xx

Error Type: Tape functional out-of-band (000045)

Severity: Error

Description: The requestor in slot xx has failed initialization diagnostics with the displayed status. The message indicates the failed tape data channel module.

Action: Refer to Appendix C to determine what the displayed status indicates the failure to be.

Possible FRUs: The tape data channel module in the indicated slot.

Reserved instruction (Trap thru 10)
Process yyyy
PC xxx
PSW xxx

Error Type: SINI out-of-band, subsystem exception (000402)

Severity: Error

Description: The I/O control processor detected an opcode, resulting in the execution of an invalid instruction. The process indicated is the process that executed the nonexistent instruction.

Action: Determine what process was active for module repair.

Possible FRUs:

- I/O control processor module
- Memory module
- Software

Resource lost to K.ci—xxx xxx HMBs

Error Type: CI-detected out-of-band (001041)

Severity: Error

Description: A control memory host message block (HMB) data structure was lost. HMBs are expected to be returned to the sequence message ready to receive queue (.KHSRR), but the indicated number of HMBs were never returned to this queue.

Action: Report the error, with frequency of occurrence, to support. Also, note sequence of events that reproduce this failure. This message indicates a software bug. Verify dc power levels are correct.

Possible FRUs:

- Software
- Main power supply

Retry limit exceeded while attempting to restore tape position

Error Type: Tape error (TMSCP event code FF31)

Severity: Error

Description: A command was issued to restore the tape position, and the command failed in the limit of retries.

Action: Check the formatter.

Possible FRUs: Formatter

Rewind failure

Error Type: Tape error (TMSCP event code FEAB)

Severity: Error

Description: A rewind command was issued, and the command failed (the controller received an unsuccessful response from the formatter).

Action: Check the drive and/or formatter.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Formatter

SCT read or verification error. Using template SCT.

Error Type: SINI out-of-band (000102)

Severity: Error

Description: An error was detected by the I/O control processor as it attempted to read the System Configuration Table (SCT) or as it attempted to verify the SCT. This error message will occur when new, previously uninitialized system diskette is booted. The default settings from SYSCOM are used instead of the SCT from the load media. The second sentence in this message indicates the SCT is new, as derived from the template SCT settings set in the factory. If the system has been previously booted from the same media, a system load device failure is indicated.

Action: Reinstall the old system diskette and enter the SHO SYSTEM command. Install the new diskette exhibiting the error and set all system diskette fields to the old values using the SET command. Reboot the HSC controller to validate these values and ensure system continuity.

Possible FRUs: System diskette

SDI exchange retry on disk unit xxx. (Requestor xx., Port xx.)
DCB addr xx Error count xx.

Error Type: Disk functional out-of-band (000544)

Severity: Informational

Description: Indicates that an SDI exchange required a retry operation. Only reported if debug flag is set.

Action: None

Possible FRUs: None

SDI Clock Persisted after INIT

Error Type: SDI error (MSCP event code 18B)

Severity: Error

Description: The drive clock did not cease following a controller attempt to initialize the SDI drive. This implies the drive did not recognize the initialization attempt. This error condition causes the HSC controller to retry the INIT command eight more times before marking the drive inoperative.

Action: Determine if this drive has encountered any other related problems which may be entered in an appropriate error log report. Also, this error may be due to an SDI cable problem.

Closely examine error logs for surrounding disk errors, as the error may be a result of a previously-reported drive error.

Possible FRUs:

- SDI cable
- Drive modules. (Refer to the drive service manual.)

SERDES Overrun

Error Type: Disk transfer or tape controller error (MSCP event code 002A)

Severity: Error

Description: This error is either a SERDES overrun or underrun error. Either the drive is too fast for the controller, there is noise on the SDI/STI cable, or a controller hardware fault prevented controller microcode from keeping up with data transfer to or from the drive.

Action: Determine if other errors have occurred that may indicate a disk data channel module problem. Move the offending drive to another requestor. If the problem persists, test the drive further. If the drive is a TA90 tape drive, verify that it is connected to a K.si module, not to a K.sti module.

Possible FRUs:

- SDI/STI cable
- Disk/tape data channel module
- Drive interface hardware

Shadow copy timeout detected copying cylinder x, group y.
Shadow unit z.

Error Type: Disk functional out-of-band (001704)

Severity: Error

Description: The HSC controller has detected several successive timeouts on a subset of a shadow copy operation. A timeout occurs when the HSC controller does not read a group of data from the source unit and write that same data to the target unit within an expected time period. This can occur due to extensive error recovery on either the source or target unit. This message will repeat every subsequent timeout period until the shadow copy of the group completes.

Action: Check both the source and target units of the shadow set for a large number of errors on any surface of the disk. A large number of errors on a surface of a disk, coupled with a large number of non-primary revectors, may indicate a need to replace the HDA on that drive.

Possible FRUs: Disk drive modules. (Refer to the disk drive service manual.)

SI Clock Resumption Failed after INIT

Error Type: SDI error (MSCP event code 016B)

Severity: Error

Description: The drive clock did not resume following a controller attempt to initialize the SDI drive. This implies the drive encountered a fatal initialization error. Closely examine error

logs for surrounding disk errors, as this error may be the result of a previously-reported drive error.

Action: Determine if this drive has encountered any other related problems which may be found in an appropriate error log report. Also, this error may be due to an SDI cable problem.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- SDI cable

SI Command Timeout

Error Type: SDI error (MSCP event code 002B)

Severity: Error

Description: The controller timeout expired for either a Level 2 exchange or the assertion of the Read/Write Ready signal after an INITIATE SEEK command. The HSC controller retries the command three more times, reinitializing the SDI drive each time. If the error persists on a single SDI Level 2 exchange, the drive is marked inoperative.

Action: Determine if this drive has encountered any other related problems which may be found in an appropriate error log report. Also, this error may be due to an SDI cable problem. Closely examine error logs for surrounding disk errors, as the error may be a result of a previously-reported drive error. The RA60 disk drive is especially prone to this error.

Ensure the drive and all HSC controller modules are at the latest revision levels.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- SDI cable

SI Receiver Ready Collision

Error Type: SDI error (MSCP event code 01AB)

Severity: Error

Description: This error occurs when the drive or controller fails to follow the SDI protocol during SDI command/reception, or more likely, the drive and controller are no longer in sync with their communications. For example, the controller sends the drive a command, asserts Controller Receiver Ready, and waits for the SDI response. The following lists the possible drive operations that lead to this error:

- The drive fails to deassert the Drive Receiver Ready signal. In this case, the drive indicates it did not receive the command.
- The drive deasserts Drive Receiver Ready and then reasserts it before sending a proper SDI response. In this case, the drive believes it has sent a response and is indicating so by reasserting Drive Receiver Ready, yet the controller has never received the response.

The disk data channel module detects this error. The HSC functional code does an SDI GET STATUS command and clears the drive of any errors found. The original command is then retried. This cycle is repeated twice before the drive is initialized by the HSC, and the entire operation is done two more times. If the failure persists, the drive is marked inoperative.

Action: Determine if this drive has encountered any other related problems which may be found in an appropriate error log report. Also, this error may be due to an SDI cable or SDI

transceiver/encoder/decoder problem. Closely examine error logs for surrounding disk errors, as this error may be the result of a previously-reported drive error.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- SDI cable
- Disk data channel module

SI Response Length or Opcode Error

Error Type: SDI error (MSCP event code 014B)

Severity: Error

Description: A Level 2 response from the drive had correct framing codes and checksum, but was not a valid response within the constraints of the SDI protocol. The response had an invalid opcode, was an invalid length, or was not a possible response in the context of the exchange.

Because the SDI and STI opcodes are different this problem frequently occurs if a disk device is attached to a tape requestor, or if a tape device is attached to a disk requestor.

The disk data channel module detects this error. The HSC functional code does an SDI GET STATUS command and clears the drive of any errors found. The original command is then retried. This cycle is repeated twice before the drive is initialized by the HSC, and the entire operation is done two more times. If the failure persists, the drive is marked inoperative.

Action: Check the configuration to make sure disk and tape drives are attached to appropriate data channels. Determine if the drive has experienced other similar errors. Closely examine error logs for surrounding disk errors, as this error may be the result of a previously-reported drive error.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module

SI Response Overflow

Error Type: SDI error (MSCP event code 01CB)

Severity: Error

Description: A drive sent back more frames than the reception buffer could hold. This can be caused by a hung drive microdiagnostic or a malfunctioning disk data channel module.

Action: Determine if the drive is failing in other ways, indicating a drive problem. If not, the disk data channel module may be the more likely cause.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Disk data channel module

Software Inconsistency
Process xxx
PC yyy
PSW zzz
Stack dump: xxx xxx xxx

Error Type: SINI out-of-band, subsystem exception (000602)

Severity: Error

Description: During operation, the operating software performs numerous consistency checks. When one of these consistency checks fails, the HSC controller crashes and reboots. The active process at the time of the crash, as well as the stack dump, is displayed.

Action: Contact the Customer Support Center, or refer to Appendix B and file a Software Problem Report (SPR).

Possible FRUs: None

Tape drive requested error log

Error Type: Tape error (TMSCP event code FF6B)

Severity: Warning

Description: The drive detected an error condition and set the EL bit for an error log to be taken.

Action: Check the drive.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Tape Formatter connected to Requestor xx Port xx.
Has been declared inoperative.
Intervention required

Error Type: Tape functional out-of-band (000705)

Severity: Error

Description: The tape data channel module has sent a retryable dialog command over the STI cable to the displayed tape formatter four times and has received back the same error each time. The HSC controller then declares the formatter inoperative and removes it from its tables. A change in the state clock will bring the formatter operative again.

Action: Replace the possible FRUs. Deasserting the tape drive's port switches, recycling power, unplugging the STI cable, or any action causing the state clock to come and go will bring the formatter back. The HSC controller will not attempt to communicate with the failing tape formatter until it detects this change in state clock. Examine any previous error reports for more specific information regarding this error message.

Possible FRUs:

- Tape formatter
- STI cabling
- Tape data channel module

Tape unit number xx connected to Requestor xx Port xx Ceased to exist while Online

Error Type: Tape functional out-of-band (000545)

Severity: Error

Description: A drive that was previously online to the formatter is no longer known.

Action: Check to see if a breaker has blown. The tape drive may be in testing mode also, causing the tape drive to go away or become unknown.

Possible FRUs:

- STI cable
- Tape drive
- Tape formatter

Tape unit number xx connected to Requestor xx Port xx Dropped state clock while Online

Error Type: Tape functional out-of-band (000345)

Severity: Error

Description: The formatter supplies the state clock over the STI cable. The state bits are encoded on this state clock waveform such as AVAILABLE and ATTENTION. Dropping the state clock can occur when the STI cable is disconnected, the port buttons are popped, or if the formatter is not operating properly.

Action: First isolate the problem to the HSC controller, STI cable, or tape drive. Next, try replacing or swapping the tape data channel module exhibiting the failure. If the problem is not solved, try a known, good tape drive.

Possible FRUs:

- STI cable
- Tape drive
- Tape data channel module

Tape unit number xx connected to Requestor xx Port xx is not asserting Available when it should be

Error Type: Tape functional out-of-band (000445)

Severity: Error

Description: The formatter is not asserting its Available signal to the HSC controller.

Action: First isolate the problem to either the HSC controller, the STI cable, or the tape drive. Next, try replacing or swapping the tape data channel module exhibiting the failure. If the problem is not solved, try a known, good tape drive.

Possible FRUs:

- STI cable
- Tape drive
- Tape data channel module

Tape unit number xx connected to Requestor xx Port xx Went Available without request

Error Type: Tape functional out-of-band (000405)

Severity: Error

Description: An available signal was received from a formatter that is online to the HSC controller. This formatter should be asserting online.

Action: First isolate the error to the formatter or to the active tape data channel module.

Possible FRUs:

- Tape data channel module
- Formatter
- STI cable

Tape unit number xx connected to Requestor xx Port xx Went Offline without request

Error Type: Tape functional out-of-band (000505)

Severity: Error

Description: The formatter lost contact with an online tape drive.

Action: Check to see if a breaker has blown. The tape drive may be in diagnostic mode also, causing the tape drive go offline.

Possible FRUs:

- Tape drive
- Tape formatter
- STI cable

TMSCP fatal initialization error—TMSCP functionality not available

Error Type: Tape functional out-of-band (000745)

Severity: Error

Description: Something went wrong during initialization with the tape functional code (TFUNCT). A routine was called to initialize some part of the functional code, and that part failed to initialize. Typically, some other message is displayed prior to this message giving more detail on the error.

Action: Take action depending on the previously displayed message.

Possible FRUs: Dependent on the previously-displayed error message

TOPOLOGY command failed

Error Type: Tape error (TMSCP event code FF0C)

Severity: Error

Description: A TOPOLOGY command was issued and the command failed.

Action: Check the formatter.

Possible FRUs: Formatter

TTRASH fatal initialization error

Error Type: Tape functional out-of-band (001005)

Severity: Error

Description: This message is similar to the message "TMSCP fatal initialization error—TMSCP functionality not available" except the process failing to initialize is TTRASH instead of the tape functional process (TFUNCT).

Action: Check for previous error reports displaying a more specific reason for this error report. If earlier error messages do not exist, reboot the HSC controller using backup HSC software copy.

Possible FRUs:

- Memory module
- Software

Unable to position before LEOT

Error Type: Tape error (TMSCP event code FE8B)

Severity: Error

Description: The position tape command completed before LEOT was detected.

Action: Check the drive.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Unable to read Program Memory Error Counter.

Error Type: SINI out-of-band (001602)

Severity: Error

Description: The memory error counter register is shared with the RX33 disk drive and cannot be read if the RX33 disk drive is active. This error is a timeout waiting for the RX33 disk drive to become inactive.

Action: Check to see if there is RX33 disk drive activity. This is a long period timeout and should not be seen under normal conditions.

Possible FRUs:

- Memory module
- RX33 disk drive

Unclearable Drive Error

Error Type: Tape error (TMSCP event code FFEB)

Severity: Error

Description: The HSC tape server issued a clear drive error command that failed.

Action: Check the formatter and drive. Further analysis of tape drive error log may be necessary.

Possible FRUs:

- Drive modules. (Refer to the drive service manual.)
- Formatter

- STI cable set
- Tape data channel module

Unclearable Formatter Error

Error Type: Tape error (TMSCP event code FFCC)

Severity: Error

Description: The HSC tape server issued a clear formatter error command that failed.

Action: Check the formatter

Possible FRUs:

- Formatter
- STI cable set
- Tape data channel module

Uncorrectable ECC Error

Error Type: Disk transfer error (MSCP event code 00E8)

Severity: Error

Description: ECC errors occur when the data read from the disk does not agree with the data written. When data is written to the disk, an ECC is calculated (by the R-S GEN) and appended to the end of the sector. When the data is subsequently read from the sector, the ECC is revalidated. This message occurs when the data error does not fall within the error correction capability of the ECC, and the error is retried according to drive dependent parameters. If all of the retries fail, an uncorrectable ECC error occurred, and a bad block is reported through an end packet.

NOTE
An uncorrectable ECC error is reported when a transfer with the Suppress Error Correction modifier encounters an ECC error of any severity.

Action: A large number of correctable or uncorrectable ECC errors can indicate a drive media problem or a failure in the drive read path. Further investigation of these errors, such as the location of the LBN in error on the disk, should be attempted.

Possible FRUs:

- Drive modules (refer to drive service manual)
- Disk data channel module

Unexpected AVAILABLE signal from ONLINE disk unit xx.

Error Type: Disk functional out-of-band (001044)

Severity: Error

Description: The disk is asserting AVAILABLE while the drive state is online. This is not an expected condition. This can occur if the HSC disk server is in a state where it is not responding to a drive attention condition. This error occasionally happens with RA60 disk drives.

Action: Determine why the disk drive is asserting the Available signal.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Unit xx. declared inoperative because no progress made on Command Reference xxxxx.

Error Type: Disk functional out-of-band (001444)

Severity: Error

Description: The HSC disk server has made no progress on the host command represented by the given reference number in an extended time period. This scenario can occur if the drive is degraded to a point where the disk path spends too much time in error recovery and can make no progress on the host command.

Action: The HSC controller was unable to complete error recovery on the drive and took it offline. Check the drive with diagnostics to determine the nature of the problem.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Unknown K.tape error

Error Type: Tape error (TMSCP event code F3AA)

Severity: Error

Description: The ER bit was set but was undefined.

Action: Check the formatter.

Possible FRUs: Formatter

Unrecoverable error on disk unit xx. Drive appears inoperative. Intervention required.

Error Type: Disk functional out-of-band (000204)

Severity: Error

Description: The HSC disk server has concluded that the drive is broken based on various detected errors with the drive. Any pending I/O is cleaned up and the drive is placed in the undefined state. The HSC controller will eventually reenable interrupts for this drive and allow it to transition back into the available state after all pending I/O is cleared up, and ILDISK has been run on the drive.

Action: Check the error log and drive.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

Unsuccessful SEEK initiation, disk unit xxx. DCB addr: xxx

Error Type: Disk functional out-of-band (000444)

Severity: Informational

Description: The HSC controller created a dialog control block to send a SEEK exchange to a drive, and the DCB was sent to its error queue by the disk data channel module. The SEEK may have been rejected, lost, or completed with an error. This message is only printed if a special debug flag is enabled.

Action: Check drive.

Possible FRUs: Drive modules. (Refer to the drive service manual.)

VC closed with node nn due to spinlock timeout

Error Type: CI-detected out-of-band (00441)

Severity: Warning

Description: The VC closure is generated by the CI manager (CIMGR) if an SCS request or response cannot be serviced within 100 seconds because some resource (notable the CB semaphore) was not available.

Action: An occasional occurrence is of no consequence. However, if condition occurs frequently, it may be caused by high load on the HSC or CI.

Possible FRUs: K.ci module set

VC closed with node nn due to disabled remote port

Error Type: CI-detected out-of-band (001141)

Severity: Warning

Description: When polling, the CI manager (CIMGR) closes a virtual circuit if it detects that the remote port is disabled. This condition typically occurs when a host is shut down.

Action: None. This condition is encountered during normal operation.

Possible FRUs: None.

VC closed with node nn due to invalid SCS op code

Error Type: CI-detected out-of-band (001201)

Severity: Warning

Description: The CI.REC routine in the CI manager (CIMGR) received an invalid SCS message. The CIMGR responds to an invalid message by breaking the virtual circuit to the offending node.

Action: If this message persists, check the remote node CI adaptor.

Possible FRUs:

- Remote node CI adaptor
- HSC K.ci module set

VC closed with node nn to test VC closure response

Error Type: CI-detected out-of-band (001241)

Severity: Warning

Description: This message occurs only when the OLMON utility routine is used to test for correct performance of the HSC under repeated virtual circuit closures.

Action: None. The OLMON utility is only used for internal testing.

Possible FRUs: None.

VC closed due to timeout of RTNDAT/CNF from host node xx

Error Type: Disk functional out-of-band (000744)

Severity: Error

Description: The HSC controller has sent data to the host and has timed out waiting for the host to return a confirm (CMF).

Action: Determine if the problem lies in the HSC K.ci module set or the host CI module. Check that the host was not crashed or stopped, and check for VC closures prior to the error.

Possible FRUs:

- K.ci module set in the HSC controller
- CI module set in the host

VC closed with node nn due to disconnect timeout

Error Type: CI-detected out-of-band (000341)

Severity: Warning

Description: A second disconnect call for the same connection block has been received by the CI manager.

Action: Verify other cluster nodes have not failed or have CI port problems. If the problem persists, run offline test K diagnostic to test the K.ci. If no failures exist, verify that the HSC SETSHO SET parameters are valid, use backup copy of the HSC software code, and replace the FRUs indicated.

Possible FRUs: Host K.ci module set

VC closed with node nn due to request from K.ci

Error Type: CI-detected out-of-band (000301)

Severity: Warning

Description: The K.ci microcode has reported that both CI paths have gone from good to bad during polling. More details are found under the description for error message "Node nn path n has gone from good to bad". Heavy CI traffic can cause both CI paths to be reported as bad.

Action: Set error and outband to info. See the descriptions and action for the following error messages:

Node nn path (A or B) has gone from bad to good
Node nn path (A or B) has gone from good to bad

Possible FRUs:

- K.ci hardware interface in HSC controller
- CI cables
- Host CI hardware

VC closed with node nn due to START received

Error Type: CI-detected out-of-band (000241)

Severity: Warning

Description: A start message is received over the CI to an already open virtual circuit (VC). This condition can occur when a host is being shut down, in which case it is a normal occurrence.

Action: If not due to host shutdown, check for two HSC controllers with the same ID (not node address) on the cluster. This happens when a new HSC controller is installed on the cluster and is given an existing ID.

Possible FRUs: CI cables

VC closed with node nn due to unexpected disconnect

Error Type: CI-detected out-of-band (000402)

Severity: Warning

Description: The HSC controller receives a DISCONNECT_REQ packet, and the following conditions exist inside the HSC controller.

- A connection is not open.
- The HSC controller is not in the disconnect_sent state. (The disconnect_sent state indicates the HSC controller also sent a disconnect_req packet.)

Action: Verify no other nodes in the cluster failed and caused sending an unexpected disconnect to the HSC controller. If failure persists, the K.ci module set may be causing this error. Run offline Test K diagnostic to test the K.ci. If no failure, verify no duplicate node addresses exist in this cluster with the port link module node address switches.

Possible FRUs: Port processor module

VC open with node nn

Error Type: CI-detected out-of-band (000501)

Severity: Informational

Description: A virtual circuit (VC) has been established with the given node. The Online indicator on the HSC OCP lights the first time a VC is established to an HSC controller.

Action: None is required; this message is for informational purposes only.

Possible FRUs: None

*****WARNING*** K.sti ucode too low for large transfers.**

Error Type: Tape functional out-of-band (001105)

Severity: Warning

Description: The K.sti module contains a down rev version of microcode. The amount of I/O the tape data channel module can accommodate is restricted. The code still attempts to do transfers, but a warning has been issued.

Action: Update the microcode version level to the proper revision.

Possible FRUs: Change the level of tape data channel module microcode to a supported version, or change the tape data channel module with the out-of-date code.

Word rate clock timeout

Error Type: Tape error (TMSCP event code FCAA)

Severity: Error

Description: The tape data channel module detected the loss of clocks from a drive during a transfer.

Action: Check the formatter and the cable.

Possible FRUs:

- Formatter
- Cable


APPENDIX A

A
Internal Cabling Diagrams

A.1 Introduction

This appendix contains diagrams of the internal cabling for the HSC, HSC50 (modified), and HSC50.

A.2 HSC Internal Cabling

Figure A–1 is a diagram of the HSC internal cabling.

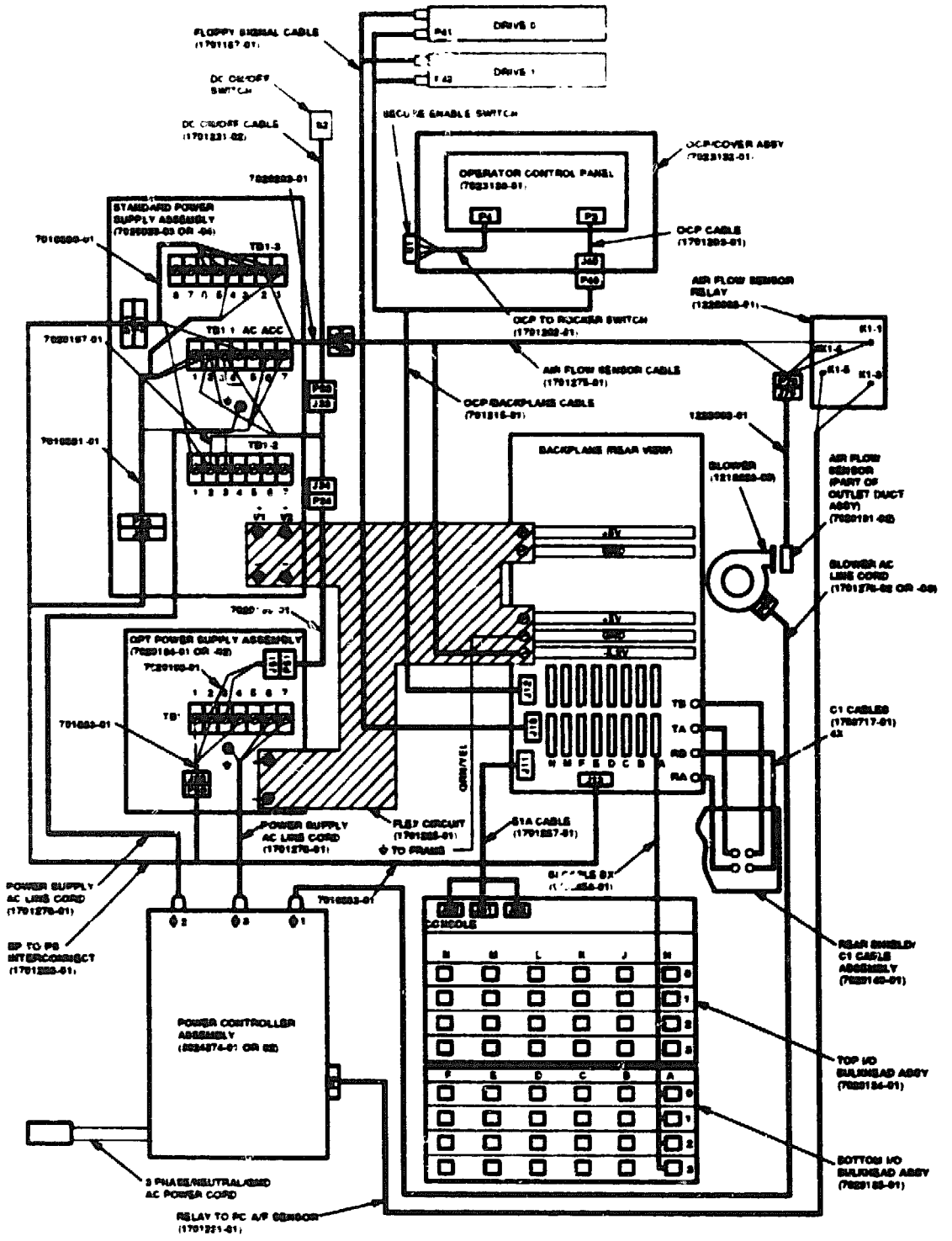


Figure A–1 (Cont.) HSC Internal Cabling

WIRE TABLE FOR 1701202-01 OCP TO ROCKER SWITCH				
COLOR	FROM	TO	SIGNAL	REMARKS
	P4-01		NO CONNECTION	KEYING PLUG
	P4-02		NO CONNECTION	
RED	P4-03	S1-3	+5 VOLT	
BLACK	P4-04	S1-6	GND (-5 VOLT)	
	P4-05		NO CONNECTION	SPARE
YELLOW	P4-06	S1-4	GND	
YELLOW	P4-07	S1-5	TERM ENABLE	
	P4-08		NO CONNECTION	SPARE
WHITE	P4-09	S1-1	INIT SWL	
WHITE	P4-10	S1-2	INIT L	

WIRE TABLE FOR 1701203-01 OCP CABLE				
COLOR	FROM	TO	OCP SIGNAL	REMARKS
YELLOW	J40-1	P3-1	STATE LAMP L	
YEL/ORG	J40-2	P3-2	POWER LAMP L	
YEL/BLU	J40-3	P3-4	LAMP ENA 0 L	
YEL/GRN	J40-4	P3-3	TERM ENA L	
YEL/BLK	J40-5	P3-6	LAMP ENA 2 L	
YEL/VIO	J40-6	P3-5	LAMP ENA 1 L	
YEL/GRY	J40-7	P3-8	LAMP ENA 4 L	
YEL/WHT	J40-8	P3-7	LAMP ENA 3 L	
YEL/RED	J40-9	P3-10	PANEL SWITCH 1 L	
YEL/BRN	J40-10	P3-9	PANEL SWITCH 0 L	
YEL/BLK/GRY	J40-11	P3-12	PANEL SWITCH 3 L	
YEL/GRN/ORG	J40-12	P3-11	PANEL SWITCH 2 L	
YEL/RED/WHT	J40-13	P3-15	BDCOKH (INIT L)	
BLACK	J40-14	P3-14	GND	
RED	J40-15	P3-16	+5V	
		P3-20		KEYING PLUG (OCP)

WIRE TABLE FOR 1701215-01 OCP/BACKPLANE				
COLOR	FROM	TO	OCP SIGNAL	REMARKS
YELLOW	J12-1	P40-01	STATE LAMP L	
YELLOW/ORG	J12-2	P40-02	POWER LAMP L	
YELLOW/BLUE	J12-3	P40-03	LAMP ENA 0 L	
YELLOW/GRN	J12-4	P40-04	TERM ENA L	
YELLOW/BLACK	J12-5	P40-05	LAMP ENA 2 L	
YELLOW/VIOLET	J12-6	P40-06	LAMP ENA 1 L	
YELLOW/GRAY	J12-7	P40-07	LAMP ENA 4 L	
YELLOW/WHITE	J12-8	P40-08	LAMP ENA 3 L	
YELLOW/RED	J12-9	P40-09	PANEL SWITCH 1 L	
YELLOW/BRN	J12-10	P40-10	PANEL SWITCH 0 L	
YEL/BLK/GRY	J12-11	P40-11	PANEL SWITCH 3 L	
YEL/GRN/ORG	J12-12	P40-12	PANEL SWITCH 2 L	
YEL/RED/WHT	J12-13	P40-13	BDCOK H (INIT L)	
BLACK	J12-14	P40-14	GND	
RED	J12-16	P40-15	+5 VOLTS	
RED	J12-19	P41-04	+5 VOLTS	
RED	J12-20	P42-04	+5 VOLTS	
BLACK	J12-21	P41-02	GND	
BLACK	J12-22	P41-03	GND	
BLACK	J12-23	P42-02	GND	
BLACK	J12-24	P42-03	GND	
VIOLET	J12-25	P41-01	+12 VOLTS	
VIOLET	J12-26	P42-01	+12 VOLTS	

CXO-944B
Sheet 2 of 5

Figure A–1 (Cont.) HSC Internal Cabling

WIRE TABLE FOR 1701231-01 RELAY TO PC A/F SENSOR				
COLOR	FROM	TO	SIGNAL	REMARKS
WHITE	K1-3	P8-1	TRIP	
WHITE	K1-5	P8-2	RETURN	

WIRE TABLE FOR 1701231-02 DC ON/OFF				
COLOR	FROM	TO	SIGNAL	REMARKS
YELLOW	S2-2	P33-4	ON/OFF (-5.2V)	
ORANGE	S2-1	P33-3	S2-	
BLUE	S2-4	P33-2	ON/OFF (+5.2V)	
BLACK	S2-3	P33-1	S1-	

WIRE TABLE FOR 1701266-01 BP TO PS					
COLOR	FROM	TO	SIGNAL	REMARKS	
VIOLET	J13-1	P31-1	+12V		STANDARD POWER SUPPLY
VIOLET	J13-2	P31-3	+12V		
VIOLET	J13-3	P31-5	+12V		
VIOLET	J13-4	P31-7	+12V		
BLACK	J13-5	P31-9	GND (+12V)		
BLACK	J13-6	P31-2	GND (+12V)		
BLACK	J13-7	P31-4	GND (+12V)	DOUBLE CRIMPED	
BLACK	J13-8		GND (+12V)		
ORANGE	J13-9	P31-6	-5.2V SENSE	TWISTED PAIR	
BLACK	J13-10	P31-8	GND (-5V SENSE)		
BROWN	J13-11	P31-10	POWER FAIL L		
BLACK	J13-14	J32-1	GND (+5V SENSE)	TWISTED PAIR	
RED	J13-13	J32-2	+5V SENSE		
BLACK	J13-16	J32-3	GND (+12V SENSE)	TWISTED PAIR	
VIOLET	J13-15	J32-4	+12V SENSE		
BLACK	J13-17	P50-2	GND (+5V SENSE)	TWISTED PAIR	OPTIONAL POWER SUPPLY
RED	J13-18	P50-1	+5V SENSE		
BROWN	J13-20	P50-3	POWER FAIL L		

WIRE TABLE FOR 1701267-01 EIA				
COLOR	FROM	TO	BACKPLANE SIGNAL	REMARKS
WHITE	J11-1	J60-20	HSC RDY+	
WHITE/BLK	J11-2	J60-6	TERM PRES L	
WHITE/BLU	J11-3	J60-1	TERM XMT-	
WHITE/ORG	J11-4	J60-2	TERM XMT+	
WHITE/RED	J11-5	J60-3	TERM RCV+	
WHITE/VIO	J11-6	J60-7	TERM RCV-	
WHITE	J11-9	J61-20	HSC RDY+	
WHITE/BLK	J11-10	J61-6	AUX1 PRES L	
WHITE/BLU	J11-11	J61-1	AUX1 XMT-	
WHITE/ORG	J11-12	J61-2	AUX1 XMT+	
WHITE/RED	J11-13	J61-3	AUX1 RCV+	
WHITE/VIO	J11-14	J61-7	AUX1 RCV-	
WHITE	J11-17	J62-20	HSC RDY+	
WHITE/BLK	J11-18	J62-6	AUX2 PRES L	
WHITE/BLU	J11-19	J62-1	AUX2 XMT-	
WHITE/ORG	J11-20	J62-2	AUX2 XMT+	
WHITE/RED	J11-21	J62-3	AUX2 RCV+	
WHITE/VIO	J11-22	J62-7	AUX2 RCV-	

CXO-944B
Sheet 3 of 5

Figure A–1 (Cont.) HSC Internal Cabling

WIRE TABLE FOR 1226092-01 A/F SENSOR				
COLOR	FROM	TO	SIGNAL	REMARKS
RED	A1-+	J70-1		
BLACK	A1-GND	J70-3		
WHITE	A1-LOAD	J70-2		

WIRE TABLE FOR 1701275-01 A/F SENSOR CABLE				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	P70-1	K1-1	+5V	DOUBLE CRIMP
VIOLET	P35			
ORANGE	P70-2	K106	LOAD (-5V)	
ORANGE	P70-3	-5.2V BUSBAR 0 BACKPLANE	-5.2V	

WIRE TABLE FOR 1701276-01 STD POWER SUPPLY				
COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	ϕ2 *	GND	*POWER CONTROLLER ϕ2
BLUE	TB1-1-7	ϕ2 *	ACC	
BROWN	TB1-1-6	ϕ2 *	AC	

WIRE TABLE FOR 1701276-01 OPT POWER SUPPLY				
COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	ϕ3 *	GND	*POWER CONTROLLER ϕ3
BLUE	TB1-1-7	ϕ3 *	ACC	
BROWN	TB1-1-6	ϕ3 *	AC	

WIRE TABLE FOR 1701276-02 BLOWER AC LINE CORD				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	IN MOLDED PLUG	P80-1	AC	NEUTRAL
BROWN		P80-2	AC	LINE
GREEN		P80-3	GND	
BLACK	P80-5	P80-4		JUMPER

WIRE TABLE FOR 1701276-03 BLOWER AC LINE CORD				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	IN MOLDED PLUG	P80-1	AC	NEUTRAL
BROWN		P80-2	AC	LINE
GREEN		P80-3	GND	
BLACK	P80-7	P80-4		JUMPER
BLACK	P80-8	P80-5		JUMPER

WIRE TABLE FOR 7019680-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J31-1	TB1-3-5	+12V	DOUBLE CRIMP
VIOLET	J31-3			
VIOLET	J31-5	TB1-3-6	+12V	DOUBLE CRIMP
VIOLET	J31-7			
BLACK	J31-9	TB1-3-3	GND (+12V)	DOUBLE CRIMP
BLACK	J31-2			
BLACK	J31-4	TB1-3-3	GND (+12V)	
ORANGE	J31-6	TB1-2-2	+5V SENSE	TWISTED PAIR
BLACK	J31-8	TB1-2-1	GND (-5V SENSE)	
BROWN	J31-10	TB1-1-4	POWER FAIL	

CXO-944B
Sheet 4 of 5

Figure A–1 (Cont.) HSC Internal Cabling

WIRE TABLE FOR 7019681-01				
COLOR	FROM	TO	SIGNAL	REMARKS
BLACK	P32-1	TB1-1-2	GROUND	TWISTED PAIR
RED	P32-2	TB1-1-1	+5V SENSE	
BLACK	P32-3	TB1-3-4	GROUND	TWISTED PAIR
VIOLET	P32-4	TB1-3-1	+12V SENSE	

WIRE TABLE FOR 7019683-01				
COLOR	FROM	TO	SIGNAL	REMARKS
RED	J50-1	TB1-1	+5V SENSE	TWISTED PAIR
BLACK	J50-2	TB1-2	GND (+5V SENSE)	
BROWN	J50-3	TB1-3	POWER FAIL	

WIRE TABLE FOR 7020197-01				
COLOR	FROM	TO	SIGNAL	REMARKS
YELLOW	J33-4	TB1-2-3	ON/OFF (-5.3V)	
ORANGE	J33-3	TB1-2-2	S2-	
BLUE	J33-2	TB1-1-3	ON/OFF (+5V)	DOUBLE CRIMP
BLUE	J34-2			
BLACK	J33-1	TB1-1-2	S1-	DOUBLE CRIMP
BLACK	J34-1			

WIRE TABLE FOR 7020198-01				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	J51-2	TB1-3	ON/OFF (+5V)	
BLACK	J51-1	TB1-2	S-	

WIRE TABLE FOR 7020199-01				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	P34-1	J51-1	S-	
BLACK	P34-2	P51-2	ON/OFF (+5V)	

WIRE TABLE FOR 7020203-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J35	TB1-3-2	+12V	

CXO-944B
Sheet 5 of 5

Figure A–1 HSC Internal Cabling

A.3 HSC50 Internal Cabling

Figure A–2 is a diagram of the HSC50 internal cabling.

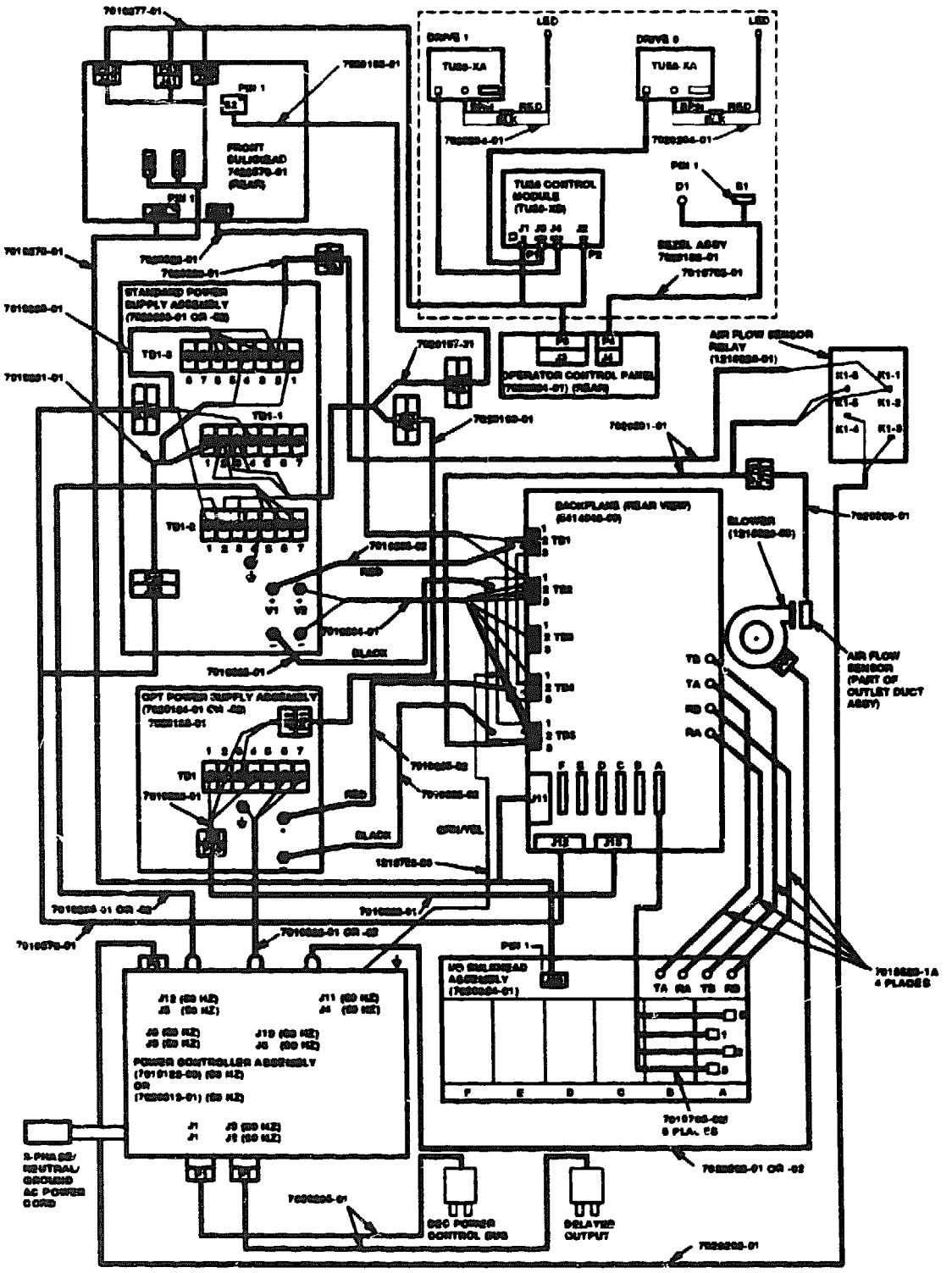


Figure A–2 (Cont.) HSC50 Internal Cabling

WIRE TABLE FOR LINE CORD OF 7019122-00			
COLOR	FROM	TO	REMARKS
BLUE	W	LF1-N	LINE SIDE
BLACK	Z	LF1-L3	
GRN/YEL	GND	LF1-GND	
BLACK	Y	LF1-L2	
BROWN	X	LF1-L1	

WIRE TABLE FOR 7019676-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J11-1	J41-01	+12V	* PINS AT J43-06 AND J60-06 ARE WIRELESS PINS. THEY ARE TIED TO J43-20 AND J60-20 BY COMMONING STRIPS.
VIOLET	J11-2	J44-01	+12V	
BLACK	J11-3	J41-02	GROUND	
BLACK	J11-4	J41-03	GROUND	
BLACK	J11-5	J44-02	GROUND	
BLACK	J11-6	J44-03	GROUND	
RED	J11-7	J41-04	+5V	
RED	J11-8	J44-04	+5V	
WHITE	J11-12	J60-20	TERM PRESS L	
WHITE	J11-13	J60-01	XMT-	
WHITE	J11-14	J60-02	XMT+	
WHITE	J11-15	J60-03	RCV+	
+——+	J60-20	J60-06	DATA SET READY COMMONING STRIP SEE NOTE *	
WHITE	J11-16	J60-07	ACV-	
WHITE	J11-18	J43-20	TERM PRESS L	
WHITE	J11-19	J43-01	XMT-	
WHITE	J11-20	J43-02	XMT+	
WHITE	J11-21	J43-03	RCV+	
+——+	J43-20	J43-06	DATA SET READY COMMONING STRIP SEE NOTE *	
WHITE	J11-22	J43-07	RCV-	
WHITE	J11-26	J42-01	TU0/1 PRESS L	
WHITE	J11-27	J42-02	TU0/1 XMT-	
WHITE	J11-28	J42-03	TU0/1 XMT+	
WHITE	J11-29	J42-04	TU0/1 REV+	
WHITE	J11-30	J42-05	TU0/1 RCV+	
WHITE	J11-34	J45-01	TU2/3 PRESS L	
WHITE	J11-35	J45-02	TU2/3 XMT-	
WHITE	J11-36	J45-03	TU2/3 XMT+	
WHITE	J11-37	J45-04	TU2/3 RCV+	
WHITE	J11-38	J45-05	TU2/3 RCV-	
YELLOW	J11-45	J40-01	STATE LAMP L	
YELLOW	J11-46	J40-02	POWER ON L	
YELLOW	J11-47	J40-03	LAMP 0 L	
YELLOW	J11-48	J40-04	TERM ENA L	
YELLOW	J11-49	J40-05	LAMP 2 L	
YELLOW	J11-50	J40-06	LAMP 1 L	
YELLOW	J11-51	J40-07	LAMP 4 L	
YELLOW	J11-52	J40-08	LAMP 3 L	
YELLOW	J11-53	J40-09	SWITCH 1 L	
YELLOW	J11-54	J40-10	SWITCH 0 L	
YELLOW	J11-55	J40-11	SWITCH 3 L	
YELLOW	J11-56	J40-12	SWITCH 2 L	
YELLOW	J11-57	J40-13	BDCOK H (INT L)	
BLACK	J11-58	J40-14	GROUND	
RED	J11-60	J40-15	+5V	

CXO-051A
Sheet 2 of 6

Figure A–2 (Cont.) HSC50 Internal Cabling

WIRE TABLE FOR 7019677-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	P41-1	P1-1	+12V	TU POWER
BLACK	P41-2	P1-3	GND (+12V)	TU POWER
BLACK	P41-3	P1-6	GND (+5V)	TU POWER
READ	P41-4	P1-5	+5V	TU POWER
WHITE	P42-1	P2-F	GND	TU SIGNAL
WHITE	P42-2	P2-D	RCV-	TU SIGNAL
WHITE	P42-3	P2-C	RCV+	TU SIGNAL
WHITE	P42-4	P2-J	XMT+	TU SIGNAL
WHITE	P42-5	P2-H	XMT-	TU SIGNAL
—	—	P2-E	—	KEYING PLUG (TU SIG)
YELLOW	P40-1	P3-1	STATE LAMP L	OCP
YELLOW	P40-2	P3-2	POWER ON L	OCP
YELLOW	P40-3	P3-4	LAMP 0 L	OCP
YELLOW	P40-4	P3-3	TERM ENA L	OCP
YELLOW	P40-5	P3-6	LAMP 2 L	OCP
YELLOW	P40-6	P3-5	LAMP 1 L	OCP
YELLOW	P40-7	P3-8	LAMP 4 L	OCP
YELLOW	P40-8	P3-7	LAMP 3 L	OCP
YELLOW	P40-9	P3-10	SWITCH 1 L	OCP
YELLOW	P40-10	P3-9	SWITCH 0 L	OCP
YELLOW	P40-11	P3-12	SWITCH 3 L	OCP
YELLOW	P40-12	P3-11	SWITCH 2 L	OCP
YELLOW	P40-13	P3-15	BDCOKH (INIT L)	OCP
BLACK	P40-14	P3-14	GND	OCP
RED	P40-15	P3-16	+5V	OCP
—	—	P3-20	—	KEYING PLUG (OCP)

WIRE TABLE FOR 7019679-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J12-1	P31-1	+12V	
VIOLET	J12-2	P31-3	+12V	
VIOLET	J12-3	P31-5	+12V	
VIOLET	J12-4	P31-7	+12V	
BLACK	J12-5	P31-9	GND (+12V)	
BLACK	J12-7	P31-2	GND (+12V)	
BLACK	J12-9	P31-4	GND (+12V)	
ORANGE	J12-11	P31-6	-5V SENSE	TWISTED PAIR
BLACK	J12-12	P31-8	GND (-5V SENSE)	
BROWN	J12-13	P31-10	POWER FAIL	
—	J12-16	—	NO CONNECTION	KEYING PLUG
BLACK	J12-17	J32-1	GND (+5V SENSE)	TWISTED PAIR
RED	J12-18	J32-2	+5V SENSE	
BLACK	J12-19	J32-3	GND (+12V SENSE)	TWISTED PAIR
VIOLET	J12-20	J32-4	+12V SENSE	

CXO-051A
Sheet 3 of 6

Figure A–2 (Cont.) HSC50 Internal Cabling

WIRE TABLE FOR 7019680-01

COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J31-1	TB1-3-5	+12V	DOUBLE CRIMP
VIOLET	J31-3			
VIOLET	J31-5	TB1-3-6	+12V	DOUBLE CRIMP
VIOLET	J31-7			
BLACK	J31-9	TB1-3-3	GND (+12V)	DOUBLE CRIMP
BLACK	J31-2			
BLACK	J31-4	TB1-3-3	GND (+12V)	
ORANGE	J31-6	TB1-2-2	+5V SENSE	TWISTED PAIR
BLACK	J31-8	TB1-2-1	GND (-5V SENSE)	
BROWN	J31-10	TB1-1-4	POWER FAIL	

WIRE TABLE FOR 7019681-01

COLOR	FROM	TO	SIGNAL	REMARKS
BLACK	P32-1	TB1-1-2	GROUND	TWISTED PAIR
RED	P32-2	TB1-1-1	+5V SENSE	
BLACK	P32-3	TB1-3-4	GROUND	TWISTED PAIR
VIOLET	P32-4	TB1-3-1	+12V SENSE	

WIRE TABLE FOR 7019686-02 STD PWR SUPPLY (50 HZ)

COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	J5*	GND	*POWER CONTROLLER J5
BLUE	TB1-2-7	J5*	ACC	
BROWN	TB1-2-6	J5*	AC	

WIRE TABLE FOR 7019686-01 AUX PWR SUPPLY (60 HZ)

COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	J13*	GND	*POWER CONTROLLER J13
BLUE	TB1-7	J13*	ACC	
BROWN	TB1-6	J13*	AC	

WIRE TABLE FOR 7019686-02 AUX PWR SUPPLY (50 HZ)

COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	J6*	GND	*POWER CONTROLLER J6
BLUE	TB1-7	J6*	ACC	
BROWN	TB1-6	J6*	AC	

WIRE TABLE FOR 7019705-01

COLOR	FROM	TO	SIGNAL	REMARKS
———	P4-01	———	NO CONNECTION	SPARE
———	P4-02	———	NO CONNECTION	KEYING PLUG
RED	P4-03	D1-1	+5V	
BLACK	P4-04	D1-2	GND (+5V)	
———	P4-05	———	NO CONNECTION	SPARE
YELLOW	P4-06	S1-4	GND	
YELLOW	P4-07	S1-5	TERM ENABLE	
———	P4-08	———	NO CONNECTION	SPARE
WHITE	P4-09	S1-1	INIT SWL	
WHITE	P4-10	S1-2	INIT L	

CXO-051A
Sheet 4 of 6

Figure A–2 (Cont.) HSC50 Internal Cabling

WIRE TABLE FOR 7020196-01				
COLOR	FROM	TO	SIGNAL	REMARKS
YELLOW	S2-2	P33-4	ON/OFF (-5.3V)	
ORANGE	S2-1	P33-3	S2-	
BLUE	S2-4	P33-2	ON/OFF (+5V)	
BLACK	S2-5	P33-1	S1-	

WIRE TABLE FOR 7019682-01				
COLOR	FROM	TO	SIGNAL	REMARKS
—	J13-2	—	—	KEYING PLUG
RED	J13-3	P50-1	+5V SENSE	TWISTED PAIR
BLACK	J13-4	P50-2	GND (+5V SENSE)	
BROWN	J13-5	P50-3	POWER FAIL	

WIRE TABLE FOR 7019683-01				
COLOR	FROM	TO	SIGNAL	REMARKS
RED	J50-1	TB1-1	+5V SENSE	TWISTED PAIR
BLACK	J50-2	TB1-2	GND (+5V SENSE)	
BROWN	J50-3	TB1-3	POWER FAIL	

WIRE TABLE FOR 7019684-01				
COLOR	FROM	TO	SIGNAL	REMARKS
BLACK	+V2	TB1-1	GROUND (-5V)	
BLACK	+V2	TB1-1	GROUND (-5V)	
BLACK	+V2	TB3-1	GROUND (-5V)	
BLACK	+V2	TB3-3	GROUND (-5V)	
ORANGE	-V2	TB2-3	-5V	
ORANGE	-V2	TB3-2	-5V	
ORANGE	-V2	TB4-1	-5V	
ORANGE	-V2	TB5-3	-5V	

WIRE TABLE FOR 7019686-01 STD PWR SUPPLY (60 HZ)				
COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	J12*	GND	*POWER CONTROLLER J12
BLUE	TB1-2-7	J12*	ACC	
BROWN	TB1-2-6	J12*	AC	

WIRE TABLE FOR 7020197-01				
COLOR	FROM	TO	SIGNAL	REMARKS
YELLOW	J33-4	TB1-2-3	ON/OFF (-5.3V)	
ORANGE	J33-3	TB1-2-2	S2-	
BLUE	J33-2	TB1-1-3	ON/OFF (+5V)	DOUBLE CRIMP
BLUE	J34-2			
BLACK	J33-1	TB1-1-2	S1-	DOUBLE CRIMP
BLACK	J34-1			

WIRE TABLE FOR 7020198-01				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	J51-2	TB1-3	ON/OFF (+5V)	
BLACK	J51-1	TB1-2	S-	

WIRE TABLE FOR 7020199-01				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	P34-1	J51-1	S-	
BLACK	P34-2	P51-2	ON/OFF (+5V)	

CXO-051A
Sheet 5 of 6

Figure A–2 (Cont.) HSC50 Internal Cabling

WIRE TABLE FOR 7020200-01				
COLOR	FROM	TO	SIGNAL	REMARKS
RED	A1-+	J70-1		
BLACK	A1-GND	J70-3		
WHITE	A1-LOAD	J70-2		

WIRE TABLE FOR 7020201-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	P70-1	K1-1	+12V	DOUBLE CRIMP
VIOLET	P35			
ORANGE	P70-2	K1-6	LOAD (-5V)	
ORANGE	P70-3	TB5-3	-5V	

WIRE TABLE FOR 7020202-01				
COLOR	FROM	TO	SIGNAL	REMARKS
WHITE	K1-3	P8-1	TRIP	
WHITE	K1-5	P8-2	RETURN	

WIRE TABLE FOR 7020203-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J35	TB1-3-2	+12V	

WIRE TABLE FOR 7020206-01 (60 HZ)				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	J11*	P80-1	AC	* POWER CONTROLLER J11
BROWN		P80-2	AC	
GRN/YEL		P80-3	GROUND	
BLACK	P80-7	P80-4		JUMPER
BLACK	P80-6	P80-5		JUMPER

WIRE TABLE FOR 7020206-02 (50 HZ)				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	S2-2	P80-1	AC	* POWER CONTROLLER J4
BROWN		P80-2	AC	
GRN/YEL		P80-3	GROUND	
BLACK	P80-5	P80-4		JUMPER

WIRE TABLE FOR 7020522-01				
COLOR	FROM	TO	SIGNAL	REMARKS
RED	TB1-2	J46-2	+5V	FROM BACKPLANE
BLACK	TB2-1	J46-1	GROUND	FROM BACKPLANE

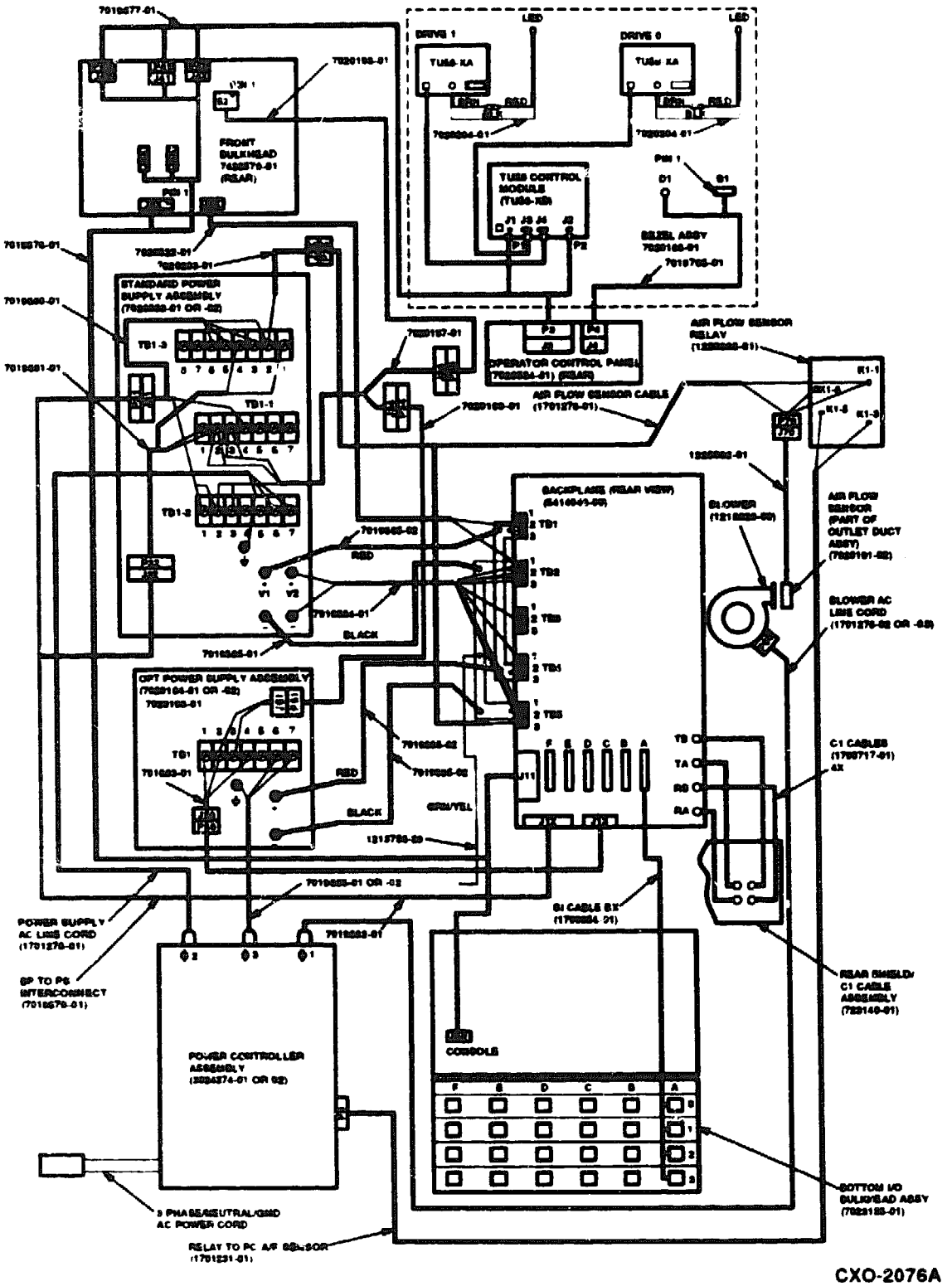
WIRE TABLE FOR LINE CORD OF 7020613-01				
COLOR	FROM	TO	SIGNAL	REMARKS
BROWN	X	LF1-PH3		LINE SIDE OF LF1
BLACK	Y	LF1-PH2		
BLACK (2)	Z	LF1-PH1		
BLUE	N	LF1-N		
GRN/YEL	GND	LF1-GND		

CXO-051A
Sheet 6 of 6

Figure A–2 HSC50 Internal Cabling

A.4 HSC50 (Modified) Internal Cabling

Figure A–3 is a diagram of the HSC50 (modified) internal cabling.



CXO-2076A
Sheet 1 of 6

Figure A–3 (Cont.) HSC50 (Modified) Internal Cabling

WIRE TABLE FOR 7019676-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J11-1	J41-01	+12V	
VIOLET	J11-2	J44-01	+12V	
BLACK	J11-3	J41-02	GROUND	
BLACK	J11-4	J41-03	GROUND	
BLACK	J11-5	J44-02	GROUND	
BLACK	J11-6	J44-03	GROUND	
RED	J11-7	J41-04	+5V	
RED	J11-8	J44-04	+5V	
WHITE	J11-12	J60-20	TERM PRESS L	
WHITE	J11-13	J60-01	XMT-	
WHITE	J11-14	J60-02	XMT+	
WHITE	J11-15	J60-03	RCV+	
+——+	J60-20	J60-06	DATA SET READY COMMONING STRIP SEE NOTE *	* PINS AT J43-06 AND J60-06 ARE WIRELESS PINS. THEY ARE TIED TO J43-20 AND J60-20 BY COMMONING STRIPS.
WHITE	J11-16	J60-07	ACV-	
WHITE	J11-18	J43-20	TERM PRESS L	
WHITE	J11-19	J43-01	XMT-	
WHITE	J11-20	J43-02	XMT+	
WHITE	J11-21	J43-03	RCV+	
+——+	J43-20	J43-06	DATA SET READY COMMONING STRIP SEE NOTE *	
WHITE	J11-22	J43-07	RCV-	
WHITE	J11-26	J42-01	TU0/1 PRESS L	
WHITE	J11-27	J42-02	TU0/1 XMT-	
WHITE	J11-28	J42-03	TU0/1 XMT+	
WHITE	J11-29	J42-04	TU0/1 REV+	
WHITE	J11-30	J42-05	TU0/1 RCV+	
WHITE	J11-34	J45-01	TU2/3 PRESS L	
WHITE	J11-35	J45-02	TU2/3 XMT-	
WHITE	J11-36	J45-03	TU2/3 XMT+	
WHITE	J11-37	J45-04	TU2/3 RCV+	
WHITE	J11-38	J45-05	TU2/3 RCV-	
YELLOW	J11-45	J40-01	STATE LAMP L	
YELLOW	J11-46	J40-02	POWER ON L	
YELLOW	J11-47	J40-03	LAMP 0 L	
YELLOW	J11-48	J40-04	TERM ENA L	
YELLOW	J11-49	J40-05	LAMP 2 L	
YELLOW	J11-50	J40-06	LAMP 1 L	
YELLOW	J11-51	J40-07	LAMP 4 L	
YELLOW	J11-52	J40-08	LAMP 3 L	
YELLOW	J11-53	J40-09	SWITCH 1 L	
YELLOW	J11-54	J40-10	SWITCH 0 L	
YELLOW	J11-55	J40-11	SWITCH 3 L	
YELLOW	J11-56	J40-12	SWITCH 2 L	
YELLOW	J11-57	J40-13	BDCOK H (INT L)	
BLACK	J11-58	J40-14	GROUND	
RED	J11-60	J40-15	+5V	

CXO-2076A
Sheet 2 of 6

Figure A–3 (Cont.) HSC50 (Modified) Internal Cabling

WIRE TABLE FOR 7019677-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	P41-1	P1-1	+12V	TU POWER
BLACK	P41-2	P1-3	GND (+12V)	TU POWER
BLACK	P41-3	P1-6	GND (+5V)	TU POWER
READ	P41-4	P1-5	+5V	TU POWER
WHITE	P42-1	P2-F	GND	TU SIGNAL
WHITE	P42-2	P2-D	RCV-	TU SIGNAL
WHITE	F42-3	P2-C	RCV+	TU SIGNAL
WHITE	P42-4	P2-J	XMT+	TU SIGNAL
WHITE	P42-5	P2-H	XMT-	TU SIGNAL
—	—	P2-E	—	KEYING PLUG (TU SIG)
YELLOW	P40-1	P3-1	STATE LAMP L	OCP
YELLOW	P40-2	P3-2	POWER ON L	OCP
YELLOW	P40-3	P3-4	LAMP 0 L	OCP
YELLOW	P40-4	P3-3	TERM ENA L	OCP
YELLOW	P40-5	P3-6	LAMP 2 L	OCP
YELLOW	P40-6	P3-5	LAMP 1 L	OCP
YELLOW	P40-7	P3-8	LAMP 4 L	OCP
YELLOW	P40-8	P3-7	LAMP 3 L	OCP
YELLOW	P40-9	P3-10	SWITCH 1 L	OCP
YELLOW	P40-10	P3-9	SWITCH 0 L	OCP
YELLOW	P40-11	P3-12	SWITCH 3 L	OCP
YELLOW	P40-12	P3-11	SWITCH 2 L	OCP
YELLOW	P40-13	P3-15	BDCOKH (INIT L)	OCP
BLACK	P40-14	P3-14	GND	OCP
RED	P40-15	P3-16	+5V	OCP
—	—	P3-20	—	KEYING PLUG (OCP)

WIRE TABLE FOR 7019679-01				
COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J12-1	P31-1	+12V	
VIOLET	J12-2	P31-3	+12V	
VIOLET	J12-3	P31-5	+12V	
VIOLET	J12-4	P31-7	+12V	
BLACK	J12-5	P31-9	GND (+12V)	
BLACK	J12-7	P31-2	GND (+12V)	
BLACK	J12-9	P31-4	GND (+12V)	
ORANGE	J12-11	P31-6	-5V SENSE	TWISTED PAIR
BLACK	J12-12	P31-8	GND (-5V SENSE)	
BROWN	J12-13	P31-10	POWER FAIL	
—	J12-16	—	NO CONNECTION	KEYING PLUG
BLACK	J12-17	J32-1	GND (+5V SENSE)	TWISTED PAIR
RED	J12-18	J32-2	+5V SENSE	
BLACK	J12-19	J32-3	GND (+12V SENSE)	TWISTED PAIR
VIOLET	J12-20	J32-4	+12V SENSE	

CXO-2076A
Sheet 3 of 6

Figure A–3 (Cont.) HSC50 (Modified) Internal Cabling

WIRE TABLE FOR 7019680-01

COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	J31-1	TB1-3-5	+12V	DOUBLE CRIMP
VIOLET	J31-3			
VIOLET	J31-5	TB1-3-6	+12V	DOUBLE CRIMP
VIOLET	J31-7			
BLACK	J31-9	TB1-3-3	GND (+12V)	DOUBLE CRIMP
BLACK	J31-2			
BLACK	J31-4	TB1-3-3	GND (+12V)	
ORANGE	J31-6	TB1-2-2	+5V SENSE	TWISTED PAIR
BLACK	J31-8	TB1-2-1	GND (-5V SENSE)	
BROWN	J31-10	TB1-1-4	POWER FAIL	

WIRE TABLE FOR 7019681-01

COLOR	FROM	TO	SIGNAL	REMARKS
BLACK	P32-1	TB1-1-2	GROUND	TWISTED PAIR
RED	P32-2	TB1-1-1	+5V SENSE	
BLACK	P32-3	TB1-3-4	GROUND	TWISTED PAIR
VIOLET	P32-4	TB1-3-1	+12V SENSE	

WIRE TABLE FOR 7019705-01

COLOR	FROM	TO	SIGNAL	REMARKS
—	P4-01	—	NO CONNECTION	SPARE
—	P4-02	—	NO CONNECTION	KEYING PLUG
RED	P4-03	D1-1	+5V	
BLACK	P4-04	D1-2	GND (+5V)	
—	P4-05	—	NO CONNECTION	SPARE
YELLOW	P4-06	S1-4	GND	
YELLOW	P4-07	S1-5	TERM ENABLE	
—	P4-08	—	NO CONNECTION	SPARE
WHITE	P4-09	S1-1	INIT SWL	
WHITE	P4-10	S1-2	INIT L	

WIRE TABLE FOR 7020196-01

COLOR	FROM	TO	SIGNAL	REMARKS
YELLOW	S2-2	P33-4	ON/OFF (-5.3V)	
ORANGE	S2-1	P33-3	S2-	
BLUE	S2-4	P33-2	ON/OFF (+5V)	
BLACK	S2-5	P33-1	S1-	

WIRE TABLE FOR 7019682-01

COLOR	FROM	TO	SIGNAL	REMARKS
—	J13-2	—	—	KEYING PLUG
RED	J13-3	P50-1	+5V SENSE	TWISTED PAIR
BLACK	J13-4	P50-2	GND (+5V SENSE)	
BROWN	J13-5	P50-3	POWER FAIL	

WIRE TABLE FOR 7019683-01

COLOR	FROM	TO	SIGNAL	REMARKS
RED	J50-1	TB1-1	+5V SENSE	TWISTED PAIR
BLACK	J50-2	TB1-2	GND (+5V SENSE)	
BROWN	J50-3	TB1-3	POWER FAIL	

CXO-2076A
Sheet 4 of 6

Figure A–3 (Cont.) HSC50 (Modified) Internal Cabling

WIRE TABLE FOR 7019684-01

COLOR	FROM	TO	SIGNAL	REMARKS
BLACK	+V2	TB2-1	GRN (-5V)	
BLACK	+V2	TB2-2	GND (-5V)	
BLACK	+V2	TB5-1	GND (-5V)	
BLACK	+V2	TB5-2	GND (-5V)	
ORANGE	-V2	TB2-3	-5V	
ORANGE	-V2	TB3-2	-5V	
ORANGE	-V2	TB4-1	-5V	
ORANGE	-V2	TB5-3	-5V	

WIRE TABLE FOR 7020197-01

COLOR	FROM	TO	SIGNAL	REMARKS
YELLOW	J33-4	TB1-2-3	ON/OFF (-5.3V)	
ORANGE	J33-3	TB1-2-2	S2-	
BLUE	J33-2	TB1-1-3	ON/OFF (+5V)	
BLUE	J34-2			
BLACK	J33-1	TB1-1-2	S1-	
BLACK	J34-1			

WIRE TABLE FOR 7020198-01

COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	J5-2	TB1-3	ON/OFF (+5V)	
BLACK	J5-1	TB1-2	S-	

WIRE TABLE FOR 7020199-01

COLOR	FROM	TO	SIGNAL	REMARKS
BLACK	P34-1	P51-1	S-	
BLUE	P34-2	P51-2	ON/OFF (+5V)	

WIRE TABLE FOR 1228092-01 A/F SENSOR

COLOR	FROM	TO	SIGNAL	REMARKS
RED	A1-+	J70-1		
BLACK	A1-GND	J70-2		
WHITE	A1-LOAD	J70-3		

WIRE TABLE FOR 1701231-01 RELAY TO PC A/F SENSOR

COLOR	FROM	TO	SIGNAL	REMARKS
WHITE	K1-3	P8-1	TRIP	
WHITE	K1-5	P8-2	RETURN	

WIRE TABLE FOR 1701275-01 A/F SENSOR CABLE

COLOR	FROM	TO	SIGNAL	REMARKS
VIOLET	P70-1	K1-1	+5V	DOUBLE CRIMP
VIOLET	P35			
ORANGE	P70-2	K106	LOAD (-5V)	
ORANGE	P70-3	-5.2V BUSBAR 0 BACKPLANE	-5.2V	

WIRE TABLE FOR 1701276-01 STD POWER SUPPLY

COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	ϕ2*	GND	*POWER CONTROLLER ϕ2
BLUE	TB1-1-7	ϕ2*	ACC	
BROWN	TB1-1-6	ϕ2*	AC	

CXO-2076A
Sheet 5 of 6

Figure A–3 (Cont.) HSC50 (Modified) Internal Cabling

WIRE TABLE FOR 1701276-01 OPT POWER SUPPLY				
COLOR	FROM	TO	SIGNAL	REMARKS
GRN/YEL	GND STUD	ϕ3 *	GND	*POWER CONTROLLER ϕ 3
BLUE	TB1-1-7	ϕ3 *	ACC	
BROWN	TB1-1-6	ϕ3 *	AC	

WIRE TABLE FOR 1701276-02 BLOWER AC LINE CORD				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	IN MOLDED PLUG	P80-1	AC	NEUTRAL
BROWN		P80-2	AC	LINE
GREEN		P80-3	GND	
BLACK	P80-5	P80-4		JUMPER

WIRE TABLE FOR 1701276-03 BLOWER AC LINE CORD				
COLOR	FROM	TO	SIGNAL	REMARKS
BLUE	IN MOLDED PLUG	P80-1	AC	NEUTRAL
BROWN		P80-2	AC	LINE
GREEN		P80-3	GND	
BLACK	P80-7	P80-4		JUMPER
BLACK	P80-8	P80-5		JUMPER

CXO-2076A
Sheet 6 of 6

Figure A–3 HSC50 (Modified) Internal Cabling


APPENDIX B

B
Exception Codes and Messages

Certain software inconsistencies can cause an exception (crash) in the HSC controller. This appendix describes all HSC controller exception codes caused by software inconsistencies and provides a description of the exception codes, the facility or program reporting them, and the action you should take. For ease of reference, these codes are arranged in numerical order (octal radix).

To determine which exception code caused a particular crash, refer to the crash dump displayed on the terminal. Note that the code number, but not the text, appears on hardcopy printouts.

B.1 Crash Dump Printout

In order to determine which exception code caused a particular crash, refer to the crash dump printed on the terminal. The following HSC crash dump example breaks down and describes the various fields. The HSCxx refers to the HSC controller model.

```
\,-*  SUBSYSTEM EXCEPTION  *-      V600          HSCxx  HSC007 ●
        at 02-Aug-1990 00:13:34.20        up    0 00:13:34.20
User ●  Pc: 000002 caused by (20      ) IOT ●
PSW:  140004
CRASH ● active, PCB addr = 036322
R0-R5:
000000    126104   000000   000000   000000   000000
Kernel SP: 000774
Kernel Stack:
017214 ● 016334   007410   077406   077406   077406  077406   077406
077406    077406   100016   077506   077506   077406  077406   077406
Supervisor SP: 000650 ●
Supervisor Stack:
052525 ● 052525   025252   025252   025252   025252   025252   025252
025252   025252   025252   025252   025252   025252   025252   025252
User SP: 000250
User Stack:
005000 ● 000110   010001   104064   000000   000520  000000   000000
000000    000000   000000   000000   000000   000000  000000   000000
KPAR(0-7):
●
   .
   .
   .
Status of requestors(1-9):
000001 ● 000206   000205   000205   000205   000205  000205   000205
(PC-6) to (PC):
NXM    003407   000004   046534
Booting..
```

Example B–1 Crash Dump Example

- This line calls out a crash and indicates the HSCxx is at software version number V600. The last field is the assigned node name (set with SET NAME).
- This line indicates the processor mode in which the crash occurred. This can be either *Kernel* or *User*.
- This three-letter mnemonic indicates the type of crash. The example mnemonic IOT indicates that this is a software inconsistency. Any other combination of letters, such as NXM (nonexistent memory) would designate a crash outside the scope of this appendix.

  Hardware exceptions are defined in Appendix D.
- The initial name on this line identifies the process active at the time of the crash. It is valid only during user-mode crashes. Use this name as a crosscheck when looking up the crash description.
- If the mode notation is *Kernel*, check the first word of the *Kernel Stack* for the crash code.
- If the HSC controller has an M.cache module installed, the crash dump will contain a *Supervisor SP* and a *Supervisor Stack* dump. This information does not appear on HSC controllers that do not have an operational M.cache module installed.
- If the mode notation is *Superv*, check the first word of the *Supervisor Stack* for the crash code.
- Because the mode notation in this example indicated *User*, check the *User Stack* for the crash code number. This code is always the first word of the stack (in this case, *005000*).
- The following ellipsis replaces other unnecessary stack dump information.
- This line denotes the identity and status of each requestor. Refer to Appendix D for a listing of the crash status codes for requestors.

B.2 SINI-E Error Printout

The following SINI-E error example appears immediately upon reboot after a subsystem exception. Information contained in this error message is condensed from the crash dump information.

```
SINI-E Seq 1. at 17-Nov-1858 00:00:02.00, Out-of band 000602 ●
        Software inconsistency ●
        Process CRASH ●
        PC  000002
        PSW 140004
        Stack dump:  005000  000110  010001
```

Example B–2 SINI-E Exception Code

- The out-of-band message number is used for troubleshooting. Refer to Chapter 8 for information on interpreting these messages.
- This line defines the cause of the crash.
- This line and the following three lines duplicate the applicable information in the crash dump.

In each of the exception descriptions in this appendix, **Facility:** indicates the process(es) running at the time the crash occurred. The first name listed is the major process. The second is the module of the process that generated the exception. This may be a subprocess of the main process or simply a different code module.

B.3 Submitting a Software Performance Report

Some of the exception messages listed in this appendix suggest submitting a Software Performance Report (SPR) with a copy of the crash dump. Before submitting the SPR, contact the Customer Services Center or your local field office to find out if additional information will be needed. Submit an SPR only after eliminating other possibilities, such as hardware-related problems.

If the customer requires immediate use of the HSC controller, you can reboot the HSC controller using the Init switch on the OCP. Rebooting the HSC controller can cause a loss of the information necessary for an SPR, so be sure to print a hardcopy of the crash dump message and other required information.

After two or three similar exception messages occur an SPR should be submitted. Look up the exception message in this appendix. If a data structure (for instance, HMB or PCB) should be included with the SPR, set the ODT parameter to cause the HSC controller to enter ODT after an exception. If a data structure is not requested in the applicable exception code, you do not need to enter ODT.

Data structures needed with the SPR must be formatted. These data structures are addressed by a register or the contents of another structure's field. To format the necessary data structure(s), substitute the *x* in Table B–1 with the pointer from the specified register or location. Substitute only the *x* and type the rest of the line exactly as you see it in the table, except for the information in parentheses. The number of equal (=) signs designates the data structure memory:

= indicates program memory
= = indicates Control memory
= == indicates data memory

Table B–1 Obtaining Data Structure Information

Data Structure Needed	Type At * Prompt
CB	x= =CB$
Counter	x=C *(and)* x= =C.
DCB	x= =DC$DISK *(or)* x= =DC$TAPE (if Tape Path problem)
DDCB	x=DD$
FRB	x= =F$
HCB	x=HC$
HMB	x= =HM$ (command packet)
	x= =HM$CPY (BACKUP)
	x= =HM$DATA (with BMBs)
	x= =HM$QUIET (diagnostic)
	x= =HM$XFR (used while work is outstanding)
	x= =HM$VC (used to alter VC state)
K Control Area	x= =KG$
PCB	x=Z.
SLCB	x=SL$
TDCB	x=TD.

Table B–1 (Cont.) Obtaining Data Structure Information

Data Structure Needed	Type At * Prompt
TFCB	x=TF
TTCB	x=TT$
XFRB	x==X

After the information is complete, the customer should fill out the SPR and submit it, together with all hardcopy, as instructed on the SPR form.

NOTE
If you call the Customer Support Center for assistance, inform the Center of the problem. Also, let them know your customer will need help gathering information related to the software error.

B.4 Exception Messages

In each of the exception messages, **Facility:** indicates the process(es) running at the time the crash occurred. The first name listed is the major process. The second name is the module of the process that generated the exception. This module may be a subprocess of the main process or simply a different code module. Include a hardcopy of the crash dump message and any other applicable information with an Software Performance Report (SPR) submission.

001002 ($CPUM1)
Previous mode not user

Facility: EXEC, EXEC

Explanation: During a context switch of user processes, the previous mode (as indicated by the program status word (PSW)) was not user mode. R5 points to the process control block (PCB).

Action: Submit an SPR with the crash dump.

001003 ($CEXPCB)
EXEC PCB was scheduled

Facility: EXEC, EXEC

Explanation: During process scheduling, the EXEC process control block (PCB) was scheduled. This dummy PCB is used only for loading the process and should never be scheduled. R2 points to the PCB.

Action: Submit an SPR with the crash dump.

001004 ($CDEBCAC)
Cache setting in PDR is in incorrect state

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. A page descriptor register (PDR) directed to program memory does not have "disable cache" set. A PDR directed to data memory does have "disable cache" set. R0 points to the PDR.

Action: Submit an SPR with a crash dump.

001005 ($CPUM2)
Previous mode not user

Facility: EXEC, EXEC

Explanation: During a context switch of user processes, the previous mode, as indicated by the program status word (PSW), was not user mode.

Action: Submit an SPR with a crash dump.

001006 ($CCB4)
Spurious interrupt from K at Control Bus Level 4

Facility: EXEC, EXEC

Explanation: One of the data channel requestor modules, or the K.ci, interrupted the P.ioc module at level four, but, upon queue examination, no elements were shown (an element should be on the level 4 interrupt queue).

Action: Submit an SPR. If this crash continues to occur, escalate the problem to Customer Services support.

001007 ($CCB5)
Spurious interrupt from K at Control Bus Level 5

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the data channel requestor modules, or the K.ci, interrupted the P.ioc at level 5, yet, upon queue examination, no elements were shown (an element should be on the level 5 interrupt queue)

Action: If this crash continues to occur, escalate the problem to Customer Services support. This is probably a hardware problem. If not, Customer Services can submit an SPR.

001010 ($CDC1)
Downcount failed

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. During processing of the level 5 interrupt queue, a down count operation failed. R1 points to the counter.

Action: Submit an SPR with a crash dump.

001011 ($CDC2)
Downcount failed

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. During processing of the level 5 interrupt queue, a down count operation failed. R1 points to the counter.

Action: Submit an SPR with a crash dump.

001012 ($CACQ)
Acquire on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The ACQ$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001013 ($CAML)
Acquire Multiple on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The AMLT$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001014 ($CRLP)
Release on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The REL$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001015 ($CRRTI)
RRTI$ on Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RRTI$P system service was called with a semaphore address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001016 ($CRTI1)
RRTI$ found Semaphore count non-zero

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. When exiting, the RRTI$ routine found an inconsistency in a semaphore count word.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001017 ($CRTI2)
RRTI$ found Semaphore count non-zero

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. When exiting, the RRTI$ routine found an inconsistency in a semaphore count word.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001020 ($CRCPP)
Receive/Dequeue from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the RCV$P FROM$P or DEQ$P FROM$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001021 ($CRCCP)
Receive/Dequeue from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the RCV$C FROM$P or DEQ$C FROM$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001022 ($CRCCV)
Receive/Dequeue from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the RCV$C FROM$P, DEQ$C FROM$P, RCV$C FROM$W, or DEQ$C FROM$W system services was called with a queue head address of zero.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001023 ($CRMPP)
Receive/Dequeue Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RCVM$P system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001024 ($CRMCP)
Receive/Dequeue Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RCVM$C system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001025 ($CRMCV)
Receive/Dequeue Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The RCVM$W system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001026 (SCRAMCV)
Receive All-Maybe from Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the RCAM$C FROM$P or RCAM$C FROM$W system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001027 (SCSPP)
Send/Enqueue to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SEND$P TO$P or ENQ$P TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001030 (SCSCP)
Send/EnQueue to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SEND$C TO$P or ENQ$C TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001031 (SCSCV)
Send/Enqueue to Queue with invalid target queue specified

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SEND$C TO$W or ENQ$C TO$W system services was called with an incorrect target queue address.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001032 (SCSHPP)
Send/Enqueue-to-Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SNDH$P TO$P or ENQH$P TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001033 ($CSHCP)
Send/Enqueue-to-Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. One of the SNDH$C TO$P, ENQH$C TO$P, SNDH$C TO$P, or ENQH$C TO$P system services was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001034 ($CIHPP)
Insert at Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The INSH$P TO$P system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001035 ($CIHCP)
Insert at Head to Queue with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The INSH$C TO$P system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001036 ($CUPCV)
Up count to Counter with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The UPC$ system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001037 ($CDWCV)
Down count to Counter with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The DWNC$ system service was called with a queue head address of 0.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001040 ($CSTTM)
Set Timer operation to active timer

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. The SETTM$ system service was called to set a timer that is already active.

Action: The process specified as active is the offender. Submit an SPR with a crash dump.

001041 (SCSNZ1)
Release of Semaphore with address of 0

Facility: EXEC, EXEC

Explanation: This software inconsistency should not appear under normal circumstances. During some circumstances, a semaphore will require a down count without subsequent scheduling considerations. This typically happens when a process enters hibernation or exits. During the implicit release operation, the semaphore had an address of 0.

Action: Submit an SPR with a crash dump.

001042 (SCTOVR)
Time-of-day overflowed

Facility: EXEC, EXEC

Explanation: During an update of the current time of day, the executive detected an overflow. This can happen if a node on the CI sets a false time to the HSC controller.

Action: Examine previous console printouts to verify accurate date and time fields. If accurate, submit an SPR with the console crash report. If inaccurate, set the HSC software outband error level to **Info**. Then verify console report of date and time set by a host node on the next HSC controller reboot. If a host node problem is not indicated, escalate the problem to Customers Services support.

001043 (SCPWFL)
Power Failure

Facility: EXEC, EXEC

Explanation: The processor is still operating five seconds after a power failure indication. Therefore, CRONIC concludes that the power failure indication was false.

Action: Verify the ac voltages are correct. If so, and the problem persists, notify Customer Services support.

001201 (SCNOHIBER)
Process on Recoverable List not Hibernating

Facility: EXEC, EXECLOAD

Explanation: Before loading a utility or diagnostic, the loader examined the recoverable memory list of cached programs to determine whether or not a program might be loaded from memory instead of from the load device. When a program was found on the recoverable memory list, its state was not Hibernate state. This software inconsistency should not be seen under normal circumstances.

Register R3 points to the process control block (PCB) for process to restart.

Action: Submit an SPR with a crash dump, noting previous activity with the program requested.

001202 (SCIMAGE)
Memory extent encroaches defined area

Facility: EXEC, EXECLOAD

Explanation: The process to be loaded specified additional memory or buffer space, as specified on the loadable file header (LFHEADER) directive. When the additional memory was allocated and mapped to the process, it had encroached upon the loaded area. This exception can also indicate that the process image did not start on a 4K word boundary. Register R0 points to the

extended function request block (XFRB) for loading the image. Register R4 points to the CH$ (canonical file header).

Action: Submit an SPR with a crash dump.

001203 ($CNOPROC)
No code parent process loaded

Facility: EXEC, EXECLOAD

Explanation: When a process was loaded, its PCB specified it should execute and share code associated with another process. When attempting to locate the code parent, the loader found that the parent was not loaded. Register R2 equals the process number of the code parent. Register R3 points to the code child's PCB.

Action: Submit an SPR with a crash dump.

001204 ($CALLOCATE)
Insufficient Kernel Pool

Facility: EXEC, EXECLOAD

Explanation: When EXEC attempted to allocate either a PCB (Z.) or an address descriptor (A.) structure from kernel pool for a new process, kernel pool was inadequate to support the additional structures.

Action: Submit an SPR with a crash dump.

001205 ($CLFAO)
FAO overrun

Facility: EXEC, EXECLOAD

Explanation: The formatted ASCII output (FAO) string returned during formatting of a module version mismatch message was too large for the buffer.

Action: Submit an SPR with a crash dump. If possible, send a copy of the RX33 diskette.

001401 ($CBUSY)
Performed receive when already busy with request

Facility: EXEC, EXECRDWR

Explanation: The READ$/WRITE$ service, while in its exception routine, was already busy with one request while a RCV$P operation was performed.

Action: Submit an SPR with a crash dump.

001402 ($CNOLOADED)
Requested driver not loaded

Facility: EXEC, EXECRDWR

Explanation: A process within the HSC software specified a READ$ or WRITE$ operation with a device control block (DDCB) for a device not configured on that model. For example, a program specified a transfer for a TU58 tape drive on an HSC controller. Because the device is not configured on the system, the driver is not loaded. R3 points to the XFRB. R4 points to the DDCB. R5 equals CSR for device.

Action: Submit an SPR with a crash dump, describing activity on the HSC controller at the time of the exception. The process listed as active may be the READ$/WRITE$ service, and not the process that performed the offending request.

001403 ($CDDCB)
Invalid DDCB specified

Facility: EXEC, EXECRDWR

Explanation: A request to the READ$/WRITE$ service specified a DDCB that was invalid, or it specified an invalid device type in the DD$TYPE field. R3 points to the XFRB. R4 points to the DDCB. R5 equals CSR for device. R0 equals device type.

Action: Submit an SPR with a crash dump, describing activity on the HSC controller at the time of the exception. The process listed as active may be the READ$/WRITE$ service and not the process that performed the offending request.

001501
Motor not Running

Facility: EXEC, EXECRX33

Explanation: The motor was not running when the motor shutdown timer expired.

Action: Submit an SPR with a crash dump.

001502
Non-RX33 command requested

Facility: EXEC, EXECRX33

Explanation: The RX33 driver received an CRONIC transfer request (XFRB), but the XFRB specified a DDCB for a non-RX33 device. R4 points to the DDCB, R5 points to the XFRB.

Action: Submit an SPR with a crash dump.

001503
Invalid Unit Number

Facility: EXEC, EXECRX33

Explanation: The DDCB specified an RX33 device, but the unit requested was not 0 or 1. R5 points to the XFRB.

Action: Submit an SPR with a crash dump.

001504
Zero byte count transfer

Facility: EXEC, EXECRX33

Explanation: A transfer was requested with a zero byte count. R2 equals byte count, R5 points to the XFRB.

Action: Submit an SPR with a crash dump.

001505
Invalid byte count

Facility: EXEC, EXECRX33

Explanation: A transfer was requested with a byte count that was not a multiple of 512 (sector size). R2 equals byte count, R5 points to the XFRB.

Action: Submit an SPR with a crash dump.

001506
Invalid internal byte count

Facility: EXEC, EXECRX33

Explanation: The remaining byte count of a partially completed transfer was not a multiple of 512. The original (requested) byte count was a multiple of 512. R2 equals byte count, R5 points to the XFRB.

Action: Submit an SPR with a crash dump.

001507
RX33 hardware registers are incorrect

Facility: EXEC, EXECRX33

Explanation: RX33 disk drive hardware signaled successful completion of an I/O operation, but the hardware registers (current sector, current track, or memory address register) did not contain the expected values.

Action: Check for RX33-related hardware failures. If the problem persists, submit an SPR with the crash dump.

001510
Invalid Head Select

Facility: EXEC, EXECRX33

Explanation: The software attempted to select a head other than 0 or 1. R0 equals head select.

Action: Submit an SPR with a crash dump.

001511
Memory Management

Facility: EXEC, EXECRX33

Explanation: Relocation is not enabled in the memory management hardware. Bit 0 is not set in MMR0.

Action: Submit an SPR with a crash dump.

001512
Invalid Virtual Address

Facility: EXEC, EXECRX33

Explanation: The virtual address passed in the XFRB is not in page 4. R5 points to the XFRB.

Action: Submit an SPR with a crash dump.

001513
Unexpected Interrupt from RX33

Facility: EXEC, EXECRX33

Explanation: An unexpected interrupt was received from the RX33 controller. This condition is not detected until a command is about to be issued; that is, the crash does not happen when the interrupt is detected.

Action: If the problem persists, submit an SPR with the crash dump. Further testing of the HSC subsystem load device area may be necessary.

001514
Invalid Internal Unit Number

Facility: EXEC, EXECRX33

Explanation: The unit number index value is not 0 or 2. This unit number index value is contained in R4.

Action: Submit an SPR with a crash dump.

001515
Non-Existent Memory

Facility: EXEC, EXECRX33

Explanation: The RX33 controller returned an NXM error.

Action: Further testing of the HSC subsystem (load device area) may be necessary. If the problem persists, submit an SPR with the crash dump.

001601 ($CPAG1)
TYPE$ crosses page boundaries

Facility: EXEC, EXECTT

Explanation: A process requested a TYPE$ system service (or an ACPT$ service with a prompt) specifying a buffer that crosses a memory management page boundary. This is a restriction of the driver. R0 equals size of print string. R1 points to the String Buffer. R4 points to the TTCB (device control block). R5 points to the XFRB.

Action: Submit an SPR with a crash dump, describing activity at the time of the exception.

001602 ($CPAG2)
ACPT$ crosses page boundaries

Facility: EXEC, EXECTT

Explanation: A process requested an ACPT$ system service specifying a buffer that crosses a memory management page boundary. This is a restriction of the driver. R4 points to the TTCB (device control block). R5 points to the XFRB.

Action: Submit an SPR with a crash dump, describing activity at the time of the exception.

001603 ($CNOPCB)
PCB not found on run queue

Facility: EXEC, EXECTT

Explanation: EXEC failed to locate the PCB in the RUN queue for the process excepted by a keyboard command. R4 points to the attached PCB.

Action: Submit an SPR with a crash dump.

001701 ($CPAGE)
READ$ or WRITE$ crossed page boundary

Facility: EXEC, EXECTU58

Explanation: A request to the TU58 tape drive specified a buffer that crossed a memory management page boundary. This is a restriction of the driver.

Action: Submit an SPR with a crash dump, describing activity at the time of the exception. The process listed as active may be the READ$/WRITE$ Service and not the process initiating the offending request.

002001
Exception routine invoked for unknown reason

Facility: DEMON

Explanation: DEMON's exception routine was activated, but not for Ctrl/y, Ctrl/c, or a diagnostic timeout.

Action: Submit an SPR with a crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. A software problem is the most likely cause of this crash.

002002
Insufficient free memory to allocate a program stack

Facility: DEMON

Explanation: When DEMON was initialized, it could not allocate enough free program memory for use as a stack.

Action: A failing memory module is the most likely cause of the problem. If no hardware problem is found, submit an SPR with a crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence.

002003
DEMON was initiated when there was no diagnostic to run

Facility: DEMON

Explanation: DEMON did a receive on its work queue and received a nondiagnostic request.

Action: Submit an SPR with a crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence.

002004
Failure in periodic control or data memory test

Facility: DEMON, PRMEMY

Explanation: One of the periodic control or data memory interface tests detected a failure. Failures in these tests are fatal, and the HSC controller must reboot after displaying a message describing the failure.

Action: A failing P.ioc module is the most probable cause of this crash. Further testing of the HSC controller memory and P.ioj may be necessary.

002005
Failure in periodic K.sdi or K.sti test

Facility: DEMON, PRKSDI, PRKSTI

Explanation: The periodic K.sdi/K.si or K.sti/K.si module tests detected a failure. Failures in these tests are fatal, and the HSC controller must reboot after displaying a message describing the type of error and requestor number of the failed module.

Action: A failing K.sdi/K.si or K.sti/K.si module is the most probable cause of this crash. The requestor number of the probable failing module is displayed in the error message preceding the crash. Further testing of HSC controller data channels and internal buses may be necessary.

002006
ILDISK received illegal queue address

Facility: DEMON, ILDISK

Explanation: ILDISK requested exclusive access to a drive's state area. The acquire operation should return the control memory address of the attention/available service queue for the specified drive. The address returned was zero, an illegal address for a queue.

Action: If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

002007
ILDISK received illegal buffer descriptor

Facility: DEMON, ILDISK

Explanation: ILDISK received a buffer descriptor from the free buffer queue. A consistency check on the buffer descriptor failed because the descriptor indicated the buffer was not in the HSC controller's buffer memory. A software problem is the most likely cause of this crash.

Action: Submit an SPR with a crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

002010
ILDISK detected inconsistency in exception routine

Facility: DEMON, ILDISK

Explanation: ILDISK's internal flags indicated exclusive ownership of a drive's state area, but the address of the K.sdi/K.si control area was not available. When ILDISK has exclusive ownership of a drive state area, the address of the K.sdi/K.si control area should always be available. A software problem is the most likely cause of this crash.

Action: Submit an SPR with a crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

002011
An ILEXER disk I/O request failed to complete

Facility: DEMON, ILEXER

Explanation: ILEXER attempted to abort all outstanding disk I/O requests. After waiting two minutes, the program found that one or more I/O requests had not completed. The HSC controller crashes and reboots because ILEXER cannot exit with a request outstanding.

Action: Submit an SPR with a crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular disk drive is tested.

A faulty disk drive is the most likely cause of this problem. Further testing of the suspect disk and associated requestor(s) may be necessary.

002012
An ILEXER tape I/O request failed to complete

Facility: DEMON

Explanation: ILEXER attempted to abort all outstanding tape I/O requests. After waiting four minutes, the program found that one or more I/O requests had not completed. The HSC controller crashed and rebooted because ILEXER cannot exit with a request outstanding.

Action: Submit an SPR with a crash dump. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is tested.

A faulty tape drive or formatter is the most likely cause of this problem. Further testing of the suspect tape subsystem and associated requestor(s) may be necessary. This crash may also be caused by the K.sti/K.si clocks stopping due to a hardware error such as an instruction parity error.

002014
ILTAPE timed-out waiting for Drive State Area

Facility: DEMON, ILTAPE

Explanation: ILTAPE requested exclusive access to a tape formatter for testing. ILTAPE timed out because the request did not complete within 60 seconds.

Action: Submit an SPR with a crash dump. Also include a summary of any tape error messages immediately preceding the crash. If a certain sequence of HSC controller operations caused this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is used.

002015
ILTAPE detected inconsistency after a command failure

Facility: DEMON, ILTAPE

Explanation: ILTAPE issued a command to the HSC tape diagnostic interface, but the command failed. In the process of preparing an error message, ILTAPE found that the command opcode was an illegal or unknown value.

Action: Submit an SPR with a crash dump. Also include a summary of any tape error messages immediately preceding the crash. If a certain sequence of HSC controller operations caused this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is used.

002016
ILTAPE detected inconsistency while restoring a TACB

Facility: DEMON, ILTAPE

Explanation: ILTAPE maintains a table of available tape access control blocks (TACBs). When a particular TACB is in use by the program, the associated table entry is set to zero. When finished with a TACB, ILTAPE stores the address of that TACB into one of the table entries containing a zero. While trying to return a TACB to the table, ILTAPE discovered that all table entries were nonzero, implying that no TACBs were in use.

Action: Submit an SPR with a crash dump. Also include a summary of any tape error messages immediately preceding the crash. If a certain sequence of HSC controller operations induced this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive or formatter is used.

002017
ILTAPE detected inconsistency in exception routine

Facility: DEMON, ILTAPE

Explanation: ILTAPE's internal flags indicated exclusive ownership of a drive state area, but the address of the K.sti/K.si control area was not available. When ILTAPE has exclusive ownership of a drive state area, the address of the K.sti/K.si control area should always be available. A software problem is the most likely cause of this crash.

Action: Submit an SPR with a crash dump. If a certain sequence of HSC controller operations caused this crash, include a description of that sequence. Also note if the problem occurs only when a particular tape drive is tested.

003001
Illegal format type specified

Facility: CERF

Explanation: An illegal format type was specified in an error message to CERF. R4 equals Format Type.

Action: Submit an SPR with a crash dump.

003002
Output length too long

Facility: CERF

Explanation: When CERF processed an MSCP error message, the FAO output of the text string was too long for CERF's buffer. R1 equals number of bytes output.

Action: Submit an SPR with a crash dump.

003003
Output length too long

Facility: CERF

Explanation: When CERF processed an out-of-band message, the FAO output of the text string was too long for CERF's buffer. R1 equals number of bytes output.

Action: Submit an SPR with a crash dump.

004002
BMB reserved but not found

Facility: DISK, many

Explanation: A big memory buffer (BMB) was reserved through a system function but was not found when the table of BMBs was searched. This indicates memory corruption or mismanagement of the BMB pool.

Action: Submit an SPR with a crash dump. Specify which process was running and make note of the activity on the system at the time of the crash.

004004
Invalid action byte in Connection Block

Facility: DISK, SDI

Explanation: The subprocess within the disk path that processes requests from the CI manager received a connection block with an invalid action byte. This indicates that an invalid structure was passed to the process, the structure was passed at the improper time, or memory was corrupted.

Action: Submit an SPR with a crash dump. Include the contents of user Register 2 in the crash dump.

004005
Datagram received from a connection

Facility: DISK, MSCP

Explanation: The main MSCP disk command server process received a nonsequenced message from some connection. This may indicate memory corruption or improper message reception. It may also indicate that an improper structure was passed to the process, possibly by the host software.

Action: Submit an SPR with a crash dump. Note all levels of host software running in the cluster.

004006
MSCP message size exceeded maximum

Facility: DISK, MSCP

Explanation: The main MSCP disk command server process received a sequenced message, with a length greater than the MSCP maximum, from some connection. This may indicate memory corruption or improper message reception. It may also indicate that an improper structure was passed to the process, possibly by the host software.

Action: Submit an SPR with a crash dump. Note all levels of host software running in the cluster.

004007
Invalid error signaled by K.ci

Facility: DISK, MSCP

Explanation: The main MSCP command server received an MSCP command packet, with invalid error bits set, from the K.ci. This may indicate memory corruption or improper message reception. It may also indicate that an improper structure was passed to the process, possibly by the host software.

Action: Submit an SPR with a crash dump. Note all levels of host software running in the cluster and the revision level of the K.ci microcode.

004010
Server queue on work queue with no items

Facility: DISK, many

Explanation: The main disk process received a subprocess work queue with no attached work items from the main work queue. This indicates either memory corruption or improper manipulation of items on the subprocess work queue. An invalid structure may have been queued to the main work queue.

Action: Submit an SPR with a crash dump. Note the currently running process.

004011
Invalid module number

Facility: DISK, many

Explanation: The main disk process detected an invalid module number when it tried to switch to a different internal process represented by the module number. This indicates that memory was corrupted or that an invalid structure was queued to the main work queue.

Action: Submit an SPR with a crash dump. Note the currently running process.

004013
State change to ONLINE requested via gatekeeper

Facility: DISK, SDI

Explanation: The state change processor within the sequential command gatekeeper received a DUCB extension requesting a state change to online. This crash indicates an improper use of the state change mechanism.

Action: Submit an SPR with a crash dump.

004014
Inconsistent drive state detected

Facility: DISK, SDI

Explanation: The state change processor within the sequential command gatekeeper received a DUCB extension containing a different state than the current state in the DUCB. This crash indicates an improper use of the state change mechanism.

Action: Submit an SPR with a crash dump.

004015
Improper state change for shadow member

Facility: DISK, SDI

Explanation: The sequential gatekeeper mechanism completes all outstanding I/O for a shadow unit before allowing a state change to take place on any of the members of the shadow set. This crash indicates the mechanism failed to operate properly.

Action: Submit an SPR with a crash dump.

004016
Disk Unit Table (DUT) inconsistency

Facility: DISK, many

Explanation: The disk server either tried to add a unit to the disk unit table (DUT) when it was already there or tried to remove a unit from the DUT that was not present. This crash indicates improper sequencing of actions to add a unit to or remove a unit from the DUT. This crash can also occur if the ordered list of DUCBs is corrupt.

Action: Submit an SPR with a crash dump.

004017
Invalid diagnostic HMB

Facility: DISK, MSCP

Explanation: The diagnostic interface within the disk path received a host message block (HMB) with a nonzero length field in the HM$LOF word. This indicates an invalid HMB received from some diagnostic or improper routing of the diagnostic HMB by the disk path.

Action: Submit an SPR with a crash dump. List any HSC utilities or diagnostics running at the time of the crash.

004021
Diagnostic release of disk unit while disk is online

Facility: DISK, MSCP

Explanation: A diagnostic or utility attempted to release a disk unit while the disk unit was still in the online state. HSC diagnostics and utilities must put the drive in the available state before releasing the unit for general use.

Action: Submit an SPR with a crash dump. Specify any HSC utilities or diagnostics running at the time of the crash.

004025
Invalid error recovery attempted on K.ci detected error

Facility: DISK, ERROR

Explanation: The disk server began error processing on an error detected by K.ci; however, the error recovery actions for that error were invalid.

Action: If this crash occurs immediately after a boot, try rebooting with a backup copy of the HSC software. Otherwise, submit an SPR with a crash dump.

004026
Invalid error recovery attempted on K.sdi/K.si detected error

Facility: DISK, ERROR

Explanation: The disk server began error processing on an error detected by a K.sdi/K.si; however, the error recovery actions taken by the disk server for that error were invalid.

Action: If this error appears to recur from the same K.sdi/K.si module, replace it.

004027
Invalid disk characteristics for operation

Facility: DISK, ERROR

Explanation: An arithmetic operation to compute some disk parameter caused an overflow or produced a result outside the allowed range. It is also possible, though unlikely, that a disk is supplying invalid characteristics to the HSC controller.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Further testing of the disk and attached requestor(s) may be necessary. If this error appears to recur from the same disk unit, repair it.

004030
S bit not set in Fragment Request Block error state

Facility: DISK, ERROR

Explanation: The S bit in the K control area port subarea for a drive in the fragment request block (FRB) error state was not set as expected. This logical inconsistency indicates improper manipulation of the port state.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Further testing of suspected requestor may be necessary. If this error appears to recur from the same K.sdi/K.si module, replace it. If no hardware problem exists, submit an SPR with a crash dump.

004031
DTSERQ not zero in Fragment Request Block error state

Facility: DISK, ERROR

Explanation: The FRB error queue in the Disk Rotational Access Table (DRAT) being processed by error recovery was not zero as expected upon returning from retrying a transfer in FRB error state. This logical inconsistency indicates improper manipulation of the port state.

Action: This error could be caused by a malfunctioning K.sdi/K.si module. Further testing of the suspected requestor may be necessary. If this error appears to recur from the same K.sdi/K.si, replace it. If no hardware problem exists, submit an SPR with a crash dump.

004032
Unable to get to Fragment Request Block error state

Facility: DISK, ERROR

Explanation: Error recovery was unable to place a disk port in the FRB error state to perform an error recovery operation. This crash can occur in an extremely unlikely compound error situation.

Action: Reboot the HSC controller. If this error persists, submit an SPR with a crash dump.

004033
Non-ECC/EDC errors remaining after ECC correction

Facility: DISK, ERROR

Explanation: ECC error correction should take place after all other errors, except EDC, have been corrected. This crash occurs because other error indicators are set after ECC correction takes place.

Action: Submit an SPR with a crash dump.

004034
Level B error recovery retry in wrong state

Facility: DISK, ERROR

Explanation: A level B error recovery retry operation was attempted without the drive port being in FRB error state.

Action: Submit an SPR with a crash dump.

004035
Level C error recovery retry in wrong state

Facility: DISK, ERROR

Explanation: A level C error recovery retry operation was attempted without the drive port being in FRB error state.

Action: Submit an SPR with a crash dump.

004036
Dialog Control Block state is busy with empty Dialog Control Block queue

Facility: DISK, ERROR

Explanation: The drive state indicator in the K control area indicates a K.sdi/K.si module is processing a dialog control block (DCB), but the DCB queue is empty. This could possibly indicate a malfunctioning K.sdi/K.si. If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log.

Further testing of the suspect requestor may be necessary. If this error appears to recur from the same K.sdi/K.si module, replace it. If no hardware problem exists, submit an SPR with a crash dump.

004037
Invalid error queue address in route

Facility: DISK, ERROR

Explanation: When the disk server attempted to route an FRB to an error queue, the error queue address in the route descriptor was invalid.

Action: Submit an SPR with a crash dump.

004040
Undefined error bit in error word

Facility: DISK, ERROR

Explanation: The error recovery routine IDENTIFY found an undefined bit in the error word stored by either a K.sdi/K.si module or K.ci module.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Customer Services. If no hardware problem exists, submit an SPR with a crash dump.

Further testing of the suspect requestor may be necessary. If this error appears to recur from the same K.sdi/K.si module, replace it. If no hardware problem exists, submit an SPR with a crash dump.

004041
No buffer found in Fragment Request Block when expected

Facility: DISK, ERROR

Explanation: The error recovery routine MAPBUF expected to map a buffer but found the buffer address to be zero.

Action: Submit an SPR with a crash dump.

004042
Fragment Request Block not in error state for level D I/O operation

Facility: DISK, ERROR

Explanation: A call to the error recovery subroutine LVLDIO was made without the port being in FRB error state.

Action: Submit an SPR with a crash dump.

004043
Stack too deep to save in thread block

Facility: DISK, ERROR

Explanation: A call to the error recovery subroutine LVLDIO was made with too many items on the stack to save in a thread block.

Action: Submit an SPR with a crash dump.

004044
Buffer not found for specified error

Facility: DISK, ERROR

Explanation: A call to the error recovery subroutine RCDHMX specified a buffer that was not in the list of buffers for the specified FRB.

Action: Submit an SPR with a crash dump.

004048
DRAT not found for Fragment Request Block retirement

Facility: DISK, ERROR

Explanation: While attempting to retire an FRB by simulating route completion, the error recovery subroutine RETIRE could not locate the associated DRAT.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Customer Services or submit an SPR. Note the K.sdi/K.si microcode revision levels.

This crash is caused by either overwritten memory or a malfunctioning K.sdi/K.si module. Further testing of requestors and HSC controller internal buses may be necessary. If this error appears to recur from the same K.sdi/K.si module, replace it. If no hardware problem exists, submit an SPR with a crash dump.

004060
DRAT queue not empty for shadow copy

Facility: DISK, MSCP

Explanation: After obtaining exclusive use of a drive, the shadow copy code found that the DRAT queue for the drive was not empty.

Action: Submit an SPR with a crash dump.

004051
Inconsistent result for repair operation

Facility: DISK, MSCP

Explanation: An impossible combination of results was found at the end of a shadow repair operation.

Action: Submit an SPR with a crash dump.

004052
Known drive not found in the Disk Unit Table (DUT)

Facility: DISK, MSCP

Explanation: When the disk server attempted to remove a known disk unit from the DUT, the unit was not found in that table.

Action: Submit an SPR with a crash dump. Note any utilities or diagnostics running at the time of the crash.

004055
Attempt to enable drive interrupt that is already enabled

Facility: DISK, many

Explanation: The ARM subroutine was called to enable the K.sdi/K.si to interrupt the disk server for certain drive state changes; however, interrupts were already enabled.

Action: Submit an SPR with a crash dump. Note the process running at the time of the crash.

004056
Attempt to enable drive interrupt when previous state change is pending

Facility: DISK, many

Explanation: The ARM subroutine was called to enable the K.sdi/K.si to interrupt the disk server for drive state changes; however, a drive state change was being processed.

Action: Submit an SPR with a crash dump. Note the process running at the time of the crash.

004057
Invalid drive state change requested

Facility: DISK, many

Explanation: The SCHSQM subroutine was called to schedule a state change operation for a drive that has been declared inoperative but whose state is still recorded as available.

Action: Submit an SPR with a crash dump. Note the process running at the time of the crash.

004070
Nonzero status for SUCCESSful Dialog Control Block

Facility: DISK, SDI

Explanation: Although a DCB (SDI command) completed with a status of SUCCESS, either the DCB error word indicated an error, or the SDI response opcode was invalid.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log. Contact Digital Customer Services. If no K.sdi/K.si hardware problem exists, submit an SPR with a crash dump. Note all K.sdi/K.si microcode revision levels. If this error appears to recur from the same K.sdi/K.si module, replace it. If no hardware problem exists, submit an SPR with a crash dump.

004072
Dialog Control Block state is busy with empty Dialog Control Block queue

Facility: DISK, many

Explanation: The drive state indicator in the K control area indicates a DCB is being processed by the K.sdi/K.si module, but the DCB queue is empty.

Action: If possible, get the number of the requestor involved from the last error log printed on the console or from the system error log.

Further testing of requestors, HSC controller internal buses, and the memory subsystem may be necessary. If this error appears to recur from the same K.sdi/K.si module, replace it. If no hardware problem exists, submit an SPR with a crash dump.

004073
K.sdi is not responding

Facility: DISK, SDI

Explanation: A K.sdi/K.si module failed to process an immediate DCB within a preset time. The lower byte of the second word on the stack is the failing requestor number.

Action: If possible, get the number of the requestor involved from the system error log. If the error persists, replace the K.sdi/K.si module.

004076
Wrong Port State for Dialog Control Block (DCB)

Facility: DISK, SDI

Explanation: Either the SDI interface was in use when not expected, the "process DCB" bit was not set when expected to be set, or the SDI interface received an error DCB when the disk port was not in the DCB error state.

Action: Submit an SPR with a crash dump.

004100
No thread block for operation

Facility: DISK, SDI

Explanation: A thread block was not available to the SDI interface in order to suspend the current process.

Action: Submit an SPR with a crash dump.

004101
Stack too deep to suspend process in thread block

Facility: DISK, SDI

Explanation: The DCBWAIT routine was called with too many words on the stack to suspend the process in a thread block.

Action: Submit an SPR with a crash dump.

004106
DRAT allocation failure

Facility: DISK, many

Explanation: There was not enough free control memory to allocate a DRAT for a specific drive type.

Action: Submit an SPR with the crash dump.

004107
A command did not complete after the drive was declared inoperative

Facility: DISK, MSCX

Explanation: Since no progress was made on executing a command after receiving several MSCP GET COMMAND STATUS commands to trace its progress, the drive was declared inoperative in an attempt to complete the command. The outstanding command however, still failed to complete within an additional timeout period.

Action: Submit an SPR with the crash dump. Note the drive type of the drive identified in the error message and any errors reported by the disk server prior to the crash.

004110
Get Command Status processing overflow

Facility: DISK, MSCX

Explanation: Processing of the MSCP GET COMMAND STATUS command determined that the calculated status will result in an overflow.

Action: Submit an SPR with the crash dump.

004111
A timer's link field values are inconsistent with its current operational state

Facility: DISK, many

Explanation: A timer was in a state that prevented adding or removing it from an active list.

Action: Submit an SPR with the crash dump.

004112
Inconsistent shadow member state detected

Facility: DISK, many

Explanation: A unit is incorrectly marked as a member of a shadow set, or the shadow unit links are inconsistent given the current state of the shadow unit.

Action: Submit an SPR with the crash dump.

004113
NO DRAT list is invalid

Facility: DISK, many

Explanation: The NO DRAT list was found to be invalid when declaring a drive inoperative.

Action: Submit an SPR with the crash dump.

004114
Connection closed after delay in attention processing

Facility: DISK, AVLATT

Explanation: While the disk server was waiting to acquire resources to send an attention message to the host, the associated disk connection closed.

Action: Submit an SPR with the crash dump.

004115
DCB address inconsistency

Facility: DISK, SDI

Explanation: While processing an error on a seek DCB, the current seek DCB address was inconsistent with the DCB address stored in the DRAT.

Action: Submit an SPR with the crash dump.

004116
Bad error completion queue in Dialog Control Block

Facility: DISK, MSCP

Explanation: An invalid error completion queue was found in the DCB when it was being set up for a seek operation. This indicates that after the previous seek operation, the DCB error completion queue was not properly restored before the DCB was retired.

Action: Submit an SPR with the crash dump.

004117
No DRAT was found on the K.sdi DRAT list when expected

Facility: DISK, many

Explanation: The DRAT list was empty when the disk server expected to find a DRAT queued to the K.sdi/K.si DRAT list.

Action: Submit an SPR with the crash dump.

004120
Too many DRATs in use during an enhanced ESE transfer operation

Facility: DISK, MSCP

Explanation: The number of DRATs in use for a transfer to an ESE in the enhanced mode of operation has exceeded the maximum value allowed.

Action: Submit an SPR with the crash dump.

004121
Replacement Block Number (RBN) access during an ESE enhanced mode transfer

Facility: DISK, MSCP

Explanation: The disk server is preparing to perform an enhanced performance mode transfer operation to an RBN on an ESE, but the ESE has no RBNs.

Action: Submit an SPR with the crash dump.

004122
Invalid DRAT bit set for ESE in enhanced performance mode of operation

Facility: DISK, MSCP

Explanation: A DRAT on the K.si DRAT list did not have the "Set D-bit on completion" flag set as expected. This indicates that the DRAT representing the enhanced mode transfer was probably not set up properly.

Action: Submit an SPR with the crash dump.

004123
DCB K.si list inconsistency for ESE in enhanced mode of operation

Facility: DISK, many

Explanation: More than one nonseek DCB was queued to the K.si DCB work queue during I/O rundown on an ESE in enhanced mode of operation. Only one nonseek DCB is expected to be active at a time while running in enhanced mode.

Action: Submit an SPR with the crash dump.

004124
Buffer count inconsistency for ESE in enhanced mode of operation

Facility: DISK, MSCP

Explanation: During ESE enhanced mode transfer processing, the DRAT buffer count indicated that the DRAT was full. However, the "DRAT full" flag was not set. This message is classified as a software inconsistency in enhanced ESE mode.

Action: Submit an SPR with the crash dump.

004125
Too many disk ports

Facility: DISK (LOADER)

Explanation: You have connected more disk ports to the HSC controller than the disk server can support.

Action: Refer to the configuration guidelines for the HSC. If the HSC is configured properly, contact Digital Customer Services.

004126
Invalid fragmentation loop count while fragmenting a transfer

Facility: DISK, MSCP

Explanation: When breaking down a transfer command into smaller fragments, a disk server count indicates that there are more FRBs to be initialized; however, the pointer to these FRBs is zero. This condition can only occur if the FRB count or the FRB pointer has been corrupted.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which problem occurs.

004127
Invalid deferred seek queue

Facility: DISK, MSCP

Explanation: The disk server, in trying to queue a new master FRB to the deferred seek queue, has discovered that the list is corrupt.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which problem occurs.

004130
No buffer descriptor for primary revectored block

Facility: DISK, ERROR

Explanation: When trying to save the buffer descriptor associated with a primary revectored block, the HSC software disk server has discovered that the buffer descriptor pointer is zero.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which problem occurs.

004131
Invalid return searching for outstanding command

Facility: DISK, MSCX

Explanation: The HSC software disk server received an MSCP GET COMMAND STATUS command from a host node and called a routine to search for the outstanding command. This routine returns to a location based on where the outstanding command is found. In this case, the return was invalid.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which the problem occurs.

004132
Active Disk Rotational Access Table on port for which format operation is scheduled

Facility: DISK, MSCP

Explanation: The disk server received a request to do a format operation on a particular port; however, the port is already processing a DRAT.

Action: Submit an SPR with the crash dump. If the problem is reproducible, note conditions and configurations under which the problem occurs.

005000
User-invoked CRASH

Facility: CRASH

Explanation: The user entered the CRASH command at the HSC> prompt.

Action: If this crash occurred due to a reason other than entering the CRASH command, submit a Software Performance Report (SPR) with the crash dump. Otherwise, no action is necessary.

005001
ECC self-diagnostic string too big for FAO

Facility: ECC

Explanation: A self-diagnostic string generated for the ECC process was too big to print with the allocated formatted ASCII output (FAO) buffer. This crash can only occur if the self-diagnostic code is present and enabled. The self-diagnostic code is not enabled for distributed base levels.

Action: Submit an SPR with a crash dump.

005002
No ECC errors to correct

Facility: ECC

Explanation: An FRB without any errors was sent to the error correction code (ECC) process.

Action: Submit an SPR with a crash dump.

005003
Cannot allocate Extended Function Control Block to print self–diagnostic messages

Facility: ECC

Explanation: The ECC process failed to allocate an extended function request block (XFRB) for printing messages during self-diagnostics.

Action: Submit an SPR with a crash dump.

005004
ECC found more than a 10-bit symbol error

Facility: ECC

Explanation: The ECC process received a buffer containing more than a 10-bit symbol error. Error recovery processing should never pass on such a buffer.

Action: Submit an SPR with a crash dump.

006000
This class of crashes is for tape path software inconsistency errors

Facility: TAPE, TFxxxx

Explanation: A software inconsistency error occurred.

Action: Submit an SPR with a crash dump. Specify the utilities or diagnostics active at the time of the crash.

006001
An STI GET LINE STATUS failed

Facility: TAPE, TFATNAVL

Explanation: When issued to the tape data channel, the STI command GET LINE STATUS returned with a failure. This command should not fail when issued to a working tape data channel. General Register 5 points to the windowed K control area for the tape data channel in question. Offset KG$SLT points to the tape requestor in question.

Action: Verify that the K.sti/K.si tape data channel is working; if so, submit an SPR with a crash dump.

006003
Received an Illegal Connection Block (CB) from the CIMGR

Facility: TAPE, TFCI

Explanation: A connection block (CB) with an illegal opcode was sent to the tape server. General Register 1 points to the windowed address of the CB in question. General Register 2 contains the opcode in question.

Action: Submit an SPR with a crash dump. Include the CB structure.

006004
An illegal diagnostic Opcode was received

Facility: TAPE, TFDIAG

Explanation: A diagnostic HMB with an illegal opcode was sent to the tape diagnostic interface. General Register 3 points to the windowed diagnostic host message block (HMB). General Register 1 contains the opcode in question.

Action: Submit an SPR with a crash dump. Specify the utilities or diagnostics active at the time of the crash. Include the HMB structure.

006005
Diagnostics trying to acquire assigned drive state area

Facility: TAPE, TFDIAG

Explanation: Diagnostics are trying to acquire the previously assigned drive state area. General Register 3 points to the windowed control memory address of the host message block (HMB). General Register 2 points to the tape formatter control block (TFCB).

Action: Submit an SPR with a crash dump. Specify the diagnostics or utilities active at the time of the crash. Include the HMB, TFCB, and tape drive control block (TDCP) structures.

006006
Inconsistencies during drive state area acquisition

Facility: TAPE, TFDIAG

Explanation: The software context word KT$SFW is not equal to the tape formatter control block (TFCB) address and/or the DIALOG list head is nonzero when diagnostics are trying to acquire the drive state area. General Register 0 points to the windowed K control area. General Register 2 points to the tape formatter control block (TFCB).

Action: Submit an SPR with the crash dump. Indicate the utilities or diagnostics active at the time of the crash. Include the TFCB structure.

006007
No Block Header buffer supplied by BACKUP

Facility: TAPE, TFDIAG

Explanation: BACKUP did not supply the initial block header buffer descriptor. General Register 3 points to the windowed host message block (HMB) address. General Register 5 should point to the buffer descriptor and, in this case, should be zero.

Action: Submit an SPR with the crash dump. Include details of the backup operation. Include the HMB (command packet) structure.

006010
No buffers supplied by the disk server for an HSC backup operation, yet the status was successful

Facility: TAPE, TFDIAG

Explanation: No disk data block buffers were supplied in the HMB for the backup operation yet the status was successful. General Register 3 points to the windowed control memory address of the HMB in question. General Register 0 should point to the buffer descriptor list for the backup operation.

Action: Submit an SPR with a crash dump. Include details of the BACKUP operation. Include the host message block (HMB) (command packet) structure.

006011
Could not allocate an XFRB

Facility: TAPE, TFLIB

Explanation: The tape server could not allocate an extended function control block (XFRB) through ALOCB, a CRONIC system service.

Action: Submit an SPR with a crash dump.

006012
Required CIMGR functionality not yet implemented

Facility: TAPE, TFMSCP

Explanation: The host sent the tape server a command packet with an opcode that was not a sequenced message. General Register 5 is the opcode received. General Register 3 is the windowed control memory address of the command packet received (host message block).

Action: Submit an SPR with a crash dump. Indicate the host software version. Include the HMB (command packet) structure.

006013
Required CIMGR functionality not yet implemented

Facility: TAPE, TFMSCP

Explanation: The tape server received a host command packet longer than allowed (36 bytes). General Register 4 is the size of the command packet received. General Register 3 is the windowed control memory address of the command packet in question.

Action: Submit an SPR with a crash dump. Indicate the host software version. Include the HMB (command packet) structure.

006014
Required CIMGR functionality not yet implemented

Facility: TAPE, TFMSCP

Explanation: The tape server received a host command packet with a status that is currently illegal. General Register 3 points to the windowed control memory address of the command packet in question. Offset HM$ERR is the field in question.

Action: Further testing of HSC controller hardware, particularly the K.ci, may be necessary. If no hardware problem exists, submit an SPR. Indicate the host software version and include the HMB (command packet) structure.

006015
Could not find correct Tape Drive Control Block (TDCB) pointer

Facility: TAPE, TFSEQUEN

Explanation: A call to remove a host's access to a drive resulted in the tape server searching the current chain of tape drive control blocks (TDCBs) in that host's HCB. Inability to find the correct TDCB pointer resulted in this crash.

General Register 4 points to the tape drive control block (TDCB) trying to have host access removed. General Register 3 points to the windowed control memory address of the HMB. Offset HM$CTX in the HMB points to the host disk block (HDB). Offset HDB.TDCB in the HDB points to the TDCB.

Action: Submit an SPR with a crash dump.

006016
Unable to allocate an HDB

Facility: TAPE, TFSEQUEN

Explanation: The tape server's attempt to add a host access, which requires allocation of a host drive block (HDB), failed for lack of resources.

Action: Submit an SPR with a crash dump.

006017
Tape formatter does not support chosen density

Facility: TAPE, TFSEQUEN

Explanation: The tape formatter does not support a density that the HSC controller supports. General Register 4 points to the TDCB for the drive in question.

Action: Submit an SPR with a crash dump. Include the host software version and tape formatter revision. Also include the TDCB structure, host software version, and tape formatter revision.

006020
An invalid density is set in the Tape Drive Control Block (TDCB)

Facility: TAPE, TFSEQUEN

Explanation: An invalid density was set in the TDCB. General Register 4 points to the TDCB in question.

Action: Submit an SPR with a crash dump. Include the HMB structure.

006021
Read-reverse emulation not flagged

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation code without read-reverse emulation being flagged. Read-reverse emulation is flagged in the TDCB at offset TD.FLAGS bit TDF.RREVEM. General Register 3 points to the windowed control memory address of the HMB. General Register 4 points to the TDCB for the drive in question. General Register 2 points to the tape formatter control block (TFCB) for the formatter in question.

Action: Submit an SPR with a crash dump. Include the following structures: HMB, TDCB, and TFCB.

006022
Route pointer for read-reverse emulation zero

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation code with a record data truncated error without having the route pointer set in the HMB. General Register 3 points to the windowed control memory address of the HMB in question.

Action: Submit an SPR with a crash dump. Include the HMB structure.

006023
Requested transfer larger than 64 Kb

Facility: TAPE, TFSEQUEN

Explanation: The requested transfer size for a read reverse is larger than 64 kilobytes. General Register 3 points to the windowed control memory address of the host message block (HMB) in question and offset HP.BC indicates the transfer size requested.

Action: Submit an SPR with a crash dump. Include the HMB structure.

006024
Read-reverse emulation not flagged

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation short retry code without read-reverse emulation being flagged. Read-reverse emulation is flagged in the tape drive control block (TDCB) at offset TD.FLAGS bit TDF.RREVEM. General Register 3 points to the windowed control memory address of the HMB. General Register 4 points to the TDCB for drive in question. General register 2 points to the tape formatter control block (TFCB) for the formatter in question.

Action: Submit an SPR with a crash dump. Include the following structures: HMB, TDCB, and TFCB.

006025
Read-reverse emulation not flagged

Facility: TAPE, TFSEQUEN

Explanation: The tape server entered the read-reverse emulation long retry code without read-reverse emulation being flagged. Read-reverse emulation is flagged in the tape drive control block (TDCB) at offset TD.FLAGS bit TDF.RREVEM. General Register 3 points to the windowed control memory address of the host message block (HMB). General Register 4 points to the tape drive control block (TDCB) for the drive in question. General Register 2 points to the tape formatter control block (TFCB) for the formatter in question.

Action: Submit an SPR with a crash dump. Include the following structures: HMB, TDCB, and TFCB.

006026
KT$SEM is less than or equal to zero

Facility: TAPE, TFSEQUEN

Explanation: The K control area offset KT$SEM is zero. General Register 3 points to the K control area in question.

Action: Submit an SPR with a crash dump. Include the K control area structure.

000031
No available stacks

Facility: TAPE, TFSERVER

Explanation: There are no available stacks for a process trying to suspend.

Action: Submit an SPR with a crash dump.

000033
Top of user stack for a resume is not set to server return

Facility: TAPE, TFSERVER

Explanation: The top of the user stack on a process resume is not set to the server return routine.

Action: Submit an SPR with a crash dump.

000035
Hit end of subprocess list

Facility: TAPE, TFSERVER

Explanation: The tape server scheduler hit the end of its work list, but it should never reach the end of this list.

Action: Call Digital Customer Services or submit an SPR with the crash dump.

000037
Trying to Queue a DCB to the K.sti when it is blocked for error

Facility: TAPE, TFST1

Explanation: The tape server is trying to queue a command to the head of the K.sti dialog queue while the requestor is blocked for error. This error condition must be cleared before inserting commands to the head of this queue. General Register 5 has the windowed K control area KT$. General Register 4 has the DCB that is being queued to the head.

Action: Submit an SPR with a crash dump. Include the HMB and DCB.

000041
A Get Line Status DCB operation timed out

Facility: TAPE, TFSTI

Explanation: A Get Line Status DCB timed out after two minutes. Since this DCB is only issued to the requestor and not the formatter it should complete right away.

Action: This usually indicates a problem in the tape data channel. The tape requestor slot in question is given as the second word on the stack. If no hardware problem exists, submit an SPR.

000043
Buffer descriptor address missing

Facility: TAPE, TXREVERSE

Explanation: The next address is missing from the linked list of buffer descriptors in an FRB. General Register 5 points to the fragment request block (FRB) in question. Offset F$BFHD points to the buffer descriptor list in question.

Action: Submit an SPR with a crash dump. Include the FRB structure.

006044
Unexpected Fragment Request Block (FRB) error received

Facility: TAPE, TFERR

Explanation: The tape server received an error from a software station rather than a hardware station. General Register 5 points to the fragment request block (FRB) in error.

Action: Submit an SPR with a crash dump. Include the FRB structure.

006045
Unknown Fragment Request Block (FRB) error received

Facility: TAPE, TFERR

Explanation: An unidentifiable error is flagged in a FRB.

Action: Submit an SPR with a crash dump. Include the FRB structure.

006046
K.ci did not return a Fragment Request Block (FRB)

Facility: TAPE, TFERR

Explanation: Transfer request blocks (TRBs) have associated FRBs that point to data buffers. When a TRB is received in error, the FRBs must be deallocated. If an FRB is held by K.ci and not returned within 20 seconds, this crash occurs.

Action: Check the K.ci. If no hardware problem exists, submit an SPR with a crash dump.

006047
Invalid down count occurred on a Host Message Block (HMB) chain

Facility: TAPE, TFERR

Explanation: In the process of *catching* HMBs in order to restart them as part of TRB error recovery, an invalid down count operation takes place. Check to ensure control memory is not corrupted by the end of the chain. General Register 5 points to the HMB.

Action: Submit an SPR with a crash dump. Include the HMB.

006050
A software inconsistency was found while purging TRB's

Facility: TAPE, TFERR

Explanation: While purging TRBs, consistency checks are done on the sequence numbers of all the TRBs being removed. The dependencies on associated DCBs are checked as well. The associated DCB for a TRB about to be removed wasn't found so this inconsistency error occurs.

Action: Submit an SPR with a crash dump.

006052
No free control blocks available to re-transfer

Facility: TAPE, TFERR

Explanation: An attempt to collect free control blocks (FCBs) during transfer error recovery has failed after waiting the timeout period for a free FCB. This is a software controller problem. Either the HSC is fully saturated and in a deadlock situation, or the free control block list has become corrupt.

Action: Submit an SPR with a crash dump.

006054
Unable to locate a FCB

Facility: TAPE, TFSEQUEN

Explanation: The tape server attempted to bring a drive online, but the attempt failed because of lack of resources.

006056
Out of timer pool

Facility: TAPE, TFSEQUEN

Explanation: The tape server attempted to initiate a rewind, but failed due to lack of timer pool.

006060
Invalid record size supplied by Backup

Facility: TAPE, TFDIAG

Explanation: HSC BACKUP supplied an invalid record size; 8, 16, and 32 kilobytes are the only record sizes supported.

006075
Reserved DCB resource is zero

Facility: TAPE, TFSTI

Explanation: A software inconsistency occurred where an internal resource for a DCB was zero.

Action: Submit an SPR with a crash dump.

006076
Reserved DCB resource is zero

Facility: TAPE, TFSTI

Explanation: A software inconsistency occurred where an internal resource for a DCB was zero.

Action: Submit an SPR with a crash dump.

007000
This class of crashes includes CIMGR software consistency errors

Facility: CIMGR, many

Explanation: This message indicates the existence of a software consistency error.

Action: Submit an SPR with a crash dump. Specify the utilities or diagnostics active at the time of the crash.

007001
Received a sequence message without a credit

Facility: CIMGR, CIDIRECT

Explanation: The SCS$DIRECT process received a sequence message in a host message block (HMB) flagged by the K.ci as not having a credit for the connection. General Register 1 has the address of the HMB in error.

Action: Submit an SPR with a crash dump. Include the HMB.

007002
Failed to acquire a control block from K.ci

Facility: CIMGR

Explanation: The POLLER process could not obtain a control block from the K.ci to resend a timed-out STACK datagram.

Action: Further testing of the HSC subsystem may be necessary, particularly the available control memory. If no hardware problem exists, submit an SPR with a crash dump.

007003
K.ci is hung

Facility: CIMGR

Explanation: During the polling interval (60 seconds), the CIMGR ensures K.ci is still running. This trap indicates it is not.

Action: Further testing of the HSC subsystem may be necessary, particularly the K.ci. If no hardware problem exists, submit an SPR with a crash dump.

007004
K.ci detected an unrecoverable error and stopped

Facility: CIMGR

Explanation: K.ci sent its control area to the CIMGR exception process. K.ci does this whenever it detects a nonrecoverable hardware error.

Action: Further testing of the HSC subsystem may be necessary, particularly the K.ci and data memory. If no hardware problem exists, submit an SPR with a crash dump.

007005
K.ci path status check failed

Facility: CIMGR

Explanation: K.ci did not respond to a path status check within 30 seconds.

Action: Further testing of the HSC subsystem may be necessary, particularly the K.ci. If no hardware problem exists, submit an SPR with a crash dump.

007006
System name is corrupted

Facility: CIMGR

Explanation: During initialization, the CIMGR discovered the system name in the SCT was corrupted.

Action: Release the Online switch (out) on the HSC controller. Reboot the HSC controller by holding the Fault switch in until the State indicator blinks. This will bypass using the SCT on the boot device. Run SETSHO to reset the system name and ID, then reboot the HSC again before pushing in the Online switch on the front panel.

007007
HMB received with wrong number of BMB

Facility: CIMGR

Explanation: CIMGR received an HMB with the wrong number of BMBs, or CIMGR detected an inconsistent state. General Register 0 points to the HMB.

Action: Further testing of the HSC subsystem may be necessary, particularly the K.ci. If no hardware problem exists, submit an SPR with a crash dump.

007011
Connection incarnation inconsistent

Facility: CIMGR

Explanation: While a connection is in the process of opening, the incarnation of that connection is flagged as formative. The final step of opening the connection is to remove the flag. This crash indicates the flag was prematurely removed, indicating a state inconsistency for the connection. General Register 2 points to the connection block (CB).

Action: Submit an SPR with a crash dump. Include the CB.

007012
Connection incarnation mismatch

Facility: CIMGR

Explanation: The incarnation of an opening connection is kept in both the connection block (CB) and the connection block vector table. As a connection opens, a check is made to ensure these incarnations agree. A disagreement indicates a dangling reference to an old incarnation of the connection.

General Register 2 points to the connection block (CB).

Action: Submit an SPR with a crash dump. Include the CB.

007013
Inconsistent connection state due to a VC closure

Facility: CIMGR

Explanation: CIMGR attempted an illegal state transition on a connection. The state transition was initiated by a virtual circuit (VC) closure. General Register 2 points to the CB.

Action: Submit an SPR with a crash dump. Include the CB.

007014
Unable to retrieve resource from K.ci during a disconnect

Facility: CIMGR

Explanation: During a disconnect, the CIMGR was unable to retrieve the resources from the K.ci associated with the credits on that connection.

Action: Submit an SPR with a crash dump.

007015
K.ci did not respond to notification of a VC closure

Facility: CIMGR

Explanation: The K.ci did not respond to notification of a VC closure within the 30-second time limit. This crash occurs if the response times out.

Action: Further testing of the HSC subsystem may be necessary, particularly the K.ci. If no hardware problem exists, submit an SPR with a crash dump.

007016
Illegal connection state

Facility: CIMGR

Explanation: CIMGR detected an illegal CB state. General Register 2 points to the CB.

Action: Submit an SPR with a crash dump. Include the CB.

007017
Attempt to deallocate a Connection Block without an incarnation

Facility: CIMGR

Explanation: A CB did not have a valid incarnation at the time it was deallocated.

Action: Submit an SPR with a crash dump. Include the CB.

007020
Failure to retrieve SCS resources from K.ci

Facility: CIMGR

Explanation: When CIMGR tried to allocate resources for use across a virtual circuit, the count of data memory resources was incorrect. The HMB for serializing VC traffic must have two BMBs. General Register 0 points to the HMB.

Action: Submit an SPR with a crash dump. Include the HMB.

007021
The count of waiters for virtual circuit resources went negative

Facility: CIMGR

Explanation: While processing the list of waiters for virtual circuit transmission resources, CIMGR detected a nonempty list to indicate a negative number of waiters. General Register 1 points to the system block (SB).

Action: Submit an SPR with a crash dump. Include the SB.

007022
Invalid BMB address

Facility: CIMGR

Explanation: An HMB arrived at the resource collector with an invalid BMB address attached to it.

Action: Enter the SHOW REQUESTORS command to view the K.pli microcode revision level. If it is less than revision 45, contact your Digital Customer Services representative for the update. Otherwise submit an SPR with the crash dump and note the disk configuration.

007023
SCS buffer retrieval failure

Facility: CIMGR, CISUBRS

Explanation: Attempt to retrieve SCS buffer failed when SB$SBS indicated it was available.

Action: Submit an SPR with the crash dump.

007024
I/O rundown did not complete 10 minutes after virtual circuit closure

Facility: CIMGR

Explanation: After closing a VC, the CIMGR starts a ten minute timer to allow servers to complete I/O rundown. If the timer expires, the CIMGR crashes the HSC to make it possible to reestablish all VCs. because the previously established connections were not closed, a virtual circuit could not be reopened.

Action: Submit an SPR with the crash dump.

07025
Unable to obtain an HMB structure to send a START datagram to host to close VC

Facility: CIMGR, CISUBRS

Explanation: When the HSC controller needs to close a virtual circuit, the CIMGR module issues a START datagram. If the CIMGR is unable to obtain an HMB after thirty tries at one-second intervals, this exception is issued.

Action: Submit an SPR with a crash dump and console log. Note if the problem occurred under heavy load.

07026
Unable to obtain a BMB structure to send a START datagram to host to close VC

Facility: CIMGR, CISUBRS

Explanation: When the HSC controller needs to close a virtual circuit, the CIMGR module issues a START datagram. If the CIMGR is unable to obtain a BMB after thirty tries at one-second intervals, this exception is issued.

Action: Submit an SPR with a crash dump and console log. Note if the problem occurred under heavy load.

07027
Unable to obtain a System Block when attempting to send a START datagram to host to close VC

Facility: CIMGR, CISUBRS

Explanation: When the HSC controller needs to close a virtual circuit, the CIMGR module issues a START datagram. This exception code is issued if the CIMGR is unable to obtain a system block (SB).

Action: Submit an SPR with a crash dump and console log.

012001
Connection Block not found

Facility: DUP

Explanation: When DUP receives an HMB, DUP tries to find a reference to the connection block in the DG$ structures. DUP was unable to find a reference to the connection block (CB).

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012002
Illegal BMB count

Facility: DUP

Explanation: The HMB (MSCP packet carrier) has an illegal number of BMBs allocated. DUP allows only one BMB. Therefore, the HMB is invalid. The third word of the stack contains the value in HM$CN—the count of the number of BMBs.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack. The second word of the stack contains the windowed address of the HMB.

012003
Illegal HMB Opcode

Facility: DUP

Explanation: The opcode specified in the HM$LOF field of the HMB was not equal to HML$RM. HMB opcodes must indicate the HMB is for a sequenced message. (Received sequence message over connection; HML$RM=000000)

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack. The second word of the stack contains the illegal opcode.

012004
Illegal HMB Error

Facility: DUP

Explanation: The error specified in the HM$ERR field of the HMB was not equal to 0, HME$EC, or HME$NC. The second word of the stack contains the value in the HM$ERR field. (Extra credits received; HME$EC=10. No credits received; HME$NC=4)

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012021
Invalid Connection Block

Facility: DUP

Explanation: The DUP process received a connection block with an invalid value in the CB$ACT field. The CB$ACT field contains the action to be performed by the DUP server.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack. The second word of the stack contains the contents of the CB$ACT field.

012024
Bad Down Count

Facility: DUP

Explanation: DUP initiates a return of the endpacket to the host by down counting the reference counter in the related control block. The down count should return a one. If the down count did not decrement the reference counter to 1, DUP crashes the HSC controller. The second word of the stack is the value of the counter following the down count.

Action: Submit an SPR with an exception dump or startup message indicating the contents of the stack.

012036
Connection Broken

Facility: DUP

Explanation: While DUP was preparing to send a message to the K.ci, the connection to the host was broken. The connection was broken after DUP did an extensive check to ensure the connection existed.

Action: Submit an SPR with a crash dump.

020001
Illegal Cache Diagnostic Opcode

Facility: CACHE, CAUPD

Explanation: The cache server update processing code received a message whose operation code was not within the range of operation codes recognized by the cache server.

Action: Submit an SPR with the crash dump.

020002
Illegal HMB Block Type

Facility: CACHE

Explanation: The block type specified in the host message block (HMB) operation code is not one recognized by the cache server. The only valid HMB block type code is HML$TP.

Action: Submit an SPR with the crash dump.

020003
Illegal HMB Opcode

Facility: CACHE

Explanation: The operation code specified in the HM$LOF field of the HMB did not indicate a sequenced message. All messages received by this facility of the cache server must be sequenced.

Action: Submit an SPR with the crash dump.

020004
Illegal HMB Request Type

Facility: CACHE

Explanation: This cache server processes diagnostic and utility requests only. However, the message received was not one of these types.

Action: Submit an SPR with the crash dump.

020020
Illegal Error Condition

Facility: MSCP

Explanation: The M.cache module indicated the presence of an error condition, but the cache server could not find the error condition in any of the hardware-software interface data structures.

Action: Submit an SPR with the crash dump. Ask Customer Services to perform diagnostics on the M.cache module.

020040
Insufficient Free Cache Block Pages

Facility: CAUPD

Explanation: The M.cache module supplies more cache memory than the cache server is able to map to its data structures. This condition may be caused by faulty M.cache hardware.

Action: Submit an SPR with the crash dump.

020060
No AE. found for this IN.

Facility: CASH

Explanation: The cache server data structures appear to be corrupt. In this case, the cache server cannot find an array entry for a particular index node.

Action: Submit an SPR with the crash dump.

020100
Data Buffer/Sector Count Inconsistency

Facility: CASH, MSCP

Explanation: The cache server has detected a data buffer/sector count inconsistency. The sector count and number of attached data buffers should agree in value, but they do not.

Action: Submit an SPR with the crash dump.

042001
FAO message buffer overflow

Facility: DIRECT

Explanation: The program DIRECT was attempting to output the formatted directory end message, but the length of that message was longer than the allotted FAO output buffer.

Action: Submit an SPR with a crash dump.

043001
Wrong HMB received when trying to bring source online

Facility: DKCOPY

Explanation: DKCOPY sent a HMB to the disk server requesting the source unit be brought online in a shadow set. When the completion queue of this HMB was checked, it pointed to a different, and incorrect, HMB. This is crash $CDKCOPY+SRC_ONL_HMB.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the previous HMB.

043002
Bad down count when trying to bring source online

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to bring the source unit online. When the online operation completed, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid. This is crash $CDKCOPY+SRC_ONL_CNT.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the counter.

043003
Wrong HMB received when trying to issue a GET COMMAND STATUS to the target unit of the copy operation

Facility: DKCOPY

Explanation: DKCOPY sent a HMB to the disk server requesting it to send a GET COMMAND STATUS (GCS) command to the target unit. When the completion queue of this HMB was checked, it pointed to a different, and incorrect, HMB. This is crash $CDKCOPY+TGT_GCS_HMB.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the previous HMB.

043004
Bad count value discovered when trying to issue a GET COMMAND STATUS to the target unit

Facility: DKCOPY

Explanation: DKCOPY issued a GCS command operation to the target unit to check on the progress of the copy operation. When the GCS end message was returned to DKCOPY from the disk server, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid. This is crash $CDKCOPY+TGT_GCS_CNT.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the counter.

043005
Bad downcount when trying to bring target unit online

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to bring the target unit online and initiate a shadow copy operation. When the operation completed, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid. This is crash $CDKCOPY+TGT_ONL_CNT.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the counter.

043006
Bad downcount when trying to issue abort command to target unit

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to abort the shadow copy operation. When the abort operation completed, DKCOPY decremented a count. The count value, however, was found to be invalid. This is crash $CDKCOPY+TGT_ABO_CNT.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the counter.

043007
Wrong host message block HMB received after issuing AVL command to shadow unit

Facility: DKCOPY

Explanation: DKCOPY sent a HMB to the disk server requesting that the shadow unit used to facilitate the copy operation be made available. When the completion queue of this HMB was checked, it pointed to a different, and incorrect, HMB. This is crash $CDKCOPY+SHA_AVL_HMB.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the previous HMB.

043010
Bad down count when trying to issue AVL command to shadow unit

Facility: DKCOPY

Explanation: DKCOPY issued a command to the disk server to put the created shadow unit into an available state. When this command completed, DKCOPY decremented a count of outstanding commands. The count value, however, was found to be invalid. This is crash $CDKCOPY+SHA_AVL_CNT.

Action: Submit an SPR with a crash dump. The top of the stack equals the crash code. The second word points to the counter.

046001
Missing disk rotational access table (DRAT) for FORMAT TRACK operation

Facility: FORMAT

Explanation: A DRAT that was to be put on its completion queue was not found on the DRAT queue.

Action: Submit an SPR with a crash dump.

051001
An XFRB was not acquired to print messages

Facility: SETSHO, SSMAIN

Explanation: SETSHO was not able to acquire an XFRB. A crash was initiated because the lack of an XFRB prevents communication between the HSC controller and the console. This is crash $CSETSHO+NOXFRB.

Action: Submit an SPR with a crash dump.

051002
Failed to properly send HMB to K.ci

Facility: SETSHO, SSMAIN

Explanation: SETSHO sent an HMB to the K.ci and a crash was initiated because SETSHO did not receive confirmation of the HMB from the K.ci within the required time. This is crash $CSETSHO+CIHMB.

Action: Submit an SPR with a crash dump.

051003
Too many characters intended for console printout

Facility: SETSHO, SSMAIN

Explanation: SETSHO called formatted ASCII output (FAO) routines and generated more characters than the allocated buffer would allow. The maximum buffer size is 510 characters. This is crash $SETSHO+PNTOVF. R1 points to the string size.

Action: Submit an SPR with a crash dump.

051004
The SCT (System Control Table) crossed a page boundary

Facility: SETSHO, SSMAIN

Explanation: The SCT must remain within one page in memory. The crash may indicate an incorrectly padded SCT. This is crash $SETSHO+SCTXPG.

Action: Submit an SPR with a crash dump.

051101
Failed in sending HMB to disk server for SET Dn [NO]HOST

Facility: SETSHO

Explanation: SETSHO sent an HMB to the disk server to set a disk drive to HOST or NOHOST access. The crash was initiated because the confirmation of this command was not received within the required time. This is crash $CSETSHO+SETDSK.

Action: Submit an SPR with a crash dump.

051102
Failed in sending HMB to tape server for SET Tn [NO]HOST

Facility: SETSHO

Explanation: SETSHO sent an HMB to the tape server to set a tape drive to HOST or NOHOST access. The crash was initiated because the confirmation of this command was not received within the required time. This is crash $CSETSHO+SETTAP.

Action: Submit an SPR with a crash dump.

051201
Failed in sending HMB to disk server for SHOW Dn

Facility: SETSHO

Explanation: SETSHO sent an HMB to the disk server to show a specified disk drive. The crash was initiated because the confirmation of this command was not received within the required time. This is crash $CSETSHO+SHODSK.

Action: Submit an SPR with a crash dump.

051202
Failed in sending HMB to tape server for SHOW Tn

Facility: SETSHO

Explanation: SETSHO sent an HMB to the tape server to show a specified tape drive. The crash was initiated because the confirmation of this command was not received within the required time. This is crash $CSETSHO+SHOTAP.

Action: Submit an SPR with a crash dump.

051203
SCT crash context table contained too many characters

Facility: SETSHO

Explanation: The SCT crash context table contained too many characters. When SETSHO called formatted ASCII output (FAO) routines, it generated more characters than the allocated buffer size would allow. The maximum buffer size is 510 characters. This is crash $SETSHO+CSHOVF. R1 points to the string size.

Action: Submit an SPR with a crash dump. To clear the condition, reset the SCT to factory settings by holding in the Fault button while pressing the Init button. You may release the Fault button when the "INIPIO-I Booting ..." message appears. The HSC controller should remain offline until the SCT is reset with user-supplied values.

052001 ($CDWMATH)
Doubleword math not consistent

Facility: SINI

Explanation: During calculation and allocation of control blocks, which are allocated as doublewords, the number of words in the control blocks was not a doubleword multiple. R0 points to the memory descriptor (MD).

Action: Submit an SPR with a crash dump.

052002 ($CDIV10)
Divide operation set overflow

Facility: SINI

Explanation: During allocation of control blocks (set as 80 percent of available control memory), a divide operation set the PSW overflow bit.

Action: Submit an SPR with a crash dump.

052003 ($CMUL8)
Multiply operation set overflow

Facility: SINI

Explanation: During allocation of control blocks (set as 80 percent of available control memory), a multiply operation set the PSW overflow bit.

Action: Submit an SPR with a crash dump.

061001
XCALL stack overflow

Facility: DIAGINT

Explanation: The DDUSUB transfer routines use a stack allocated from common pool for XCALLs (cross-address space calls) from the disk server. The low word of this stack is initialized to a special value that should never change. This crash occurs when the routine DDUTIO is called. The low word of the stack contains a value different than the initialization value. The most probable cause of the crash is corruption by the process running.

Action: Submit an SPR with a crash dump. Note the diagnostics or utilities running at the time of the crash.

062001 ($CNOWINDOW)
Process does not have windows declared

Facility: SUBLIB, ERTYP

Explanation: A process requesting an out-of-band error log be issued by the ERTYP$ service in SUBLIB does not have windows declared in its process control block (PCB) declaration. A window set is required to use this service.

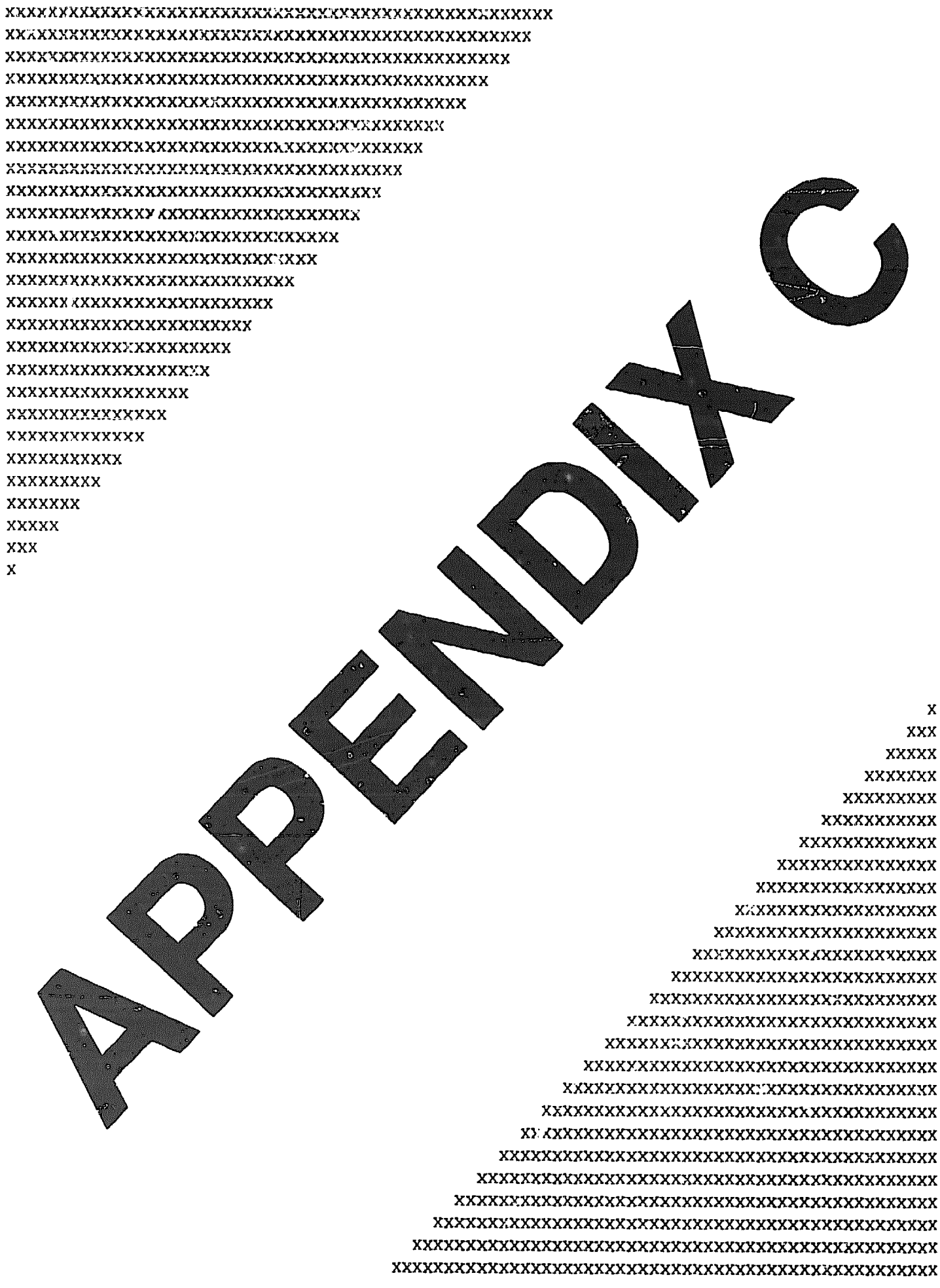
Action: Submit an SPR with a crash dump.

062003 ($NKCNTAR)
Data channel control table inconsistency

Facility: SUBLIB

Explanation: A table of bandwidth values has an entry that does not correspond to a known data channel control area.

Action: Submit an SPR with the crash dump. Include the disk and tape configuration.


APPENDIX C

C
Generic Error Log Fields

C.1 Introduction

Some fields described on HSC console message printouts are generic, regardless of error type.

The following example is a typical printout of the error log fields. Table C–1 describes the error fields. In this example, the error log fields listed after the Event field are optional and are shown in Table C–1 for completeness. Refer to Chapter 8 for information on these optional fields.

```
ERROR-S Bad Block Replacement (Success) at 28-Feb-1991 18:05:37.1
        Command Ref #    0A66000D
        RA81 unit #      77.
        Err Seq #        166.
        Format Type      09.
        Error Flags      80
        Event            002B
        Replace Flags    8000
        LBN              205.
        Old RBN          0.
        New RBN          5.
        Cause Event      00E8
ERROR-I End of Error
```

Example C–1 Error Log Fields Example

Table C–1 Generic Error Log Fields

Field	Description
ERROR-x	The x represents the severity level of the error message. Severity levels are E for error, S for success, W for warning, I for informational, and F for fatal. Other information given in this line includes an English description of the event code, the date, and the time.
Command Ref #	This is the hexadecimal MSCP command number that caused the reported error. This field is set to zero if the error does not correspond to a specific outstanding command.
Err Seq #	This is the decimal sequence number of this error log message since the last time the MSCP server lost context. This is basically a sequential number count of the error log messages since the MSCP/TMSCP server established a connection with the host. The field is set to zero if the MSCP/TMSCP server does not implement error log sequence numbers.

Table C–1 (Cont.) Generic Error Log Fields

Field	Description
Format Type	This hexadecimal number describes the detailed format of the error log message. The number basically defines the "type" of error packet. Refer to Table 8–11 for a description of these error format types.
Error Flags	This hexadecimal number indicates bit flags, collectively called error log message flags, used to report various attributes of the error. Refer to Table C–2 for a description of the error flags.
Event	This hexadecimal number identifies the specific error or event being reported by this error log message. This code consists of a 5-bit major event code and an 11-bit subcode. The event codes and their meanings are listed in Table C–3.

C.2 Error flags

Table C–2 defines the MSCP/TMSCP error flags that can be set in an error log. The first column is the bit number that is set. The second column is the bit mask hex number. The third column is the format description of the error flag.

Table C–2 Error Flags

Bit Number	Bit Mask Hex	Format Description
7	80	If set, the operation causing this error log message has successfully completed. The error log message summarizes the retry sequence necessary to successfully complete the operation.
6	40	If set, the retry sequence for this operation continues. This error log message reports the unsuccessful completion of one or more retries.
5	20	This is MSCP-specific. If set, the identified logical block number (LBN) needs replacement.
4	10	This is MSCP-specific. If set, the reported error occurred during a disk access initiated by the controller bad block replacement process.
1	2	If set, the data contained in this error log message is informational only. The information is not necessarily related to any single command or event and does not signify the occurrence of an error.
0	1	If set, the error log sequence number has been reset by the MSCP server since the last error log message sent to the receiving class driver.

C.3 MSCP/TMSCP Status or Event Codes

Event codes are values reported to error logs and are equivalent to the status code reported to a host in an MSCP command end packet, if the error is related to an outstanding command.

The following table is a sequential list of MSCP and TMSCP event codes. Each event code cross references to an error description. The first column is the event code number in hexadecimal. The second column references the class of the error. The third column is the expanded description that matches the event code.

In the description field, a "status code only" statement means that the code is only reported as an error in an MSCP command end message and is not used as an error event code. The statement "event code only" means that the code is used only to report an error event in an error log and is not used as an MSCP status code.

Table C–3 MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
0000	Success	Normal; used only as a status code.
0001	Invalid Command	Invalid message length. Used only as a status code. Other invalid command subcode values should be referenced as follows (note that this is combined with the status code): offset * 256. + code where *offset* is the command message offset value for the command field in error and *code* is the symbol for the "invalid command" status code. The Invalid Command status code value is one.
0002	Command Aborted	Command aborted. Used only as a status code.
0003	Unit–Offline	Unit unknown or online to another controller. Used only as a status code.
0004	Unit–Available	Unit available. Used only as a status code.
0005	Disk Media Format Error	Sector in the RCT or FCT was written with the forced error modifier. Used only as a status code.
0007	Compare Error	Used only as an event code when the error occurs during a read-compare or write-compare operation.
0008	Data Error	Disk—Sector was written with the force error modifier. Used only as a status code. Tape—Long gap encountered.
0009	Host Buffer Access Error	The cause for this host buffer access error is not available to the HSC controller. The controller was unable to access a host buffer to perform a transfer but has no visibility into the cause of the error. Used only as a status code.
000A	Controller Error	Reserved for host-detected command timeout logging. This error is never reported by a controller.
000C	Shadow Set Status Has Changed	Disk—Shadow set status has changed. A shadow member has been removed by the HSC controller from a controller-based shadow set. Tape – Formatter error.
000D	Tape BOT Encountered	BOT encountered.
000E	Tape Mark Encountered	Tape mark encountered.
0010	Tape Record Data Truncated	Record data truncated, data transfer operation.
0013	Tape LEOT Detected	LEOT detected.
0014	Disk Bad Block Replacement Completion	Bad block successfully replaced. Used only as an event code.
0020	Success	Disk—Spindown ignored. Used only as a status code. Tape—Unload ignored.
0023	Unit-Offline	Disk—No volume mounted or drive disabled via RUN/STOP switch. Unit is in known substate. Used only as a status code. Tape—No media mounted, disabled via switch setting, or online to another controller.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
0029	Host Buffer Access Error	Odd transfer address. Used only as a status code.
002A	Controller Error	SERDES overrun or underrun error. Either the drive is too fast for the controller, or more typically, a controller hardware fault has prevented controller microcode from keeping up with data transfer to or from the drive.
002B	Drive Error	Drive command timeout. For drives, the controller timeout expired for either a Level 2 exchange or the assertion of Read/Write Ready after an Initiate Seek.
0034	Disk Bad Block Replacement Completion	Block verified good—not a bad block. Used only as an event code.
0035	Media Loader Error	Loader command timeout. The key length is too short for the specified key type.
0036	Informational	Media Quantity Log. Used only as an event code.
0040	Success	Still connected. Used only as a status code.
0043	Unit–Offline	Unit is inoperative. Used only as a status code. For SDI drives, the controller has marked the drive inoperative due to an unrecoverable error in a previous Level 2 exchange, the drive's C1 flag is set, or the drive has a duplicate unit identifier.
0044	Unit–Available	Shadow set copy in progress. Used only as a status code. This subcode is returned while a controller-based shadow copy operation is in progress if any of the following circumstances should occur: • When any command is issued directly to the copy recipient. • When the controller-dependent number of copy operations in progress limit has been reached. • When another host has already initiated a copy operation to the unit.
0045	Media Format Error	Invalid header detected reading an RCT or FCT block. The subsystem read an invalid or inconsistent header for the requested RCT or FCT sector. For recoverable errors, this code implies that a retry of the transfer read a valid header. For unrecoverable errors, this code implies that the header was never read correctly, even with transfer retries. Causes of an invalid header include a header mis-sync, a header sync timeout, and an inconsistent header.
0048	Disk Data Error	Invalid header. The subsystem read an invalid or inconsistent header for the requested sector. For recoverable errors, this code implies a retry of the transfer read a valid header. For unrecoverable errors, this code implies the subsystem attempted nonprimary revectoring and determined the requested sector was not revectored. As an example, the RCT indicates the sector is not revectored. Causes of an invalid header include header mis-sync, header sync timeout, and an inconsistent header.
0049	Host Buffer Access Error	Odd byte count. Used only as a status code.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
004A	Controller Error	EDC error. The sector was read with correct or correctable ECC and an invalid EDC. A fault probably exists in the ECC logic of either this controller or the controller that last wrote the sector. This can also be caused by any K module (including the K.ci) writing bad EDC into data memory.
004B	Drive Error	Controller-detected transmission error. For SI drives, the controller detected an invalid framing code or a checksum error in a Level 2 response from the drive.
0054	Disk Bad Block Replacement Completion	Replacement failure—The REPLACE command or its analog failed. For the HSC controller, this means that an error occurred trying to format the headers of a bad block to indicate it is replaced. Used only as an event code.
0055	Media Loader Error	Controller-detected transmission error. The controller does not implement the specified key type.
0056	Informational	Unload/spin down statistics. Used only as an event code.
0065	Media Format Error	Data sync not found (data sync timeout) reading an RCT or FCT sector.
0068	Disk Data Error	Data sync not found (data sync timeout).
0069	Host Buffer Access Error	Nonexistent memory error.
006A	Controller Error	Inconsistent internal control structure. A high-level check detected an inconsistent data structure. For example, a reserved field contained a nonzero value, or the value in a field was outside its valid range. This error almost always implies the existence of a microcode problem.
006B	Disk Drive Error	Positioner error (mis-seek). The drive reported a seek operation was successful, but the controller determined the drive had positioned itself to an incorrect cylinder.
0074	Disk Bad Block Replacement Completion	Replacement failure—inconsistent RCT. Used only as an event code.
0075	Media Loader Error	Controller detected protocol error.
0080	Success	Duplicate unit number. Used only as a status code.
0083	Unit Offline	Duplicate unit number. Used only as a status code.
0084	Unit-Available	No members in shadow set. An MSCP ONLINE command was addressed to a virtual unit of an existing shadow set from which all members have been removed. Used only as a status code.
0085	Media Format (Shadowing) Error	Characteristics or protection mismatch for controller-based shadow member. Used only as a status code. The geometry or write-protect state of a physical unit being added to a shadow set does not match that of the shadow set, or the physical unit's write-protect (data safety) unit flag is set.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
0088	Disk Data Error	Correctable error in ECC field. A transfer encountered a correctable error where only the ECC field was affected. All data bits were correct, but a portion of the ECC field was incorrect. The severity of the error (the number of symbols in error) is unknown. If the number of symbols in error is known, an "n symbol" ECC error subcode should be returned instead. Used only as an event code.
0089	Host Buffer Access Error	Host memory parity error.
008A	Controller Error	Internal EDC error. A low-level check detected an inconsistent data structure. For example, a microcode-implemented checksum or vertical parity (hardware parity is horizontal) associated with internal sector data was inconsistent. This error usually implies a fault in the memory addressing logic of one or more controller processing elements. It can also result from a double bit error or other error exceeding the error detection capability of the controller hardware memory checking circuitry.
008B	Drive Error	Lost Read/Write Ready during or between transfers. For SI drives, Read/Write Ready dropped when the controller attempted to initiate a transfer or at the completion of a transfer, and Read/Write Ready had previously been asserted. This usually results from a drive-detected transfer error, where an additional error log message containing the drive-detected error subcode may be generated.
0094	Disk Bad Block Replacement Completion	Replacement failure—drive access failure. One or more transfers specified by the replacement algorithm failed. Used only as an event code. On the HSC controller, this code generally indicates that the drive has been declared inoperative due to some kind of drive transfer problem.
0095	Media Loader Error	Loader-detected error
00A5	Media Format Error	Disk—The disk is not formatted with 512-byte sectors. Used only as a status code. The disk FCT indicates it is formatted with 576-byte sectors, although either the controller or the drive supports only 512-byte sectors. Tape—Block mode device not formatted for tape operations.
00A9	Host Buffer Access Error	Invalid page table entry.
00AA	Controller Error	LESI adapter card parity error on input (adapter to controller).
00AB	Drive Error	Drive clock dropout. For SI drives, either data or state clock was missing when it should have been present. This is usually detected by means of a timeout.
00B4	Disk Bad Block Replacement Completion	Replacement failure, no replacement block available. Replacement was attempted for a bad block, but a replacement block could not be allocated. For example, the volume's RCT is full. Used only as an event code.
00C5	Disk Media Format Error	Disk not formatted or FCT corrupted. Used only as a status code. The disk FCT indicates the disk is not formatted in either 512- or 576-byte mode.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
00C9	Host Buffer Access Error	Invalid buffer name. The key in the buffer name does not match the key in the buffer descriptor, the V bit in the buffer descriptor is clear, or the index into the Buffer Descriptor Table is too large.
00CA	Controller Error	LESI adapter card parity error on output (controller to adapter).
00CB	Drive Error	Lost Receiver Ready for transfer. For SI drives, Receiver Ready was negated when the controller attempted to initiate a transfer or did not assert at the completion of a transfer. This includes all cases of the controller timeout expiring for a transfer operation (Level 1 real-time command).
00D4	Disk Bad Block Replacement Completion	Replacement failure; recursion failure. Two successive RBNs were bad. Used only as an event code.
00E5	Disk Media Format Error	Uncorrectable ECC error reading an RCT or FCT sector. A transfer to an RCT or FCT sector without the Suppress Error Correction modifier encountered an ECC error exceeding the correction capability of the subsystem error correction algorithms, or a transfer with the Suppress Error Correction modifier encountered an ECC error of any severity.
00E8	Data Error	Disk—Uncorrectable ECC error. A transfer without the Suppress Error Correction modifier encountered an ECC error exceeding the correction capability of the subsystem error correction algorithms, or a transfer with the Suppress Error Correction modifier encountered an ECC error of any severity. Tape—Unrecoverable read error.
00E9	Host Buffer Access Error	Buffer length violation. The number of bytes requested in the MSCP or TMSCP command exceeds the buffer length as specified in the buffer descriptor.
00EA	Controller Error	LESI adapter card *cable in place* not asserted.
00EB	Disk Drive Error	Drive-detected error. For SDI drives, the controller received a get status or unsuccessful response with EL set, or the controller received a response with the DR flag set and it does not support automatic diagnosis for that drive type.
0100	Success	Already online. Used only as a status code.
0103	Unit-Offline	Unit disabled by field service or diagnostic. Used only as a status code. For SDI drives, the drive DD flag is set.
0105	Disk Media Format Error	RCT corrupted. The RCT search algorithm encountered an invalid RCT entry. The subcode may be returned when replacing a block, when revectoring a block, or when bringing a unit into the unit online state.
0106	Write-Protected	Unit is data safety write-protected. Used only as a status code.
0108	Disk Data Error	One-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
0109	Host Buffer Access Error	Access control violation. The access mode specified in the buffer descriptor is protected against the PROT field in the PTE.
010A	Controller Error	Controller overrun or underrun. The controller attempted to perform too many concurrent transfers, causing one or more of them to fail due to a data overrun or underrun.
010B	Drive Error	Controller-detected pulse or state parity error. For SI drives, the controller detected a pulse error on either the state or data line, or the controller detected a parity error in a state frame.
0125	Disk Media Format Error	No replacement block available. Replacement of a faulty block was attempted, but a replacement block could not be allocated (that is, the RCT is full). This code may be returned during actual replacement and when an interrupted replacement is completed as part of bringing a unit into the Unit-Online state. Used only as an event code.
0128	Disk Data Error	Two-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.
012A	Controller Error	Controller memory error. The controller detected an error in an internal memory, such as a parity error or nonresponding address. This code applies only to errors not affecting the ability of the HSC to properly generate end and error log messages. Errors affecting end and error log messages are not reported via MSCP. For most controllers, this code is returned only for controller memory errors in data or buffer memory and noncritical control structures. If the controller has several such memories, the specific memory involved is reported as part of the error address in the error log message
0145	Disk Media Format Error	No multicopy protection. All but one copy of a block in a multicopy structure are bad. The disk should be reformatted or replaced at the earliest convenient time. Used only as an event code.
0148	Disk Data Error	Three-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.
014A	Controller Error	Insufficient resources for shadowing operation. The controller is unable to honor a request to create a controller-based shadow set or to add an additional member to an existing shadow set. This is due to the lack of internal resources to support the new entity. Used only as a status code.
014B	Drive Error	Controller-detected protocol error. For SI drives, a Level 2 response from the drive had correct framing codes and checksum but was not a valid response within the constraints of the SI protocol. The response had an invalid opcode, was an improper length, or was not a possible response in the context of the exchange.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
0168	Disk Data Error	Four-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.
016B	Drive Error	Drive failed initialization. For SI drives, the drive clock did not resume following a controller attempt to initialize the drive. This implies the drive encountered a fatal initialization error.
0188	Disk Data Error	Five-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.
018A	Controller Error	Host interface hardware error. The controller detected an error that indicates a fault in the host interface hardware. For the HSC controller, this means that a PLI transmit or receiver buffer parity error occurred.
018B	Drive Error	Drive ignored initialization. For SI drives, the drive clock did not cease following a controller attempt to initialize the drive. This implies the drive did not recognize the initialization attempt.
01A8	Disk Data Error	Six-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.
01AB	Drive Error	Receiver Ready collision. For SI drives, the controller attempted to assert its Receiver Ready when the Receiver Ready of the drive was still asserted.
01C8	Disk Data Error	Seven-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.
01E8	Disk Data Error	Eight-symbol ECC error. A transfer encountered a correctable ECC error with the specified number of ECC symbols in error. The number of symbols in error roughly corresponds to the severity of the error.
0200	Success	Still online. Used only as a status code.
0203	Unit-Offline	Exclusive use. Used only as a status code.
0220	Tape Success	Still online, unload ignored.
0400	Success	Disk—Incomplete replacement. Used only as a status code. Tape—EOT encountered.
0404	Unit-Available	Already in use. Used only as a status code.
044B	Tape Drive Error	Controller retry limit exhausted.
0800	Success	Invalid RCT. Used only as a status code.
1000	Success	Read only volume format. Used only as a status code.
1006	Write-Protected	Unit is software write protected. Used only as a status code.
2006	Write-Protected	Unit is hardware write protected. Used only as a status code.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

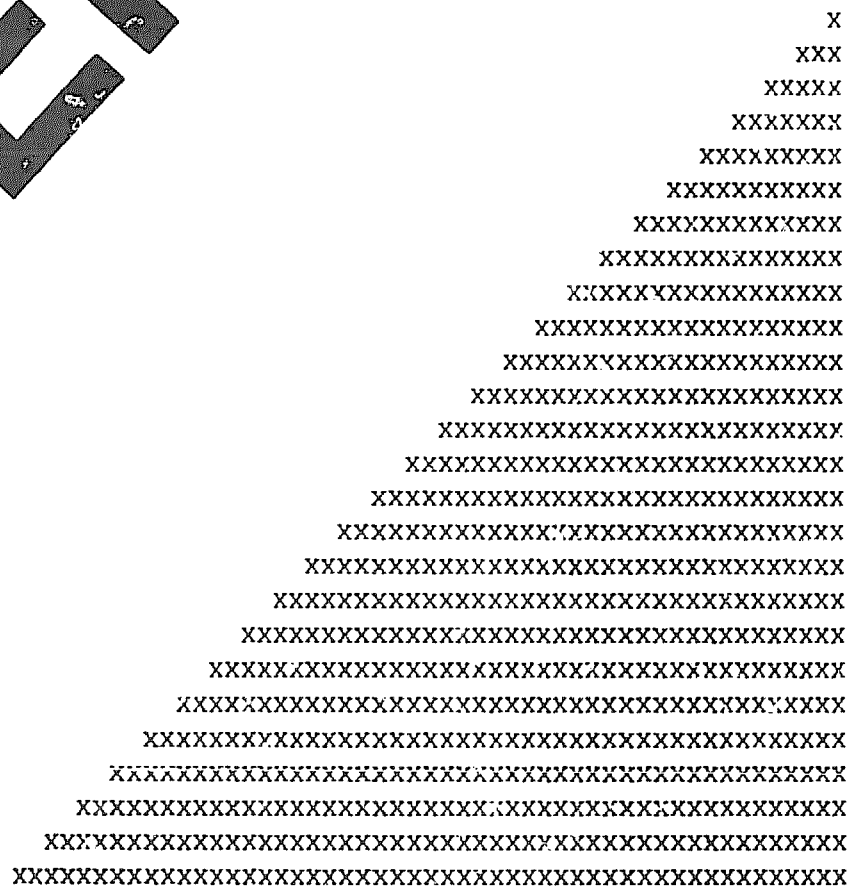
Event Code Hex	Class	Description
F3AA	Tape Controller Error	Unknown K.sti/K.si error.
FCAA	Tape Controller Error	Word rate clock timeout. The K.sti/K.si detected the loss of clocks from a drive during a transfer.
FCEA	Tape Controller Error	Receiver Ready not asserted at start of transfer. The HSC controller is ready to start a transfer by sending the formatter a Level 1 command, and the formatter does not have Receiver Ready asserted.
FD2A	Tape Controller Error	Data ready timeout. This controller did not detect data ready from the formatter within 5 ms after sending it a Level 1 command.
FD6A	Tape Controller Error	Acknowledge not asserted at start of transfer. The HSC controller is ready to start a transfer by sending the formatter a Level 1 command, and the formatter does not have Acknowledge asserted.
FDEC	Tape Formatter Error	Could not get extended drive status.
FE0C	Tape Formatter Error	Could not get formatter summary status while trying to restore tape position.
FE2A	Tape Controller Error	Record EDC error. On a read from tape operation the EDC calculated by the K.sti/K.si did not match the EDC generated by the tape formatter.
FE2B	Tape Drive Error	Could not set byte count.
FE4B	Tape Drive Error	Could not write tape mark.
FE6B	Tape Drive Error	Could not set unit characteristics.
FE8A	Tape Controller Error	Lower Processor timeout. The upper processor in the K.sti/K.si detected the lower processor had stopped and restarted it.
FE8B	Tape Drive Error	Unable to position to before L EOT .
FEAB	Tape Drive Error	Rewind failure.
FECB	Tape Drive Error	Could not complete online sequence.
FEEB	Tape Drive Error	Erase gap failed.
FF0B	Tape Drive Error	ERASE command failed.
FF0C	Tape Formatter Error	TOPOLOGY command failed.
FF2C	Tape Formatter Error	Cache busy with LS set.
FF4C	Tape Formatter Error	Could not clear CDL with CCE (clear formater errors) command.
FF8C	Tape Formatter Error	Cache data lost.
FF31	Tape Drive Position Lost	Retry limit exceeded while attempting to restore tape position.
FF68	Tape Data Error	Formatter retry sequence exhausted.
FF6A	Tape Controller Error	Lower processor error. A bit was set in the lower processor error register. Bits included in the lower processor error register are data bus NXM, data SERDES overrun, data bus overrun, data bus par err, data pulse missing, and sync real-time par err.

Table C–3 (Cont.) MSCP/TMSCP Status or Event Codes

Event Code Hex	Class	Description
FF6B	Tape Drive Error	Tape drive requested error log.
FF6C	Tape Formatter Error	Formatter requested error log.
FF71	Tape Drive Position Lost	Formatter-detected position lost.
FF88	Tape Data Error	Controller transfer retry limit exceeded.
FF8A	Tape Controller Error	Buffer EDC error. The K.sti/K.si detected an EDC error on the data buffer it read from memory on a Write operation.
FFA8	Tape Data Error	Host requested retry suppression on a K.sti/K.si-detected error.
FFAA	Tape Controller Error	Data overflow due to pipeline error. No data buffers in HSC data memory were available when the K.sti/K.si needed one during a data transfer.
FFAC	Tape Formatter Error	Cannot do CFE (clear formatter errors).
FFC8	Tape Data Error	Reverse retry currently not supported.
FFCB	Tape Drive Error	Could not position for (formatter) retry.
FFCC	Tape Formatter Error	Cannot clear formatter errors.
FFD1	Tape Drive Position Lost	Formatter and HSC controller disagree on tape position.
FFE8	Tape Data Error	Host requested retry suppression on a formatter-detected error.
FFEB	Tape Drive Error	Cannot clear drive errors.
FFEC	Tape Formatter Error	Could not get formatter summary status during transfer error recovery.
FFF1	Tape Drive Position Lost	Controller-detected position lost.



APPENDIX D



D

Interpretation of Status Code Bytes

D.1 Introduction

This appendix lists all possible codes each K (such as, K.ci or data channel) can generate after detecting a fatal error. Only K-detected errors are listed here.

When a K detects a fatal error, it puts a code in its status register and performs a Level 7 control bus interrupt to the P.io. This interrupt causes the HSC controller to trap through location 134 and crash. The crash message contains the status codes from all Ks in the *Status of requestors (1-9):* field.

The following shows a printout example from a K detected error. In this case, as in many others, the crash was not caused by the K but was detected by the K which forced the crash. Section D.2 explains this crash is detail. For additional explanations of the fields in the crash message, refer to Appendix B.

```
-* SUBSYSTEM EXCEPTION *-     V# Y10B       HSC70 HSC002
       at 18-Jan-1986 01:15:14.50  up   0 00:08:46.20

User   PC: 0027360 caused by (134   ) Kint
PSW: 140000

KBCTRL active, PCB addr = 102636

R0-R5:
024302   047632   000020   047626   0000000   141404

Kernel SP: 000774

Kernel Stack:

005046 000004 053354 046022 001012 050476 050476 000000
047062 047466 047466 000000 047264 000000 055352 000000

User SP: 023346

User Stack:
052525 052525 025252 025252 025252 025252 025252 025252
025252 025252 025252 025252 025252 025252 025252 025252

KPAR(0-7):
000440 000640 001040 001440 002040 001240 000240 177600

KPDR(0-7):
077506 077506 177506 077506 077406 077506 077506 077506

UPAR(0-7):
000440 000640 001040 001440 002040 001240 000240 177600
```

Example D–1 (Cont.) K-detected Error Example

```
UPDR(0-7):
007406 007406 177406 007406 007406 007406 007406 100016

MMSR(0-2): 000017 000020 037654

Window index reg: 000015

Window Bus Reg: 140105

WADR(0-7):
160004 161004 162004 163004 164004 165004 166034 167034

Translated WADR(0-7):
001401 0014C1 001401 001401 001401 001401 001407 001607

Error regs: 170024  000077

Status of requestors (1-9):
000177 000002 000002 000377 000377 000377 000377 000377 000203

(PC-6) TO (PC):
104002 012600 000003 011505
Control area for slot #000001
Control area address: 022010
Register area contents:
000000
000000
100307
040003
104000
140143
100007
000552
000200
012002
000000
000533
104000
000401
022000
000000
000001
000003
004572
000003
017176
000003
000063
000150
000000
000000
000372
040003
002501
002431
000000
000000
000000
```

Example D–1 K-detected Error Example

D.2 K-Detected Error Example Examination

Notice the third line of Example D-1 states the crash was caused by (134) Kint. The 134 indicates a K detected a fatal problem and interrupted the P.ioj with a level 7 interrupt.

In this crash, Requestor 1 (the K.ci) status shows a 000177. The K.ci detected a fatal condition. The two digits in the status code are 77 (from the 000177 failure code).

Tables D–2 and D–3 provide additional information regarding status code 77. The description of this error indicates the HSC controller received a HOST CLEAR command from a host node. The description for the 77 status also shows that the node number of the host which sent the HOST CLEAR is found in R17.

To find R17, look at the *Register area contents:* field on the second page of the example. The first entry in the register area contents is always the Q register from the K. The Q register contains important information for some crashes. The second entry is R0. In the example, count in *octal* up to R17 (remember the first entry is the Q register). The contents of R17 are 000001. Many of the error descriptions in the following tables indicate additional information exists in one of these registers.

Notice other entries below R17 in the register area contents. In the K.sdi, K.sti, and K.si register areas, these other entries are RAM0 through RAM17, and they sometimes contain important information. On the K.ci, these entries are not significant for troubleshooting crash messages.

D.3 Normal Operation Status Codes for K-Requestors

After successfully completing all internal diagnostics, the status code register contains a code to indicate the type of requestor. Table D–1 lists these status codes.

Table D–1 Normal Operation Status Codes for K-requestors

Status Code (Octal)	Description
001	K.ci host interface with proper parity
002	K.sdi/K.si disk data channel module with proper parity
004	K.si data channel module with proper parity and no microcode loaded
007	8-port K.si data channel module with microcode loaded.
075	Secondary P.io module with proper parity
203	K.sti/K.si tape data channel module with proper parity
205	4-port K.si data channel module with disk microcode loaded
206	4-port K.si data channel module with tape microcode loaded
210	K.ci2 host interface with no microcode loaded
211	K.ci2 host interface with microcode loaded
212	8-port K.si data channel module with no microcode loaded
277	P.ioc module with proper parity
377	No requestor present

Status codes other than those listed in Table D–1 indicate that the K-requestor has detected an error. Error status is indicated if bit 6 of the K status bits is set.

D.4 K-Detected Failure Code Analysis

The following sections aid field service in analyzing the K-detected failure codes through use of the status code tables. This appendix contains one status code table for each type of K.

- Table D–2 describes the K.ci host interface status codes for the HSC40, HSC50, and HSC70 controllers during initialization, and applies only to requestor number 1.
- Table D–3 describes the K.ci host interface status codes for the HSC60 and HSC90 controllers during initialization, and applies only to requestor number 1.
- Table D–4 describes the K.sdi disk data channel module status codes.
- Table D–5 describes the K.sti tape data channel module status codes.
- Table D–6 describes the K.si data channel module status codes with disk microcode loaded.
- Table D–7 describes the K.si data channel module status codes with tape microcode loaded.
- Table D–8 describes the K.si data channel module status bytes when microcode loading has failed.

The use of the status code tables requires information about the type of requestor involved. In order to determine which requestor detected the error, check the *Status of requestors (1-9):* field in the crash message. This field shows the status register contents of all requestors present in the subsystem.

NOTE
The registers referred to in this appendix are not general registers, but the internal K registers. All status codes followed by an asterisk (*) are hardware-detected errors. More detailed information for these errors is found in the appropriate sequencer error register.

Because the K.ci is always requestor 1, a K.ci-detected error always shows in the far left position in the *Status of requestors (1-9):* field of the message. In any other position, the type of requestor must be determined.

Count over the *Status of requestors (1-9):* field to the status contents showing an error (this is the requestor number). When the HSC reboots, enter **SHOW REQUESTOR** at the HSC> prompt to see whether the requestor detecting the error is a K.sdi, K.sti, or K.si. Find the number of the data channel that found the error in the displayed response. This display shows whether that requestor number is either a K.sdi, K.sti, or K.si.

NOTE
If the HSC is not operational or the requestor in question fails initialization self-tests, check the module utilization label above the card cage to determine whether the involved requestor number is a K.sdi, K.sti, or K.si.

Tables in this appendix consider only the rightmost two octal characters in failure code. Use the appropriate table (dependent upon requestor type) to find the meaning of the status code.

Table D–2 K.ci Status Code Bytes For HSC40, HSC50, and HSC70 Controllers During Initialization

Status Code (Octal)	Description
00	Two conditions cause failure of the 2911 sequencer test upon powerup or reinitialization. In one case, the requestor sent status back to the Pio while Init was asserted. In the other case, the sequencer had already released the Init signal but the sequencer failed to reach the point in its code where it could change the status bits. A common reason for this status code is from an HSC false power fail crash dump. In this type of crash dump (IOT through 20), all requestors present report a 00 status code.
01	2901 ALU test failed upon powerup or reinitialization.
02	Data bus (DBUS) test failed upon powerup or reinitialization.
03	Control bus (CBUS) test failed upon powerup or reinitialization.
04	CROM test failed upon powerup or reinitialization.
06	K.pli RAM test failed upon powerup or reinitialization.
07	PLI interface test failed upon powerup or reinitialization.
10	Packet buffer test failed upon powerup or reinitialization.
11	LINK board test failed upon powerup or reinitialization.
12	Control bus/memory error occurred during a lock cycle while the K.ci was attempting to locate the K-Init packet in control memory upon powerup or reinitialization.
13	K.ci could not find a properly formatted K-Init packet in control memory after completing powerup/Init diagnostics.
14	An error was detected by the upper (control) sequencer. While attempting to update the next buffer pointer in an FRB, the pointer was found to be zero (illegal). R11 contains the FRB address.
15 *	An error was detected by the upper (control) sequencer. (See NOTE at the end of this table.)
16	An error was detected by the upper (control) sequencer. The control stream found a structure on its own work queue which is not an HMB or FRB. R11 contains the structure address.
17	An error was detected by the upper (control) sequencer. While constructing a slot (SNDDAT, REQDAT) from an FRB, the FRB address was found to be zero (illegal). R12 contains the slot address.
20 *	An error was detected by the upper (control) sequencer. (See NOTE at the end of this table.)
21	An error was detected by the upper (control) sequencer. A buffer allocate request was initiated without sufficient buffers on the allocated queue in the control area to satisfy the request. R11 contains the FRB address.
22	An error was detected by the upper (control) sequencer. The queue head for an allocated send buffer was zero.
23 *	An error was detected by the upper (control) sequencer. (See NOTE at the end of this table.)

Table D–2 (Cont.) K.ci Status Code Bytes For HSC40, HSC50, and HSC70 Controllers During Initialization

Status Code (Octal)	Description
24	An error was detected by the lower (control) sequencer. The lower sequencer encountered an inconsistent internal data structure. R2 contains the message slot address.
25	An error was detected by the lower (control) sequencer. During the RTNDAT routine, the lower sequencer finds a zero (illegal) FRB address.
27	An error was detected by the lower (control) sequencer. This error occurs when the lower sequencer polling loop calls a routine which adds or removes big message block (BMB) pointers to or from the BMB chain, if the queue that is supposed to contain these pointers is empty.
30	An error was detected by the lower (control) sequencer. This error occurs when the lower sequencer determines that BMBs need to be returned to the free BMB pool and during a consistency check finds no BMBs to return. R2 contains the message slot address.
31 *	An error was detected by the upper (control) sequencer. (See NOTE at the end of this table.)
32	An error was detected by the upper (control) sequencer. While attempting to transmit over a connection, the upper sequencer found an incarnation number of zero (invalid) in the connection block (CB) structure. R11 contains the HMB address and R14 contains the CB address.
33 through 41 *	An error was detected by the upper (control) sequencer. (See NOTE at the end of this table.)
42	An error was detected by the upper (control) sequencer. A hardware error was detected following a block move to Control memory. R10 contains the upper processor error register contents. R16 contains the last control memory address in the block that was moved.
43 *	An error was detected by the upper (control) sequencer. A hardware error was detected following a block move out of control memory. R10 contains the upper processor error register contents. R16 contains the last control memory address in the block that was moved.
44 *	An error was detected by the upper (control) sequencer. A hardware error was detected following a control memory receive operation. R10 contains the upper processor error register contents. R16 contains the control memory address of the item received. R17 contains the control memory address of the queue head.
45 and 46 *	An error was detected by the upper (control) sequencer. (See NOTE at the end of this table.)
47 *	An error was detected by the upper (control) sequencer. A hardware error was detected during a downcount operation. R10 contains the upper processor error register value. R17 contains the counter address.
50 *	An error was detected by the upper (control) sequencer. A hardware error was detected while de-queueing a control memory item from a scratchpad list. R10 contains the upper processor error register contents. R11 contains the control memory address of the item.
51 *	An error was detected by the upper (control) sequencer. A hardware error was detected while internalizing an FRB. R10 contains the contents of the upper processor error register, R11 contains the FRB address and R14 contains the CB address. The Q register contains the work queue index.
52	An error was detected by the upper (control) sequencer.

Table D–2 (Cont.) K.ci Status Code Bytes For HSC40, HSC50, and HSC70 Controllers During Initialization

Status Code (Octal)	Description
	Either a consistency problem was found with the scratchpad queue or an attempt was made to send to a queue at address zero (illegal address).
53 through 55 *	An error was detected by the upper (control) sequencer. (See NOTE at the end of this table.)
56 through 71 *	An error was detected by the lower (control) sequencer. (See NOTE at the end of this table.)
72 *	An error was detected by the lower (control) sequencer. This error occurs while the lower processor is trying to link a BMB on the BMS free chain. R10 contains the lower processor error register contents. R5 contains the BMB data memory address.
73 *	An error was detected by the lower (control) sequencer. A hardware error was detected during a BMB list operation. R10 contains the lower processor error register contents. R5 contains the BMB data memory address.
74 *	An error was detected by the lower (control) sequencer. A hardware error was detected during a BMB list operation. R10 contains the lower processor error register contents. R5 contains the BMB data memory address.
75 *	An error was detected by the lower (control) sequencer. (See NOTE at the end of this table.)
76	An error was detected by the upper (control) sequencer. While copying data from an HMB to a message slot, the upper sequencer found the byte count of the HMB was larger than the slot capacity. R12 contains the slot address and R17 contains the text length.
77	An error was detected by the upper (control) sequencer. A host clear sequence has been received. R17 contains the address of the issuing node number.

NOTE

The sequencers access control memory several times before checking for a hardware error. Thus, to help determine the particular cause of the error, the sequencer saves the contents of the error register present at the time of the error check in R10 (octal). The contents of R10 are visible within the crash dump and can help in narrowing the error possibilities.

The following lists show the bits available from both the upper and lower processor error registers. Those bits marked with an asterisk (*) may cause a crash.

- Upper Processor error register:
  - — Bit 0 = Even/odd bit control memory address
  - — Bits 3, 2, 1 = CCYCLE 2, 1, 0
  - — * Bit 4 = Control bus error (illegal cycle)
  - — * Bit 5 = Control bus NXM
  - — * Bit 6 = Control data parity error
  - — * Bit 7 = Instruction (CROM) parity error
  - — * Bit 8 = Scratchpad parity error
  - — Bit 9 = PLI parity error
  - — Bits 10 through 15 indicate K.ci hardware revision level

- Lower Processor error register:
  - Bit 0 = Data memory address bit 16
  - Bit 1 = Data memory address bit 17
  - Bit 2 = Data memory NMA
  - * Bit 5 = Data bus NXM
  - * Bit 6 = Data memory parity error
  - * Bit 7 = Data memory overrun
  - * Bit 8 = Scratchpad parity error
  - * Bit 9 = PLI parity error
  - Bits 10 through 15 indicate K.ci hardware revision level

Table D–3 K.ci Status Code Bytes For HSC60 and HSC90 Controllers During Initialization

Status Code (Octal)	Description
00	Two conditions cause failure of the 2911 sequencer test upon powerup or reinitialization. In one case, the requestor sent status back to the P.io while Init was asserted. In the other case, the sequencer had already released the Init signal but the sequencer failed to reach the point in its code where it could change the status bits. A common reason for this status code is from an HSC false power fail crash dump. In this type of crash dump (IOT through 20), all requestors present report a 00 status code.
01	2901 ALU test failed upon powerup or reinitialization.
02	Data bus (DBUS) test failed upon powerup or reinitialization.
03	Control bus (CBUS) test failed upon powerup or reinitialization.
04	CROM test failed upon powerup or reinitialization.
06	K.oli RAM test failed upon powerup or reinitialization.
07	PLI interface test failed upon powerup or reinitialization.
10	Packet buffer test failed upon powerup or reinitialization.
11	LINK board test failed upon powerup or reinitialization.
12	Control bus/memory error occurred during a lock cycle while the K.ci was attempting to locate the K-Init packet in control memory upon powerup or reinitialization.
13	K.ci could not find a properly formatted K-Init packet in control memory after completing powerup/Init diagnostics.
14	A SNDDAT FRB was sent to the K.ci with a buffer list=0. R11=FRB address
15*	A hardware error was detected when the upper processor accessed scratch pad. R10=upper processor error register value
16	A structure other than an HMB or FRB was found on the K.ci work queue. Note: The "P" uses this path to create a K.ci crash. R11=structure address
17	FRB=0 detected when constructing DMA slot. R2=slot address
20*	A hardware error was detected when upper processor accessed scratch pad while polling. R10=upper processor error register value

Table D–3 (Cont.) K.ci Status Code Bytes For HSC60 and HSC90 Controllers During Initialization

Status Code (Octal)	Description
21 and 22	Not used
23*	A hardware error was detected when upper processor accessed scratch pad while polling. R10=upper processor error register value
24	FRB=0 detected while stuffing transmission buffer. R2=slot address
25	XID=0 detected while processing REQDAT slot. R2=slot address
26	CB=0 detected during UP HMB TX process. R11=HMB address, R12=slot address, R13=slot flags
27	Hardware inconsistency when reading scratch pad
30	Inconsistent BMB count, probably hardware. R2=slot address
31*	A hardware error was detected during upper processor polling loop. R10=upper processor error register value
32	An incarnation number of "0" was detected during a transmission attempt. R11=HMB address, R14=CB address
33 and 34*	A hardware error was detected when the upper processor accessed control memory. R10=upper processor error register value
35*	A hardware error was detected when the upper processor accessed scratch pad. R10=upper processor error register value
36*	A hardware error was detected when the upper processor was writing from scratch pad to control memory. R10=upper processor error register value
37 and 40*	A hardware error was detected when the upper processor accessed scratch pad. R10=upper processor error register value
41*	A hardware error was detected when the upper processor was moving data from scratch pad to control memory. R10=upper processor error register value
42*	A hardware error was detected following a "block move" to control memory. R10=upper processor error register value, R16=last control memory address in block moved
43*	A hardware error was detected following a "block move" from control memory. R10=upper processor error register value, R16=last control memory address in block moved
44*	A hardware error was detected following a control memory "receive operation". R10=upper processor error register value, R16=last control memory address in block moved, R17=control memory address of queue head
45*	A hardware error was detected following a control memory "receive operation". R16=last control memory address in block moved, R17=control memory address of queue head
46*	A hardware error was detected when the upper processor attempted to read scratch pad. R10=upper processor error register value
47*	A hardware error was detected during a downcount operation. R10=upper processor error register value, R17=counter address
50*	A hardware error was detected while dequeuing a control memory item from a scratch pad list. R10=upper processor error register value, R11=control memory address of item
51*	A hardware error was detected while "internalizing" an FRB. R10=upper processor error register value, R11=FRB address, R14=CB address, Q=work queue index

Table D–3 (Cont.) K.ci Status Code Bytes For HSC60 and HSC90 Controllers During Initialization

Status Code (Octal)	Description
52	General error for scratch pad dequeuing error.
53*	A hardware error was detected while the upper processor was allocating buffer descriptors. R10=upper processor error register value
54 and 55*	A hardware error was detected when upper processor scratch pad while polling. R10=upper processor error register value
56**	A hardware error was detected when the lower processor was accessing scratch pad. R10=lower processor error register value
57**	A hardware error was detected during "transmission in progress". R10=lower processor error register value
60**	A hardware error was detected while lower processor was stuffing transmission buffer. R10=lower processor error register value
61**	A hardware error was detected while lower processor was moving data to PLI module/buffer. R10=lower processor error register value
62**	A hardware error was detected while lower processor was reading scratch pad. R10=lower processor error register value
63**	A hardware error was detected when lower processor processed a TX status. R10=lower processor error register value
64**	A hardware error was detected while lower processor was processing RTNDAT packet. R10=lower processor error register value
65**	A hardware error was detected when lower processor was processing a COMPARE transmission. R10=lower processor error register value
66**	A hardware error was detected when lower processor finished writing to PLI/LINK module. R10=lower processor error register value
67**	A hardware error was detected when lower processor released PLI receiver buffer. R10=lower processor error register value
70**	A hardware error was detected when lower processor completed a packet reception. R10=lower processor error register value
71**	A hardware error was detected while lower processor was selecting a PLI receiver buffer. R10=lower processor error register value
72 through 74**	A hardware error was detected during a BMB List operation. R10=lower processor error register value, R5=BMB DM address
75**	A hardware error was detected during a lower processor polling loop. R10=lower processor error register value
76	An HMB was received with a message length exceeding the capacity of scratch pad slots. R12=slot address, R17=text length
77	A host clear sequence has been received. R17=issuing node

A single asterisk (*) indicates that the upper processor status register has an error bit set. The upper processor status register, R10, contains the following information:

- Upper processor error register:
  - Bit 15 = Always zero
  - Bit 14 = WCS online

    NOTE
    Scratch pad parity error and PLI bus parity error are common to both upper and lower error registers
  - Bit 13 = MFG mode switch 3
  - Bit 12 = MFG mode switch 2
  - Bit 11 = MFG mode switch 1
  - Bit 10 = MFG mode switch 0
  - Bit 09 = PLI bus parity error (wss.pl)

    NOTE
    Error bits 08 through 04 are logically or'd into the signal Cntl Error Sum. If any of the or'd bits are set to one, the Kci generates the appropriate fatal error listed in Table D–3.

    Some bits in the error registers have been assigned as status bits, such as wss.fp. This has no meaning since any error occurring in these hardware registers results in a Kci crash with one of the codes listed in Table D–3.
  - Bit 08 = Scratch pad parity error (wss.pl)
  - Bit 07 = Instruction parity error
  - Bit 06 = CBUS parity error
  - Bit 05 = Control NXM error
  - Bit 04 = CBUS cycle error
  - Bit 03 = CCYCLE 2
  - Bit 02 = CCYCLE 1
  - Bit 01 = CCYCLE 0
  - Bit 00 = CADR 00

A double asterisk (**) indicates that the lower processor status register has an error bit set. The lower processor status register, R10, contains the following information:

- Lower processor error register:
  - Bit 15 = Instruction parity error—byte 7
  - Bit 14 = Instruction parity error—byte 6
  - Bit 13 = Instruction parity error—byte 5
  - Bit 12 = Instruction parity error—byte 4
  - Bit 11 = Instruction parity error—byte 3

— Bit 10 = Instruction parity error—byte 2

NOTE
Error bits 09 through 05 are logically or'd into the signal Data Error Sum. If any of the or'd bits are set to one, the K.ci generates the appropriate fatal error listed in Table D–3.

— Bit 09 = PLI bus parity error (wss.pl)

— Bit 08 = Scratch pad parity error (wss.fp)

— Bit 07 = DBUS overrun error (wss.do)

— Bit 06 = DBUS parity error (wss.dp)

— Bit 05 = Data NXM error (wss.dn)

— Bit 04 = Instruction parity error—byte 1

— Bit 03 = Instruction parity error—byte 0

— Bit 02 = DNMA

— Bit 01 = DADR 17

— Bit 00 = DADR 16

Table D–4 K.sdi Status Code Bytes

Status Code (Octal)	Description
00	Two conditions cause failure of the 2911 sequencer test upon powerup or reinitialization. In one case, the requestor sent status back to the P.io while Init was asserted. In the other case, the P.io had already released the Init signal but the sequencer failed to reach the point in its code where it could change the status bits. A common occurrence of this status code is from an HSC false power fail crash dump. In this type of crash dump (IOT through 20), all requestors present report a 00 status code.
01	2901 ALU test failed upon powerup or reinitialization.
02	Data bus (DBUS) test failed upon powerup or reinitialization.
03	Control bus (CBUS) test failed upon powerup or reinitialization.
04	PROM test failed upon powerup or reinitialization.
06	Scratchpad RAM test failed upon powerup or reinitialization.
07	R-S/Gen test failed upon powerup or reinitialization.
10	Partial SDI test failed upon powerup or reinitialization.
12	The K.sdi encountered a control bus/memory problem while searching for the K-Init packet in control memory.
13	After completing powerup/Init diagnostics, the K.sdi could not find a properly formatted K-Init packet in control memory.
14	While trying to write the microcode version into the control area at address R7+44 (R7 is base address), the upper sequencer encountered a control bus error. R11 contains the contents of the upper error register. (See NOTE at the end of this table.)

Table D–4 (Cont.) K.sdi Status Code Bytes

Status Code (Octal)	Description
15	The upper processor tried to advance the buffer descriptor pointer when the old value of the pointer is zero (illegal).
16	While attempting to read the block number (LBN) from a buffer descriptor in control memory, the upper processor encountered a hardware error. R11 contains the contents of the upper error register. (See NOTE at the end of this table.)
17 through 30 *	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents. (See NOTE at the end of this table.)
31	This error occurs if, during transfer completion, a DRAT counter goes to zero and the DRAT list head in the control area is not locked and not equal to the current DRAT value.
32 through 42 *	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents. (See NOTE at the end of this table.)
43	This error occurs while processing an active DCB if the dialogue state indicator is not locked (a value of 100000 is not in KS$DHD) and not valid (KS$IND does not contain the values 0, 1, 2, 3, OR 4, or –1).
44	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents. (See NOTE at the end of this table.)
45	This error occurs if, after completing state 0 processing, the upper sequencer cannot find a valid DCB opcode. (No valid state is present to go to next.)
46 through 55 *	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents. (See NOTE at the end of this table.)
74 through 76	The upper processor attempted to downcount a counter that was already at zero.

NOTE

The upper sequencer accesses control memory several times before checking for a control bus error. Thus, to help determine the particular cause of the error, the upper sequencer saves the contents of the error register present at the time of the error in R11 (octal). The contents of R11 are visible within the crash dump and may help in narrowing the error possibilities.

The following list defines all the bits contained within the upper processor error register (value loaded in R11). Those bits that may cause a crash are denoted with an asterisk (*).

- Upper processor error register:
  - Bit 0 = Even/odd bit Control memory address
  - Bits 3, 2, 1 = CCYCLE 2, 1, 0
  - * Bit 4 = Control bus error (illegal cycle)
  - * Bit 5 = Control bus NXM
  - * Bit 6 = Control data parity error
  - * Bit 7 = Instruction (CROM) parity error
  - Bits 8 through 12 not used
  - * Bit 13 = Response pulse missing on SDI RD/RES Line (pulse error)
  - Bit 14 = Upper processor RTCS clock present
  - Bit 15 = Parity error on RTDS Line

Table D–5 K.sti Status Code Bytes

Status Code (Octal)	Description
00	Two conditions cause failure of the 2911 sequencer test upon powerup or reinitialization. In one case, the requestor sent status back to the Pio while Init was asserted. In the other case, the Pio had already released the Init signal but the sequencer failed to reach the point in its code where it could change the status bits. A common occurrence of this status code is from an HSC false power fail crash dump. In this type of crash dump (IOT through 20), all requestors present report a 00 status code.
01	2901 ALU test failed upon powerup or reinitialization.
02	Data bus (DBUS) test failed upon powerup or reinitialization.
03	Control bus (CBUS) test failed upon powerup or reinitialization.
04	PROM test failed upon powerup or reinitialization.
06	Scratchpad RAM test failed upon powerup or reinitialization.
07	R-S/Gen test failed upon powerup or reinitialization.
10	Partial STI test failed upon powerup or reinitialization.
12	The K.sti encountered a control bus/memory problem while searching for the K-Init packet in control memory.
13	After completing powerup/Init diagnostics, the K.sti could not find a properly formatted K-Init packet in control memory.
14 through 22 *	Control bus error. (See NOTE at the end of this table.)
23	During transfer completion, the buffer descriptor link word in the FRB was zero. RAM7 contains the lower processor status.
24 through 33 *	Control bus error. (See NOTE at the end of this table.)

Table D–5 (Cont.) K.sti Status Code Bytes

Status Code (Octal)	Description
34	The lower processor has timed out on a transfer operation and the upper processor cannot restart it.
35 and 36 *	Control bus error. (See NOTE at the end of this table.)
37	A software inconsistency. The STI state zero processing code was entered when the drive state indicator was not zero.
40	State zero processing is complete. However, the next state (such as Send Level 1 Frame or Get Drive Status) is not specified. Thus, the state is undefined.
41 through 43 *	Control bus error. (See NOTE at the end of this table.)
44	While setting up a transfer, the next buffer descriptor in the FRB was zero (no buffer was there).
74	Attempted to downcount a counter that was already zero. R14 contains the FRB. R16 contains the counter minus one. R17 contains the address of the counter structure.
75 and 76 *	Control bus error. (See NOTE at the end of this table.)

NOTE

In the following status codes, bit 7 is the parity bit. Parity is always odd for microdiagnostic failures and is always even for functional code failures. Bit 6 is the error bit and is set for microdiagnostic and functional code failures.

000	Two conditions cause failure of the 2911 sequencer test upon powerup or reinitialization. In one case, the requestor sent status back to the P.io while Init was asserted. In the other case, the sequencer had already released the Init signal but the sequencer failed to reach the point in its code where it could change the status bits. A common occurrence of this status code is from an HSC false power fail crash dump. In this type of crash dump (IOT through 20), all requestors present report a 00 status code.
103	Control bus (CBUS) test failed upon powerup or reinitialization.
106	Scratchpad RAM test failed upon powerup or reinitialization.
110	Partial STI test failed upon powerup or reinitialization.
112	The K.sti encountered a control bus/memory problem while searching for the K-Init packet in control memory.
301	2901 ALU test failed upon powerup or reinitialization.
302	Data bus (DBUS) test failed upon powerup or reinitialization.
304	PROM test failed upon powerup or reinitialization.
307	SERDES test failed upon powerup or reinitialization.
313	After completing powerup/Init diagnostics, the K.sti could not find a properly formatted K-Init packet in control memory.

NOTE

The upper sequencer accesses control memory several times before checking for a control bus error. Thus, to help determine the particular cause of the error, the upper sequencer saves the contents of the error register present at the time of the error in R11 (octal). The contents of R11 are visible within the crash dump and may help in narrowing the error possibilities.

The following list defines all the bits contained within the upper processor error register (value loaded in R11). Those bits that may cause a crash are denoted with an asterisk (*).

- Upper processor error register:
  - Bit 0 = Even/odd bit Control memory address
  - Bits 3, 2, 1 = CCYCLE 2, 1, 0
  - * Bit 4 = Control bus error (illegal cycle)
  - * Bit 5 = Control bus NXM
  - * Bit 6 = Control data parity error
  - * Bit 7 = Instruction (CROM) parity error
  - Bits 8 through 12 not used
  - * Bit 13 = Response pulse missing on SDI RD/RES Line (pulse error)
  - Bit 14 = Upper Processor RTCS clock present
  - Bit 15 = Parity error on RTDS Line

Table D–6 K.si Disk Status Code Bytes

Status Code (Octal)	Description
00	2911 test failed at powerup or reinitialization. Alternately, the built-in self-test (BIST) DEMON code was unable to begin testing the module.
01	2901 ALU test failed at powerup or reinitialization.
02	Data bus (DBUS) test failed at powerup or reinitialization.
03	Control bus (CBUS) test failed at powerup or reinitialization.
04	The PROM/writable control store (WCS) parity test failed at powerup or reinitialization.
06	Scratchpad RAM test failed at powerup or reinitialization.
07	RTS Gate Array test failed at powerup or reinitialization.
10	Calibration of the SIECL failed during powerup or reinitialization.
11	WCS moving inversions test failed during offline diagnostics.
12	The K.si encountered a control bus/memory problem while searching for the K-init packet in control memory.
13	Attempt to load module's WCS failed during powerup or offline load attempt.
14	While trying to write the microcode version into the control area at KG$VRSN, the upper sequencer encountered a control Bus error. R11 contains the contents of the upper error register.
15	The upper processor tried to advance the buffer descriptor pointer because the old value of the pointer is zero (illegal action).
16	While attempting to read the logical block number (LBN) from a buffer descriptor in control memory, the upper processor encountered a hardware error. R11 contains the contents of the upper error register. See note at the end of this table.
17–30	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents. See note at the end of this table.

Table D–6 (Cont.) K.sl Disk Status Code Bytes

Status Code (Octal)	Description
31	During transfer completion, a DRAT counter went to zero while the DRAT list head in the control area was not locked and not equal to the current DRAT value.
32–42	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents. See note at the end of this table.
43	While processing an active DCB, the dialog state indicator was not locked (a value of 100000 is not in KS$DHD) and not valid (KS$IND does not contain the values 0, 1, 2, 3, or 4, or -1).
44	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents.
45	After completing state 0 processing, the upper sequencer could not find a valid DCB opcode because no further valid state was present.
46–55	The upper processor encountered an error while attempting to access control memory. R11 contains the upper processor error register contents. See note at the end of this table.
56	The upper processor encountered an error and began executing microinstructions in a reserved area.
60–62	Same as errors 17 through 30.
63	The upper processor could not fetch buffers because of F$CNT=0 software inconsistency.
64	Same as errors 17 through 30.
70–73	Diagnostic Test: If SIECL/SERDES path loop testing failed during power up or reinitialization because of one of the following conditions: 70 — Frame loopback from upper to lower 71— Frame loopback from lower to upper 72— Sector loopback from upper to lower 73— Sector loopback from lower to upper
74–76	The upper processor attempted to downcount a counter that was already zero.

NOTE

When an error occurs, the upper processor transfers the contents of the upper processor error register at the time of the error to register R11 (octal).

The contents of R11 are given in the crash dump to help you narrow the error possibilities. The following list defines the bits contained in R11 from the upper processor error register. Those bits that can indicate the possible cause of a crash are denoted with an asterisk (*).

Bit 0	Even/odd bit for control memory address
Bits 3,2,1	CCYCLE 2,1,0
Bit 4*	Control bus error (illegal cycle)
Bit 5*	Control bus NXM
Bit 6*	Control data parity error
Bit 7*	Instruction (CROM) parity error

Bits 8 through 12	Not used
Bit 13	Response pulse missing on SDI RD/RES line
Bit 14	Upper processor RTC clock pulse present
Bit 15	Parity error on RTDS line

Table D–7 K.si Tape Status Code Bytes

Status Code (Octal)	Description
00	2911 test failed at powerup or reinitialization. Alternately, the built-in self-test (BIST) DEMON code was unable to begin testing the module.
01	2901 ALU test failed upon powerup or reinitialization.
02	Data bus (DBUS) test failed at powerup or reinitialization.
03	Control bus (CBUS) test failed at powerup or reinitialization.
04	The PROM/writable control store (WCS) parity test failed at powerup or reinitialization.
06	Scratchpad RAM test failed at powerup or reinitialization.
07	RTS Gate Array test failed at powerup or reinitialization.
10	Calibration of the SIECL failed during powerup or reinitialization.
11	WCS moving inversions test failed during off-line diagnostics.
12	The K.si encountered a control bus/memory problem while searching for the K-init packet in control memory.
13	Attempt to load module's WCS failed during powerup or offline load attempt.
14	While trying to write the microcode version into the control area at KG$VRSN, the upper sequencer encountered a control bus error. R11 contains the contents of the upper error register.
15–22	Control Bus error. See note at the end of this table.
23	During transfer completion, the buffer descriptor link word in the FRB was zero. RAM7 contains the lower processor status.
24–33	Control Bus error. See note at the end of this table.
34	The lower processor has timed out on a transfer operation and the upper processor cannot restart it.
35–36	Control bus error. See note at the end of this table.
37	Software inconsistency. The STI state zero processing code was entered when the drive state indicator was not zero.
40	State zero processing is complete. However, the next state (such as Send Level 1 Frame, or Get Drive Status) is not specified. Thus, the state is undefined.
41–43	Control Bus error. See note at the end of this table.
44	While setting up a transfer, the next buffer descriptor in the FRB was zero because the buffer descriptor named a nonexistent buffer.
45	Control bus error.

Table D–7 (Cont.) K.sl Tape Status Code Bytes

Status Code (Octal)	Description
70–73	If SIECL/SERDES path loop testing failed during powerup or reinitialization because of one of the following conditions: 70 — Frame loopback from upper to lower 71— Frame loopback from lower to upper 72— Sector loopback from upper to lower 73— Sector loopback from lower to upper
74	The upper processor attempted to downcount a counter that was already zero. R14 contains the FRB. R16 contains the counter minus one. R17 contains the address of the counter structure.
75–76	Control bus error. See note at the end of this table.

NOTE

When an error occurs, the upper processor transfers the contents of the upper processor error register at the time of the error to register R11 (octal).

The contents of R11 are given in the crash dump to help you narrow the error possibilities. The following list defines all the bits contained in R11 from the upper processor error register. Those bits that can indicate the possible cause of a crash are denoted with an asterisk (*).

Bit 0	Even/odd bit for control memory address
Bits 3,2,1	CCYCLE 2,1,0
Bit 4*	Control bus error (illegal cycle)
Bit 5*	Control bus NXM
Bit 6*	Control data parity error
Bit 7*	Instruction (CROM) parity error
Bits 8 through 12	Not used
Bit 13	Response pulse missing on SDI RD/RES line
Bit 14	Upper processor RTC clock pulse present
Bit 15	Parity error on RTDS line

Table D–8 Status Codes for K.si Requestors With Microcode Load Failure

Status Code[1] (Octal)	Description
171	K.si module microcode not found on boot media.
172	K.si module microcode file size exceeds INIPIO buffer size.
174	Load device failure prevented microcode load.
373	Insufficient memory to load K.si module microcode file.
375	K.si module microcode load failed.

[1]These status codes are displayed on the HSC console immediately upon boot.


INDEX

Index

A

ac power removal
  HSC, 3–5
Airflow sensor
  HSC, 3–68
  HSC50, 3–70
Alphabetic error message listing, 8–59 to 8–106
Auxiliary power supply
  HSC, 3–88
  HSC50, 3–91
Auxiliary terminal connection
  HSC50, 4–3

B

Baud rate jumper
  I/O control processor module (P.ioc), 3–29
BBR errors, 8–39
  bad block replacement (block OK), 8–60
  bad block replacement (drive inoperative), 8–60
  bad block replacement (RCT inconsistent), 8–61
  bad block replacement (recursive failure), 8–61
  bad block replacement (REPLACE failed), 8–61
  bad block replacement (success), 8–61
  field definition, 8–39
Bit descriptions
  replace flags, 8–40
Block diagram, 1–18
Blower, 1–9
  HSC, 3–72
  HSC50, 3–74
Boot
  diagnostic indications, 8–28
  flow/troubleshooting chart
    HSC, 8–17
    HSC50, 8–23

C

Cabinet, front view, 1–6
Cabinet, rear view, 1–9
Cabinet back door removal, 3–12
Cabinet front door removal
  HSC, 3–10
  HSC50, 3–11
Cabling, 1–9
CI bus, 1–9, 1–16
  connecting to hosts, 1–2
CI-detected out-of-band errors
  bad dispatch state in CB.., 8–62
  cables have gone from uncrossed to crossed, 8–86
  cannot reopen VC to node (x). I/O rundown not yet complete..., 8–63
  date/time set by node nn, 8–68
  HML$ER set—HM$ERR = nn, 8–74
  K.ci exception detected, code = nnn, 8–78
  K.ci loopback microcode loaded, 8–79
  no control block available to satisfy HMB request., 8–84
  node nn cables have gone from crossed to uncrossed, 8–85
  node nn path (A or B) has gone from good to bad, 8–87
  node nn path n has gone from bad to good, 8–86
  resource lost to K.ci—xxx xxx HMBs, 8–92
  VC closed with node nn due to disabled remote port, 8–103
  VC closed with node nn due to disconnect timeout, 8–104
  VC closed with node nn due to invalid SCS op code, 8–103
  VC closed with node nn due to request from K.ci, 8–104
  VC closed with node nn due to spinlock timeout, 8–103
  VC closed with node nn due to START received, 8–105
  VC closed with node nn due to unexpected disconnect, 8–105

CI-detected out-of-band errors (cont'd)
VC closed with node nn to test VX closure response, 8–103
VC open with node nn, 8–105
CI manager, 1–26
Communications error report, 5–52
Configuration problems
data channel module (K.si), 3–41
Console terminal
connection, 4–1
troubleshooting, 8–16
Control bus error conditions (hardware-detected), 8–54
Controller byte field, 8–35
Controller errors
compare error, 8–63
data bus overrun, 8–66
data memory error (NXM or parity), 8–67
EDC error, 8–72
internal consistency error, 8–77
MSCP, 8–31
PLI buffer parity error, 8–88
SERDES overrun, 8–94
TMSCP, 8–31
Control program, 1–25
Cooling, 1–9
Crash dump, 13–1
CSR breakdown
RX33 disk drive, 8–51

D

Data channel module (K.si), 1–23
see also K.si
Description and flags
MSCP error format, 8–28
TMSCP error format, 8–28
Device integrity tests
generic error message format, 5–2
generic prompt syntax, 5–1
ILCACH, 5–9
ILMEMY, 5–7
ILRX33, 5–2
ILTU58, 5–5
Diagnostic indications
boot, 8–28
Diagnostic manager, 1–26
Diagnostic subroutines, 1–26
Disk data channel module (K.sdi), 1–23
see also K.sdi
Disk drive, 3–50
see RX33 disk drive
prompts, 5–44
Disk drive integrity test
ILDISK, 5–12
Disk error processor, 1–26
Disk functional errors, 8–53
Disk functional out-of-band errors
aborting error recovery due to excessive recals, 8–59
Disk functional out-of-band errors (cont'd)
aborting error recovery due to excessive timeouts, 8–60
clock dropout from ONLINE disk unit xx., 8–63
disk unit xx. (requestor xx., port xx.) being INITialized, 8–69
disk unit xx. ready to transfer, 8–69
disk unit xx cannot be brought available. HSC is currently set up..., 8–68
disk unit xxx. (requestor xx., port xx.) declared inoperative, 8–69
DRAT/SEEK timeout, disk unit xxx., 8–70
duplicate disk unit xx, 8–71
illegal bit change in status from disk unit xxx, 8–77
K.sdi/K.si in slot xx. failed its Init DIT, status = xxx, 8–79
LBN restored with forced error in RESTOR operation!, 8–80
LBN xx. repaired for shadow member unit xx., 8–80
positioner error on disk unit xxx. DRAT addr:xxx, 8–89
premature LP flag in RTNDAT sequence from host node xx, 8–89
SDI exchange retry on disk unit xxx, 8–93
shadow copy timeout detected copying cylinder x..., 8–94
unexpected AVAILABLE signal from ONLINE disk unit xx, 8–101
unit xx. declared inoperative because no progress made on Command Reference xxxxx., 8–102
unrecoverable error on disk unit xx. Drive appears inoperative, 8–102
unsuccessful SEEK initiation, disk unit xxx. DCB addr: xxx, 8–102
VC closed due to timeout of RTNDAT/CNF from host node xx, 8–104
Disk I/O manager, 1–26
Disk status code bytes
K.si, D–16
Disk transfer errors
data sync not found, 8–68
eight-symbol ECC error, 8–84
five-symbol ECC error, 8–84
forced error, 8–72
four-symbol ECC error, 8–84
MSCP, 8–36
MSCP field description, 8–36
one-symbol ECC error, 8–84
seven-symbol ECC error, 8–84
six-symbol ECC error, 8–84
three-symbol ECC error, 8–84
two-symbol ECC error, 8–84
uncorrectable ECC error, 8–101

Disk transfer errors
RCT corrupted error, 8-90
DKUTIL, 7-1 to 7-15
command descriptions, 7-3
command modifiers, 7-2
command prompt, 7-10
command summary, 7-3
command syntax, 7-2
DEFAULT command, 7-4
DEFAULT command modifiers, 7-4
DEFAULT command usage, 7-4
DISPLAY command, 7-5
DISPLAY command examples, 7-6
DISPLAY command modifiers, 7-5
DISPLAY command parameters, 7-5
DISPLAY command syntax, 7-5
DISPLAY command usage, 7-5
DKUTIL-E all copies of xCT block n are bad, 7-13
DKUTIL-E cannot ONLINE unit, 7-13
DKUTIL-E copy n of xCT block n (xBN n) is bad, 7-13
DKUTIL-E drive must be acquired to execute this command, 7-13
DKUTIL-E drive must be online to execute this command, 7-13
DKUTIL-E drive went AVAILABLE, 7-13
DKUTIL-E drive went OFFLINE, 7-13
DKUTIL-E error log corrupted, cannot display entries, 7-13
DKUTIL-E error log corrupted, cannot display header, 7-13
DKUTIL-E error log not implemented in drive, 7-14
DKUTIL-E illegal response, 7-14
DKUTIL-E invalid ASCII byte count from drive, 7-14
DKUTIL-E invalid block number for xBN space, 7-14
DKUTIL-E invalid decimal number, 7-14
DKUTIL-E invalid octal number, 7-14
DKUTIL-E invalid sector size; only 512 and 576 are legal, 7-14
DKUTIL-E missing modifier only "/" was specified, 7-14
DKUTIL-E missing parameter, 7-14
DKUTIL-E n is an invalid par number; maximum is n, 7-14
DKUTIL-E nonexistent unit number, 7-14
DKUTIL-E SDI command was unsuccessful, 7-14
DKUTIL-E there is no buffer to dump, 7-14
DKUTIL-E there is no buffer to push, 7-14
DKUTIL-E there is no pushed buffer to pop, 7-14
DKUTIL (cont'd)
DKUTIL-E unable to read error log, 7-14
DKUTIL-E unit is not available, 7-14
DKUTIL-E xxx is an invalid xxx, 7-14
DKUTIL-F I/O request was rejected, 7-13
DKUTIL-F insufficient resources to RUN, 7-13
DKUTIL-I Ctrl/Y or Ctrl/C abort, 7-15
DKUTIL-I exiting, 7-15
DUMP command, 7-6
DUMP command modifiers, 7-7
DUMP command parameters, 7-6
DUMP command syntax, 7-6
DUMP command usage, 7-7
error messages, 7-12
error message severity levels, 7-13
error message variables, 7-12
EXIT command, 7-8
EXIT command syntax, 7-8
EXIT command usage, 7-8
fatal error messages, 7-13
GET command, 7-8
GET command modifiers, 7-8
GET command parameters, 7-8
GET command syntax, 7-8
GET command usage, 7-8
information and error messages, 7-13
POP command, 7-9
POP command syntax, 7-9
POP command usage, 7-9
PUSH command, 7-9
PUSH command syntax, 7-9
PUSH command usage, 7-9
sample session, 7-10
SET command, 7-9
SET command examples, 7-9
SET command parameters, 7-9
SET command syntax, 7-9
SET command usage, 7-9
starting, 7-1

E

Error byte field, 8-35
Error conditions (hardware-detected)
control bus, 8-54
Error information
categories of software errors, 8-28
DKUTIL, 7-12
flags, C-2
FORMAT, 7-26
generic error log fields, C-1
ILEXER error messages, 5-55
ILMEMY error messages, 5-8
ILTCOM error messages, 5-41
initialization, 8-2
MSCP flags, 8-30
offline bus interaction test, 6-27
offline cache test, 6-21
offline control store loader, 6-90

Error information (cont'd)
offline diagnostics bootstrap, 6–4
offline K/P memory test, 6–45
offline K test selector, 6–35
offline memory cache test (OMCA), 6–68
offline memory test, 6–56
offline OCP test, 6–83
offline refresh test, 6–77
offline RX33 exerciser, 6–72
PATCH, 7–33
SDI, 8–32
SINI-E printout, B–2
TMSCP flags, 8–30
VERIFY, 7–18
Error message example
ILCACH, 5–11
Error message fields
MSCP, 8–29
RX33 message last line breakdown, 8–52
TMSCP, 8–29
Error message listing
aborting error recovery due to excessive recals, 8–59
aborting error recovery due to excessive timeouts, 8–60
acknowledge not asserted at start of transfer, 8–60
bad block replacement (block OK), 8–60
bad block replacement (drive inoperative), 8–60
bad block replacement (RCT inconsistent), 8–61
bad block replacement (recursive failure), 8–61
bad block replacement (REPLACE failed), 8–61
bad block replacement (success), 8–61
bad dispatch state in CB..., 8–62
buffer EDC error, 8–62
cables have gone from uncrossed to crossed, 8–86
cache disabled due to failure, 8–78
cache functionality requested but M.cache hardware not present, 8–62
cannot reopen VC to node (x). I/O rundown not yet complete..., 8–63
clock dropout from ONLINE disk unit xx., 8–63
compare error, 8–63
controller-detected position lost, 8–64
controller-detected transmission or time out error, 8–64
controller transfer retry limit exceeded, 8–64
control microprocessor running with memory bank or board swap enabled, 8–64
Error message listing (cont'd)
could not complete on-line sequence, 8–65
could not get extended drive status, 8–65
could not get formatter summary status during transfer error recovery, 8–65
could not get formatter summary status while trying to restore tape position, 8–65
could not position for formatter retry, 8–66
could not set byte count, 8–66
could not set unit characteristics, 8–66
data bus overrun, 8–66
data error flagged in backup record, 8–67
data memory error (NXM or parity), 8–67
data ready timeout, 8–67
data sync not found, 8–68
date/time set by node nn, 8–68
disk unit xx. (requestor xx., port xx.) being INITialized, 8–69
disk unit xx. ready to transfer, 8–69
disk unit xx cannot be brought available. HSC is currently set up..., 8–68
disk unit xxx. (requestor xx., port xx.) declared inoperative, 8–69
DRAT/SEEK timeout, disk unit xxx., 8–70
drive clock dropout, 8–70
drive-detected error, 8–71
drive inoperative, 8–71
duplicate disk unit xx, 8–71
EDC error, 8–72
eight-symbol ECC error, 8–84
ERASE command failed, 8–72
ERASE GAP command failed, 8–72
five-symbol ECC error, 8–84
forced error, 8–72
formatter and HSC disagree on tape position, 8–73
formatter-detected position lost, 8–73
formatter-requested error log, 8–73
formatter retry sequence exhausted, 8–73
four-symbol ECC error, 8–84
hard transfer error loading (file) xx, 8–74
hard transfer error writing SCT xx, 8–74
header error, 8–74
HML$ER set—HM$ERR = nn, 8–74
host clear from CI node xx, 8–75
host interface (K.ci) failed INIT diags, status = xxx, 8–76
host interface (K.ci) is required but not present, 8–76

Error message listing (cont'd)
host requested retry suppression on a formatter-detected error, 8–76
host requested retry suppression on a K.sti/K.si-detected error, 8–76
illegal bit change in status from disk unit xxx, 8–77
increase drive structures through SET MAX_TAPES command, 8–85
increase formatter structures through SET MAX_FORMATTERS command, 8–85
insufficient Control memory for K.sti/K.si in requestor xx, 8–77
internal consistency error, 8–77
invalid module configuration, 8–78
K.ci exception detected, code = nnn, 8–78
K.ci loopback microcode loaded, 8–79
K.sdi/K.si in slot xx. failed its Init DIT, status = xxx, 8–79
K.sti/K.si in requestor xx has microcode incompatible with this TMSCP Server, 8–79
last soft Init resulted from unknown cause, 8–79
LBN restored with forced error in RESTOR operation!, 8–80
LBN xx. repaired for shadow member unit xx., 8–80
less than 87.5 percent of control memory is available, 8–80
less than 87.5 percent of data memory is available, 8–80
less than 87.5 percent of program memory is available, 8–81
lost Read/Write Ready, 8–81
lost Receiver Ready, 8–82
Lower Processor error, 8–82
Lower Processor timeout, 8–82
M.cache comparator error, 8–83
M.cache disabled due to excessive errors, 8–83
M.cache multiple bit ECC error, 8–83
M.cache single bit ECC error, 8–83
no control block available to satisfy HMB request., 8–84
node nn cables have gone from crossed to uncrossed, 8–85
node nn path (A or B) has gone from good to bad, 8–87
node nn path n has gone from bad to good, 8–86
no tape drive structures available for Requestor xx Port xx Unit xx, 8–85
no tape formatter structures available for Requestor xx Port xx, 8–85
no usable K.sti/K.si boards were found by the TMSCP Server, 8–85
one-symbol ECC error, 8–84
parameter change, process yyy..., 8–88

Error message listing (cont'd)
parity error Trap thru 114, 8–88
PLI buffer parity error, 8–88
positioner error on disk unit xxx. DRAT addr:xxx, 8–89
position or unintelligible header error, 8–89
premature LP flag in RTNDAT sequence from host node xx, 8–89
program memory single bit ECC error, 8–90
pulse or parity error, 8–90
RCT corrupted error, 8–90
Receiver Ready not asserted at start of transfer, 8–91
record EDC error, 8–91
requestor xx failed INIT DIT, status = xxx, 8–91
requestor xx failed INIT DIT with status = xx, 8–91
reserved instruction Trap thru 10, 8–92
resource lost to K.ci—xxx xxx HMBs, 8–92
retry limit exceeded while attempting to restore tape position, 8–92
rewind failure, 8–93
SCT read or verification error. Using template SCT., 8–93
SDI clock persisted after Init, 8–93
SDI exchange retry on disk unit xxx, 8–93
SERDES overrun, 8–94
seven-symbol ECC error, 8–84
shadow copy timeout detected copying cylinder x..., 8–94
SI clock resumption failed after Init, 8–94
SI command timeout, 8–95
SI Receiver Ready collision, 8–95
SI response length or Opcode error, 8–96
SI response overflow, 8–96
six-symbol ECC error, 8–84
software inconsistency, 8–97
subsystem exception, Level 7 K interrupt Trap thru 134, 8–81
subsystem exception, MMU Trap through 250, 8–83
subsystem exception, NXM Trap thru 4, 8–87
tape drive requested error log, 8–97
tape formatter has been declared inoperative, 8–97
tape unit number xx connected to requestor xx port xx ceased to exist while online, 8–98
tape unit number xx connected to requestor xx port xx dropped state clock, 8–98

Error message listing (cont'd)
tape unit number xx connected to requestor xx port xx is not asserting available when it should be, 8–98
tape unit number xx connected to requestor xx port xx went available without request, 8–99
tape unit number xx connected to requestor xx port xx went offline without request, 8–99
three-symbol ECC error, 8–84
TMSCP fatal initialization error—TMSCP functionality not available, 8–99
topology command failed, 8–99
TTRASH fatal initialization error, 8–100
two-symbol ECC error, 8–84
unable to position to before LEOT, 8–100
unable to read program memory error counter, 8–100
unclearable drive error, 8–100
unclearable formatter error, 8–101
uncorrectable ECC error, 8–101
unexpected AVAILABLE signal from ONLINE disk unit xx, 8–101
unit xx. declared inoperative because no progress made on Command Reference xxxxx., 8–102
unknown K.tape error, 8–102
unrecoverable error on disk unit xx. Drive appears inoperative, 8–102
unsuccessful SEEK initiation, disk unit xxx DCL addr: xxx, 8–102
VC closed due to timeout of RTNDAT/CNF from host node xx, 8–104
VC closed with node nn due to disabled remote port, 8–103
VC closed with node nn due to disconnect timeout, 8–104
VC closed with node nn due to invalid SCS op code, 8–103
VC closed with node nn due to request from K.ci, 8–104
VC closed with node nn due to spinlock timeout, 8–103
VC closed with node nn due to START received, 8–105
VC closed with node nn due to unexpected disconnect, 8–105
VC closed with node nn to test VX closure response, 8–103
VC open with node nn, 8–105
WARNING K.sti ucode too low for large transfers., 8–105
word rate clock timeout, 8–106

Error messages
BBR, 8–39
DKUTIL, 7–12
FORMAT, 7–26
ILCACH, 5–11
ILDISK, 5–18
ILEXER, 5–56
ILMEMY, 5–9
ILRX33, 5–4
ILTAPE, 5–35
ILTCOM, 5–41
ILTU58, 5–6
miscellaneous, 8–53
offline bus interaction test, 6–28
offline cache test, 6–21
offline control store loader, 6–90
offline K/P memory test, 5–46
offline K test selector, 6–35
offline memory cache test (OMCA), 6–68
offline memory test, 6–57
offline OCP test, 6–83
offline refresh test, 6–78
offline RX33 exerciser, 6–73
PATCH, 7–33
RX33 disk drive, 8–50
SINI, 8–53
TMSCP, 8–40
VERIFY, 7–18
EXAMINE and DEPOSIT commands
asterisk (*) symbolic address, 6–11
at (@) symbolic address, 6–11
command repeats, 6–12
minus sign (–) symbolic address, 6–11
plus sign (+) symbolic address, 6–11
qualifiers (switches), 6–13
qualifier switch /byte, 6–13
qualifier switch /DECIMAL, 6–13
qualifier switch /HEX, 6–13
qualifier switch /INHIBIT, 6–13
qualifier switch /long, 6–13
qualifier switch /next, 6–13
qualifier switch /OCTAL, 6–13
qualifier switch /quad, 6–13
qualifier switch /word, 6–13
relocation register, 6–12
set default command, 6–13
symbolic addresses, 6–11
Exception codes and messages, B–1
Exception messages listing, B–4 to B–50
External interfaces, 1–15
External loop test
data channel module (K.si), 3–38

F

Failover procedure, 3–2
Fault code displays
interpretation, 4–8
OCP, 8–2
Field descriptions
BBR errors, 8–39

Field descriptions (cont'd)
original error flags, 8–38
recovery flags, 8–38
SDI error, 8–32
FORMAT, 7–23 to 7–29
caution, 7–23
Ctrl/C caution, 7–23
Ctrl/Y caution, 7–23
error and information messages, 7–26
error messages, 7–29
error message severity levels, 7–26
error message variables, 7–26
fatal error messages, 7–26
FORMAT–E illegal response to start-up question, 7–29
FORMAT–E nondefaultable parameter, 7–29
FORMAT–F cannot FORMAT this drive type, 7–26
FORMAT–F cannot position to DBN area, 7–26
FORMAT–F current maximum sector size is 512, 7–27
FORMAT–F DBN format error, 7–27
FORMAT–F drive does not support 576 mode on this media, 7–27
FORMAT–F drive is write-protected, 7–27
FORMAT–F FCT does not have enough good copies of each block, 7–27
FORMAT–F FCT is improper, 7–27
FORMAT–F FCT nonexistent, 7–27
FORMAT–F FCT read error, 7–27
FORMAT–F FCT write error, 7–27
FORMAT–F formatter initialization error, 7–27
FORMAT–F GET STATUS failure, 7–27
FORMAT–F LBN format error, 7–27
FORMAT–F nonexistent unit number, 7–27
FORMAT–F RCT does not have enough good copies of each block, 7–27
FORMAT–F RCT is full, 7–27
FORMAT–F RCT read error, 7–27
FORMAT–F RCT write error, 7–27
FORMAT–F SDI receive error, 7–27
FORMAT–F too many bad RBNs found before RCT was formatted, 7–27
FORMAT–F unsuccessful SDI command, 7–28
FORMAT–I bad LBN n (x), a non-primary revector, 7–28
FORMAT–I bad LBN n (x), a primary revector to RBN n, 7–28
FORMAT–I bad LBN n (x), in the RCT area, 7–28
FORMAT–I bad RBN n (x), 7–28
FORMAT–I Ctrl/Y or Ctrl/C abort, 7–28
FORMAT (cont'd)
FORMAT–I cylinder n, group n, track n, position n, PBN n, 7–28
FORMAT–I FCT was not used, 7–28
FORMAT–I FCT was used successfully, 7–28
FORMAT–I n cylinders left in XBN space at hh:mm:ss.xx, 7–28
FORMAT–I only DBN area formatted (n bad DBNs), 7–28
FORMAT–S format begun, 7–29
FORMAT–S format completed, 7–29
FORMAT–W possible head addressing problem, 7–28
information messages, 7–28
running, 7–23
sample session, 7–25
special option prompts, 7–24
success messages, 7–29
VERIFY requirement, 7–25
warning message, 7–28
Format type codes
MSCP, 8–29
TMSCP, 8–29
Front view of cabinet, 1–6
FRU removal and replacement, 3–3
FRU removal sequence chart
HSC, 3–8
HSC50, 3–9
Functional errors
disk, 8–53
tape, 8–53

G

GEDS text field breakdown, 8–45
Generic error messages
device integrity tests, 5–2
generic error log fields, C–1
ILEXER, 5–58
MSCP, 8–28
offline diagnostics, 6–7
TMSCP, 8–28
Generic prompt syntax
device integrity tests, 5–1
Global prompts
ILEXER, 5–47
GSS text field breakdown, 8–46

H

HSC
boot flow/troubleshooting chart, 8–17
cooling, 1–6
initialization, 4–5
internal cabling, A–1
packaging, 1–6
power, 1–6
software overview, 1–25
software release notes, 1–25

HSC40 controller
module utilization label, 1–15
HSC40 controller to HSC60 controller upgrade kit, 1–5
HSC40 controller to HSC70 controller upgrade kit, 1–5
HSC50
auxiliary and maintenance terminal, 4–3
initialization, 4–7
internal cabling, A–7
offline diagnostics tape, 4–7
HSC50 (modified)
internal cabling, A–14
HSC50 auxiliary power supply
removal, 3–91
replacement, 3–91
HSC50 controller
airflow sensor, 3–70
blower, 3–74
boot flow/troubleshooting chart, 8–23
cables, 1–16
dc power switch location, 3–6
failover procedure, 3–2
front door removal, 3–11
FRU removal sequence chart, 3–9
inside front door controls/indicators, 2–7
module utilization label, 1–14
OCP removal, 3–65
OCP replacement, 3–67
OCP testing, 3–67
removing ac power, 3–7
removing power, 3–6
taking offline for maintenance, 3–2
HSC50 main power supply
removal, 3–85
replacement, 3–85
voltage test points, 3–86
HSC50 power controller
removal, 3–79
replacement, 3–79
HSC60 controller
module utilization label, 1–13
HSC60 controller to HSC90 controller upgrade kit, 1–5
HSC70 controller
module utilization label, 1–12
HSC70 controller to HSC90 controller upgrade kit, 1–5
HSC90 controller
module utilization label, 1–11
HSC auxiliary power supply
removal, 3–88
replacement, 3–88
voltage test points, 3–90
HSC controller
airflow sensor, 3–68
blower, 3–72
cabinet back door removal, 3–12
dc power switch, 3–51
dc power switch location, 3–3
HSC controller (cont'd)
differences between models, 1–3
failover procedure, 3–2
front door removal, 3–10
FRU removal sequence chart, 3–8
OCP removal, 3–63
OCP replacement, 3–64
OCP testing, 3–65
power removal, 3–3
removing ac power, 3–5
taking offline for maintenance, 3–2
HSC controller module card cage, 1–11
HSC crashes, B–1
HSC main power supply
removal, 3–81
replacement, 3–81
voltage test points, 3–84
HSC memory module
removal, 3–47
replacement, 3–47
testing, 3–48
HSC power controller, 2–15
BUS/ON/OFF switch, 2–16
circuit breaker, 2–16
fuse, 2–16
operating instructions, 2–16
Power Control bus connections, 2–16
removal, 3–76
replacement, 3–76
TOTAL OFF connector, 2–17

I

I/O control processor module (P.ioj/c), 1–19
see also P.ioj/c
ILCACH
device integrity tests, 5–9
error message example, 5–11
error messages, 5–11
between 25% and 50% of CACHE is bad, 5–12
cannot allocate a timer, test aborted, 5–11
mcache hardware module not present, or not installed correctly, 5–11
mcache memory address error, 5–11
MCACHE memory address error, 5–12
mcache module is unusable... status register, 5–11
mcache must be disabled..., 5–11
more than 50% of CACHE is bad, 5–12
status word not expected value, 5–12
timed out reading the MCACHE status register, 5–12

ILCACH
error messages (cont'd)
unable to transfer one sector from CACHE to DATA memory, 5–12
unsupported invocation of ILCACH, 5–12
ILCACH cannot be aborted via CTRL/Y or CTRL/C, 5–11
operating instructions, 5–10
progress reports, 5–10
system requirements, 5–10
test summaries, 5–11
test termination, 5–10
ILDISK
availability, 5–13
disk drive integrity test, 5–12
error message example, 5–18
error messages, 5–18
attention not set in available drive, 5–18
attention set after seek, 5–18
attention set in online drive, 5–18
available not set in available drive, 5–18
available set in online drive, 5–18
512-byte format failed, 5–18
can't acquire Drive State Area, 5–18
can't acquire specific unit, 5–18
can't read any sector on track, 5–18
can't write any sector on track, 5–19
change mode failed, 5–19
command failure, 5–19
DCB not returned, K failed for unknown reason, 5–19
DDUSUB initialization failure, 5–19
drive acquired but can't find control area, 5–19
drive can't be brought online, 5–20
drive diagnostic detected fatal error, 5–20
drive diagnostic error, 5–20
drive did not clear errors, 5–20
drive disabled bit set, 5–20
drive online in enhanced ESE mode, 5–20
drive online in normal mode., 5–20
drive online in normal mode. HSC variants not currently enabled., 5–20
drive online in normal mode. Requested variant is not supported., 5–20
drive online in normal mode. Retry operation later., 5–20
drive spindle not up to speed, 5–21
ILDISK
error messages (cont'd)
drive transfer queue not empty before format, 5–21
drive unavailable, 5–21
drive unknown to disk functional code, 5–21
drive went off line, 5–21
duplicate unit detected, 5–21
echo data error, 5–21
echo framing error, 5–21
error bit set in drive status error byte, 5–21
error in DCB on completion, 5–22
error reading LBN, 5–22
error releasing drive, 5–22
error starting I/O operation, 5–22
failed to reacquire unit, 5–22
failure while updating drive status, 5–22
format DRAT was not returned to completion queue, 5–23
format operation timed out, 5–23
format tests skipped due to previous error, 5–23
I/O operation lost, 5–23
Init did not stop state line clock, 5–23
insufficient memory, test not executed, 5–23
insufficient resources to perform test, 5–23
invalid requestor or port number, 5–24
K.sdi/K.si detected error in read preceding format, 5–24
K.sdi/K.si does not support echo, 5–24
K.sdi/K.si does not support microdiagnostics, 5–24
K microdiagnostic reported error, 5–24
microdiagnostic did not complete, 5–24
not good enough DBNs for format, 5–24
Read/Write Ready not set in online drive, 5–24
Read/Write Ready set in available drive, 5–25
read DRAT not returned to completion queue, 5–24
Read operation timed out, 5–24
Receiver Ready not set, 5–25
req/port number information unavailable, 5–25
requestor does not have control area, 5–25
requestor is not a K.sdi/K.si, 5–25
run drive resident diagnostics, 5–25

ILDISK
error messages (cont'd)
SDI enable variant command failed, 5–25
specified port contains a known drive, 5–25
state line clock did not start up after Init, 5–25
state line clock not running, 5–25
testing aborted, 5–26
The K.sdi/K.si module detected error during format, 5–24
unexpected item on drive service queue, 5–26
unit selected is not a disk, 5–26
unknown status from DDUSUB, 5–26
wrong structure on completion queue, 5–26
hardware requirements, 5–13
MSCP status codes, 5–26
operating instructions, 5–13
progress reports, 5–15
software requirements, 5–13
specifying requestor and port, 5–15
system requirements, 5–13
test parameters, 5–14
tests performed, 5–12
test summaries, 5–15
test termination, 5–14
ILEXER
communications error format, 5–56
communications error report, 5–52
data compare error format, 5–55
data patterns, 5–49
data transfer error report, 5–50
disk drive prompts, 5–44
disk errors, 5–59
command failed—invalid header code, 5–59
command failed—no buffer available, 5–59
command failed—no control structures available, 5–59
couldn't put drive in DBN space, 5–59
data compare error, 5–59
disk unit numbers must be between 0 and 4095 decimal, 5–59
drive error not up to speed, 5–59
drive no longer on line, 5–59
EDC error, 5–60
hard failure on compare operation, 5–60
hard failure on disk, 5–60
hard failure on initial write operation, 5–60
hard failure on read operation, 5–60
ILEXER
disk errors (cont'd)
hard failure on write operation, 5–60
no DACB available, 5–60
pattern number error, 5–60
some disk I/O failed to complete, 5–60
this drive removed from test, 5–59
unknown unit number not allowed in ILEXER, 5–60
write requested on write-protected drive, 5–60
error message format, 5–55
error messages, 5–56
drive online in enhanced ESE mode, 5–56
drive online in normal mode., 5–57
drive online in normal mode. HSC variants not currently enabled, 5–57
drive online in normal mode. Requested variant is not supported., 5–57
drive online in normal mode. Retry operation later., 5–57
SDI enable variant command failed, 5–57
generic errors, 5–58
couldn't get drive status, 5–58
could not get buffers for transfers, 5–58
could not get control block for timer, 5–58
could not get timer for MDE, 5–58
could not return drive to available state, 5–58
disk functionality unavailable, 5–58
drive cannot be brought on line, 5–58
drive is unavailable, 5–58
drive is unknown, 5–58
invalid time entered, 5–58
no disk or tape functionality, 5–59
no tape mounted on unit, 5–59
record length larger that 12K or 0, 5–59
tape functionality unavailable, 5–59
tape rewind commands were lost, 5–59
this unit already acquired, 5–59
user requested write on write-protected unit, 5–59
global prompts, 5–47
informational message
disk interface not available, 5–56
number must be between 0 and 15, 5–57

ILEXER
informational message (cont'd)
pattern number must be within specified bounds, 5–57
please mount a scratch tape, 5–57
please wait—clearing outstanding I/O, 5–57
starting LBN is either larger than ending LBN or larger than total LBN on disk, 5–57
tape interface not available, 5–57
you may enter at most 16 words in a data pattern, 5–57
informational messages, 5–56
multidrive exerciser, 5–42
operating instructions, 5–43
pattern word error format, 5–56
performance summary, 5–50
progress reports, 5–50
prompt error format, 5–55
setting/clearing flags, 5–50
system requirements, 5–42
tape drive exercise commands, 5–54
tape drive prompts, 5–46
tape errors, 5–60
comm error: TDUSUB call failed, 5–60
controller error...hard error, 5–60
couldn't get formatter characteristics, 5–60
couldn't get unit characteristics, 5–60
couldn't set unit char, 5–60
data pattern word error, 5–60
data read EDC error, 5–60
drive error...hard error, 5–60
drive went available, 5–61
drive went offline, 5–61
formatter error...hard error, 5–61
hard error limit exceeded, 5–61
read data error, 5–61
retry required on tape drive, 5–61
short transfer error, 5–61
some tape I/O failed to complete, 5–61
tape mark error, 5–61
tape position discrepancy, 5–61
tape position lost, 5–61
truncated record data error, 5–61
unexpected BOT encountered, 5–61
unexpected error condition, 5–61
unrecoverable read error, 5–61
unrecoverable write error, 5–61
test parameter, 5–43
test summaries, 5–52
test termination, 5–43
ILMEMY
device integrity tests, 5–7
error message example, 5–8
error messages, 5–9
ILMEMY
error messages (cont'd)
can't allocate timer, test aborted, 5–9
error 000, tested twice with no error, 5–9
memory data error, 5–9
memory parity error, 5–9
NXM Trap (Buffer Retired), 5–9
returned buffer to free buffer queue, 5–9
hardware requirements, 5–7
operating instructions, 5–8
progress reports, 5–8
software requirements, 5–7
system requirements, 5–7
test summary, 5–8
test termination, 5–8
ILRX33
device integrity tests, 5–2
entering test parameters, 5–3
error message example, 5–4
error messages, 5–4
block number out of range, 5–4
data compare error, 5–4
hard I/O error, 5–4
illegal device name, 5–4
no diskette mounted, 5–5
operation aborted, 5–5
retries required, 5–5
unknown status, 5–5
write-protected, 5–5
operating instructions, 5–3
progress reports, 5–3
system requirements, 5–3
test summary, 5–4
test termination, 5–3
ILTAPE
boot process, 5–28
data entry prompt, 5–31
data pattern prompt, 5–30
drive unit number prompt, 5–28
enter canned sequence run time in minutes prompt, 5–29
enter port number prompt, 5–28
enter requestor number prompt, 5–28
error message example, 5–34
error messages, 5–35
available set in online drive, 5–35
chosen density is not supported, 5–35
command failure, 5–35
data compare error, 5–35
DCB not returned, K failed for unknown reason, 5–35
echo data error, 5–35
EDC error, 5–35
error in DCB on completion, 5–35
formatter device integrity test detected error, 5–35
formatter device integrity test detected fatal error, 5–35

ILTAPE
error messages (cont'd)
formatter state not preserved across Init, 5–35
Init did not stop state line clock, 5–35
initialization failure, 5–35
insufficient resources to acquire specified device, 5–35
insufficient resources to acquire timer, 5–35
invalid multiunit code from GUS command, 5–36
invalid requestor/port number, 5–36
K.sti does not support microdiagnostics, 5–36
K microdiagnostic did not complete, 5–36
K microdiagnostic reported error, 5–36
load device read error, 5–36
load device write error—check if write-locked, 5–36
pattern word error, 5–36
read memory byte count error, 5–36
receiver ready not set, 5–36
requested device is busy, 5–36
requested device unknown, 5–36
requestor not a K.sti/K.si, 5–36
RX33 error—file not found, 5–36
selected unit not a tape, 5–36
state line clock did not start up after Init, 5–36
state line clock not running, 5–36
tape write protected—test terminating, 5–36
timeout acquiring drive service area, 5–37
unable to release device, 5–37
unexpected item on drive service queue, 5–37
unit unknown or on line to another controller, 5–37
unit went offline or available, 5–37
unknown status from TDUSUB, 5–37
execute formatter device integrity test prompt, 5–28
execute test of tape transport prompt, 5–28, 5–29
functional test sequence number prompt, 5–29, 5–32
how many data entries prompt, 5–31
input step 00: prompt, 5–29
input step prompt, 5–32
is media mounted prompt, 5–29
iterations prompt, 5–31
memory region number prompt, 5–29
new user sequence dialogue, 5–32
ILTAPE (cont'd)
operating instructions, 5–27
progress reports, 5–33
select density prompt, 5–30
select fixed speed prompt, 5–30
select record size prompt, 5–31
select variable speed prompt, 5–30
store sequence as sequence number prompt, 5–32
system requirements, 5–27
tape device integrity test, 5–27
test summaries, 5–33
test termination, 5–28
user dialog, 5–28
user sequence commands, 5–31
user sequence input step entries prompt, 5–32
variable speeds available prompt, 5–30
ILTCOM
error message example, 5–41
error messages, 5–41
can't find end of bunch, 5–41
chosen density is not supported, 5–41
command failure, 5–41
data compare error, 5–41
data EDC error, 5–42
device is unknown, 5–42
error releasing drive, 5–42
insufficient resources to acquire drive, 5–42
invalid user selection, 5–42
specified unit cannot be brought on line, 5–42
TDUSUB initialization failure, 5–42
unknown status from TDUSUB, 5–42
operating instructions, 5–39
system requirements, 5–38
tape compatibility test, 5–37
test parameters, 5–39
test summaries, 5–41
test termination, 5–39
ILTU58
device integrity test, 5–5
error messages, 5–6
bad opcode, 5–6
bad record, 5–6
bad unit #, 5–6
data compare error, 5–6
end of medium, 5–6
failed self-test, 5–6
hard I/O error, 5–6
illegal device name, 5–6
no cassette mounted, 5–6
operation aborted, 5–6
retries required, 5–6
seek error, 5–6
unknown status, 5–6
write protected, 5–6
operating instructions, 5–6

ILTU58 (cont'd)
system requirements, 5–5
test termination, 5–6
Indicators
K.pli, 2–10
K.sdi, 2–10
K.si 4-port, 2–10
K.si 8-port, 2–10
K.sti, 2–10
LINK, 2–10
logic module, 2–8
M.cache, 2–11
M.std, 2–10
M.std2, 2–10
M.std4, 2–10
P.ioc, 2–11
P.ioj, 2–11
P.ioj–18, 2–11
INIPIO
system requirements for test, 4–6
test description, 4–6
test load failure steps, 4–7
test operation, 4–6
test prerequisites, 4–6
Initialization
data channel module (K.si), 3–40
errors, 8–2
HSC, 4–5
HSC50, 4–7
Init P.ioc diagnostic, 4–7
Internal cabling
HSC, A–1
HSC50, A–7
HSC50 (modified), A–14

J

Jumpers
I/O control processor module (P.ioj/c), 3–29
port link module (LINK), 3–20
RX33 disk drive, 3–53
TU58 tape drive, 3–61

K

K.ci modules
LEDs, 8–16
path status information, 6–33
status code bytes for HSC40, HSC50, HSC70 controllers, D–5
status code bytes for HSC60, HSC90 controllers, D–8
K.pli
indicators, 2–10
removal, 3–26
replacement, 3–28
switches, 3–27
testing, 3–28
K.pli/K.pli2
interfaces, 1–23
K.sdi
indicators, 2–10
LEDs, 8–14
removal, 3–32
replacement, 3–33
status code bytes, D–12
testing, 3–33
K.si
configuration problems, 3–41
disk status code bytes, D–16
external loop test, 3–38
initialization, 3–40
LEDs, 8–14
mismatch conditions, 3–40
new boot microcode, 3–42
removal, 3–36
replacement, 3–38
requestor configuration, 3–37
switches, 3–36
tape status code bytes, D–18
testing, 3–43
K.si 4-port
indicators, 2–10
K.si 8-port
indicators, 2–10
K.sti
indicators, 2–10
LEDs, 8–14
removal, 3–34
replacement, 3–34
status code bytes, D–14
testing, 3–35
K-detected errors, D–1
K-detected failure code analysis, D–4

L

LA12 parameters, 4–4
Lamp bit check
offline OCP test, 6–85
LEDs
K.ci modules, 8–16
K.sdi module, 8–14
K.si module, 8–14
K.sti module, 8–14
M.cache module, 8–15
M.std2 module, 8–14
M.std4 module, 8–14
M.std module, 8–14
P.ioj/c module, 8–13
LINK
indicators, 2–10
jumpers, 3–20
removal, 3–15
replacement, 3–24
switches, 3–15
testing, 3–24
Loader
HSC50 offline diagnostics, 6–2
HSC offline diagnostics, 6–2
offline diagnostics, 6–8

Logic module indicators, 2–8

M

M.cache
indicators, 2–11, 8–15
module LEDs, 8–15
removal, 3–42
removal and replacement, 3–44
replacement, 3–44
software version, 3–44
testing, 3–45
M.std
indicators, 2–10
LEDs, 8–14
removal, 3–48
replacement, 3–49
testing, 3–49
M.std2
indicators, 2–10
LEDs, 8–14
M.std4
indicators, 2–10
LEDs, 8–14
Main power supply
HSC, 3–81
HSC50, 3–85
Maintenance features, 1–27
Maintenance strategy, 1–26
Maintenance terminal connection
HSC50, 4–3
32-Mbyte cache option (M.cache), 1–24
Memory module (M.std), 1–20
Memory module (M.std2), 1–20
Memory module (M.std4), 1–20
Memory test configuration
Offline bus interaction test, 6–28
Miscellaneous errors, 8–53
Mismatch conditions
data channel module (K.si), 3–40
Mode byte field, 8–34
Module names, 1–3
Module removal and replacement, 3–13
MSCP
class server, 1–26
controller errors, 8–31
Disk transfer error field description, 8–36
disk transfer errors, 8–36
error flags, 8–30
error format description and flags, 8–28
error message fields, 8–29
format type codes, 8–29
generic error format, 8–28
SDI errors, 8–32
software errors, 8–31
status codes in ILDISK, 5–26
status or event codes, C–2
Multidrive exerciser
ILEXER, 5–42
Multiple HSCs in cluster failover, 3–2

N

New boot microcode
data channel module (K.si), 3–42

O

OCP
controls and indicators, 2–1
fault code displays, 8–2
offline control store loader (OCSL), 6–88
offline OCP test (OOCP), 6–78
OCP fault code interpretation
fault code 1, port processor error, 8–4
fault code 10, P.ioj cache failure, 8–5
fault code 11, K.ci failure, 8–5
fault code 12, data channel module failure, 8–6
fault code 2, K.sdi/K.si incorrect version of microcode, 8–4
fault code 21, I/O control processor module failure, 8–6
fault code 22, memory module failure, 8–6
fault code 23, boot device failure, 8–7
fault code 25, port link node address switches out of range, 8–8
fault code 26, missing files required, 8–8
fault code 3, K.sti/K.si incorrect version of microcode, 8–5
fault code 30, no working K.ci, K.sdi, K.sti, or K.si in subsystem, 8–9
fault code 31, initialization failure, 8–9
illegal inst, 8–10
K.ci host reset, 8–11
Level 7 interrupt, 8–11
Memory management unit (MMU) trap, 8–11
NXM trap, 8–10
parity trap, 8–10
software crash, 8–11
fault code 32, software inconsistency, 8–11
fault code 33, illegal configuration, 8–12
Offline bus interaction test (OBIT), 6–24
error 000—memory test error, 6–28
error 001—K timed-out during Init, 6–29
error 002—K timed-out during test, 6–29
error 003—parity trap, 6–29
error 004—NXM trap, 6–30
error 005—memory test error (P.ioj/c) detected, 6–30
error 011—RX33 drive not ready, 6–30

Offline bus interaction test (OBIT) (cont'd)
error 012—RX33 CRC error during seek, 6–30
error 013—RX33 track 0 not set on recalibrate, 6–30
error 014—RX33 seek timeout, 6–30
error 015—RX33 seek error, 6–30
error 016—RX33 read timeout, 6–31
error 017—RX33 CRC/RNF error on read command, 6–31
error 10 (12 octal)—cache parity error, VPC = xxxxxx, 6–30
error information, 6–27
memory test configuration, 6–28
operating instructions, 6–25
parameter entry, 6–25
prerequisites, 6–25
progress reports, 6–26
requestor error summary, 6–28
system requirements, 6–24
test summaries, 6–27
test termination, 6–25
Offline cache test (OFLCXT), 6–16
error 00—memory parity error, 6–21
error 01—NXM trap, 6–21
error 02—cache parity error, 6–21
error 03—bit stuck in cache control register, 6–21
error 04—forced miss operation failed, 6–22
error 05—forced miss with abort failed, 6–22
error 06—expected cache hit did not occur, 6–22
error 07—expected cache miss did not occur, 6–22
error 10—value in hit/miss register incorrect, 6–22
error 11—write byte operation caused cache update, 6–22
error 12—write byte did not cause cache update, 6–22
error 13—cache failed to flush successfully, 6–22
error 14—access with force bypass did not cause invalidate, 6–22
error 15—tag parity error did not set, 6–22
error 16—abort on parity error did not occur, 6–22
error 17—unexpected parity trap during abort test, 6–22
error 20—content of memory system error register incorrect, 6–22
error 21—return PC wrong during abort/interrupt test, 6–22
error 22 cache data parity bit(s) did not set, 6–22
error 23—interrupt on parity error did not occur, 6–23
Offline cache test (OFLCXT) (cont'd)
error 24—expected NXM trap did not occur, 6–23
error 25—parity error was not blocked by NXM, 6–23
error 26—cache data miscompare on word operation, 6–23
error 27—cache data miscompare on byte operation, 6–23
error 30—DMA write to memory did not cause cache to invalidate, 6–23
error 31—instruction still completed during abort condition, 6–23
error 32—load device error during DMA test, 6–23
error 33—PDR cache bypass failed, 6–23
error 34—tag store address hit failure, 6–23
error 35—tag store address miss failure, 6–23
error 41—processor type is not J11, 6–23
error information, 6–21
leave cache enabled parameters, 6–17
number of passes parameter, 6–17
operating instructions, 6–17
parameter entry, 6–17
progress reports, 6–18
select data reliability test parameter, 6–17
system requirements, 6–17
test summaries, 6–18
test termination, 6–17
troubleshooting, 6–24
Offline Control Store Loader (OCSL), 6–88
error 00—parity trap, VPC = xxxxxx, 6–90
error 01—nxm trap, VPC = xxxxxx, 6–90
error 02—cache parity error, VPC = xxxxxx, 6–90
error 03 – requested file not found, 6–90
error 05—K timed out during INIT, 6–90
error 06—K does not support WCS, 6–90
error 07—K failed during WCS load, 6–90
error information, 6–90
error messages, 6–90
operating instructions, 6–88
parameter entry, 6–89
system requirements, 6–88
test summaries, 6–89
test termination, 6–89
Offline diagnostics
bootstrap error information, 6–4
bootstrap failures, 6–3

Offline diagnostics (cont'd)
bootstrap failure troubleshooting, 6–4
Init and Fault both lit, 6–4
Init and Fault both off, 6–4
Init is off, Fault is lit, 6–4
bootstrap initialization, 6–3
bootstrap operational requirements, 6–2
bootstrap progress reports, 6–3
Fault lamp, 6–4
Init lamp, 6–3
lamps clear, 6–3
RX33 drive-in-use, 6–3
State lamp, 6–4
bootstrap test summaries, 6–4
common characteristics, 6–1
EXAMINE and DEPOSIT commands, 6–10
generic error message format, 6–7
LOAD command, 6–10
loader, 6–8
HELP file, 6–16
system requirements, 6–8
loader commands, 6–9
loader HELP command, 6–9
loader operating instructions, 6–8
loader prerequisites, 6–8
loader SIZE command, 6–9
loader TEST command, 6–9
load procedure for HSC, 6–2
load procedure for HSC50, 6–2
software requirements, 6–1
START command, 6–10
tests, 6–9
trap and interrupt vectors, 6–15
unexpected traps and interrupts, 6–14
Offline diagnostics tape
HSC50, 4–7
Offline K/P memory test (OKPM), 6–41
error 000, 6–46
error 001, 6–47
error 002, 6–47
error 003, 6–48
error 004, 6–48
error 005, 6–49
error 006, 6–49
error 007, 6–50
error 008, 6–51
error 009, 6–51
error 010, 6–51
error 011, 6–51
error 013—cache parity trap, VPC = xxxxxx, 6–52
error information, 6–45
error summary information, 6–45
operating instructions, 6–42
parameter entry, 6–42
parity errors, 6–44
progress reports, 6–43
system requirements, 6–41
test summaries, 6–44
test termination, 6–42
Offline K test selector (OKTS), 6–31
error 000, 6–36
error 001, 6–36
error 002, 6–37
error 003, 6–37
error 004, 6–38
error 005, 6–39
error 006, 6–39
error 007, 6–40
error 008, 6–40
error 009, 6–40
error 010, 6–40
error 011, 6–41
error 012, 6–41
error 013—cache parity trap, VPC = xxxxxx, 6–41
error information, 6–35
K ci path status information, 6–33
operating instructions, 6–31
parameter entry, 6–32
progress reports, 6–32
system requirements, 6–31
test summaries, 6–33
test termination, 6–31
Offline memory cache test
error information, 6–68
error messages, 6–68
operating instructions, 6–66
Offline memory cache test (OMCA), 6–65
Offline memory test (OMEM), 6–52
error 000, 6–57
error 001, 6–58
error 002, 6–58
error 003, 6–59
error 004, 6–59
error 005, 6–60
error 006, 6–60
error 007, 6–61
error 008, 6–62
error 009, 6–62
error 010, 6–63
error 011, 6–63
error 012, 6–63
error 013, 6–64
error 014, 6–64
error 015, 6–64
error 020, 6–64
error 021, 6–64
error 022, 6–64
error 023, 6–65
error 024, 6–65
error 025, 6–65
error 026, 6–65
error 027, 6–65
error 028, 6–65
error 029, 6–65
error 030, 6–65
error 031, 6–65
error information, 6–56
operating instructions, 6–52
parameter entry, 6–53
parity errors, 6–54
progress report, 6–54

Offline memory test (OMEM) (cont'd)
quick verify algorithm, 6–52
system requirements, 6–52
test summaries, 6–55
test termination, 6–52
Offline OCP test (OOCP), 6–78
error 000—wrong bit set, 6–83
error 001—bit set when Init is pressed, 6–84
error information, 6–83
error messages, 6–83
lamp bit check, 6–85
operating instructions, 6–79
parameter entry, 6–79
Secure/Enable switch check, 6–86
state LED check, 6–87
switch check, 6–84
system requirements, 6–79
test summaries, 6–81
test termination, 6–79
troubleshooting registers and displays, 6–84
Offline refresh test (ORFT), 6–75
error 01, 6–78
error 02, 6–78
error 03, 6–78
error 04, 6–78
error 05—cache parity trap, VCP = xxxxxx, 6–78
error information, 6–77
operating instructions, 6–76
parameter entry, 6–76
progress reports, 6–77
system requirements, 6–76
test summaries, 6–77
test termination, 6–76
Offline RX33 exerciser (OFLRXE), 6–69
data patterns, 6–72
error 00—parity trap, VPC = xxxxxx, 6–73
error 01—NXM trap, VPC = xxxxxx, 6–73
error 02—bit stuck in register, 6–73
error 03—interrupt occurred without enable set, 6–73
error 04—RX33 interrupt occurred at wrong priority, 6–73
error 05—unexpected interrupt from RX33, 6–73
error 06—track 0 did not set after recalibrate command, 6–73
error 07—RX33 did not interrupt as expected, 6–73
error 10—seek error detected during positioning operation, 6–73
error 11—current track resister incorrect, 6–74
error 12—CRC error in header detected during position verify, 6–74
error 13—processor type is not J11, 6–74
Offline RX33 exerciser (OFLRXE) (cont'd)
error 14—drive under test is not ready, 6–74
error 15—last command did not complete, 6–74
error 16—RX33 header does not compare, 6–74
error 17—record not found during read (could also say write), 6–74
error 20—CRC error in date during read (could also say write), 6–74
error 21—lost data detected during read (could also say write), 6–74
error 23—invalid pattern code in buffer, 6–74
error 24—drive is write-protected, 6–74
error 25—CRC error in header during read (could also say write), 6–75
error 26—data incorrect after DMA test mode command, 6–75
error 27—data compare error, 6–75
error 30—RX33 detected parity error during read (could also say write), 6–75
error 31—RX33 detected NXM during read (could also say write), 6–75
error 32—RX33 MAR value incorrect after DMA transfer, 6–75
error 33—parity error was not forced in main memory, 6–75
error 34—parity error did not set in CSR, 6–75
error 35—NXM did not set in CSR, 6–75
error 36—parity error set along with NXM in CSR, 6–75
error 37—cache parity error, VPC - xxxxxx, 6–75
error information, 6–72
operating instructions, 6–69
parameter entry, 6–70
progress reports, 6–70
system requirements, 6–69
test summaries, 6–71
test termination, 6–69
Operating instructions
ILCACH, 5–10
ILDISK, 5–13
ILEXER, 5–43
ILMEMY, 5–8
ILRX33, 5–3
ILTAPE, 5–27
ILTCOM, 5–39
ILTU58, 5–6
offline bus interaction test, 6–25
offline control store loader, 6–88
offline K/P memory test, 6–42
offline K test selector, 6–31
offline memory cache test (OMCA), 6–66
offline memory test, 6–52

Operating instructions (cont'd)
offline OCP test, 6–79
offline refresh test, 6–76
offline RX33 exerciser, 6–69
Operational status codes
K.si requestors microcode load failed, D–20
normal operation for K-requestors, D–3
Operator control panel (OCP), 2–1
Ordering related documentation, xxii
Original error flags
field description, 8–38
Out-of-band errors, 8–50

P
P.ioc
indicators, 2–11
P.ioj
indicators, 2–11
P.ioj/c
INIPIO diagnostic (P.ioj), 4–6
Init P.ioc diagnostic, 4–7
jumpers, 3–29
module LEDs, 8–13
module LEDs power-up sequence, 8–13
removal, 3–29
replacement, 3–31
ROM bootstrap, 6–2
testing, 3–32
P.ioj–18
indicators, 2–11
Parameter entry
offline bus interaction test, 6–25
offline cache test, 6–17
offline control store loader, 6–89
offline K/P memory test, 6–42
offline K test selector, 6–32
offline memory test, 6–53
offline OCP test, 6–79
offline refresh test, 6–76
offline RX33 exerciser, 6–70
Parity errors
offline K/P memory test, 6–44
offline memory test, 6–54
PATCH, 7–29 to 7–34
commands, 7–29
error and information messages, 7–33
error messages, 7–33
fatal error messages, 7–33
information messages, 7–34
PATCH–E incorrect checksum, 7–33
PATCH–E invalid command, 7–33
PATCH–E invalid device name or switch, 7–33
PATCH–F cannot access PATCH data file, 7–33
PATCH–F cannot access version on off-line diagnostic medium, 7–33
PATCH–F cannot access version on system medium, 7–33
PATCH (cont'd)
PATCH–F cannot access version on utility medium, 7–33
PATCH–F file not found, 7–33
PATCH–F insufficient resources to run, 7–33
PATCH–F read failure: block–number, 7–33
PATCH–F unit(s) write-protected: update was not done, 7–33
PATCH–F version on system medium does not match utility medium, 7–33
PATCH–F write failure: block–number, 7–33
PATCH–F write failure during write check, status: block number, 7–33
PATCH–F you cannot PATCH this file, 7–33
PATCH–I checksum = octal–checksum (0), 7–34
PATCH–I Ctrl/Y or Ctrl/C abort, 7–34
PATCH–I no patches recorded, 7–34
PATCH–I patches made:, 7–34
PATCH–S patch–count changes Made, 7–34
PATCH–S wait..., 7–34
PATCH–W buffer space exhausted, 7–34
PATCH–W nonfile structured mode assumed, 7–34
running, 7–30
sample session, 7–32
success messages, 7–34
warning messages, 7–34
PILA
indicators, 2–10
removal, 3–25
replacement, 3–25
switches, 3–25
testing, 3–26
Port buffer module (PILA/PILA2), 1–22
see also PILA/PILA2
8-port data channel module (8-port K.si), 1–24
Port link module (LINK/LINK2), 1–21
see also LINK/LINK2
Port processor module (K.pli/K.pli2), 1–22
see also K.pli/K.pli2
Power controller, 1–9
HSC, 3–76
HSC50, 3–79
Power removal
HSC50, 3–6
HSC controller, 3–3
Precautions, 3–2
Progress reports
ILCACH, 5–10
ILDISK, 5–15
ILEXER, 5–50
ILMEMY, 5–8

Progress reports (cont'd)
ILRX33, 5–3
ILTAPE, 5–33
offline bus interaction test, 6–26
offline cache test, 6–18
offline K/P memory test, 6–43
offline K test selector, 6–32
offline memory tests, 6–54
offline refresh test, 6–77
offline RX33 exerciser, 6–70

Q

Qualifiers (switches)
EXAMINE and DEPOSIT, 6–13
Quick verify algorithm
offline memory test, 6–52

R

Rear view of cabinet, 1–9
Recovery flags
field description, 8–38
Related documentation, xxii
Relocation register
EXAMINE and DEPOSIT, 6–12
Removal
data channel module (K.si), 3–36
Disk data channel module (K.sdi), 3–32
HSC50 airflow sensor, 3–70
HSC50 auxiliary power supply, 3–91
HSC50 blower, 3–74
HSC50 main power supply, 3–85
HSC50 OCP, 3–65
HSC50 power controller, 3–79
HSC airflow sensor, 3–68
HSC auxiliary power supply, 3–88
HSC blower, 3–72
HSC main power supply, 3–81
HSC memory module, 3–47
HSC OCP, 3–63
HSC power controller, 3–76
I/O control processor module (P.ioj/c), 3–29
M.cache, 3–44
Memory Module (M.std), 3–48
port buffer module (PILA), 3–25
Port processor module (K.pli), 3–26
RX33 disk drive, 3–50
Tape data channel module (K.sti), 3–34
TU58 tape drive, 3–58
Removal and replacement
FRUs, 3–3
M.cache, 3–44
subunits, 3–50
Replace flags bit descriptions, 8–40
Replacement
data channel module (K.si), 3–38
Disk data channel module (K.sdi), 3–33
HSC50 airflow sensor, 3–70
HSC50 auxiliary power supply, 3–91
HSC50 blower, 3–74
Replacement (cont'd)
HSC50 main power supply, 3–85
HSC50 OCP, 3–67
HSC50 power controller, 3–79
HSC airflow sensor, 3–68
HSC auxiliary power supply, 3–88
HSC blower, 3–72
HSC main power supply, 3–81
HSC memory module, 3–47
HSC OCP, 3–64
HSC power controller, 3–76
I/O control processor module (P.ioj/c), 3–31
M.cache, 3–44
Memory module (M.std), 3–49
port buffer module (PILA), 3–25
port link module (LINK), 3–24
Port processor module (K.pli), 3–28
RX33 disk drive, 3–57
Tape data channel module (K.sti), 3–34
TU58 tape drive, 3–62
Request byte field, 8–33
Requestor
status, 8–17
Requestor configuration
data channel module (K.si), 3–37
Requestor error summary
offline bus interaction test, 6–28
Requestor status codes, 8–17
ROM bootstrap, 6–2
RX33 disk drive, 3–50
CSR breakdown, 8–51
error code table, 6–6
error message last line breakdown, 8–52
errors, 8–50
jumpers, 3–53
offline RX33 exerciser (OFLRXE), 6–69
removal, 3–50
replacement, 3–57
status register summary, 8–51
testing, 3–57

S

Safety, 3–2
SDI bus, 1–9, 1–16
SDI errors
controller-detected transmission or time out error, 8–64
drive clock dropout, 8–70
drive-detected error, 8–71
drive inoperative, 8–71
error example, 8–32
field descriptions, 8–32
header error, 8–74
lost Read/Write Ready, 8–81
lost Receiver Ready, 8–82
MSCP, 8–32
position or unintelligible header error, 8–89
pulse or parity error, 8–90

SDI errors (cont'd)
SDI clock persisted after Init, 8–93
SI clock resumption failed after Init, 8–94
SI command timeout, 8–95
SI Receiver Ready collision, 8–95
SI response length or Opcode error, 8–96
SI response overflow, 8–96
SDI manager, 1–26
Secure/Enable switch
offline OCP test (OOCP), 6–86
SINI errors, 8–53
cache disabled due to failure, 8–78
SINI-E error printout, B–2
SINI out-of-band errors
cache functionality requested but M.cache hardware not present, 8–62
control microprocessor running with memory bank or board swap enabled, 8–64
hard transfer error loading (file) xx, 8–74
hard transfer error writing SCT xx, 8–74
host clear from CI node xx, 8–75
host interface (K.ci) failed INIT diags, status = xxx, 8–76
host interface (K.ci) is required but not present, 8–76
invalid module configuration, 8–78
last soft Init resulted from unknown cause, 8–79
less than 87.5 percent of Control memory is available, 8–80
less than 87.5 percent of data memory is available, 8–80
less than 87.5 percent of program memory is available, 8–81
M.cache comparator error, 8–83
M.cache disabled due to excessive errors, 8–83
M.cache multiple bit ECC error, 8–83
M.cache single bit ECC error, 8–83
parameter change, process yyy..., 8–88
parity error Trap thru 114, 8–88
program memory single bit ECC error, 8–90
requestor xx failed INIT DIT, status = xxx, 8–91
reserved instruction Trap thru 10, 8–92
SCT read or verification error. Using template SCT., 8–93
software inconsistency, 8–97
subsystem exception, Level 7 K interrupt Trap thru 134, 8–81
subsystem exception, MMU Trap through 250, 8–83
SINI out-of-band errors (cont'd)
subsystem exception, NXM Trap thru 4, 8–87
unable to read program memory error counter, 8–100
Software errors
error message categories, 8–28
MSCP, 8–31
Software inconsistencies, B–1
Software overview, 1–25 to 1–26
Software version
M.cache, 3–44
Specifications, 1–27
State LED check
offline OCP test, 6–87
Status code bytes
K.ci modules for HSC40, HSC50, HSC70 controllers, D–5
K.ci modules for HSC60, HSC90 controllers, D–8
K.sdi, D–12
K.sti, D–14
Status register summary
RX33 disk drive, 8–51
STI bus, 1–9, 1–16
STI errors, 8–41
drive error log, 8–42
drive error log (TA78 drive specific), 8–43
drive error log example, 8–42
drive error log field description, 8–42
example, 8–41
field description, 8–41
formatter E log, 8–42
formatter error log, 8–41
formatter error log field description, 8–42
GEDS text, 8–43
tape transfer log example, 8–49
STI manager, 1–26
Submitting an SPR, B–3
Subunit removal and replacement, 3–50
Switches
data channel module (K.si), 3–36
offline OCP test, 6–84
port buffer module (PILA), 3–25
port link module (LINK), 3–15
Port processor module (K.pli), 3–27
System requirements
ILCACH, 5–10
ILDISK, 5–13
ILEXER, 5–42
ILMEMY, 5–7
ILRX33, 5–3
ILTAPE, 5–27
ILTCOM, 5–38
ILTU58, 5–5
offline bus interaction test, 6–24
offline cache test, 6–17
offline control store loader, 6–88
offline diagnostics loader, 6–8
offline K/P memory test, 6–41
offline K test selector, 6–31

System requirements (cont'd)
offline memory test, 6–52
offline OCP test, 6–79
offline refresh test, 6–76
offline RX33 exerciser, 6–69

T
Tape compatibility test
ILTCOM, 5–37
Tape data channel module (K.sti), 1–23
see also K.sti
Tape device integrity test
ILTAPE, 5–27
Tape drive, 3–58
see TU58 tape drive
prompts, 5–46
Tape errors
acknowledge not asserted at start of transfer, 8–60
buffer EDC error, 8–62
controller-detected position lost, 8–64
controller transfer retry limit exceeded, 8–64
could not complete on-line sequence, 8–65
could not get extended drive status, 8–65
could not get formatter summary status during transfer error recovery, 8–65
could not get formatter summary status while trying to restore tape position, 8–65
could not position for formatter retry, 8–66
could not set byte count, 8–66
could not set unit characteristics, 8–66
data ready timeout, 8–67
ERASE command failed, 8–72
ERASE GAP command failed, 8–72
formatter and HSC disagree on tape position, 8–73
formatter-detected position lost, 8–73
formatter-requested error log, 8–73
formatter retry sequence exhausted, 8–73
host requested retry suppression on a formatter-detected error, 8–76
host requested retry suppression on a K.sti/K.si-detected error, 8–76
ILEXER, 5–60
Lower Processor error, 8–82
Lower Processor timeout, 8–82
Receiver Ready not asserted at start of transfer, 8–91
record EDC error, 8–91
retry limit exceeded while attempting to restore tape position, 8–92
rewind failure, 8–93
tape drive requested error log, 8–97
Tape errors (cont'd)
topology command failed, 8–99
unable to position to before LEOT, 8–100
unclearable drive error, 8–100
unclearable formatter error, 8–101
unknown K.tape error, 8–102
word rate clock timeout, 8–106
Tape functional errors, 8–53
Tape functional out-of-band errors
data error flagged in backup record, 8–67
increase drive structures through SET MAX_TAPES command, 8–85
increase formatter structures through SET MAX_FORMATTERS command, 8–85
insufficient Control memory for K.sti/K.si in requestor xx, 8–77
K.sti/K.si in requestor xx has microcode incompatible with this TMSCP Server, 8–79
no tape drive structures available for Requestor xx Port xx Unit xx, 8–85
no tape formatter structures available for Requestor xx Port xx, 8–85
no usable K.sti/K.si boards were found by the TMSCP Server, 8–85
requestor xx failed INIT DIT with status = xx, 8–91
tape formatter has been declared inoperative, 8–97
tape unit number xx connected to requestor xx port xx ceased to exist while online, 8–98
tape unit number xx connected to requestor xx port xx dropped state clock, 8–98
tape unit number xx connected to requestor xx port xx is not asserting available when it should be, 8–98
tape unit number xx connected to requestor xx port xx went available without request, 8–99
tape unit number xx connected to requestor xx port xx went offline without request, 8–99
TMSCP fatal initialization error—TMSCP functionality not available, 8–99
TTRASH fatal initialization error, 8–100
WARNING K.sti ucode too low for large transfers., 8–105
Tape I/O manager, 1–26
Tape status code bytes
K.si, D–18
Testing
data channel module (K.si), 3–43

Testing (cont'd)
Disk data channel module (K.sdi), 3–33
HSC50 OCP, 3–67
HSC memory module, 3–48
HSC OCP, 3–65
I/O control processor module (P.ioj/c), 3–32
M.cache, 3–45
Memory module (M.std), 3–49
port buffer module (PILA), 3–26
port link module (LINK), 3–24
Port processor module (K.pli), 3–28
RX33 disk drive, 3–57
Tape data channel module (K.sti), 3–35
TU58 tape drive, 3–63
Test parameters
ILDISK, 5–14
ILEXER, 5–43
ILRX33, 5–3
ILTCOM, 5–39
Test summaries
ILCACH, 5–11
ILDISK, 5–15
ILEXER, 5–52
ILRX33, 5–4
ILTAPE, 5–33
ILTCOM, 5–41
offline cache test, 6–18
offline control store loader, 6–89
offline K test selector, 6–33
offline memory test, 6–55
offline OCP test, 6–81
offline refresh test, 6–77
offline RX33 exerciser, 6–71
Test summary
ILMEMY, 5–8
Test termination
ILCACH, 5–10
ILDISK, 5–14
ILEXER, 5–43
ILMEMY, 5–8
ILRX33, 5–3
ILTAPE, 5–28
ILTCOM, 5–39
ILTU58, 5–6
offline bus interaction test, 6–25
offline cache test, 6–17
offline control store loader, 6–89
offline K/P memory test, 6–42
offline K test selector, 6–31
offline memory test, 6–52
offline OCP test, 6–79
offline refresh test, 6–76
offline RX33 exerciser, 6–69
TMSCP
class server, 1–26
controller errors, 8–31
error flags, 8–30
error format description and flags, 8–28
error message fields, 8–29
errors, 8–40
format type codes, 8–29
TMSCP (cont'd)
GEDS text field breakdown, 8–45
generic error format, 8–28
GSS text field bit interpretation, 8–46
GSS text field breakdown, 8–46
status or event codes, C–2
STI drive error log, 8–42
STI drive error log (TA78 drive specific), 8–43
STI drive error log example, 8–42
STI drive error log field description, 8–42
STI error example, 8–41
STI error field description, 8–41
STI errors, 8–41
STI formatter E log, 8–42
STI formatter error log, 8–41
STI formatter error log field description, 8–42
STI GEDS text, 8–43
tape transfer error log, 8–49
tape transfer error log example, 8–49
Traps, 8–53
Level 7 K interrupt (Trap through 134), 8–54
Level 7 K interrupt example, 8–55
MMU (Trap through 250), 8–57
NXM (Trap through 4), 8–53
parity error (Trap through 114), 8–54
reserved instruction (Trap through 10), 8–54
software inconsistency (Trap through 20), 8–58
Troubleshooting
console terminal, 8–16
registers and displays, 6–84
TU58 tape drive
jumpers, 3–61
removal, 3–58
replacement, 3–62
testing, 3–63

U

Unexpected traps and interrupts, 6–14
Upgrade kit
HSC40 controller to HSC60 controller, 1–5
HSC40 controller to HSC70 controller, 1–5
HSC60 controller to HSC90 controller, 1–5
HSC70 controller to HSC90 controller, 1–5
Upper and lower processor
K.ci error register bits HSC40, HSC50, HSC70 controllers, D–7
K.sdi error register bits, D–14
K.sti error register bits, D–16
Utilities
command prompt, 7–1

Utilities (cont'd)
default prompts, 7–1
DKUTIL, 7–1
FORMAT, 7–23
PATCH, 7–29
VERIFY, 7–15
Utility processes, 1–26

V

VERIFY, 7–15 to 7–23
after running FORMAT, 7–25
error and information messages, 7–18
error classes, 7–16
error message severity levels, 7–18
fatal error messages, 7–19
information messages, 7–21
n bad DBNs, 7–22
n bad RBNs verified, 7–22
n blocks with EDC errors, 7–22
n blocks with hard EDC errors, 7–22
n blocks with header compare errors, 7–22
n blocks with non–header, non–EDC errors, 7–22
n blocks with n symbol ECC errors, 7–22
n blocks with positioner errors, 7–22
n blocks with solid (non–ECC) errors, 7–22
n blocks with transient errors, 7–22
n blocks with uncorrectable ECC errors, 7–22
n good RBNs marked bad in the RCT, 7–22
n LBNs with corrupted data, 7–22
NOTE: table is null or empty (no bad PBNs), 7–23
n revectors verified, 7–23
n total blocks with any error, 7–23
n total ECC symbols corrected, 7–23
n unused RBNs with good EDC, 7–23
running, 7–16
sample session, 7–17
steps to verify disk, 7–15
variable output error fields, 7–18
VERIFY–F all copies of the xCT block n are bad, 7–19
VERIFY–F current system sector size is 512, 7–19
VERIFY–F drive went offline, 7–19
VERIFY–F I/O request was rejected, 7–19
VERIFY–F insufficient resources to run, 7–19
VERIFY–F mode is bad or format is in progress on this unit, 7–19
VERIFY–F too many bad blocks., 7–19
VERIFY–I copy of n of xCT block n (XBN n.) is bad, 7–21
VERIFY–I Ctrl/Y or Ctrl/C abort, 7–21
VERIFY (cont'd)
VERIFY–I DBN area should probably be reformatted, 7–21
VERIFY–I drive is OK, 7–21
VERIFY–I Exiting, 7–22
VERIFY–I initial write should be specified for ILEXER, 7–21
VERIFY–I LBN n., a primary, has a bad header (is non-primary), 7–21
VERIFY–I RBN n is good but not used for a revector, 7–21
VERIFY–I RBN n marked bad in the RCT was not bad, 7–21
VERIFY–I there were n inconsistencies found for this drive, 7–21
VERIFY–I xBN n. has a n symbol correctable ECC error, 7–21
VERIFY–I xBN n. has an uncorrectable ECC error, 7–22
VERIFY–I XBN n. has a transient (n out of 6) *error_type* error, 7–22
VERIFY–I xBN n. has corrupted data (forced error), 7–22
VERIFY–I xBN n. has solid errors: *error_type*, 7–22
VERIFY–W cannot online unit, 7–19
VERIFY–W cannot read track with starting xBN n, 7–19
VERIFY–W copy n of xCT block n (xBNn.) does not compare, 7–19
VERIFY–W illegal response to start-up question, 7–19
VERIFY–W LBN n., a non-primary revector, is improper, 7–19
VERIFY–W LBN n., a primary revector, is improper, 7–19
VERIFY–W LBN *n*. marked primary in RCT, not revectored to its primary, 7–20
VERIFY–W LBN n. revectors to RBN n. which is bad, 7–20
VERIFY–W LBN *n* has corrupted data (forced error), 7–19
VERIFY–W n bad PBNs not in the RCT, 7–20
VERIFY–W nonexistent unit number, 7–20
VERIFY–W RBN *n*. is good but not used for a revector, 7–20
VERIFY–W RBN *n*. marked bad in the RCT was not bad, 7–20
VERIFY–W unit is not available, 7–21
VERIFY–W xBN n. has a hard EDC error, 7–20
VERIFY–W xBN n has an uncorrectable ECC error, 7–20
VERIFY–W xBN n I/O error in access (MSCP code: o), 7–21
VERIFY–W xBN n is bad but not in the RCT, 7–21

VERIFY (cont'd)
warning messages, 7–19
Voltage test points
HSC50 auxiliary power supply, 3–93
HSC50 main power supply, 3–86
HSC auxiliary power supply, 3–90
HSC main power supply, 3–84